NIST CSF 2.0 and ISO 27001 - Framework Analysis for Cybersecurity Auditing

Francisco Catarino Mendes
Department of Informatics Engineering
University of Coimbra
Coimbra, Portugal
uc2019222823@student.uc.pt

Leonardo Oliveira Pereira
Department of Informatics Engineering
University of Coimbra
Coimbra, Portugal
uc2020239125@student.uc.pt

***Abstract*—This paper deals with both the NIST CSF 2.0 and ISO 27001:2022. The end goal is to understand whether these two frameworks can work together in cybersecurity auditing efforts or if they just are not compatible with each other. To begin with, an introduction to the topic is going to be made, followed by a state-of-the-art about the current auditing frameworks that exist. Then, both NIST CSF 2.0 and ISO 27001:2022 will be explained in detail, involving a comparison between their previous version and the need for updating them, their main functionalities, and some examples of real-life implementations of these frameworks. Finally, their chemistry and connection in cybersecurity auditing will be exposed, going through the common aspects, key differences, compatibility and synergies, so that it becomes understandable how organizations should proceed when dealing with auditing matters.**

Keywords: Cybersecurity, Auditing, NIST CSF, ISO 27001

I. Introduction

Nowadays, it is very important to implement robust cybersecurity practices to safeguard sensitive information, maintain customer trust, and ensure business continuity. Cyber threats are becoming increasingly sophisticated, and organizations must proactively defend against them. A crucial component in achieving these objectives is the process of security auditing, which serves as a critical mechanism for assessing and validating an organization's adherence to established cybersecurity frameworks and standards. Security audits help identify vulnerabilities, ensure compliance with regulatory requirements, and enhance overall security posture.

In this context, two prominent frameworks provide comprehensive guidance for cybersecurity management and auditing: the NIST Cybersecurity Framework (CSF) 2.0 and ISO 27001:2022. These frameworks offer structured approaches to managing and mitigating cybersecurity risks, each with its own methodologies, principles, and focus areas.

The NIST Cybersecurity Framework (CSF) 2.0, developed by the National Institute of Standards and Technology, provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber-attacks. It emphasizes a risk-based approach to managing cybersecurity and aligns with industry best practices.

On the other hand, ISO 27001:2022, an international standard developed by the International Organization for Standardization, specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). This framework is globally recognized and applicable to organizations of all types and sizes, providing a systematic approach to managing sensitive company information so that it remains secure.

While both frameworks aim to enhance cybersecurity, they have distinct methodologies and areas of emphasis. Understanding their similarities and key differences is essential for organizations seeking to implement effective cybersecurity strategies and ensure compliance with relevant standards.

By comparing the NIST CSF 2.0 and ISO 27001:2022, organizations can better understand how to leverage these frameworks to build a robust cybersecurity program that meets their specific needs and regulatory requirements. This comparison will provide insights into their respective strengths, helping organizations to choose the framework that best aligns with their security objectives and operational context.

II. State-of-the-art - Auditing Frameworks

IT security is made more challenging by compliance regulations and standards, such as HIPAA, PCI DSS, the Sarbanes-Oxley Act, and GDPR. These regulations mandate stringent controls to protect sensitive data and ensure accountability, and from an audit perspective, it is crucial to maintain compliance with these standards. Failure to comply can result in significant penalties, legal liabilities, and damage to an organization's reputation [7].

To manage this complex process, there are many available security frameworks that can help organizations structure

their information security efforts. These frameworks are very important because they provide a starting point for establishing processes, policies, and administrative activities for information security management. They offer best practices and guidelines that organizations can tailor to their specific needs, helping to systematically address security risks and compliance requirements.

The top IT security frameworks and standards are the ISO 27000 series, NIST SP 800-53, NIST SP 800-171, NIST CSF, NIST SP 1800 series, COBIT, CIS CONTROLS, HITRUST Common Security Framework, GDPR, COSO, FISMA and NERC CIP [7].

Organizations have unique requirements and operational contexts, so it is essential to research each security framework to select the best fit. Choosing the right framework involves understanding the organization's risk profile, regulatory environment, industry standards, and business objectives. Some of the most prominent security frameworks include:

- **NIST Cybersecurity Framework (CSF) 2.0:** Developed by the National Institute of Standards and Technology, this framework emphasizes a risk-based approach to managing cybersecurity and aligns with industry best practices. It is widely used in the United States, particularly by private-sector organizations seeking to improve their ability to prevent, detect, and respond to cyber threats.

- **ISO 27001:2022:** This international standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). ISO 27001 is globally recognized and applicable to organizations of all types and sizes, providing a systematic approach to managing sensitive company information so that it remains secure.

- **COBIT:** Developed by ISACA, COBIT focuses on governance and management of enterprise IT. It provides a comprehensive framework that helps organizations achieve their objectives for the governance and management of enterprise IT.

- **CIS Controls:** The Center for Internet Security (CIS) offers a set of actionable, prioritized controls designed to mitigate the most prevalent cyber threats. These controls are widely recognized and used by organizations seeking to improve their cybersecurity posture.

- **COBIT:** Developed by ISACA, COBIT focuses on governance and management of enterprise IT. It provides a comprehensive framework that helps organizations achieve their objectives for the governance and management of enterprise IT.

Selecting the right framework can help organizations establish a robust cybersecurity program, ensuring they meet regulatory requirements, protect sensitive information, and maintain customer trust. By implementing a framework tailored to their specific needs, organizations can systematically address their cybersecurity challenges, improve resilience against cyber threats, and support business continuity.

Ultimately, the choice of a security framework should align with the organization's strategic goals, regulatory requirements, and operational environment. A thorough evaluation of each framework's strengths and applicability will enable organizations to make informed decisions, optimizing their cybersecurity investments and efforts.

III. NIST CSF 2.0

A. *NIST CSF Overview*

The Cybersecurity Framework (CSF) 2.0 was designed to help organizations of all sizes and sectors manage and reduce their cybersecurity risks. This framework provides a flexible and cost-effective approach to enhancing cybersecurity and is applicable across industries and various organizational contexts. The CSF 2.0 includes the following components [19]:

- **CSF Core:** The CSF Core is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. It consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a strategic view of the lifecycle of an organization's management of cybersecurity risk. Each function is further divided into categories and subcategories that provide specific outcomes and activities, enabling organizations to achieve the desired state of cybersecurity.

- **CSF Organizational Profiles:** CSF Organizational Profiles serve as a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes. These profiles enable organizations to align their cybersecurity activities with their business requirements, risk tolerance, and resources. By developing and maintaining a current profile, organizations can better understand their cybersecurity risks and prioritize actions to improve their security posture. Target profiles allow organizations to set goals for future improvements, guiding strategic planning and resource allocation.

- **CSF Tiers:** CSF Tiers are applied to CSF Organizational Profiles to characterize the rigour of an organization's cybersecurity risk governance and management practices. There are four tiers: Partial, Risk Informed, Repeatable,

and Adaptive. These tiers reflect a progression from informal, reactive responses to more formalized, risk-informed, and adaptive practices. The tiers help organizations assess the maturity of their cybersecurity practices and identify opportunities for enhancement. By advancing through the tiers, organizations can improve their ability to manage and reduce cybersecurity risks effectively.

In addition to these core components, CSF 2.0 emphasizes the importance of communication and collaboration across the organization. It encourages the integration of cybersecurity risk management into the broader enterprise risk management process. This holistic approach ensures that cybersecurity is not siloed but rather incorporated into the organization's overall risk strategy.

The flexibility and scalability of CSF 2.0 make it suitable for organizations with varying levels of cybersecurity maturity. Whether an organization is just starting to develop its cybersecurity program or looking to enhance an existing one, CSF 2.0 provides a robust framework for managing and mitigating cybersecurity risks. It supports continuous improvement and adaptation to the evolving threat landscape, helping organizations stay resilient in the face of cyber threats.

By adopting the CSF 2.0, organizations can better protect their critical assets, maintain customer trust, and ensure business continuity. The framework's structured yet flexible approach allows organizations to tailor their cybersecurity practices to meet specific needs, making it a valuable tool for enhancing overall cybersecurity resilience.

B. NIST CSF 1.0 and NIST CSF 2.0 - Why was it updated?

The Cybersecurity Framework (CSF) 2.0 is the framework's first major update since its creation in 2014. Published on February 26, 2024, this new framework now explicitly aims to help all organizations manage and reduce cybersecurity risks more effectively. In response to the numerous comments received on the draft version, the National Institute of Standards and Technology (NIST) has expanded the CSF's core guidance and developed related resources to help users maximize the benefits of the framework. This update is the outcome of a multiyear process of discussions and public comments aimed at making the framework more effective and user-friendly [23].

The key updates and enhancements in CSF 2.0 include [23]:

- **Expanded Core Guidance:** The CSF Core has been refined to provide clearer, more actionable guidance for organizations. The core functions—Identify, Protect, Detect, Respond, and Recover—remain central, but the subcategories and categories within these functions have been updated to reflect current cybersecurity practices and threats. This ensures that the framework remains relevant and effective in addressing today's cybersecurity challenges.

- **Enhanced Resources and Tools:** NIST has developed new resources and tools to help organizations implement the CSF 2.0. These include detailed implementation guides, case studies, and templates that provide practical assistance. The aim is to make it easier for organizations to adopt and customize the framework to fit their specific needs and contexts.

- **Improved Alignment with Other Standards:** CSF 2.0 has been aligned more closely with other prominent cybersecurity and risk management standards, such as ISO 27001:2022 and COBIT. This alignment facilitates easier integration for organizations that need to comply with multiple standards and helps streamline their cybersecurity efforts.

- **Focus on Governance and Workforce:** CSF 2.0 places greater emphasis on governance and workforce development. It highlights the importance of strong leadership, clear policies, and skilled personnel in achieving effective cybersecurity. This focus helps organizations build a robust cybersecurity culture and ensures that they have the necessary human resources to manage cybersecurity risks.

By integrating these enhancements, CSF 2.0 provides a more comprehensive and practical tool for managing cybersecurity risks. Organizations can use the updated framework to better align their cybersecurity activities with their business goals, regulatory requirements, and risk tolerance. The iterative and inclusive development process of CSF 2.0 underscores NIST's commitment to continuous improvement and collaboration with the cybersecurity community.

C. CSF Core

The CSF Core is a set of cybersecurity outcomes arranged by Function, Category, and finally Subcategory [19].

- The CSF Core Functions organize cybersecurity outcomes at their highest level.

- Each function is divided into Categories, which are related cybersecurity outcomes that collectively comprise the Function.

- Furthermore, each category is divided into Subcategories, which are more specific outcomes of technical and management activities.

The Functions, Categories, and Subcategories apply to all ICT used by an organization. They also apply to all types of technology environments, including cloud, mobile, and artificial intelligence systems [19].

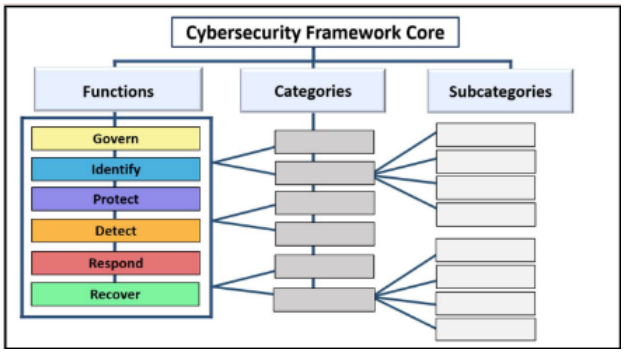

Fig. 1. CSF Core Structure

CSF Core-Functions

The CSF Core functions are as follows [19] [20]:

- **Govern (GV)**: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

- **Identify (ID)**: The organization's current cybersecurity risks are understood. Understanding the organization's assets, suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. Lessons learned are also used to identify improvements.

- **Protect (PR)**: Safeguards to manage the organization's cybersecurity risks are used. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security; and the resilience of technology infrastructure.

- **Detect (DE)**: Possible cybersecurity attacks and compromises are found and analyzed. This Function supports successful incident response and recovery activities.

- **Respond (RS)**: Actions regarding a detected cybersecurity incident are taken. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.

- **Recover (RC)**: Assets and operations affected by a cybersecurity incident are restored. With the RECOVER function, it is expected to understand roles and responsibilities, execute the recovery plan, double-check the work and communicate with internal and external stakeholders.

Fig. 2. CSF Core Functions

GOVERN, **IDENTIFY**, and **PROTECT** outcomes help prevent and prepare for incidents, while **GOVERN**, **DETECT**, **RESPOND**, and **RECOVER** outcomes help discover and manage incidents [19].

D. CSF Profiles

A CSF Organizational Profile describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes. Used to understand, tailor, assess, prioritize, and communicate the Core's outcomes [19].

Organizational Profiles can be categorized as [21]:

- A **Current Profile** that specifies the CSF outcomes an organization is currently achieving and characterizes how or to what extent each outcome is being achieved.

- A **Target Profile** that specifies the desired CSF outcomes an organization has selected and prioritized for achieving its cybersecurity risk management objectives.

CSF Profiles-Steps

CSF 2.0 describes the following five-step process for creating and using Organizational Profiles [21]:

- **Scope the Organizational Profile**: The scope defines the high-level facts and assumptions on which the Profiles will be based. An organization can have as many Organizational Profiles as desired, each with a different scope. The scope of a Profile determines the applicability of a given CSF outcome.

- **Gather needed information**: Examples of information may include organizational policies, risk management

priorities and resources, cybersecurity requirements and standards. The sources of information needed will depend on the use case, the elements that the Profiles will capture, and the level of detail desired.

- **Create the Organizational Profile**: Determine what types of information the Profile should include for the selected CSF outcomes. Consider the risk implications of the Current Profile to inform Target Profile planning and prioritization. Also, consider using a Community Profile as the basis for the Target Profile.

- **Analyze gaps and create an action plan**: Identifying and analyzing the differences between the Current and Target Profiles enables an organization to find gaps and develop a prioritized action plan for addressing those gaps. This helps organizations make better-informed decisions about how to improve cybersecurity risk management in a prioritized and cost-effective way.

- **Implement action plan and update Profile**: The Action Plan is fulfilled through any combination of management, programmatic, and technical controls. As those controls are implemented, the Organizational Profile can be used to track implementation status. Furthermore, implementing activities that follow the Action Plan is part of an ongoing cyber risk management program. Changes in risks, likelihoods, and/or impacts may all result in updates to the Organizational Profile.

Fig. 3. Steps for creating and using a CSF Organizational Profile

Given the value of continuous improvement, an organization can repeat these steps as often as needed.

E. CSF Tiers

CSF Tiers characterize the rigor of an organization's cybersecurity risk governance and management practices. The Tiers, as shown in Fig. 4, reflect an organization's practices for managing cybersecurity risk as Partial (Tier 1), Risk-Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4) [19] [26]. These Tiers describe a progression from unexpected reactions to methods that are flexible, aware of risks, and always evolving.

The selection of Tiers helps to understand how business requirements influence a company's overall risk management procedures and cybersecurity risk management.

Here is the explanation of the four tiers [3]:

- **Tier 1 - Partial**: This tier includes companies with on-demand or no security procedures. Businesses in Tier 1 are categorized as having very little awareness of cybersecurity risk.

- **Tier 2 - Risk-Informed**: The majority of corporate executives are now aware of the main threats they face. Organizations often lack a coordinated strategy and uniform departmental rules.

- **Tier 3 - Repeatable**: The third tier is for companies with risk management and cybersecurity best practices that have received executive approval. Businesses in this category are often more equipped to deal with vulnerabilities, cybersecurity risks, and threats.

- **Tier 4 - Adaptive**: The topmost tier requires the greatest time and money to deploy. High-tech solutions are incorporated into adaptive information security. These organizations contribute to the community's broader awareness of risks.

Fig. 4. CSF Tiers for Cybersecurity risk governance and management

Tiers should complement an organization's cybersecurity risk management rather than replace it.

F. Examples of Real-World Implementations - Success Stories

NIST highlights brief "success stories" explaining how diverse organizations use the Framework to improve their cybersecurity risk management. Here, two of those stories are provided [12]:

Saudi Aramco - the national oil company of Saudi Arabia adopted the NIST Cybersecurity Framework for Critical Infrastructure to ensure the organization's overall approach to cybersecurity supports high standards of governance.

Government of Bermuda - implemented NIST's Cybersecurity Framework to ensure that effective cybersecurity practices are implemented across the Government.

Success Stories - Saudi Aramco

Saudi Aramco's adoption of the NIST Cybersecurity Framework represents a strategic approach to enhancing cybersecurity across its organization.

Here are the key elements [13]:

- **Strategic Adoption Process**: The decision to adopt the NIST Cybersecurity Framework was not arbitrary but stemmed from a strategic need to streamline cybersecurity efforts and address communication challenges among different departments. This demonstrates a proactive approach to cybersecurity governance.

- **Comprehensive Implementation Strategy**: Saudi Aramco didn't just decide to adopt the framework; they devised a comprehensive implementation strategy. This involved forming a dedicated team, engaging consultants, conducting workshops for leadership and subject matter experts, and ensuring buy-in from corporate management. Such a structured approach ensures alignment and commitment throughout the organization.

- **Customized Maturity Assessment**: The organization utilized established models like the Capability Maturity Model Integration (CMMI) and the Cybersecurity Capability Maturity Model (C2M2) to assess its current cybersecurity maturity. This tailored assessment provided a clear understanding of existing capabilities and allowed for targeted improvements based on risk tolerances.

- **Continuous Monitoring and Improvement**: The journey didn't end with the implementation; instead, Saudi Aramco focused on continuous monitoring and improvement. Regular meetings with stakeholders, updates to corporate management, and the establishment of in-house capabilities for cybersecurity maturity assessment ensured that progress was tracked and adjustments made as necessary.

- **Standardized Language and Communication**: One of the significant benefits highlighted is the adoption of a standardized language for cybersecurity communication across all levels of the organization. This fosters a common understanding of cybersecurity risks and initiatives, facilitating more effective collaboration and decision-making.

- **Alignment with Regulations and Best Practices**: By aligning with the NIST Cybersecurity Framework, Saudi Aramco not only ensured compliance with national and international regulations but also incorporated multiple best practices and frameworks. This comprehensive approach enhances the organization's resilience to cyber threats and positions it as a leader in cybersecurity within the industry.

- **Knowledge Sharing and Outreach**: The translation of the Framework into Arabic reflects Saudi Aramco's commitment to knowledge sharing and capacity building beyond its own organization. By enabling accessibility to cybersecurity best practices in the Arabic-speaking world, the company contributes to raising cybersecurity capabilities regionally.

Overall, Saudi Aramco's success story illustrates the importance of strategic planning, comprehensive implementation, and continuous improvement in building robust cybersecurity capabilities within a large organization.

Success Stories - Government of Bermuda

Facing inconsistent security measures across ministries and departments, compounded by penalties under the Personal Information Protection Act 2016, the government recognized the growing importance of cybersecurity for economic resilience.

Here are the key aspects of this success story [14]:

- **Drivers for Change**: The Government recognized the increasing dependence on Information and Communication Technology (ICT) and the importance of cybersecurity for economic resilience. The launch of high-profile Fintech Initiatives further underscored the need for robust cybersecurity measures. Additionally, the intensification of the cyber threat environment highlighted the urgency of improving cyber awareness and defence capabilities.

- **Initiating the Process**: To address these challenges and drivers, the Government took proactive steps. It established the Cabinet Cybersecurity Committee to oversee the development and administration of the Information Systems Risk Management Programme. Self-assessment using the NIST Cybersecurity Framework helped identify gaps, control deficiencies, and areas of high risk, laying the foundation for targeted action plans.

- **Collaborative Efforts and Partnerships**: The Government fostered strategic partnerships with both public and private entities to develop a comprehensive Cybersecurity Strategy for the jurisdiction. This collaborative approach ensured that the strategy aligned

with stakeholder needs and addressed the evolving cyber threat landscape effectively.

- **Results and Impacts**: Through the adoption of the NIST Cybersecurity Framework and the implementation of remediation initiatives, the Government achieved significant results and impacts. These include a consistent standardized approach to addressing cybersecurity across ministries and departments, making the management of complex cybersecurity risks more manageable. Moreover, security activities are now closely aligned with business needs, and policies and processes have been developed to enable effective risk management.

- **Continuous Improvement**: The Government emphasizes the importance of continuous investment in enhancing collective cybersecurity capabilities. Regular reporting to the Cabinet using the Cybersecurity Framework as a dashboard ensures ongoing monitoring and evaluation of the security posture.

Overall, this success story demonstrates the transformative impact of adopting a comprehensive cybersecurity framework like NIST, coupled with proactive governance, collaboration, and a commitment to continuous improvement.

IV. ISO 27001:2022

A. *ISO 27001 Overview and Origin*

ISO 27001 is an information security standard created by the International Organization for Standardization (ISO), which provides a framework and guidelines aimed at companies of any size and from all sectors of activity to help them establish, implement and manage an information security management system [1].

With cybercrime on the rise and new threats constantly emerging, organizations do not have it easy when it comes to securing their digital assets. Therefore, ISO 27001 helps them become risk-aware and proactively identify and address weaknesses [1].

ISO 27001 was released as the first standard in the ISO 27000 series of standards for information security or cybersecurity. It was first published in 2005 and was lastly revised in 2022 to better accommodate the changing information security challenges. The current version is called ISO 27001:2022 [2].

As per ISO 27001 definition, the basic goal of an Information Security Management System is to protect three aspects of information:

- **Confidentiality:** involves protecting sensitive data from unauthorized access. This includes protecting information from bad actors with malicious intent, as well as limiting access to only authorized individuals within an organization [4].

- **Integrity:** means data are trustworthy and have not been accidentally altered or modified by an unauthorized user. The integrity of data may be compromised intentionally via attacks or unintentionally by a system malfunction, errors in entering data or forgetting to maintain an up-to-date backup [5].

- **Availability:** data is accessible at all times. The availability of data is crucial to the daily operations of all organizations [6].

There are four essential business benefits that a company can achieve with the implementation of ISO 27001 [2]:

- **Comply with legal requirements:** there is an ever-increasing number of laws and regulations related to information security, but most of them can be obliged by implementing ISO 27001. For example, ISO 27001 can help guide the creation of a company's security policy to be compliant with GDPR.

- **Achieve competitive advantage:** if a company gets its ISMS ISO 27001 certified, it automatically gets ahead of its competitors who do not possess the same status as customers who are sensitive about keeping their information safe will notice the differences.

- **Lower costs:** the main philosophy of ISO 27001 is to prevent security incidents from happening, incidents that come with high financial losses. Therefore, by preventing them, companies will be able to save money. Investment in ISO 27001 is far smaller than what could be potentially lost.

- **Better organization:** fast-growing companies often do not know what needs to be done, when, and by whom regarding their business processes. An ISO 27001-compliant ISMS helps resolve such situations as it encourages companies to write down their main procedures and maintain critical organizational knowledge.

ISO 27001 is separated into two parts. The first one consists of 11 clauses. Clauses 0 to 3 of the standard (Introduction, Scope, Normative references, Terms and Definitions) serve as an introduction to the ISO 27001 standard. Clauses 4 to 10, which provide the ISO 27001 requirements, are mandatory if the company wants to be compliant with the standard, and are examined in more detail later in this paper [2].

The second part, called Annex A, provides the guidelines for

93 control objectives and controls. Annex A supports the ISO 27001 clauses and their requirements with a list of controls that are selected as part of the risk management process [2].

B. ISO 27001:2013 and ISO:27001:2022 - Why was it updated?

ISO 27001:2022 is a moderate update from the previous version of the standard: ISO 27001:2013. The main part of ISO-27001, clauses 4 to 10, has changed only slightly, mainly to align with other ISO management standards like ISO 9001 and ISO 14001, and with Annex SL, the common structure and terminology for all ISO management system standards [8].

The most significant changes in ISO-27001:2022 are in Annex A, which contains the security controls that can be implemented to address the information security risks identified by organizations. These controls have decreased from 114 to 93 and were organized into four themes: Organizational, People, Physical, and Technical. Figure 5 demonstrates these changes in a simplistic way:

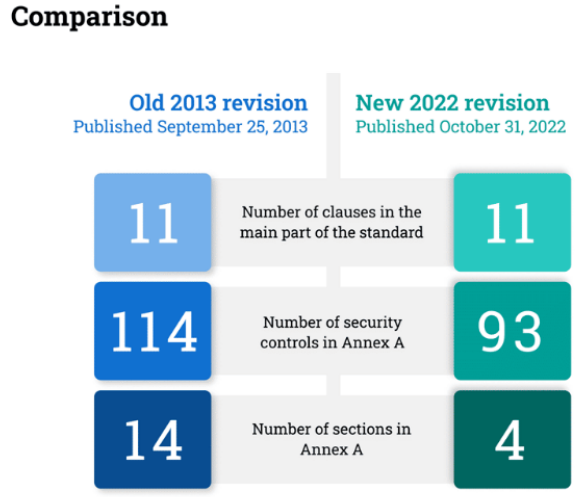

Fig. 5. Comparison between ISO 27001:2013 and ISO 27001:2022 [9]

New requirements focus on understanding the needs of interested parties, planning for ISMS processes, clarifying the term “business” in leadership, and emphasizing controlled planning for ISMS changes. The modifications concerning the clauses can be seen below [10]:

- **Clause 4.2 - Understanding the Needs and Expectations of Interested Parties:** a new subclause was added requiring an analysis of which of the interested party requirements must be addressed through the ISMS.
- **Clause 4.4 - Information Security Management System:** a phrase was added, which requires organizations to identify necessary processes and their interactions within the ISMS.
- **Clause 5.3 - Organizational Roles, Responsibilities, and Authorities:** a minor update to the language clarified that communication of roles relevant to information security are to be communicated within the organization.
- **Clause 6.2 - Information Security Objectives and Planning to Achieve Them:** now includes additional guidance on the information security objectives. This gives more clarity about how objectives should be monitored regularly and formally documented.
- **Clause 6.3 - Planning of Changes:** added to set a standard around planning for changes. It states that if changes are needed to the ISMS, they shall be adequately planned for.
- **Clause 7.4 - Communication:** subclauses **(d)** (who should communicate) and **(e)** (the process by which communication should be affected) have been simplified and combined into a newly renamed subclause **(d)** (how to communicate).
- **Clause 8.1 - Operational Planning and Control:** new requirements were added for establishing criteria for security processes, and for implementing processes according to those criteria. Also, the requirement to implement plans for achieving objectives was deleted.
- **Clause 9.3 - Management Review:** a new item **9.3.2 c)** was added that clarifies that inputs from interested parties need to be about their needs and expectations, and relevant to the ISMS.
- **Clause 10 - Improvement:** structural changes to this clause now list Continual Improvement (10.1) first, and Nonconformity and Corrective Action (10.2) second.

As for Annex A, despite the reduction in sections from 14 to 4, the changes are only moderate because most of the controls have either stayed the same (35) or have only been renamed (23). 57 controls were merged, which reduced the overall number, but the requirements within those controls remained almost the same. Moreover, one control was split into two separate controls, while the requirements stayed the same [9]. Finally, 11 new controls were added, which are described below [11]:

- **A.5.7 - Threat intelligence:** This control requires the internal or external gathering and analysis of information about threats so that appropriate mitigation actions can be taken. This information could be about particular attacks, about methods and technologies the attackers are using, or about attack trends.

- **A.5.23 - Information security for use of cloud services:** requires setting security requirements for cloud services in order to have better protection of the information in the cloud. This includes purchasing, using, managing, and terminating the use of cloud services.

- **A.5.30 - ICT readiness for business continuity:** information and communication technology has to be ready for potential disruptions so that required information and assets are available when needed. This includes readiness planning, implementation, maintenance, and testing.

- **A.7.4 - Physical security monitoring:** the monitoring of sensitive areas to only enable authorized people to access them.

- **A.8.9 - Configuration management:** managing the whole cycle of the security configuration for the technology to ensure a proper level of security and to avoid any unauthorized changes. This includes configuration definition, implementation, monitoring, and review.

- **A.8.10 - Information deletion:** requires the deletion of data when no longer required, to avoid leakage of sensitive information and to enable compliance with privacy and other requirements.

- **A.8.11 - Data masking:** using data masking together with access control to limit the exposure of sensitive information. This primarily means personal data, as it is heavily regulated through privacy regulations, but it could also include other categories of sensitive data.

- **A.8.12 - Data leakage prevention:** requires the application of various data leakage measures to avoid unauthorized disclosure of sensitive information, and if such incidents happen, to detect them in a timely manner.

- **A.8.16 - Monitoring activities:** an organization must monitor its systems to recognize unusual activities and, if needed, to activate the appropriate incident response.

- **A.8.23 - Web filtering:** websites users access must be managed so that IT systems are protected. This way, systems can be prevented from being compromised by malicious code, and also prevent users from using illegal materials from the Internet.

- **A.8.28 - Secure coding:** secure coding principles must be established and applied to software development.

C. Clauses 4 - 10

An overview is now displayed of the requirements from ISO 27001, clauses 4 to 10, targeting a better understanding of the standard [2]:

- **Clause 4 - Context of the organization:** the context of the organization has to be understood. External and internal issues, as well as interested parties, need to be identified and considered. Requirements may include regulatory issues, but they may also go far beyond. To cover this topic, ISO 27001 requires the definition of the organizational context, referring to ISO 31000, the ISO standard for risk management, for detailed guidance [15]. Furthermore, the ISMS scope needs to be defined here. It defines which information a company intends to protect. It sets responsibility for protecting that information no matter where, how, and by whom it is accessed [17].

- **Clause 5 - Leadership:** objectives need to be established according to the strategic direction and objectives of the organization. Obligations include the ability to provide resources needed for the ISMS, to support people in their contribution to the ISMS, and having a established top-level policy for information security, as well as roles and responsibilities correctly assigned.

- **Clause 6 - Planning:** highlights the importance of identifying risks associated with the business, documenting how they will be addressed, and then analysing, evaluating, and prioritising those risks. A risk assessment needs to be conducted, followed by the development of a risk treatment plan.

- **Clause 7 - Support:** resources, competence of employees, awareness, and communication are key for supporting the ISMS. Information needs to be documented, created, and updated, as well as controlled. A suitable set of documentation, including a communications plan needs to be maintained in order to support the success of the ISMS.
- **Clause 8 - Operation:** stipulates the processes needed to implement Clause 6. These processes need to be planned, implemented, and controlled, with the help of some criteria that also needs to be established. Risk assessment and treatment, which need to be on top management‘s minds, have to be put into action.

- **Clause 9 - Performance Evaluation:** here, the requirements of the ISO 27001 standard expect monitoring, measurement, analysis, and evaluation of the Information Security Management System, as well as internal audits and a management review.

- **Clause 10 - Improvement:** improvement follows the evaluation. Nonconformities need to be addressed by taking action and eliminating their causes. Moreover, a continual improvement process should be implemented.

D. Annex A - Security Controls

The ISO 27001:2022 Annex controls have been restructured and consolidated to reflect current security challenges. The core ISMS management processes remain unchanged, but the Annex A control set has been updated to reflect more modern risks and their associated controls [18]. The new 4 categories are the following [18]:

- **Organizational:** 37 controls, encompass regulations and measures which dictate an organization's comprehensive attitude towards data protection over a broad range of matters.
- **People:** 8 controls, enable businesses to regulate the human component of their information security program, by defining the manner in which personnel interact with data and each other.
- **Physical:** 14 controls, employed to ensure the security of tangible assets like entry systems, guest access protocols, asset disposal processes, storage medium protocols, and clear desk policies. Such safeguards are essential for the preservation of confidential information.
- **Technological:** 34 controls, dictate the cybernetic regulations and proceedings that corporations should adopt to execute a protected, compliant IT infrastructure.

Annex A serves as a time and resource-saving tool for the initial certification and subsequent processes and provides a basis for audits, process reviews and strategic planning [18].

E. Implementation and Certification Process

If a company intends to go through the certification process of ISO 27001, it must prepare itself first, and implement the following steps [24]:

- **Develop the ISO 27001 implementation plan:** someone within an organization needs to be responsible for overseeing the process, setting expectations, and managing milestones. Education on ISO 27001 standards and its 114 controls is also a key part of this process.
- **Define the scope of its ISMS:** each enterprise is unique and possesses different types of data. Before building an ISMS, a company needs to determine exactly what kind of information it needs to protect. For some businesses, the scope of their ISMS includes their entire organization while for others, it includes only a specific department or system. Top management needs to discuss what is wanted to be represented in the scope statement of the ISO 27001 certificate.
- **Perform a risk assessment and gap analysis:** a risk assessment is a requirement for ISO 27001 compliance. The data, analysis, and results of said risk assessment must be documented. Legal, regulatory, and contractual obligations must be investigated in order to evalutate what is the business held to. An experienced consultant can provide expert guidance to help meet compliance requirements, as well as help establish best practices that strengthen the overall security posture.
- **Design and implement policies and controls:** now, risks need to be assigned into tolerable or not tolerable. The auditor will want to review the decisions made regarding each identified risk during the certification audit. A Statement of Applicability and a Risk Treatment Plan also need to be part of the audit evidence. The Statement of Applicability summarizes and explains which ISO 27001 controls and policies are relevant to an organization. This document is one of the first things an external auditor will review during a certification audit.
- **Implement a risk treatment plan:** the Risk Treatment Plan is another essential document for ISO 27001 certification. It records how organizations will respond to the threats identified during risk assessment processes. The risks can be modified by establishing controls that reduce the likelihood of occurrence, avoided by preventing the circumstances where they could occur, shared with a third party, or accepted when the cost of addressing them is greater than the potential damage of leaving them be. Finally, policies and controls should be implemented in response to the identified risks.
- **Document and collect all the evidence:** to get the ISO 27001 certification, a company needs to prove to the auditor that it established effective policies and controls and that those are functioning as required by the ISO 27001 standard.

As for the Certification Audit Process, an external auditor will evaluate the current ISMS to verify that it meets ISO 27001 requirements and issue the certification. The phases of this procedure are as follows [24] [25]:

- **Document review:** in this first stage, the auditor will look for the documented scope, the ISMS policy and objectives, the description of the risk assessment methodology, the Risk Assessment Report, the Statement of Applicability, the Risk Treatment Plan, and the procedures for document control, corrective and preventive actions, and internal audit. Furthermore, some

of the controls from ISO 27001 Annex A must be documented, along with records of at least one internal audit and management review.

- **Main audit:** the auditor will check whether the ISMS has really been successfully implemented in the company, or if it is only there on paper. Checking will be performed through observation, interviewing the employees, and by checking the records. If there are no major nonconformities, the certification body will issue the ISO 27001 certificate to the company. Otherwise, a deadline by which the non-conformity must be resolved will be given (usually 90 days).

- **Surveillance audit:** the certificate issued by the certification body will be valid for three years, during which the certification body will check if the ISMS is maintained properly, therefore the existence of surveillance audits. These are very similar to main audits but are only about 30% of the duration of them. There will be at least one surveillance audit each year.

- **Recertification audit:** during the last year of the three-year ISO certification term, an organization can undergo a recertification audit. After completing the recertification audit, the ISO 27001 certification is valid for another three years.

F. Examples of Real-World Implementations - Success Stories

ISO standards play a pivotal role in shaping the operational landscape of businesses across diverse industries. Here are some case studies of real-life implementations of ISO 27001:

InteliSecure: a Managed Security Service Provider (MSSP) that specializes in Data Loss Prevention (DLP). The company protects critical data assets and intellectual property for businesses in over 22 countries. InteliSecure is known for its pioneering work in security humanistic, focusing on the role of human behaviour in security [27].

In 2014, after receiving Series A funding, InteliSecure sought ISO/IEC 27001 certification to enhance internal and customer data security, codify disaster recovery plans, position the company for growth, and differentiate itself in the marketplace. The main needs addressed were to secure internal and customer assets, prepare for disaster recovery, position for growth, and differentiate in the marketplace [27].

The benefits of achieving ISO 27001 certification included standardized documentation and workflows, the reduction of risk-related gaps, employee empowerment and improved training, enhanced market differentiation, and customer trust. The ISO 27001 certification has positioned InteliSecure as a leader in the data loss prevention industry, enhancing its ability to secure customer data, streamline operations, and support business growth. Also, it enabled InteliSecure to streamline growth through standardized processes, minimize the risk of exposing confidential information, enhance disaster recovery planning, and improve overall security posture [27].

Pervasive Health: a company providing the Apervita platform, which enables healthcare professionals to connect evidence-based insights to health practices. Apervita integrates current and historical patient data into a unified source, making it easily accessible and usable for health professionals. The platform is built with best-of-breed technologies to handle big data, privacy, Personally Identifiable Information (PII), Protected Health Information (PHI), and compliance with HIPAA standards [28].

Pervasive Health aimed to achieve ISO 27001 certification to ensure the security of sensitive health data, improve internal processes, and strengthen business operations in the U.S. and Europe. The certification aimed to formalize their Information Security Management System, enhance data protection, and comply with the highest security standards [28].

ISO27001 certification provided numerous benefits, like enhanced security for internal processes and client data, formalized and improved data protection practices, increased confidence among clients and partners in the security measures, ability to connect health insights securely, ensuring better health outcomes, and strengthened competitive advantage in a data-sensitive market. The certification enabled Pervasive Health to promote their rigorous security standards, leading to positive responses from partners and anticipated business growth [28].

V. NIST CSF 2.0 AND ISO 27001:2022

A. Common Aspects

Both NIST CSF and ISO 27001 help organizations implement best practices for a strong cybersecurity posture. Both frameworks focus on helping organizations better identify, track, mitigate, prepare for, and recover from security incidents and data breaches.

They're both built on widely-accepted best practices in cybersecurity and experts agree on many recommendations and strategies from them. Both are pivotal tools designed to help businesses manage and mitigate threats. They share several similarities that make them compatible and complementary, such as [29]:

- **Risk Management Focus:** at their core, they are designed around the concept of threat management. ISO 27001 requires firms to conduct a thorough assessment to pinpoint, analyze, and evaluate risk. Similarly, NIST

CSF is structured around identifying and mitigating hazards across various organizational functions.

- **Control Measures:** both offer a set of controls aimed at addressing identified vulnerabilities.
- **Flexibility and Scalability:** ISO 27001 is designed to be applicable to enterprises of all sizes and industries, while NIST CSF offers a similar level of adaptability, enabling organizations to tailor it according to their specific requirements.
- **Holistic Approach:** the two standards advocate for a holistic approach to digital safety. They consider the technological aspects and the human and procedural elements, emphasizing the need for a comprehensive strategy.

B. Key Differences

However, the two frameworks are not interchangeable. The NIST CSF is designed as a guide, whereas ISO 27001 is designed as a standard. The difference here is that NIST CSF serves as an instruction manual and ISO 27001 is more of a test that requires certain measures to pass.

Also, becoming ISO 27001 compliant is more expensive than adhering to the NIST CSF. The NIST CSF is free to access and doesn't require a third-party audit or certification.

Figure 6 displays some of these differences:

	NIST	ISO 27001
PURPOSE	Designed as a guide	Designed as a compliance standard
COMPLIANCE PROCESS	No certification; serves as a guide to establish cybersecurity	Requires a formal audit that results in a certification
MATURITY	Used in the early stages of a business' security journey	Used by organizations with more mature security and advanced risk
COSTS	Free download and implement	Requires you to buy the standard and hire and auditor

Fig. 6. Some of the key differences between NIST CSF and ISO 27001 [30]

Furthermore, risk maturity has to be addressed. ISO 27001 is characterised as a great option for operationally mature organizations seeking certification, while the NIST CSF may be best for organizations that are in the first stages of developing a cybersecurity risk management plan or attempting to mitigate prior failures or data breaches [31]. That said, there is a possibility that the two can be used together for organizations in any stage of development and operational growth, which will be seen in the next sections of the paper.

While ISO 27001 does not have maturity tiers, the NIST CSF provides four implementation tiers that illustrate an organization's security maturity based on adherence to NIST's guidance. Companies seeking to evaluate their security performance against industry benchmarks and elevate the maturity of their cybersecurity risk programs can use NIST's tiers to target higher levels of implementation [31].

Finally, the targeted industries are also a little different. ISO 27001 is widely used across various industries globally, but NIST CSF is primarily used in the United States, especially in government and critical infrastructure, since the framework was created in the United States [29].

C. Compatibility - Does it make sense to use them simultaneously?

Using NIST CSF 2.0 and ISO 27001:2022 simultaneously can provide a robust, comprehensive approach to cybersecurity and information security management. The complementary nature of these frameworks allows organizations to leverage the operational focus of NIST CSF alongside the structured management system of ISO 27001, resulting in enhanced security posture, compliance, and risk management. These are the topics that make the two standards compatible [32]:

- **Objective Alignment:** both NIST CSF and ISO 27001 aim to improve organizational security and risk management practices. They both focus on protecting the confidentiality, integrity, and availability of information.
- **Structure and Approach:** NIST CSF focuses on practical, operational aspects of cybersecurity. It provides a comprehensive, risk-based approach with its five core functions. On the other hand, ISO 27001 focuses on establishing a management framework for information security. It is more prescriptive in terms of processes and documentation. Together, they have the best of the two worlds.
- **Risk Management:** both frameworks emphasize the importance of risk assessment and risk management. NIST CSF outlines the process within its Identify function, while ISO 27001 dedicates specific clauses to risk assessment and treatment.
- **Control Sets:** NIST CSF provides a broad set of activities that can be mapped to specific controls found in ISO 27001. This allows for the alignment and integration of both frameworks. ISO 27001 Annex A contains controls that can be directly mapped to the NIST CSF core functions and categories.

- **Continual Improvement:** both frameworks advocate for continuous monitoring and improvement of security practices. ISO 27001 includes a Plan-Do-Check-Act (PDCA) cycle, while NIST CSF encourages ongoing assessment and improvement of cybersecurity posture.

Moreover, there are several benefits that come from choosing to implement NIST CSF and ISO 27001 at the same time [32]:

- **Comprehensive Security Posture:** utilizing both frameworks can provide a more holistic approach to cybersecurity. NIST CSF's practical guidelines complement ISO 27001's structured management system.
- **Improved Compliance:** using both standards can help organizations meet diverse regulatory and industry requirements, enhancing compliance and reducing legal risks.
- **Enhanced Risk Management:** the combination allows organizations to benefit from NIST CSF's detailed risk management practices alongside ISO 27001's formalized risk treatment processes.
- **Operational Efficiency:** NIST CSF's practical recommendations can enhance the operationalization of ISO 27001's policies and procedures, leading to more efficient and effective security practices.
- **Scalability and Flexibility:** organizations of varying sizes and industries can tailor the implementation of both frameworks to suit their specific needs, ensuring scalable and flexible security management.

D. How can they work together?

ISO 27001 and NIST CSF each tackle information security and risk management from different angles and different scopes. But by implementing both, they essentially help each other in benefiting the security of an enterprise.

Once again, for example, organizations just starting to build their information systems can start with the NIST CSF guidelines, as they are easily available. This helps them paint a clear picture of their situation, after which they can aim for cybersecurity improvement and work toward ISO 27001 certification.

Integrating NIST CSF with ISO 27001 can provide a robust cybersecurity management approach by leveraging the strengths of both [32]:

Strategic and Operational Alignment: NIST CSF's flexible framework allows it to align strategically with an organization's larger business objectives and cybersecurity vision, while ISO 27001 provides the detailed, tactical steps required to implement the strategic vision, focusing on specific controls and operational efficiency.

Complementing Governance Approaches: NIST CSF's Implementation Tiers can help evaluate how mature an organization's cybersecurity practices are and guide the depth and sophistication of ISO 27001 controls implementation, while ISO 27001's systematic process ensures that all aspects of cybersecurity are covered, from policy and planning to operations and monitoring, thus operationalizing the high-level framework provided by NIST CSF.

1) Synergy - Strategic and Operational Alignment

: The synergy between the strategic guidance of NIST CSF and the operational detail of ISO 27001 can be realized through a series of integrative steps:

- **Strategic Risk Identification with NIST CSF:** firstly, NIST CSF is used to define the current cybersecurity posture of the company, aligning this with strategic business objectives, and to determine the high-level risks and vulnerabilities that can impact business operations.
- **Operationalization with ISO 27001:** then, the high-level risks identified through NIST CSF are translated into detailed risk assessments as required by ISO 27001, and specific controls from ISO 27001 are implemented to address these risks. The selection of controls is influenced by the strategic priorities established through NIST CSF.
- **Feedback Loop for Continuous Improvement:** using the performance evaluation and improvement aspects of ISO 27001, it is possible to feed back into NIST CSF's continuous improvement loop. Adjustments to the cybersecurity program can be made strategically (via NIST CSF) and operationally (via ISO 27001) based on ongoing monitoring and assessment outcomes.
- **Governance and Communication:** clear communication channels and governance structures are established to ensure strategic decisions made with NIST CSF are effectively translated into operational actions through ISO 27001. This helps in maintaining alignment between the cybersecurity initiatives and business objectives.

This strategic and operational synergy ensures that not only are the security needs aligned with business strategies as laid out by NIST CSF, but they are also practically achievable and maintainable on a day-to-day basis through the structured approach of ISO 27001.

2) Synergy - Complementing Governance Approaches

: The integration of governance approaches from both NIST CSF and ISO 27001 can be achieved through a structured process that ensures both strategic alignment and operational compliance:

- **Strategic Governance Establishment with NIST CSF:** NIST CSF can be used to facilitate the involvement of senior management in defining the strategic direction for cybersecurity, based on a clear understanding of business objectives and cyber risk landscape. From there, cybersecurity policies and objectives that reflect the organization's strategic goals can be developed and used to guide the development of the ISMS in ISO 27001.

- **Operational Governance Structure with ISO 27001:** the detailed governance structures required by ISO 27001 to manage the ISMS effectively must be implemented, including defining roles, responsibilities, and processes for risk management, control implementation, and incident response. One needs to be sure that these structures support and enforce the strategic decisions made using NIST CSF, creating a cohesive governance approach.

- **Feedback and Continuous Improvement:** feedback mechanisms are then established to monitor the effectiveness of the ISMS and governance practices, ensuring that they continue to support strategic objectives as outlined by NIST CSF. The continuous improvement process from ISO 27001 refines governance practices, policies, and controls based on operational experiences and changes in the cyber risk environment.

- **Compliance and Reporting:** finally, comprehensive compliance and reporting processes that leverage ISO 27001's requirements must be developed for documentation and audit trails. These processes inform and update senior management (as per NIST CSF's guidance) about the status of information security and compliance with strategic objectives.

By synergistically integrating the strategic governance framework provided by NIST CSF with the operational governance requirements of ISO 27001, organizations can create a comprehensive governance system that not only meets global standards but also aligns with and supports the organization's specific business goals. This ensures that cybersecurity governance is both effective and sustainable, supporting long-term strategic success and operational security resilience.

3) Conclusion - Synergies between NIST CSF and ISO 27001

: The partnership between NIST CSF and ISO 27001 presents a comprehensive approach to cybersecurity, combining strategic flexibility with rigorous operational control.

NIST CSF offers a high-level, adaptable framework that aids organizations in aligning their cybersecurity strategies with broader business objectives, making it accessible and actionable for senior management.

On the other hand, ISO 27001 provides a detailed, systematic approach to implementing these strategies through its prescriptive set of controls and rigorous Information Security Management System (ISMS).

Overall, and once again, when these frameworks are integrated, organizations benefit from:

- **Enhanced Risk Management:** by combining NIST CSF's broad risk assessment and prioritization with ISO 27001's detailed control implementation, organizations can cover all bases—from identifying potential threats to actively mitigating them.

- **Streamlined Compliance and Governance:** the integration helps streamline compliance efforts by aligning NIST CSF's flexible approach with ISO 27001's strict compliance requirements, creating a cohesive governance structure that supports continuous improvement.

- **Effective Resource Allocation:** through strategic alignment and detailed control, organizations can effectively allocate their resources, prioritizing critical areas that maximize cybersecurity impact relative to business goals.

Ultimately, the complementary nature of NIST CSF and ISO 27001 allows companies to develop a dynamic, responsive cybersecurity posture that not only protects against threats but also supports strategic business objectives.

VI. Conclusion

In this work, a presentation of the NIST CSF 2.0 and the ISO 27001:2022 frameworks was made. Their key aspects were discussed, including their origins, how they compare to their previous versions, their principles, and their implementation processes, as well as the certification process in the case of ISO 27001. Additionally, two examples of real-life implementations by companies and organizations were provided for each framework, offering a more "action-based" perspective.

Furthermore, an important topic was addressed: how these two frameworks can work together and form a partnership to improve the overall cybersecurity and functioning of organizations. The discussion focused on their synergy in strategic and operational alignment, as well as their complementary governance approaches. By integrating the NIST CSF 2.0's flexible, risk-based approach with ISO 27001's structured, comprehensive ISMS requirements, organizations can create a robust, resilient cybersecurity posture that leverages the strengths of both frameworks.

In conclusion, the integration of NIST CSF 2.0 and ISO 27001:2022 offers a powerful combination that can help organizations strengthen their cybersecurity posture, improve resilience against cyber threats, and achieve regulatory compliance. By understanding and leveraging the unique strengths of each framework, organizations can develop a holistic cybersecurity strategy that is both comprehensive and adaptable to their specific needs and challenges. This synergy not only enhances security but also supports the overall strategic and operational goals of the organization, ensuring sustainable and resilient business operations.

REFERENCES

[1] ISO: "ISO/IEC 27001:2022", available at https://www.iso.org/standard/27001.

[2] Kosutic, D: "What is ISO 27001? A quick and easy explanation", available at https://advisera.com/27001academy/what-is-iso-27001/.

[3] Shivam Jha, Shivam: "Nist Implementation Tiers 101: All you need to know", available at https://sprinto.com/blog/nist-implementation-tiers/. January 2024.

[4] Coursera: "What Is the CIA Triad?", available at https://www.coursera.org/articles/cia-triad. November, 2023.

[5] Washington University in St.Louis: "Integrity", available at https://informationsecurity.wustl.edu/items/integrity/.

[6] Washington University in St.Louis: "Availability", available at https://informationsecurity.wustl.edu/items/availability/.

[7] Kirvan, Paul: "Top 12 IT security frameworks and standards explained", available at https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one/. October 2023.

[8] Dahlgren, L.: "ISO-27001 2013 vs ISO-27001 2022: What's changed?", available at https://codific.com/iso-27001-2013-vs-iso-27001-2022/.

[9] Kosutic, D.: "ISO 27001 2013 vs. 2022 revision – What has changed?", available at https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/. February, 2022.

[10] A-LIGN: "What's the Difference Between ISO 27001:2013 and ISO 27001:2022?", available at https://www.a-lign.com/articles/blog-whats-the-difference-between-iso-27001-2013-and-iso-27001-2022.

[11] Kosutic, D.: "Detailed explanation of 11 new security controls in ISO 27001:2022", available at https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/.

[12] NIST: "Success Stories", available at https://www.nist.gov/cyberframework/success-stories/. March, 2024.

[13] NIST: "Success Story: Saudi Aramco", available at https://www.nist.gov/cyberframework/success-stories/saudi-aramco/. January, 2021.

[14] NIST: "Success Story: Government of Bermuda", available at https://www.nist.gov/cyberframework/success-stories/government-bermuda/.

[15] Leal, R.: "How to define context of the organization according to ISO 27001", available at https://advisera.com/27001academy/knowledgebase/how-to-define-context-of-the-organization-according-to-iso-27001/. November, 2022.

[16] Aramco: "About Aramco", available at https://www.aramco.com/en/about-us/.

[17] Kosutic, D.: "All you need to know about setting the ISO 27001 scope", available at https://advisera.com/27001academy/knowledgebase/how-to-define-the-isms-scope/. March, 2023.

[18] Edwards, M.: "ISO 27001:2022 Annex A Explained", available at https://www.isms.online/iso-27001/annex-a/. March, 2024.

[19] NIST: "CSF 2.0", available at https://doi.org/10.6028/NIST.CSWP.29/. February, 2024.

[20] NIST: "Navigating NIST's CSF 2.0 Quick Start Guides - Resource and Overview Guide", available at https://doi.org/10.6028/NIST.SP.1299/. February, 2024.

[21] NIST: "Navigating NIST's CSF 2.0 Quick Start Guides - CSF 2.0 Organizational Profiles", available at https://doi.org/10.6028/NIST.SP.1301/. February, 2024.

[22] NIST: "CSF 2.0 Informative References - CSF 2.0 Implementation Examples", available at https://www.nist.gov/document/csf-20-implementations-pdf/. February, 2024.

[23] NIST: "NIST Releases Version 2.0 of Landmark Cybersecurity Framework", available at https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework/. February, 2024.

[24] Secureframe: "The ISO 27001 Certification Process: A Step-by-Step Guide", available at https://secureframe.com/hub/iso-27001/certification-process.

[25] Kosutic, D: "ISO 27001 certification - Everything you need to know about getting ISO 27001 certified", available at https://advisera.com/27001academy/iso-27001-certification/. November, 2023.

[26] NIST: "Navigating NIST's CSF 2.0 Quick Start Guides - Tiers", available at https://doi.org/10.6028/NIST.SP.1302.ipd/. February, 2024.

[27] BSI: "ISO/IEC 27001 Positions InteliSecure for Growth, Leadership in Data Loss Prevention Industry", available at https://www.bsigroup.com/LocalFiles/en-US/Case-Studies/InteliSecure_CaseStudy.pdf.

[28] IT Governance: "Pervasive Health protects data with ISO27001", available at https://www.itgovernance.co.uk/download/Case-Study-Pervasive-Health.pdf.

[29] Eden Data: "ISO 27001 and NIST Cybersecurity Framework: Know the Differences", available at https://www.edendata.com/post/iso-27001-vs-nist-cybersecurity-frameworks. October, 2023.

[30] Vanta: "NIST CSF and ISO 27001: What's the difference?", available at https://www.vanta.com/collection/iso-27001/nist-csf-vs-iso-27001nist-csf-vs-iso-27001-what-they-have-in-common.

[31] Vicente, V.: "NIST and ISO: What's the Difference?", available at https://www.auditboard.com/blog/nist-vs-iso-whats-the-difference/.

April, 2023.

[32] Buker, H.: ”How ISO 27001 and NIST CSF complement each other?”, available at https://www.6clicks.com/resources/blog/how-do-iso-27001-and-nist-csf-complement-each-other. January, 2023.