electronics

MDPI

Article

Holistic Information Security Management and Compliance Framework

Šarūnas Grigaliūnas [1,*,†], Michael Schmidt [2], Rasa Brūzgienė [1,†], Panayiota Smyrli [3], Stephanos Andreou [3] and Audrius Lopata [4]

[1] Department of Computer Sciences, Kaunas University of Technology, Studentu Str. 50, 51368 Kaunas, Lithuania; rasa.bruzgiene@ktu.lt
[2] Leibniz Supercomputing Centre, Boltzmann Str. 1, 85748 Garching b. München, Germany; mic.schmidt@lmu.de
[3] Cyprus Research & Academic Network, 33 Neas Egkomis, Egkomi, Nicosia 2409, Cyprus; yiota.smyrli@cynet.ac.cy (P.S.); stephanos.andreou@cynet.ac.cy (S.A.)
[4] Department of Information Systems, Kaunas University of Technology, Studentu Str. 50, 51368 Kaunas, Lithuania; audrius.lopata@ktu.lt
* Correspondence: sarunas.grigaliunas@ktu.lt
† These authors contributed equally to this work.

Abstract: The growing complexity of cybersecurity threats demands a robust framework that integrates various security domains, addressing the issue of disjointed security practices that fail to comply with evolving regulations. This paper introduces a novel information security management and compliance framework that integrates operational, technical, human, and physical security domains. The aim of this framework is to enable organizations to identify the requisite information security controls and legislative compliance needs effectively. Unlike traditional approaches, this framework systematically aligns with both current and emerging security legislation, including GDPR, NIS2 Directive, and the Artificial Intelligence Act, offering a unified approach to comprehensive security management. The experimental methodology involves evaluating the framework against five distinct risk scenarios to test its effectiveness and adaptability. Each scenario assesses the framework's capability to manage and ensure compliance with specific security controls and regulations. The results demonstrate that the proposed framework not only meets compliance requirements across multiple security domains but also provides a scalable solution for adapting to new threats and regulations efficiently. These findings represent a significant step forward in holistic security management, indicating that organizations can enhance their security posture and legislative compliance simultaneously through this integrated framework.

Keywords: information security; security controls; OpSec; TechSec; HumSec; PhySec

Citation: Grigaliūnas, Š.; Schmidt, M.; Brūzgienė, R.; Smyrli, P.; Andreou, S.; Lopata, A. Holistic Information Security Management and Compliance Framework. *Electronics* **2024**, *13*, 3955. https://doi.org/10.3390/electronics13193955

Academic Editors: George Hatzivasilis, Sotiris Ioannidis, Vasileios Mavroeidis and Vasilis Katos

Received: 14 September 2024
Revised: 28 September 2024
Accepted: 5 October 2024
Published: 7 October 2024

1. Introduction

Organizations in the EU are faced with complex regulatory demands, as GDPR (Regulation (EU) 2016/679) [1], Directive on Security of Network and Information Systems (NIS2 Directive [2]), and the Artificial Intelligence Act (AI Act [3]) impose stringent requirements to safeguard data and critical infrastructures. Concurrently, the ISO/IEC 27001 [4] standard provides a comprehensive set of controls for information security. This paper presents a framework that addresses these challenges by integrating multiple security domains to ensure regulatory compliance and mitigate cybersecurity risks. Unlike traditional frameworks, this solution systematically aligns with current and emerging security legislation, offering a unified approach to comprehensive security management. The primary contributions of this work are as follows:

- Development of a comprehensive information security management and compliance framework that integrates various security domains (operational, technical, human,

and physical security) to address the complexity of cybersecurity requirements and compliance with evolving regulations.
- Ontology-based mapping of security controls to systematically align with current and emerging security legislation, including GDPR, Cybersecurity Act (Regulation (EU) 2019/881 [5]), NIS2 Directive, Artificial Intelligence Act, Coordinated Plan on Artificial Intelligence [6], Ethics Guidelines for Trustworthy AI [7], ISO/IEC 27001:2022, The Critical Entities Resilience Directive (CER) [8] and Critical Security Controls (CIS) [9].
- Categorization of security domains into detective, preventive, and corrective measures, applying these across the outlined security domains and mapped security controls to enhance the understanding and implementation of compliance activities.

This research explores the intersection of EU security legislation and the ISO/IEC 27001 standard, aiming to map legislative requirements to specific controls from the Annex A of ISO/IEC 27001. By examining five distinct risk scenarios, this research identifies the relevant regulatory requirements for each scenario and correlates these with the appropriate ISO/IEC 27001 controls that mitigate associated risks. This approach not only facilitates a deeper understanding of compliance obligations but also highlights potential overlaps and redundancies in regulatory requirements.

Furthermore, by leveraging the updated classification from ISO/IEC 27002 [10], which categorizes controls as detective, preventive, or corrective, this paper assigns these classifications to legislative requirements. This additional layer of analysis aids organizations in recognizing the nature of their compliance activities, thereby enhancing their ability to design and implement an effective and efficient information security management system. The ISO/IEC 27002 provides guidance on every control and helps organizations to implement it. By understanding whether a control is intended to detect, prevent, or correct security risks (a classification that reflects if a control affects the impact or likelihood of the corresponding risk), organizations can better prioritize and allocate resources to their most critical security needs.

The results of this research demonstrate that the proposed framework not only meets the compliance requirements across different security domains but also provides a scalable approach to adapt to new threats and regulations efficiently. This scalability is necessary, considering the volume of existing regulations and the anticipation of future rules. These findings indicate a significant step forward in holistic security management, suggesting that organizations can enhance their security posture and legislative compliance simultaneously through the implementation of common security controls.

The ultimate goal of this research is to provide organizations with a clear and actionable framework for navigating EU security regulations. By understanding the synergies between legislative requirements and ISO/IEC 27001 controls, organizations can streamline their compliance efforts, reduce redundancy, and build a more resilient security posture. This comprehensive mapping and classification effort empowers organizations to not only meet regulatory demands but also to proactively manage and mitigate security risks in a systematic and strategic manner. In doing so, organizations can achieve a unified, efficient, and adaptable approach to information security management that keeps pace with evolving regulations and the increasing sophistication of cybersecurity threats.

The remainder of this article is structured as follows: Section 2 discusses relevant literature and other related works concerning different legislation. Section 3 outlines the methodology for the proposed information security management and compliance framework, comparing various security requirements, domains and controls. Section 4 presents an experimental analysis of five distinct use cases to assess the security risks addressed by a given legislation. Section 5 discusses the findings, and Section 6 summarizes key contributions and suggesting directions for future research.

2. Related Works

Implementing a cybersecurity framework is widely regarded as best practice, demonstrating an organization's commitment to fulfilling its responsibility to protect and secure

its assets. Nevertheless, in today's era of digital transformation, this by itself is no longer adequate. The rapidly evolving threat landscape requires customized and innovative solutions to prevent cyber-attacks and disruptions. Regulations play a crucial role in safeguarding sensitive information and defending against cyber threats, necessitating the implementation and maintenance of controls across various regulatory frameworks. Adhering to these standards is essential for mitigating risks and strengthening digital defenses. Organizations must remain well-informed of current regulations to effectively navigate the complex and constantly changing security environment, ensuring compliance. In recent years, researchers have assessed the cybersecurity landscape within the EU in response to the growing complexity of cyber threats and have conducted comparative studies on the interrelationships between existing regulatory frameworks. The research primarily focuses on an ontological framework designed to effectively identify essential security controls and meet legislative compliance requirements. This section seeks to explore these studies in depth, demonstrating how emerging cybersecurity regulations can be compared using generalized requirements and identifying potential overlaps and redundancies.

In 2018, the authors in [11] proposed a security ontology-based approach, integrated with a decision support system, designed to unify security concepts with standard frameworks and formalize information security features. This approach enhanced the checking process of information security by ensuring compliance with industrial management standards and ISO 27002 controls. Additionally, it facilitated the identification of the most effective strategies to mitigate risks to acceptable levels.

In 2019, Valentina Casola et al. [12] developed an ISO-based, dual-layer security domain ontology to support the management of standards and compliance-related documentation throughout the entire lifecycle of an Information Security Management System (ISMS). Their modeling approach consisted of a high-level ontology, grounded in the principles of Basic Formal Ontology (BFO), designed to classify overarching modeling concepts, and a low-level domain specific ontology aligned with the International Organization for Standardization (ISO) standards and their standardization processes.

In the same year, a comprehensive comparative study of six ontologies based on the ISO/IEC 27000 series security standards was detailed in [13]. Meriah et al. evaluated each ontology by identifying relevant security concepts, features of the ISO 27000 series, ontology methodologies used, integration with other security standards, and best practices. This analysis aimed to elucidate the structure of each ontology, highlighting their advantages and limitations, and offering recommendations to security decision-makers for selecting or developing an appropriate ontological framework based on their security needs. The study underscored the ongoing need for a unified security ontology that encompasses all pertinent security concepts, integrates multiple requirements from the ISO 27000 series, adheres to a well-defined methodology, and undergoes rigorous assessment and validation. The primary objective of ontology development is to comprehend the information structure of a specific domain and to share this understanding among users. Achieving this goal requires meticulous ontology design to ensure clarity, accurate comprehension, and effective utilization of domain knowledge.

Dmitrij Olifer et al. [14] conducted a comprehensive analysis highlighting the increasing regulatory pressures in the field of information security. They identified that applying multiple security standards can result in challenges such as duplicate or contradictory requirements, elevated costs, and monitoring difficulties. To mitigate these challenges, the authors suggested employing graph theory techniques to map and align key cybersecurity protocols, including Minimum Security Baselines. Their methods, incorporating ISO 27002, PCI DSS, and GDPR, demonstrate operational efficiency. Throughout their research, Dmitrij et al. meticulously concluded that this approach effectively eliminates redundant requirements and mitigates cybersecurity threats by processing graphs at each stage and integrating comparable elements to improve usability.

In 2020, Andrea Mussmann et al. [15] presented a comprehensive review of research focused on mapping security standards (e.g., ISO 27001, ISO 27002, ITIL, COBIT, NIST

SP800-53 [16], GDPR). They examined the methodologies developed for these mappings and discussed tool-assisted techniques, like mapping tables that aid in the process. The authors observed that mappings between standards are often partial, typically addressing only subsets of controls or general mappings. They also highlighted the challenge of accurately aligning standards with system security requirements. Emphasizing the need for full automation in this mapping process, they recommended that future research in security standard mappings should incorporate Natural Language Processing (NLP) techniques, presumably in conjunction with established security ontologies and manual comparison approaches.

Taherdoost [17] provided a narrative overview and comparative analysis of the most widely used cybersecurity standards and frameworks, examining their applications across various fields to protect data from cyber threats. His study aimed to assist decision-makers in selecting the most suitable cybersecurity standard or framework that best aligns with their specific security requirements. Although numerous cybersecurity frameworks integrate industry standards and best practices to help organizations manage cybersecurity risks, each has unique characteristics. Recognizing that no single standard may fully meet an organization's requirements, this review underscored the importance of adopting and combining multiple standards to safeguard sensitive data, strengthen digital defenses, and ensure the resilience of communication systems against cyber threats and data loss.

Djebbar F. and Nordstrom K. in [18] conducted a thorough overview of the widely recognized domain-specific cybersecurity standards: ETSI EN 303 645 v2.1.1, ISA/IEC 62443-3-3:2019 [19] and ISO/IEC 27001:2022—which provide a robust foundation for mitigating cybersecurity threats. These prominent standards were deliberately chosen from different domains of focus to underscore both substantial overlaps and gaps, despite their design for distinct environments and application contexts. The study pinpointed existing gaps and uncovered compliance challenges resulting from the considerable overlap in requirements and controls among the selected standards. The authors asserted that their findings could assist organizations and cybersecurity professionals in selecting the most appropriate standards to meet their security needs, while balancing effectiveness and cost-efficiency. Additionally, Djebbar F. et al. contended that their results could rationalize compliance efforts for organizations confronting the difficulty of complying with multiple standards concurrently. This optimization could save valuable resources, reduce redundancy, and foster their cybersecurity posture.

Wicklund Lindroth in [20] developed and introduced a cybersecurity ontology elucidating dependencies among vulnerabilities, standards and regulatory requirements. This ontology, which incorporates Common Weakness Enumerations (CWEs), two security and privacy standards, and selected articles from the GDPR, has the capacity to strengthen asset resilience and security strategies by delineating how specific controls address existing vulnerabilities while ensuring adherence to legal and regulatory mandates.

Agalit et al. [21] conducted a comprehensive evaluation of the ISO/IEC 27001 and NIST Cybersecurity Framework (CSF) standards, critically analyzing the policies and procedures outlined in these frameworks. The focus of their analysis was on identifying vulnerabilities that expose information systems to risks such as data theft, natural disasters, malware attacks, and, most notably, unintended factors like human error and natural calamities. Their key objective was to identify the most effective strategies for enhancing information security in Higher Education Institutions, particularly within the rapidly evolving landscape of information technology. The study's results indicated that ISO/IEC 27001, highly regarded as an information security standard, is adaptable to the specific needs of organizations. Furthermore, the NIST-CSF is identified as a robust framework designed to complement ISO/IEC 27001, offering Higher Education Institutions the flexibility to develop tailored cybersecurity strategies that meet their unique requirements.

In their work, Giampaolo Bella et al. [22] showcased an automated approach that advances ontology engineering and development to achieve an accurate representation of the NIS2 Directive, thereby facilitating automated compliance verification. The proposed method innovatively integrated specific NLP techniques for grammatical POS tagging

with precise modeling decisions for ontology construction. The development of the NIS 2 ontology adhered to a waterfall (Methontology) technique, following a structured sequence of refined and refocused stages—from specification and implementation to evaluation—resembling conventional software development processes. The study's findings indicated that cutting-edge NLP techniques encountered challenges in handling the complex legal language and intricate structure of the NIS2 directive. As a result, further research will be required to enhance automation, complete the target ontology, and finalize its accompanying documentation.

In our prior research [23], Sarunas Grigaliunas et al. introduced the Security Baseline framework for National Research and Education Networks (NRENs) and a consolidated security maturity model specifically tailored for research and education entities. This model was derived from established security best practices to meet the unique needs of NRENs, universities, and various research institutes. The authors identified and emphasized the lack of a unified mechanism in existing models to effectively align varying levels of requirements for different user groups or scenarios with a cohesive set of security standards and current regulations. This deficiency compromises the community's ability to achieve uniformity, compatibility, and comprehensive compliance with these standards and regulations. To address this critical issue, Sarunas Grigaliunas et al. developed taxonomies focused on a compliance framework that elucidates the correlations between different standards. The findings of this research suggest that, while adhering to multiple standards can provide more comprehensive coverage of security requirements, it should be carefully balanced with considerations of cost-effectiveness.

Giampaolo Bella et al. in [24] introduced an ontological approach for compliance verification and the conversion of security documents into a mathematically grounded framework. The developed ontology offers a representative model of the fundamental entities and relationships underlying the European Network and Information Security (NIS) 2 Directive, specifically concentrating on Articles 7 and 10. It adheres to the FAIR principles and is partially integrated with the 'Ontology for Agents, Systems, and Integration of Services' (OASIS). The authors assert that, in its current form, the ontology can assist cybersecurity analysts in rapidly verifying an institution's compliance status, thereby functioning as an efficient search engine for defense mechanisms.

Eleni-Maria Kalogeraki et al. [25] meticulously analyzed the interdependency and mapping between the EU legislative framework and international area-specific standards, thereby contributing to the alignment of standards efforts. The authors formulated a standards-driven cybersecurity taxonomy designed to help stakeholders in comprehending the purpose of each standard and making informed decisions regarding which standards to adopt to fulfill their organizational requirements. The proposed taxonomy was structured within a semantic ontology, employing the knowledge engineering methodology of Web Ontology Language Edition 2. Additionally, a practical use-case scenario was provided to demonstrate the taxonomy's effectiveness.

Daniele Granata et al. in [26] developed a tool that operates in a semi-automated fashion to aid in managing key phases of the compliance process related to GDPR implementation. Their research utilized the NIST SP-800-53 security control framework to assess GDPR compliance, establishing a correlation between GDPR articles and NIST SP-800-53 security controls. The effectiveness of this mapping and the proposed method were confirmed through their application in a real-world scenario using their university as a case study. According to the authors, this solution can be seamlessly applied across various contexts.

André Fernandes et al. in [27] carried out a Systematic Literature Review (SLR) to examine the impacts, difficulties and artifacts resulting from the alignment and consolidation of ISO/IEC family standards. The study focused on pinpoint the potential benefits and drawbacks associated with aligning and consolidating ISO/IEC standards, as well as to compile the various methods or techniques documented in the literature for implementing these procedures. The findings identified several issues, notably the difficulties associated

with repetitive mapping across standards, which arise from the absence of automation tools capable of balancing time-consuming processes with cost-effectiveness. Additionally, the study pointed out the difficulty of choosing between bi-directional mapping and broader coverage when mapping to ontologies. Another significant challenge identified was the difficulty of making future updates to the mapping, as the rationale behind each control's mapping is often not documented.

In their study, Giampaolo Bella et al. [28] presented SecOnto, a novel methodology designed for converting security directives into ontologies, thereby providing valuable insights to assist organizations in navigating the complexities of security regulations. This methodology is demonstrated through its application to the NIS 2 Directive. Built upon the Methontology framework, SecOnto disaggregates the task of converting the legal language of contemporary security regulations into detailed ontologies into five semi-automated steps: 'Preprocessing, Interpretation, Structuring, Representation, and Verification', each demonstrated with real-world scenarios. Additionally, the research provides an extensive elaboration of the ontological approach to compliance verification.

Previous studies have deepened our understanding of security framework adoption, particularly in aligning security controls and standards. However, a gap remains in optimizing compliance by mapping regulatory standards to cybersecurity frameworks. This can reduce redundancies, streamline processes, and strengthen defenses while improving implementation time, performance, and cost efficiency. The overlap among standards also simplifies the selection process. Thus, the proposed information security management and compliance framework meets compliance requirements across different security domains and adapts to evolving security regulations, offering a scalable and comprehensive solution for holistic security management.

3. Information Security Management and Compliance Methodology

A proposed information security management and compliance framework integrates operational (Figure 1), human (Figure 2), physical (Figure 3) and technical (Figure 4) security domains. This integration ensures exhaustive coverage of potential vulnerabilities for information security, allowing for a holistic approach to organizational security that addresses threats from multiple vectors. Such a unified strategy not only aligns policies, processes, and controls across various domains but also facilitates the identification and mitigation of security gaps potentially exploitable by attackers. This approach enhances risk management by incorporating diverse risk factors from each domain, including policy and procedural risks, IT system vulnerabilities, insider threats, and physical breaches. Furthermore, integrating security domains into a framework promotes efficient resource allocation, enabling organizations to balance security investments across all domains, thereby optimizing cost-effectiveness and resource utilization. It also ensures comprehensive compliance with regulatory requirements that often span several aspects of security, from technical safeguards to procedural and human factors. Improved incident response and recovery processes are another advantage, as a unified framework allows for coordinated actions in the event of security incidents that impact multiple domains.

In every security domain, the CIA triad, comprising confidentiality, integrity, and availability, is foundational for information security, encapsulating the primary objectives necessary for the design and implementation of security controls. It is important for security laws such as GDPR (Regulation (EU) 2016/679), Cybersecurity Act (Regulation (EU) 2019/881), NIS2 Directive, Artificial Intelligence Act (AI Act), Coordinated Plan on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, ISO/IEC 27001:2022, The Critical Entities Resilience Directive (CER), and Critical Security Controls (CIS) to focus on CIA principles because they are at the heart of keeping information safe.

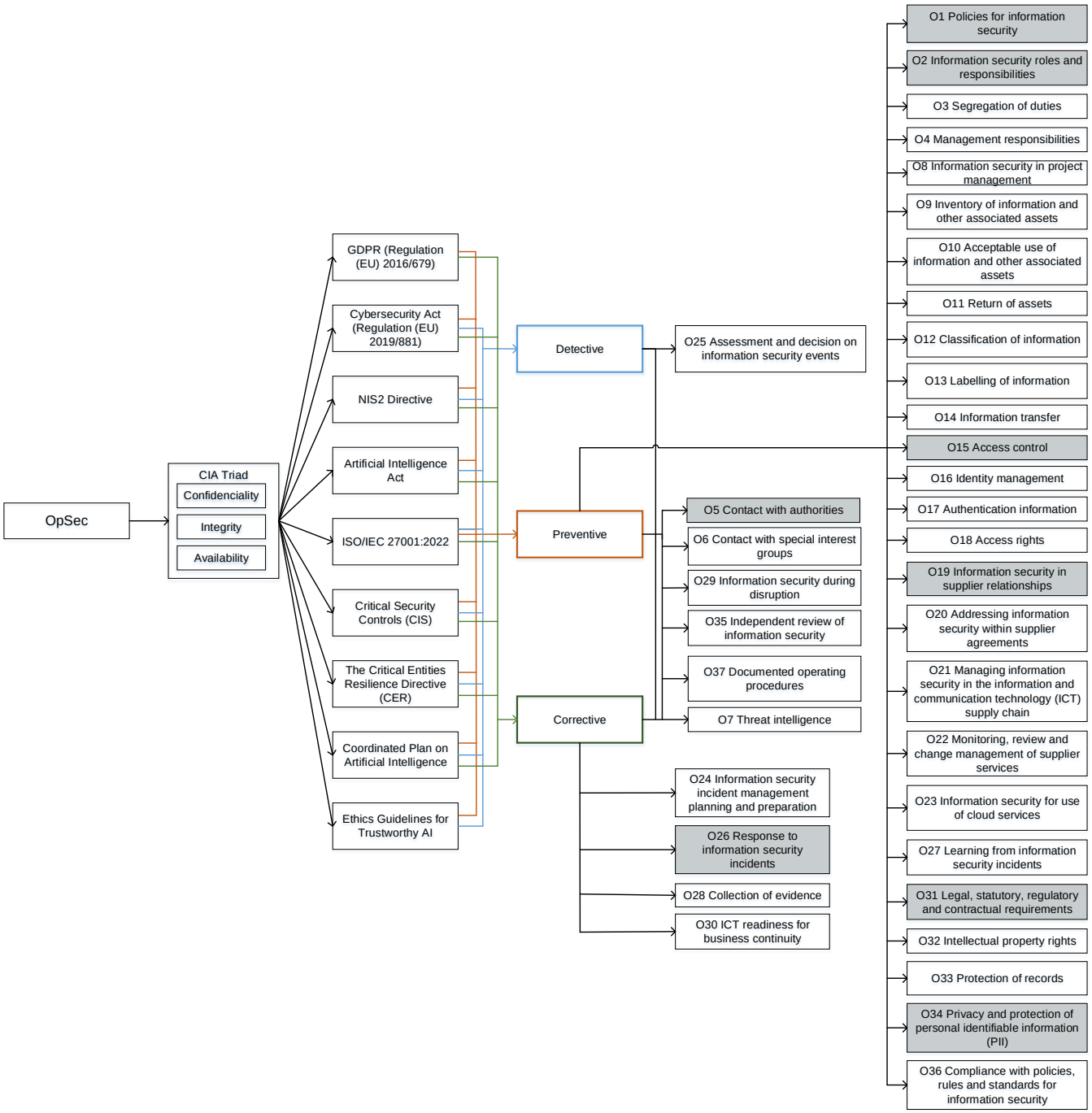

Figure 1. Ontology of security controls for the operational security domain.

These principles not only aid in building trust and ensuring compliance with legal frameworks but also enhance risk management strategies and operational resilience against disruptions caused by security breaches or data loss. Focusing on the CIA triad allows organizations to prioritize security efforts, allocate resources efficiently, and align with broader security governance and risk management approaches necessary in our increasingly interconnected digital landscape.

In every security domain, the correlation between legislative requirements and particular security controls from Annex A of ISO/IEC 27001 follows to the categorization of security measures based on their functional level, namely detection, prevention, and correction. The compliance of security legislation to the security measures is marked in dif-

ferent colors (see Figures 1–4): in blue—for detective measures, in orange—for preventive measures and in green—for corrective measures. Specifically, Figure 1 demonstrates that all legislation, with the exception of GDPR, complies to detective measures in the domain of operational security. These measures include security controls such as O7 "Threat intelligence" and O25 "Assessment and decision on information security events". However, the Ethics Guidelines for Trustworthy AI do not comply with the corrective measures in this domain. It is worth noting that these security controls that are required in the majority of the above-mentioned security legislation have been marked as priority controls in gray color in Figures 1–4. In this case, the security controls O1, O2, O15, O19, O31 and O34 are priorities as preventive measures, O26 as corrective measures, and O5 as both preventive and corrective measures for operational security (Figure 1).

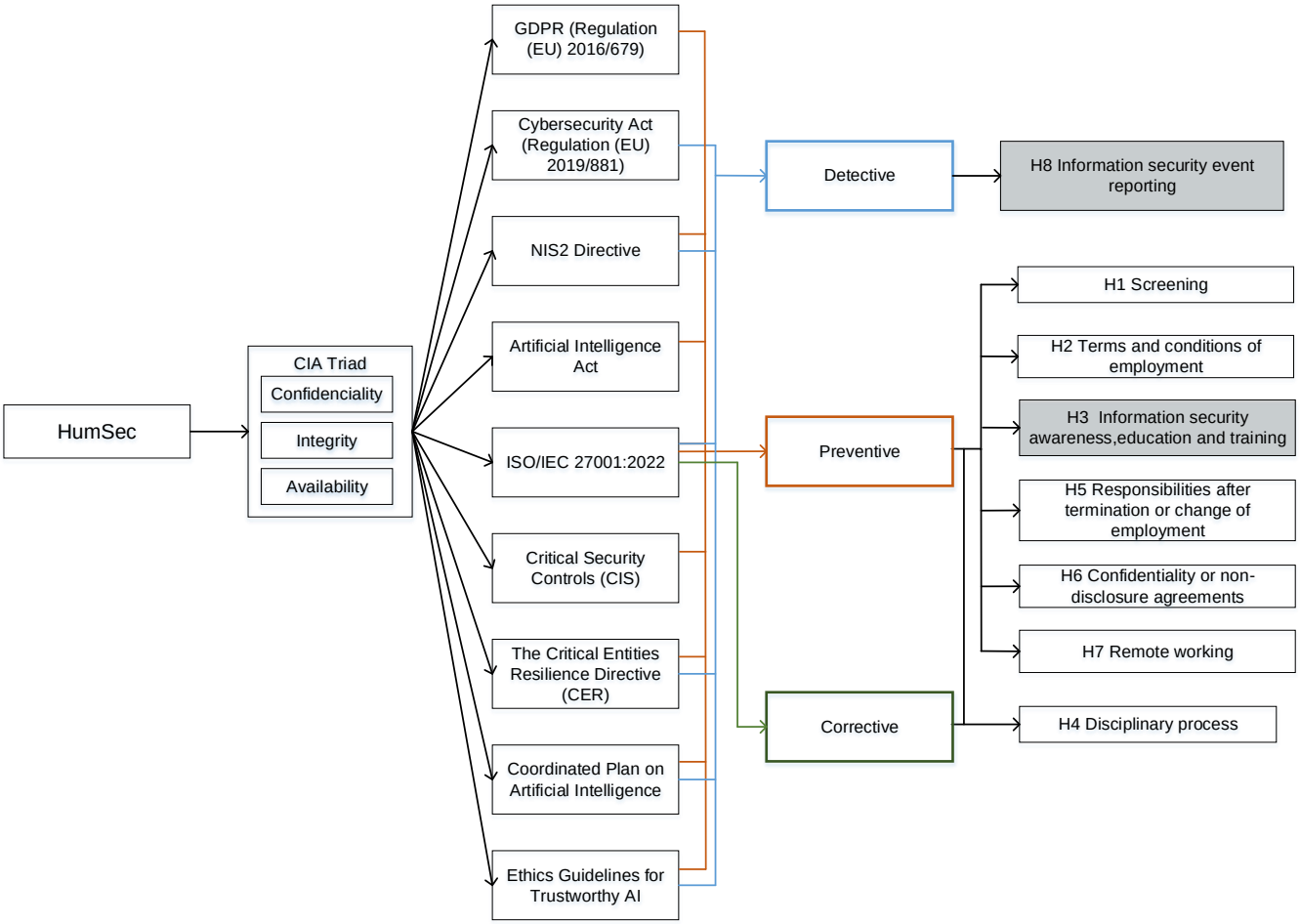

Figure 2. Ontology of security controls for the human security domain.

Only ISO/IEC 27001 complies with the corrective measures for human security (Figure 2). This is because ISO/IEC 27001 emphasizes corrective measures for human security to mitigate risks associated with human errors or actions by systematically addressing incidents through its process-based approach and continuous improvement principle. Information security awareness, education and training (H3) is recognized as priority in preventive measures and Information security event reporting (H8) as priority in detective measures for human security.

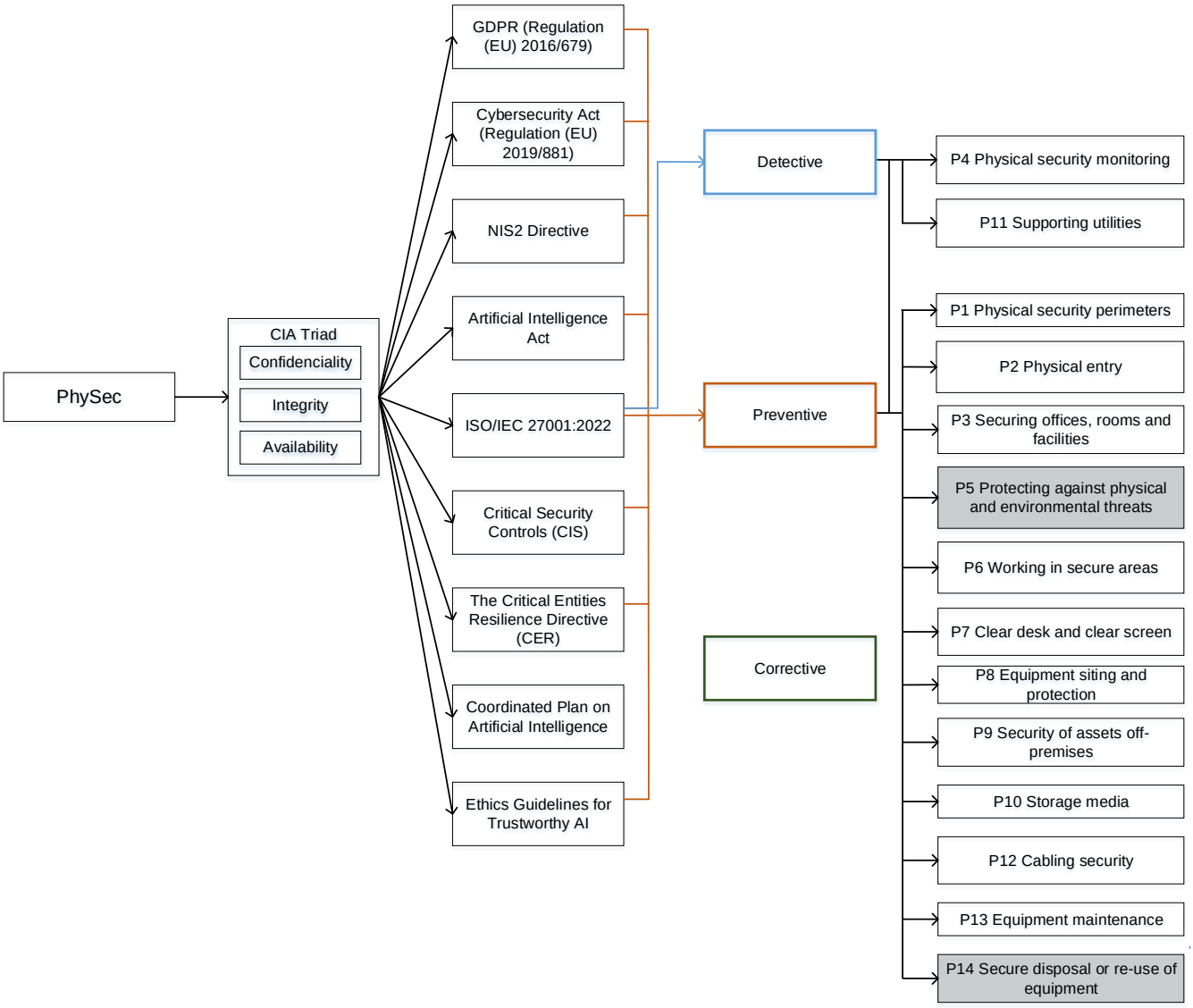

Figure 3. Ontology of security controls for the physical security domain.

It is important to mention that corrective measures for physical security are not included in any of the analyzed security legislation (Figure 3). The lack of explicit compliance with corrective measures for physical security in analyzed security legislation can be attributed to several reasons. Primarily, legislation tends to emphasize preventive measures such as protecting against physical and environmental threats (P5) or secure disposal or re-use of equipment (P14) and detective measures rather than corrective actions, focusing on deterring and detecting incidents before they occur. Physical security corrective measures are often reactive, dealing with the aftermath of a security breach, which might be considered less effective compared to proactive strategies. Moreover, the nature of physical threats frequently necessitates that specific corrective actions depend on the incident's circumstances, potentially falling under broader emergency response or continuity planning rather than specific security protocols. Security legislation generally focus on overarching principles and governance rather than delving into detailed, scenario-specific corrective actions. This leaves room for organizations to tailor corrective measures based on individual risk assessments and security needs. Occasionally, organizations integrate physical security measures with other security domains, and the general requirements for incident management in these broader areas may encompass corrective actions. Legislators

might also assume that organizations inherently implement corrective measures as part of their business continuity and disaster recovery plans, omitting specific mandates for these actions within the security legislation. This indicates a potential area for legislative enhancement to ensure more comprehensive security frameworks and robust response strategies.

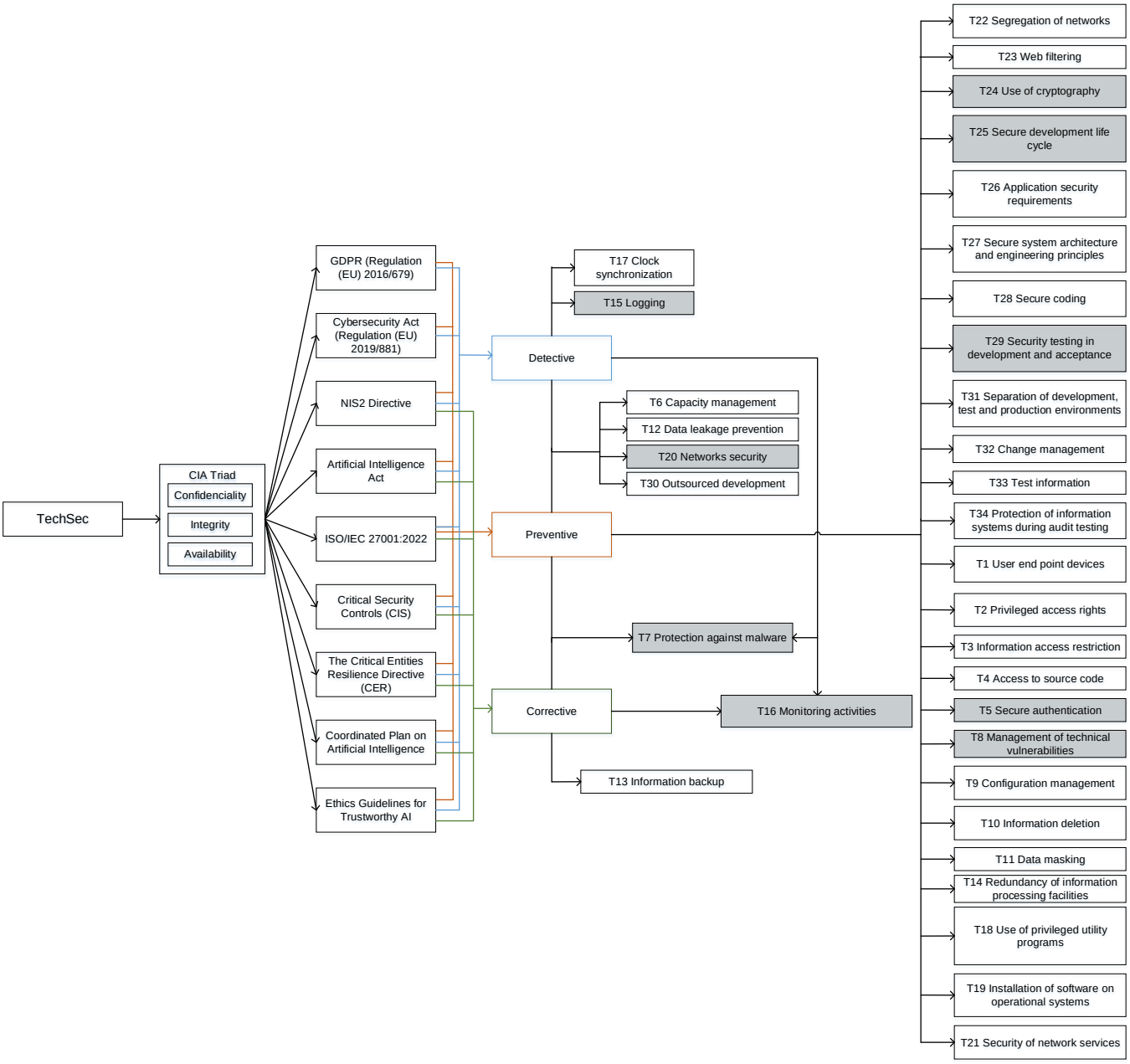

Figure 4. Ontology of security controls for the technical security domain.

In the technical security domain (Figure 4), certain security controls are emphasized across major security regulations due to their critical role in maintaining the integrity, confidentiality, and availability of information systems and in preventing, detecting, and responding to cyber threats.

Secure authentication (T5) is prioritized to ensure that system access is granted only to verified users, which is essential for preventing unauthorized access—a key provision in almost all data protection and cybersecurity regulations. Management of technical vulnerabilities (T8) is crucial for identifying and mitigating potential points of exploitation

in software and hardware, aligning with directives that call for robust security measures across essential services. The use of cryptography (T24), safeguards data integrity and confidentiality, fulfilling requirements from laws that mandate the protection of personal and sensitive data. T25, which focuses on integrating security practices within the software development life cycle, ensures that applications are built with inherent security measures, a principle increasingly required by regulations that emphasize privacy by design. Security testing in development and acceptance processes (T29), is vital for preemptively identifying and addressing security gaps, thereby enhancing the overall security posture of the developed solutions. Protection against malware (T7) spans preventive, detective, and corrective measures, reflecting its importance in safeguarding systems against malicious software—an essential aspect of comprehensive cybersecurity strategies.

Logging and monitoring activities, T15 and T16, respectively, play detective and corrective roles by recording system activities and enabling real-time security oversight, which is crucial for incident response and compliance with accountability and transparency requirements. Lastly, network security (T20) encompasses both preventive and detective functions, protecting the data transit routes to prevent and detect intrusions and breaches, which are critical for maintaining system operations and data integrity across networked environments.

The ontological mapping for the proposed information security management and compliance framework was developed collaboratively by the GÉANT community. GÉANT is a pan-European network that connects and supports research and education institutions across Europe, serving over 50 million users. The development process was led by experts from National Research and Education Networks (NRENs) who created the security baseline methodology [23], ensuring the framework addresses the specific needs of research and education networks. To reach consensus on the mapping, the team used a multi-stage approach similar to the Delphi method. They started with an initial draft based on their collective expertise, which was then reviewed by a wider group of GÉANT community members. The mapping underwent several rounds of revision based on feedback. The final version was put to a vote among NREN representatives. When compared to other frameworks in the field, this proposed framework shows both strengths and limitations. It provides more specific guidance for research and education networks than the NIST Cybersecurity Framework but may be less applicable across different industries. Compared to ISO 27001, it offers a more integrated approach to different security domains. This aligns well with European regulatory frameworks, giving it an advantage for EU-based institutions.

Figure 5 highlights how complex information security can be and how different aspects of security must be considered together through a comprehensive information security management and compliance framework. This framework, by integrating the OpSec, HumSec, TechSec, and PhySec domains, can be helpful in understanding the relationships between different security regulations and standards and developing a comprehensive security plan. The NIS2 Directive, ISO/IEC 27001:2022, and the Critical Entities Resilience Directive (CER) are identified as top legislation that emphasize a wide array of security controls across security domains to ensure the confidentiality, integrity, and availability of information. These directives focus on enhancing confidentiality, integrity, and availability by requiring to implement a suite of controls across various security domains, each addressing specific aspects of the CIA triad.

In the Operational security (OpSec) domain, controls like O1 (Policies for information security) and O31 (Legal, statutory, regulatory, and contractual requirements) ensure compliance with laws and protect the integrity and confidentiality of data through rigorous policy enforcement and adherence to legal standards. O15 (Access control) and O34 (Privacy and protection of personal identifiable information) directly safeguard confidentiality by limiting data access to authorized personnel and securing personal data. O19 (Information security in supplier relationships) extends these protections to third-party interactions, maintaining integrity across the supply chain. O26 (Response to information security

incidents) and O5 (Contact with authorities) enhance the availability and resilience of systems by ensuring rapid incident response and communication with regulatory bodies.

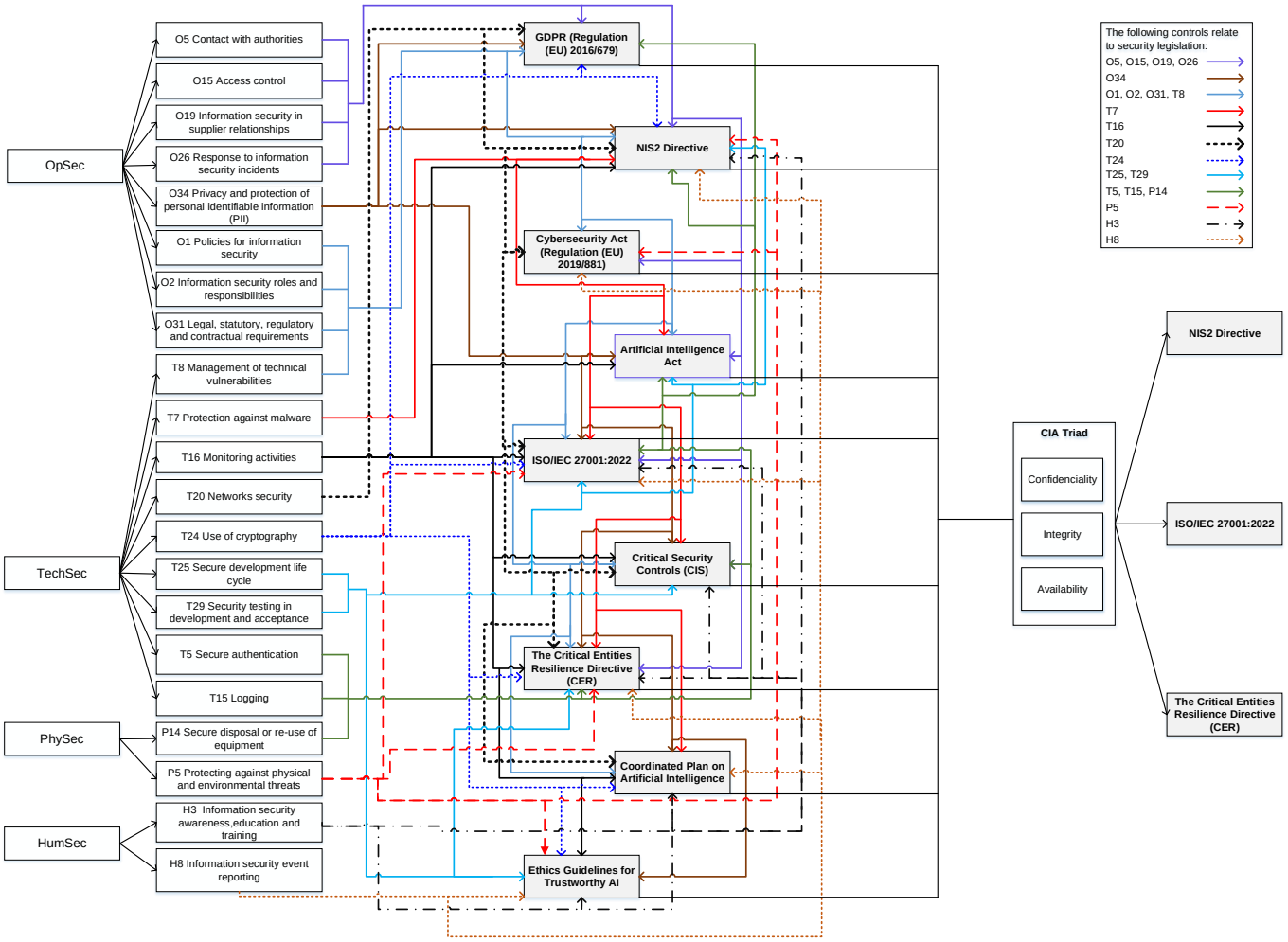

Figure 5. Ontology of security legislation covering mostly security controls over all security domains.

In the Human security (HumSec) domain, H3 (Information security awareness, education, and training) promotes an informed workforce capable of protecting integrity and confidentiality, while H8 (Information security event reporting) supports the availability of systems by fostering a responsive security incident handling environment.

Physical security (PhySec) measures such as P5 (Protecting against physical and environmental threats) and P14 (Secure disposal or re-use of equipment) are critical for maintaining the integrity and availability of physical assets and environments, ensuring that physical breaches do not compromise system operations or lead to data loss.

In the Technical security (TechSec) realm, T5 (Secure authentication) and T24 (Use of cryptography) directly protect confidentiality by ensuring that data is accessible only to authorized entities and is encrypted to prevent unauthorized disclosure. T7 (Protection against malware) and T8 (Management of technical vulnerabilities) uphold the integrity of systems by preventing malicious software and exploitation of vulnerabilities. T16 (Monitoring activities) and T20 (Networks security) are pivotal for maintaining both the integrity and availability by detecting and responding to threats in real-time, thus ensuring systems are operational and secure. T25 (Secure development life cycle) and T29 (Security testing in development and acceptance) reinforce all aspects of the CIA triad by embedding security into the development process, reducing the risk of vulnerabilities, and ensuring robust system performance.

By adhering to these comprehensive controls, these directives not only strengthen detective, protective and corrective measures but also ensure compliance with a wide range of regulatory requirements, thereby securing critical information and systems effectively. Adopting an integrated security framework can engender a cultural shift within the organization, embedding security awareness and practices into every operational layer, thereby fostering a shared responsibility for security among all employees. This cultural integration not only enhances the general security posture but also aligns with best practices for maintaining resilience and compliance in the face of evolving cyber threats.

4. An Experimental Analysis of Use Cases

The experimental evaluation of the proposed information security management and compliance framework was conducted across five distinct risk scenarios, as described in Table 1.

Table 1. Risk scenarios.

No.	Scenario	Description
1	An unauthorized person enters the premises of the Technical Centre	Unauthorized individuals breach the Technical Center's premises, sneaking past the security guards to reach the server room, home to the most crucial equipment. The person deliberately damages the servers, destroying critical equipment and stopping all services. This attack results in a complete disruption of the Technical Center's operations and services.
2	Cyberattack	The Technical Center network becomes the target of a DDoS attack by external cybercriminals. The attack intensity overwhelms the network resources, generating a massive volume of requests that surpasses the expected capacity. This makes the Technical Center's services unavailable externally, causing great frustration for users of email and other services.
3	Lack of disk capacity in the database	The Technical Center's email database suddenly stops working due to a lack of disk space, which disrupts the database's ability to process requests. This renders the core system of the Technical Center service non-functional, causing severe user disruption and disrupting daily operations.
4	Data leakage	A malicious employee with access to the email database downloads all the information containing confidential data and uploads it to the dark web, posing a serious threat to the Technical Center's security and reputation.
5	Erroneous IS update	The Technical Center's staff implements software updates, but errors occur in the system they manage, causing data incompatibility and service disruption, which negatively impacts the user experience.

These five risk scenarios correspond with actual instances and applications across many industries and contexts in real-world. Risk scenario no. 1 "An unauthorized person enters the premises of the Technical Centre", exemplify actual physical security violations that have transpired in data centers and critical infrastructure installations. In 2014, a physical breach occurred at a water company in the Chicago area, allowing intruders to access the control room [29]. Another illustrative instance is the 2020 event at Tesla's Gigafactory in Nevada [30]. A Russian citizen endeavored to illicitly infiltrate the facility to deploy software for a ransomware assault. Despite the plan's failure, it illustrates how physical breaches can result in significant cyber and operational hazards.

Risk scenario no. 2 "The Technical Center network becomes the target of a DDoS attack by external cybercriminals", highlights the prevalence and escalation of such threats in reality. Distributed Denial of Service (DDoS) assaults, which inundate a network with traffic to incapacitate it, are more prevalent. A notable incident was the 2016 DDoS assault

on Dyn, a DNS provider, resulting in extensive outages affecting platforms such as Twitter, Netflix, and Reddit [31].

Risk scenario no. 3 "The Technical Center's email database ceases functioning abruptly due to insufficient disk space" exemplifies a prevalent operational challenge that may result in service interruptions. Numerous firms, particularly cloud service providers, have encountered downtime because to storage complications. In 2017, GitLab saw a significant outage resulting from a database fault that was aggravated by inadequate storage space [32]. In 2022, Google Cloud suffered an outage due to inadequate storage space, impacting Gmail and other services [33].

Risk scenario no. 4 "A malicious employee with access to the email database downloads all the information containing confidential data and uploads it to the dark web" highlights an insider threats that pose a substantial risk to enterprises. An illustrative case is the 2019 Capital One data breach, in which a former employee leveraged misconfigured firewalls to gain unauthorized access to and exfiltrate customer data [34]. The 2018 Facebook-Cambridge Analytica controversy exemplifies the exploitation of Facebook data by a third-party researcher for personal benefit [35].

Risk scenario no. 5 "The Technical Center's staff implements software updates, but errors occur in the system they manage, causing data incompatibility and service disruption" illustrates the hazards linked to software updates and change management. In 2012 Knight Capital event a flawed software upgrade resulted in substantial financial losses [36]. In 2019, a software update to Cisco's Webex platform resulted in incompatibility concerns, causing service outages for several clients [37].

A matrix that identifies the compliance of specific security controls within specific risk scenarios is provided in Table 2. This method is a well-known approach while performing risk management and security assessments in an attempt to identify possible vulnerabilities and focus on the mitigation process.

To begin with, it is essential to clarify what the security control domains stand for:

- OpSec: policies, procedures, risk management;
- TechSec: network, systems, data protection;
- PhySec: physical access, physical environmental protection;
- HumSec: employee awareness, training, social engineering prevention.

For this matrix, five risk scenarios were used (Table 1). Multiple security controls may be applied to a single scenario, showing that a structured and layered separated approach is important. On the other hand, some controls are applicable only to specific scenarios, indicating that they are prone to sophisticated and targeted risks.

The positioning of security controls between OpSec, TechSec, PhySec and HumSec provides a better understanding of the specific risk types that an organization must address.

Moving next with the analysis, the first scenario approaches a vast range of risks, indicating a well-adjusted managed methodology to security; the second scenario focuses on information system/technical security, indicating that information systems and network-related vulnerabilities are the main concern. On the contrary, the third scenario focuses on technical security but has a narrow focus on operational and physical security. Human factors and social engineering are one of the most common and most easily exploitable vulnerabilities within an organization, and considering this, the fourth scenario has been prioritized in the aforementioned vulnerabilities.

The experimental methodology to validate the proposed information security management and compliance framework employed five distinct risk scenarios and for each of them the relevant security controls from the framework were identified and mapped across four security domains: Operational (OpSec), Technical (TechSec), Physical (PhySec), and Human (HumSec). These mapped controls were then cross-referenced with major security legislation and standards, including GDPR, NIS2 Directive, AI Act, ISO/IEC 27001:2022, and others. The security controls were further categorized as preventive, detective, or corrective measures, providing insight into their role in risk mitigation. Key controls that appeared consistently across multiple scenarios or were emphasized in mul-

tiple pieces of legislation were identified as priority controls. The mapping process also revealed areas where certain types of controls, such as corrective measures in physical security, were not explicitly covered by existing legislation, highlighting potential gaps in current security frameworks. The framework's effectiveness was assessed based on its ability to provide comprehensive coverage across all security domains for each scenario, and its alignment with relevant legislation. This methodological approach allowed for a systematic evaluation of the framework's applicability to diverse security challenges and its compliance with current regulatory requirements, demonstrating its potential as a holistic approach to information security management in the context of research and education networks.

Table 2. Compliance of security controls to risk scenarios.

Scenario	OpSec	TechSec	PhySec	HumSec
No. 1	O1,O2,O4,O5,O9, O15,O16,O17,O18, O24,O25,O26,O27, O28,O29, O30, O31, O35, O36, O37	T2,T3,T5,T15	P1,P2,P3,P4,P5, P6,P7,P8,P9,P10, P12,P14	H3,H8
No. 2	O1,O2,O4,O5,O6, O7,O14,O19,O20, O21,O22,O23,O24, O25,O26,O27,O29, O30,O31,O35,O36, O37	T1,T6,T7,T8, T14, T15,T16,T17,T20, T21,T22,T23	P5	H3,H8
No. 3	O1,O2,O4,O8,O9, O24,O25,O26, O27, O29, O30, O31, O35, O36, O37	T6,T9,T13,T14, T16,T26	P8,P10,P11,P13	H3,H8
No. 4	O1,O2,O3,O4,O5, O6,O7,O9,O10,O11, O12,O13,O14,O15, O16,O17,O18,O19, O20,O21,O22,O23, O24,O25,O26,O27, O28,O29,O30,O31, O32,O33,O34,O35, O36,O37	T2,T3,T5,T7, T8,T10,T11,T12, T15,T16,T17,T20, T23,T24		H1,H2,H3,H4, H5,H6,H7,H8
No. 5	O1,O2,O3,O4, O8,O10,O12,O13, O14,O19,O20,O21, O22,O23,O24,O25, O26,O27,O29,O30, O31,O35,O36,O37	T4,T8,T9,T13,T15, T16,T18,T19,T24, T25,T26,T27,T28, T29,T30,T31,T32, T33,T34		H3,H8

4.1. Mapping of Security Controls for Risk Scenario Unauthorised Access

In the first scenario, where unauthorized individuals breach a technical center and cause significant disruptions, a range of OpSec controls are crucial for addressing such an incident. According to Table 3, these OpSec controls are broadly supported by key legislations such as the NIS2 Directive, AI Act, ISO/IEC 27001:2022 and Critical Security Controls (CIS), all of which stress the need for a comprehensive, multi-layered approach to security management.

Key OpSec controls include the establishment of robust information security policies (O1), defining clear roles and responsibilities (O2), ensuring management's commitment to security (O4), and maintaining quick communication channels with authorities (O5). Controls like strict access management (O15) are essential to prevent unauthorized access to

sensitive areas, thereby potentially mitigating or entirely preventing the described scenario. In the event of a breach, having an effective response mechanism (O26) and maintaining operations during disruptions (O29) are critical. Ensuring ICT readiness for business continuity (O30) and adhering to legal, statutory, regulatory, and contractual requirements (O31) also play pivotal roles in rapid recovery and compliance adherence during such security incidents.

These controls, supported by the mentioned legislations, enable organizations not only to prevent such incidents through stringent access controls and robust policy frameworks but also to react appropriately when they occur, ensuring minimal damage and quick recovery.

Table 3. OpSec controls for risk scenario No. 1 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
O1	x	x	x	x	x		x	x	x
O2	x	x	x	x	x		x	x	x
O4			x	x			x	x	x
O5	x	x	x	x			x	x	x
O9				x			x		x
O15	x	x	x	x			x	x	x
O16	x			x			x		x
O17	x			x			x		x
O18	x		x	x			x		x
O24		x	x	x			x	x	x
O25				x			x		x
O26	x	x	x	x			x	x	x
O27			x	x			x		x
O28			x	x			x		x
O29		x	x	x			x	x	x
O30			x				x	x	
O31	x	x	x	x	x		x	x	x
O35			x				x	x	
O36	x		x	x			x	x	x
O37			x	x			x	x	x

AI Act, ISO/IEC 27001:2022 and CIS cover majority of specific TechSec controls (see Table 4) that are crucial in this context. This includes T2 (Privileged Access Rights), which ensures that only authorized personnel have special access privileges, reducing the risk of unauthorized actions that could be harmful. T3 (Information Access Restriction) complements this by limiting access to information based on roles and responsibilities, thereby tightening security measures around sensitive data. T5 (Secure Authentication) is fundamental in verifying the identities of those attempting to access the system, ensuring that only authorized users can gain entry. Finally, T15 (Logging) is instrumental in recording activities, which not only aids in real-time monitoring but also provides a critical forensic tool to investigate and understand the sequence of events during and after the security incident.

Table 4. TechSec controls for risk scenario No. 1 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
T2			x	x			x	x	x
T3				x			x		x
T5	x		x	x			x	x	x
T15	x		x	x			x	x	x

Physical Security (PhySec) controls are critical in mitigating risks and preventing such incidents, with substantial backing from major legislations like NIS2, ISO/IEC 27001:2022, and the Critical Entities Resilience Directive (CER) (Table 5). These controls collectively establish a secure physical environment that safeguards the facility and the sensitive information it houses. Key measures include establishing secure perimeters (P1) to deter unauthorized entry and managing physical entries (P2) with secured doors and manned areas. Additionally, securing critical rooms and facilities (P3) with access controls, and monitoring these measures through surveillance and alarm systems (P4), helps in effectively detecting and responding to intrusions.

Table 5. PhySec controls for risk scenario No. 1 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
P1			x				x	x	
P2							x		
P3			x				x	x	
P4							x		
P5		x	x			x	x	x	
P6							x		
P7							x		
P8			x				x	x	
P9							x		
P10							x		
P12			x				x	x	
P14	x		x	x			x	x	x

Protecting against physical and environmental threats (P5) is crucial for safeguarding hardware and maintaining data integrity, while policies like clear desk and clear screen (P7) minimize the risk of information exposure. Securing off-premises assets (P9) ensures data protection outside the facility, and strategic equipment positioning and protection (P8) safeguard against tampering or theft. Furthermore, securing storage media (P10) through encryption, managing cabling systems (P12) to prevent physical network breaches, and ensuring secure disposal or reuse of equipment (P14) prevent data leakage from decommissioned devices.

HumSec controls such as H3 (Information security awareness, education, and training) and H8 (Information security event reporting) are instrumental in enhancing the security posture in the first scenario (Table 6). These controls are robustly supported by legislations like the NIS2 Directive, Ethics Guidelines for Trustworthy AI, ISO/IEC 27001:2022, and the Critical Entities Resilience Directive (CER).

Table 6. HumSec controls for risk scenario No. 1 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
H3			x		x	x	x	x	x
H8		x	x		x	x	x	x	

4.2. Mapping of Security Controls for Risk Scenario Cyberattack

Table 7 maps OpSec controls to major legislation such as the NIS2 Directive, ISO/IEC 27001:2022 and the Critical Entities Resilience Directive (CER), demonstrating their relevance in managing a DDoS attack scenario where the Technical Center's network is overwhelmed, causing service disruptions. These OpSec controls are critical for both mitigating the immediate impacts of the attack and strengthening long-term security strategies.

Table 7. OpSec controls for risk scenario No. 2 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
O1	x	x	x	x	x		x	x	x
O2	x	x	x	x	x		x	x	x
O4			x	x			x	x	x
O5	x	x	x	x			x	x	x
O6		x	x				x	x	
O7		x	x		x		x	x	
O14			x				x		
O19	x	x	x	x			x	x	x
O20	x			x			x		x
O21		x	x	x			x	x	x
O22			x	x			x	x	x
O23			x				x		
O24		x	x	x			x	x	x
O25				x			x		x
O26	x	x	x	x			x	x	x
O27			x	x			x		x
O29		x	x	x			x	x	x
O30			x				x	x	
O31	x	x	x	x	x		x	x	x
O35			x				x	x	
O36	x		x	x			x	x	x
O37			x	x			x	x	x

For instance, controls like O1 (Policies for Information Security) and O37 (Documented Operating Procedures) ensure that there are robust protocols and clear roles defined for responding to such incidents. O2 (Information Security Roles and Responsibilities) and O4 (Management Responsibilities) assign and clarify responsibilities during the attack, ensuring a coordinated and swift response. Controls like O24 (Information Security Incident Management Planning and Preparation) and O26 (Response to Information Security Incidents) facilitate a prepared and effective response mechanism specifically tailored for DDoS scenarios.

Further enhancing response and resilience, O29 (Information Security During Disruption) and O30 (ICT Readiness for Business Continuity) ensure operational continuity through redundant systems and alternative processing capabilities. Communications controls like O5 (Contact with Authorities) and O6 (Contact with Special Interest Groups) enable effective coordination and support from external bodies, enhancing the ability to mitigate and analyze the attack.

Additionally, O7 (Threat Intelligence) provides insights into potential threats, aiding in proactive defenses against DDoS attacks, while O19 (Information Security in Supplier Relationships) and O20 (Addressing Information Security within Supplier Agreements) secure commitments from network and security service providers to uphold robust defenses during such incidents. Post-incident controls like O25 (Assessment and Decision on Information Security Events) and O27 (Learning from Information Security Incidents) are crucial for evaluating the attack response and integrating lessons learned into future security measures. Compliance and review controls like O31 (Legal, Statutory, Regulatory, and Contractual Requirements) and O35 (Independent Review of Information Security) ensure the organization adheres to legal obligations and benefits from external expertise in strengthening its security framework.

TechSec controls, where the Technical Center's network is targeted by a DDoS attack, broadly covered by major legislations such as the NIS2 Directive, ISO/IEC 27001:2022, and CER ensure a resilient and responsive strategy to defend against and recover from such disruptive cyber events (Table 8).

Table 8. TechSec controls for risk scenario No. 2 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
T1			x				x	x	x
T6							x		
T7			x	x	x		x	x	x
T8	x	x	x	x	x		x	x	x
T14			x				x	x	
T15	x		x	x			x	x	x
T16			x	x	x	x	x	x	x
T17							x		
T20	x	x	x		x		x	x	x
T21			x				x	x	
T22			x				x	x	
T23							x		

T6 Capacity Management is pivotal in ensuring that network resources can handle unexpected surges in demand, like those from a DDoS attack, by scaling and balancing the load to maintain service availability. T20 Networks Security and T21 Security of Network Services work together to protect network integrity by implementing strong firewalls, intrusion detection systems, and other protective measures that block malicious traffic and attacks. T22 Segregation of Networks helps isolate critical network segments from each other, preventing the spread of attacks within the network, while T23 Web Filtering can prevent malicious traffic from entering the network. T7 Protection Against Malware and T8 Management of Technical Vulnerabilities are essential to guard against the malware that might be introduced during a DDoS attack and to patch any security vulnerabilities that could be exploited. T14 Redundancy of Information Processing Facilities ensures that there are backup systems in place, which can take over if the primary systems are compromised, thus maintaining service continuity. T15 Logging and T16 Monitoring Activities are vital for detecting the onset of an attack and for ongoing surveillance of network behavior, enabling rapid response to anomalies. T17 Clock Synchronization ensures that all system logs from different network devices are consistent and accurate, which is critical for effective incident analysis and response. T1 User End Point Devices also plays a role by securing entry points into the network, ensuring that devices connected to the network do not become unwitting conduits for the attack.

In this scenario, the primary threat targets the network's infrastructure and the Protecting against physical and environmental threats (P5) remains essential (Table 9).

Table 9. PhySec controls for risk scenario No. 2 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
P5		x	x				x	x	

This control secures the physical hardware—such as servers, routers, and switches—that supports network operations. These components could be at risk of overheating or power supply issues due to the intense volume of requests characteristic of a DDoS attack. Maintaining optimal environmental conditions within data centers, including controlled temperature and humidity levels, is vital to prevent hardware malfunction or failure during such high-stress periods. Additionally, ensuring the physical integrity of these critical devices is crucial for the continuity of operations and quick recovery post-attack. Physical security measures protect the infrastructure from environmental hazards like fire or flooding, which could further complicate recovery efforts if the hardware is damaged. Thus, while the attack is digitally

oriented, maintaining the resilience of the physical infrastructure is an indispensable part of the overall defense strategy.

In this scenario, HumSec controls (Table 10) such as H3 (Information security awareness, education, and training) and H8 (Information security event reporting) helps in managing the situation. These controls are widely recognized and supported by major legislation, ensuring that they form an essential part of the security framework for organizations facing cyber threats. H3 (Information security awareness, education, and training) equips employees with the necessary knowledge and skills to recognize signs of a DDoS attack early, understand the potential risks, and respond appropriately. By fostering a culture of security awareness, this control helps minimize the impact of the attack through quick detection and informed decision-making by the staff who monitor network traffic and system alerts. H8 (Information security event reporting) ensures that once a potential security incident like a DDoS attack is detected, it is promptly reported according to established procedures. This allows for a swift organizational response, leveraging predefined escalation paths to mobilize specialized response teams and implement mitigation strategies. Effective reporting helps in documenting the attack patterns and outcomes, which are crucial for post-event analysis and strengthening future defenses.

Table 10. HumSec controls for risk scenario No. 2 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
H3			x		x	x	x	x	x
H8		x	x		x	x	x	x	

4.3. Mapping of Security Controls for Risk Scenario Lack of Disk Capacity in the Database

In the third scenario where the Technical Center's email database suddenly stops functioning due to a lack of disk space, OpSec controls predominantly are mostly supported by the AI Act, ISO/IEC 27001:2022, and Critical Security Controls (CIS), and form an integral part of the response and recovery framework (Table 11). O1 (Policies for Information Security) and O37 (Documented Operating Procedures) establish the foundational guidelines and procedures for managing IT resources, including the maintenance and monitoring of disk space to prevent such incidents. O2 (Information Security Roles and Responsibilities) and O4 (Management Responsibilities) delineate the accountability and responsibilities within the organization to ensure swift action and decision-making in response to operational disruptions. O9 (Inventory of Information and Other Associated Assets) helps in tracking resource usage and capacity planning, which is crucial in preventing system overloads that lead to failures. O8 (Information Security in Project Management) ensures that all projects, including system upgrades or expansions, consider security implications and resource requirements, potentially avoiding scenarios of inadequate resource allocation.

During the incident, O24 (Information Security Incident Management Planning and Preparation), O26 (Response to Information Security Incidents), and O25 (Assessment and Decision on Information Security Events) ensure that there are predefined plans and processes in place for an immediate and effective response. These controls facilitate quick recovery actions such as freeing up disk space or switching to backup systems to restore functionality. O27 (Learning from Information Security Incidents) and O29 (Information Security During Disruption) are vital for analyzing the incident to improve future response strategies and maintaining essential services during disruptions, respectively. O30 (ICT Readiness for Business Continuity) ensures that there are backup systems and fail-safes that keep critical services running even when primary systems fail. Lastly, O31 (Legal, Statutory, Regulatory, and Contractual Requirements) and O35 (Independent Review of Information Security) provide a framework for compliance with legal standards and for conducting audits that could prevent future occurrences by identifying underlying issues.

Table 11. OpSec controls for risk scenario No. 3 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
O1	x	x	x	x	x		x	x	x
O2	x	x	x	x	x		x	x	x
O4			x	x			x	x	x
O8				x			x		x
O9				x			x		x
O24		x	x	x			x	x	x
O25				x			x		x
O26	x	x	x	x			x	x	x
O27			x	x			x		x
O29		x	x	x			x	x	x
O30			x				x	x	
O31	x	x	x	x	x		x	x	x
O35			x				x	x	
O36	x		x	x			x	x	x
O37			x	x			x	x	x

TechSec controls (Table 12), widely supported by the NIS2 Directive, ISO/IEC 27001:2022, and the Critical Entities Resilience Directive (CER), provide a robust framework for managing technical resources and ensuring system reliability.

Table 12. TechSec controls for risk scenario No. 3 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
T6							x		
T9			x	x			x	x	x
T13			x				x	x	
T14			x				x	x	
T16			x	x	x	x	x	x	x
T26			x				x	x	

T6 (Capacity Management) is essential in this context as it involves the proactive management of system resources to ensure sufficient disk space and processing power to handle demand without service degradation. T9 (Configuration Management) plays a pivotal role in maintaining system settings optimized for efficient space usage and in preventing misconfigurations that could lead to space shortages. T13 (Information Backup) ensures that data is regularly backed up, allowing for quick restoration in case of system failure. This is critical in minimizing downtime and data loss during disruptions. T14 (Redundancy of Information Processing Facilities) provides additional assurance by duplicating critical components of the IT infrastructure, ensuring that if one system fails due to disk space issues or other faults, another can seamlessly take over. T16 (Monitoring Activities) is vital for the early detection of potential capacity issues before they escalate into critical failures. Continuous monitoring can trigger alerts when disk space thresholds are approached, allowing IT staff to intervene timely. T26 (Application Security Requirements), while generally focused on protecting applications from malicious attacks, also includes best practices for managing application data storage and resource allocation efficiently.

PhySec controls (see Table 13), predominantly supported only by the ISO/IEC 27001:2022 standard, address the physical aspects of IT infrastructure that can indirectly impact system performance and reliability.

Table 13. PhySec controls for risk scenario No. 3 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
P8			x				x	x	
P10							x		
P11							x		
P13							x		

P8 (Equipment Siting and Protection) ensures that servers and other essential IT infrastructure are located in optimal parts of the facility, where environmental factors such as overheating or accidental damage can be minimized. This control directly addresses potential risks that may aggravate disk space shortages by preventing physical threats like heat or environmental hazards that might otherwise worsen system performance. P10 (Storage Media) relates directly to the management of physical devices where data is stored. Ensuring that storage media is adequately handled, used, and maintained can prevent data loss and improve system efficiency, which is crucial when disk space is a limiting factor. P11 (Supporting Utilities), such as power supplies and HVAC systems, play a critical role in maintaining the operational integrity of data centers. Proper management of these utilities ensures that the physical environment remains conducive to optimal server performance, which can help mitigate issues arising from overloaded systems. P13 (Equipment Maintenance) is vital for ensuring that all physical components of the IT infrastructure are in good working order. Regular maintenance can help identify and rectify issues such as failing hard drives or other hardware problems that could lead to or exacerbate system capacity issues.

HumSec controls (Table 14) such as H3 (Information Security Awareness, Education, and Training) and H8 (Information Security Event Reporting), supported by the majority of security legislation, help mitigate the impact and improve the response to such incidents as provided in the third scenario.

Table 14. HumSec controls for risk scenario No. 3 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
H3			x		x	x	x	x	x
H8		x	x		x	x	x	x	

4.4. Mapping of Security Controls for Risk Scenario Data Leakage

In the scenario where a malicious employee compromises the Technical Center by leaking confidential data from the email database to the dark web, a comprehensive suite of operational security controls (Table 15) are well-supported by major legislation such as the NIS2 Directive, AI Act, ISO/IEC 27001:2022, and Critical Security Controls (CIS).

O1 (Policies for Information Security) and O37 (Documented Operating Procedures) establish foundational guidelines for handling sensitive information and outline procedures that restrict unauthorized data access. O2 (Information Security Roles and Responsibilities) and O4 (Management Responsibilities) ensure that responsibilities are clearly defined within the organization, which is crucial for maintaining stringent security practices and oversight.

O3 (Segregation of Duties) helps prevent any single individual from having control over critical processes that could lead to data breaches, while O15 (Access Control), O16 (Identity Management), O17 (Authentication Information), and O18 (Access Rights) ensure that only authorized personnel have access to sensitive information, with mechanisms to authenticate and manage user identities effectively.

O14 (Information Transfer) controls secure methods of data transmission both internally and externally. O12 (Classification of Information), O13 (Labelling of Information), and O34 (Privacy and Protection of Personal Identifiable Information) ensure data is appropriately categorized and protected according to its sensitivity, minimizing the risk of unauthorized disclosure.

O24 (Information Security Incident Management Planning and Preparation), O25 (Assessment and Decision on Information Security Events), and O26 (Response to Information Security Incidents) are critical in the immediate aftermath of a breach, enabling swift action to mitigate impact. O27 (Learning from Information Security Incidents) and O28 (Collection of Evidence) facilitate post-incident analysis and help in fortifying security measures based on learned insights.

Further supporting controls like O5 (Contact with Authorities) and O6 (Contact with Special Interest Groups) ensure the organization can reach out for external support and stay informed about emerging threats through O7 (Threat Intelligence). O19 (Information Security in Supplier Relationships) and O20 (Addressing Information Security within Supplier Agreements) protect against third-party risks, extending security protocols outside the organization.

Table 15. OpSec controls for risk scenario No. 4 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
O1	x	x	x	x	x		x	x	x
O2	x	x	x	x	x		x	x	x
O3							x		
O4			x	x			x	x	x
O5	x	x	x	x			x	x	x
O6		x	x				x	x	
O7		x	x		x		x	x	
O9				x			x		x
O10							x		
O11							x		
O12				x			x		x
O13				x			x		x
O14			x				x		
O15	x	x	x	x			x	x	x
O16	x			x			x		x
O17	x			x			x		x
O18	x		x	x			x		x
O19	x	x	x	x			x	x	x
O20	x			x			x		x
O21		x	x	x			x	x	x
O22			x	x			x	x	x
O23			x				x		
O24		x	x	x			x	x	x
O25				x			x		x
O26	x	x	x	x			x	x	x
O27			x	x			x		x
O28			x	x			x		x
O29		x	x	x			x	x	x
O30			x				x	x	
O31	x	x	x	x	x		x	x	x
O32			x	x	x		x	x	
O33	x		x	x			x	x	x
O34	x		x	x	x	x	x	x	x
O35			x				x	x	
O36	x		x	x			x	x	x
O37		x	x	x			x	x	x

TechSec controls (Table 16), supported by legislation such as the NIS2 Directive, ISO/IEC 27001:2022, Critical Entities Resilience Directive (CER), and Critical Security Controls (CIS), offer a robust framework for safeguarding sensitive information and maintaining the security integrity of the Technical Center.

T2 (Privileged Access Rights) and T3 (Information Access Restriction) ensure that only authorized personnel with necessary privileges can access sensitive data, reducing the risk of internal threats. T5 (Secure Authentication) is crucial to verify the identity of users accessing the system, preventing unauthorized access through strong authentication mechanisms. T7 (Protection Against Malware) and T8 (Management of Technical Vulnerabilities) protect the system from malicious software and exploits that could be used to facilitate data theft. T10 (Information Deletion) and T11 (Data Masking) are essential for properly disposing of or anonymizing sensitive information, ensuring that once data is no longer needed, it does not pose a risk if accessed improperly. T12 (Data Leakage Prevention) programs help monitor and block unauthorized attempts to extract data, which is crucial in preventing incidents like the one described. T15 (Logging) and T16 (Monitoring Activities) provide a detailed record of system activities and real-time surveillance of security events, enabling rapid detection and response to potential breaches. T17 (Clock Synchronization) ensures that all system logs from different network devices are consistent and precise, aiding in accurate incident analysis and response. T20 (Networks Security), along with T23 (Web Filtering), secure the network against unauthorized data transmission and block malicious traffic. T24 (Use of Cryptography) plays a pivotal role in securing data both at rest and in transit, ensuring that even if data is intercepted, it remains unreadable to unauthorized users.

Table 16. TechSec controls for risk scenario No. 4 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
T2			x	x			x	x	x
T3				x			x		x
T5	x		x	x			x	x	x
T7			x	x	x		x	x	x
T8	x	x	x	x	x		x	x	x
T10	x			x			x		x
T11							x		
T12	x		x				x	x	
T15	x		x	x			x	x	x
T16			x	x	x	x	x	x	x
T17							x		
T20	x	x	x		x		x	x	x
T23							x		
T24	x		x		x	x	x	x	

If a malicious employee accesses and leaks confidential data from the email database, PhySec controls, while important in broader contexts, are less pertinent compared to HumSec controls (Table 17). The focus here shifts significantly towards HumSec controls, particularly given the nature of the threat involving internal actions and data handling practices. These controls, comprehensively covered by ISO/IEC 27001:2022, are crucial for mitigating risks posed by internal threats and ensuring the integrity and confidentiality of sensitive information.

Table 17. HumSec controls for risk scenario No. 4 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
H1							x		
H2	x						x		
H3			x		x	x	x	x	x
H4							x		
H5	x						x		
H6				x			x		x
H7							x		
H8		x	x		x	x	x	x	

4.5. Mapping of Security Controls for Risk Scenario Erroneous IS Update

In the scenario where the Technical Center's staff encounters issues with software updates leading to data incompatibility and service disruptions, a broad array of OpSec controls are extensively covered by the NIS2 Directive, AI Act, ISO/IEC 27001:2022, and Critical Security Controls (CIS) (see Table 18).

Table 18. OpSec controls for risk scenario No. 5 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
O1	x	x	x	x	x		x	x	x
O2	x	x	x	x	x		x	x	x
O3							x		
O4			x	x			x	x	x
O8				x			x		x
O10							x		
O12				x			x		x
O13				x			x		x
O14			x				x		
O15	x	x	x	x			x	x	x
O19	x	x	x	x			x	x	x
O20	x			x			x		x
O21		x	x	x			x	x	x
O22			x	x			x	x	x
O23			x				x		
O24		x	x	x			x	x	x
O25				x			x		x
O26	x	x	x	x			x	x	x
O27			x	x			x		x
O29		x	x	x			x	x	x
O30			x				x	x	
O31	x	x	x	x	x		x	x	x
O35			x				x	x	
O36	x		x	x			x	x	x
O37			x	x			x	x	x

O1 (Policies for Information Security) and O37 (Documented Operating Procedures) establish the foundational guidelines and protocols for managing software updates securely. O2 (Information Security Roles and Responsibilities) and O4 (Management Responsibilities) ensure clear assignment of duties related to update processes, emphasizing accountability and oversight. O3 (Segregation of Duties) helps prevent conflicts of interest and reduces risks by dividing responsibilities among different individuals or teams, particularly in the testing and deployment phases of software updates. O8 (Information Security in Project Management) integrates security considerations into project management practices, ensuring updates are implemented without compromising system security. O10 (Acceptable

Use of Information and Other Associated Assets) and O14 (Information Transfer) govern how data and software are handled during updates, minimizing the risk of errors and data breaches. O12 (Classification of Information) and O13 (Labelling of Information) ensure data is accurately categorized and labeled, reducing the likelihood of incompatibility issues during updates. O19 (Information Security in Supplier Relationships), O20 (Addressing Information Security Within Supplier Agreements), and O21 (Managing Information Security in the ICT Supply Chain) ensure that all third-party software or updates comply with organizational security standards, while O22 (Monitoring, Review, and Change Management of Supplier Services) and O23 (Information Security for Use of Cloud Services) provide oversight and management of external services involved in the update process.

When issues arise, O24 (Information Security Incident Management Planning and Preparation), O25 (Assessment and Decision on Information Security Events), and O26 (Response to Information Security Incidents) enable quick and effective responses to minimize disruptions. O27 (Learning from Information Security Incidents) ensures that lessons are drawn from each incident to improve future update procedures. O29 (Information Security During Disruption), O30 (ICT Readiness for Business Continuity), and O31 (Legal, Statutory, Regulatory, and Contractual Requirements) ensure that even during disruptions, the organization remains operationally resilient and compliant with all necessary regulations.

Technical security controls are broadly supported by the NIS2 Directive, ISO/IEC 27001:2022, and the Critical Entities Resilience Directive (CER), provide a comprehensive framework for effectively managing updates and minimizing their impact on system functionality and user experience (Table 19).

Table 19. TechSec controls for risk scenario No. 5 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
T4				x			x		x
T8	x	x	x	x	x		x	x	x
T9			x	x			x	x	x
T13			x				x	x	
T15	x		x	x			x	x	x
T16			x	x	x	x	x	x	x
T18							x		
T19							x		
T24	x		x		x	x	x	x	
T25			x	x		x	x	x	x
T26			x				x	x	
T27			x	x			x	x	x
T28			x				x	x	x
T29			x	x		x	x	x	x
T30			x				x	x	
T31			x	x			x	x	x
T32			x	x			x	x	x
T33							x		
T34			x				x	x	

T8 (Management of Technical Vulnerabilities) and T9 (Configuration Management) are central to preventing and resolving errors that arise during updates by ensuring that systems are correctly configured and vulnerabilities are addressed promptly. T13 (Information Backup) safeguards data integrity by allowing systems to be restored to their pre-update state if necessary. T15 (Logging) and T16 (Monitoring Activities) play crucial roles in documenting the update process and detecting issues in real time, providing essential data for troubleshooting and resolution. T24 (Use of Cryptography) ensures data security during transmission and storage, particularly important during updates that involve sensitive

information. T25 (Secure Development Life Cycle) and T28 (Secure Coding) guide the creation and implementation of updates, emphasizing security at every stage of development to prevent the introduction of new vulnerabilities.

T29 (Security Testing in Development and Acceptance) and T32 (Change Management) ensure that updates are thoroughly tested and managed throughout their lifecycle, from development to deployment, reducing the risk of disruptive errors. T31 (Separation of Development, Test, and Production Environments) prevents untested or unstable code from affecting live systems, a crucial factor in maintaining operational stability during updates. T18 (Use of Privileged Utility Programs), T19 (Installation of Software on Operational Systems), and T30 (Outsourced Development) address specific risks associated with software installation and third-party involvement, ensuring that all modifications to the system adhere to stringent security standards.

T26 (Application Security Requirements), T27 (Secure System Architecture and Engineering Principles), and T33 (Test Information) further reinforce the security and integrity of the system by establishing comprehensive requirements and practices that guide the secure handling of all aspects of system updates. T34 (Protection of Information Systems During Audit Testing) ensures that security audits and tests do not compromise the operational systems, safeguarding against additional disruptions during such evaluations. HumSec controls (Table 20), supported by the majority of relevant legislation, are in higher importance than PhySec to this scenario because they address the direct causes of the disruptions—human errors and oversight during the update process. By focusing on enhancing security awareness and ensuring robust incident reporting mechanisms, the organization can better manage software updates and reduce the likelihood and impact of similar incidents in the future.

Table 20. HumSec controls for risk scenario No. 5 covered by security legislation.

Security Control	GDPR	Cyber Security Act	NIS2 Directive	AI Act	Coordinated Plan on AI	Ethics Guidelines for Trustworthy AI	ISO/IEC 27001:2022	CER	CIS
H3			x		x	x	x	x	x
H8		x	x		x	x	x	x	

5. Discussion

The proposed information security management and compliance framework integrates operational, technical, human, and physical security domains, offering a comprehensive solution to cybersecurity management that is systematically aligned with both current and emerging security legislation. One of the main advantages of this framework is its ability to enable organizations to identify and effectively implement the requisite information security controls and legislative compliance needs. By incorporating an ontology-based mapping of security controls, the framework ensures a thorough alignment with regulations such as GDPR, the Cybersecurity Act, NIS2 Directive, and more. This holistic approach not only enhances an organization's ability to adapt to new threats and regulations efficiently but also reduces redundancies and ensures a unified, efficient security posture.

Consideration should also be given to the framework's global applicability, extending its reach beyond EU regulations to encompass global security standards. As technology continues to evolve, the framework could be expanded to explicitly address security concerns related to emerging technologies such as artificial intelligence, quantum computing, and the Internet of Things. The proposed framework can be customized for various organizational contexts using a risk-based approach. Organizations may prioritize controls according to their unique threat landscape, operational environment, and resource limitations. A small research institution may prioritize basic operational and human security controls, whereas a large university handling sensitive research data may focus on advanced technical controls and physical security measures. In addition to regulatory compliance, our framework integrates organizational cybersecurity goals and objectives via a flexible, risk-based structure.

This enables organizations to align security measures with strategic objectives, including the protection of intellectual property, the assurance of research integrity, and the maintenance of high availability of educational resources. The framework categorizes controls into preventive, detective, and corrective types, allowing organizations to align their security investments with their risk appetite and security maturity level.

The proposed framework can be adopted as a guidelines for the enterprises. The adoption process commences with an initial assessment that includes a quantitative risk evaluation across all security domains: operational, technical, physical, and human. This assessment employs standardized metrics to objectively evaluate the existing security posture. A comprehensive gap analysis is conducted, mapping existing controls to the framework's ontology and identifying discrepancies between the current state and framework requirements. The implementation efforts are prioritized using a weighted scoring system, emphasizing high-impact, low-effort improvements at the outset. Regulatory alignment is achieved through the cross-referencing of framework controls with relevant legislation and standards, including GDPR, NIS2, and ISO 27001. A phased implementation strategy is developed, incorporating established key performance indicators for each stage. The simultaneous integration of controls across all domains ensures comprehensive coverage, employing system integration techniques to establish a unified security ecosystem. Continuous monitoring systems are implemented for real-time threat detection, supported by data analytics for trend analysis and predictive security measures. Incident response protocols are formulated and routinely assessed according to the framework's scenarios, with simulation exercises measuring the effectiveness of responses. A structured, role-based security education program is implemented, and its effectiveness is measured through periodic assessments and behavioral analysis. The framework is subject to iterative enhancement via routine audits and penetration testing, utilizing statistical analysis to perpetually refine processes. Cultural integration is accomplished via change management strategies and principles of behavioral science to promote a security-focused organizational culture. Adaptive management maintains the framework's relevance by creating a feedback loop that integrates new threats and regulatory changes, supported by regular updates informed by empirical data and emerging research.

However, the framework has limitations. Its effectiveness depends on the accuracy of ontological mappings and comprehensive legislative inputs. Any omissions or inaccuracies in these areas could lead to gaps in compliance or security coverage. Additionally, the rapid evolution of cybersecurity threats and regulations necessitates frequent updates to the framework, which may be challenging to maintain over time.

6. Conclusions

The proposed holistic information security management and compliance framework successfully integrates operational, technical, human, and physical security domains, while aligning with both current and future legislative landscapes. This integration not only enhances security posture and regulatory compliance but also fosters adaptability to evolving threats and legal requirements. By successfully integrating operational, technical, human, and physical security domains, the framework offers organizations a comprehensive approach to security management that is both robust and adaptable. Its strong alignment with current and emerging security legislation, including GDPR, NIS2 Directive, and the AI Act, ensures that organizations can more easily navigate the intricate regulatory landscape while maintaining a strong security posture.

The framework's effectiveness is validated through application in five distinct risk scenarios, demonstrating versatility across real-world security challenges. This practical approach, coupled with the identification of priority security controls, allows organizations to focus their resources on the most critical aspects of information security. The study highlights the interconnected nature of different security domains, emphasizing the need for a unified approach to security management.

The analysis reveals that certain pieces of legislation, such as the NIS2 Directive, ISO/IEC 27001:2022, and the Critical Entities Resilience Directive (CER), provide more comprehensive coverage across security domains compared to others. This insight can guide organizations in prioritizing their compliance efforts and identifying potential gaps in their security strategies. The framework's emphasis on human security controls, particularly in scenarios involving internal threats or human error, highlights the critical role of the human factor in overall security management. This focus aligns with growing recognition of the importance surrounding security awareness and training in building a robust security culture within organizations.

For future work, the authors intend to further refine the ontological mappings in order to ensure more precise alignment with emerging legislation and cybersecurity standards. Additionally, expanding the framework's adaptability to better anticipate future threats and regulatory changes is also recommended. Implementing more automated processes for updating the framework in response to new information could also be explored to maintain its effectiveness without intensive manual oversight. These enhancements could mitigate the limitations identified and bolster the framework's utility for organizations seeking to stay ahead in the cybersecurity landscape.

Author Contributions: Conceptualization, Š.G. and R.B.; methodology, Š.G., R.B. and A.L.; software, A.L.; validation, Š.G., R.B. and S.A.; formal analysis, P.S. and M.S.; investigation, Š.G. and R.B.; resources, Š.G.; data curation, Š.G. and R.B.; writing—original draft preparation, Š.G., R.B., P.S., M.S. and S.A.; writing—review and editing, A.L.; visualization, R.B.; supervision, Š.G.; project administration, Š.G.; funding acquisition, Š.G. All authors have read and agreed to the published version of the manuscript.

Funding: © GÉANT Association on behalf of the GN5-1 project. The research leading to these results has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No. 101100680 (GN5-1). Co-funded by the European Union. The views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this paper available on request from the corresponding author. The project's incompleteness prevents the data from being publicly available.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. European Commission. General Data Protection Regulation. Regulation, The European Parliament and the Council of the European Union. 27 April 2016. Available online: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679 (accessed on 12 August 2024).
2. European Commission. Artificial Intelligence Act. Regulation, The European Parliament and the Council of the European Union. 13 June 2024. Available online: http://data.europa.eu/eli/reg/2024/1689/oj (accessed on 12 August 2024).
3. European Commission. Network and Information Security Directive. Regulation, The European Parliament and the Council of the European Union. 14 December 2022. Available online: https://eur-lex.europa.eu/eli/dir/2022/2555 (accessed on 12 August 2024).
4. *ISO/IEC JTC 1/SC 27*; ISO/IEC 27001:2022 Information Security Management Systems—Requirements. Standard 3. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/27001 (accessed on 12 August 2024).
5. European Commission. Cybersecurity Act. Regulation, The European Parliament and the Council of the European Union. 7 June 2019. Available online: https://eur-lex.europa.eu/eli/reg/2019/881/oj (accessed on 12 August 2024).
6. European Commission. Coordinated Plan on Artificial Intelligence. Regulation, The European Parliament and the Council of the European Union. 7 December 2018. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0795 (accessed on 12 August 2024).
7. European Commission. Ethics Guidelines for Trustworthy AI. Regulation, The European Parliament and the Council of the European Union. 8 April 2019. Available online: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (accessed on 12 August 2024).

8. European Commission. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. Regulation, The European Parliament and the Council of the European Union. 27 December 2022. Available online: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed on 12 August 2024).
9. CIS Critical Security Controls Version 8. Available online: https://www.cisecurity.org/controls/v8 (accessed on 14 July 2024).
10. *ISO/IEC JTC 1/SC 27*; ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Controls. Standard 3. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/75652.html (accessed on 12 August 2024).
11. Fenz, S.; Neubauer, T. Ontology-based information security compliance determination and control selection on the example of ISO 27002. *Inf. Comput. Secur.* **2018**, *26*, 551–567. [CrossRef]
12. Casola, V.; Catelli, R.; De Benedictis, A. A First Step Towards an ISO-Based Information Security Domain Ontology. In Proceedings of the 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 12–14 June 2019; pp. 334–339. [CrossRef]
13. Meriah, I.; Arfa Rabai, L.B. Comparative Study of Ontologies Based ISO 27000 Series Security Standards. *Procedia Comput. Sci.* **2019**, *160*, 85–92. [CrossRef]
14. Olifer, D.; Goranin, N.; Cenys, A.; Kaceniauskas, A.; Janulevicius, J. Defining the Minimum Security Baseline in a Multiple Security Standards Environment by Graph Theory Techniques. *Appl. Sci.* **2019**, *9*, 681. [CrossRef]
15. Mussmann, A.; Brunner, M.; Breu, R. Mapping the State of Security Standards Mappings. In Proceedings of the Wirtschaftsinformatik (Zentrale Tracks), Potsdam, Germany, 9–11 March 2020; pp. 1309–1324.
16. *NIST SP 800-53 Rev. 5*; Security and Privacy Controls for Information Systems and Organizations. NIST Joint Task Force: Gaithersburg, MD, USA, 2020. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (accessed on 12 August 2024).
17. Taherdoost, H. Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics* **2022**, *11*, 2181. [CrossRef]
18. Djebbar, F.; Nordström, K. A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access* **2023**, *11*, 85315–85332. [CrossRef]
19. *ISA-62443-3-3*; Framework for Improving Critical Infrastructure Cybersecurity. International Society of Automation: Durham, NC, USA, 2019.
20. Wicklund Lindroth, O. *Cybersecurity Ontology—The Relationship between Vulnerabilities, Standards, Legal and Regulatory Requirements*; Stockholm University: Stockholm, Sweden, 2022.
21. Amine, A.M.; Chakir, E.M.; Issam, T.; Khamlichi, Y.I. A Review of Cybersecurity Management Standards Applied in Higher Education Institutions. *Int. J. Saf. Secur. Eng.* **2023**, *13*, 1109–1116. [CrossRef]
22. Bella, G.; Castiglione, G.; Santamaria, D.F. An automated method for the ontological representation of security directives. *arXiv* **2023**, arXiv:2307.01211.
23. Grigaliūnas, Š.; Schmidt, M.; Brūzgienė, R.; Smyrli, P.; Bidikov, V. Leveraging taxonomical engineering for security baseline compliance in international regulatory frameworks. *Future Internet* **2023**, *15*, 330. [CrossRef]
24. Castiglione, G.; Santamaria, D.F.; Bella, G. An Ontological Approach to Compliance Verification of the NIS 2 Directive. *arXiv* **2024**, arXiv:2306.17494.
25. Kalogeraki, E.M.; Polemi, N. A taxonomy for cybersecurity standards. *J. Surveill. Secur. Saf.* **2024**, *5*, 95–115. [CrossRef]
26. Granata, D.; Mastroianni, M.; Rak, M.; Cantiello, P.; Salzillo, G. GDPR compliance through standard security controls: An automated approach. *J. High Speed Netw.* **2024**, *30*, 147–174. [CrossRef]
27. Fernandes, A.; Cruz, J.; Da Silva, M.M.; Pereira, R. Mapping and Integrating Security and Risk Standards: A Systematic Literature Review. *J. Univers. Comput. Sci.* **2024**, *30*, 433–448. [CrossRef]
28. Castiglione, G.; Bella, G.; Santamaria, D.F. Seconto: Ontological Representation of Security Directives. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4862271 (accessed on 25 August 2024). [CrossRef]
29. Schlosser, C.A.; Strzepek, K.; Gao, X.; Fant, C.; Blanc, É.; Paltsev, S.; Jacoby, H.; Reilly, J.; Gueneau, A. The future of global water stress: An integrated assessment. *Earth's Future* **2014**, *2*, 341–361. [CrossRef]
30. Schwartz, M.J. Elon Musk Says Tesla Saved from 'Serious' Ransom Attempt. Available online: https://www.bankinfosecurity.com/elon-musk-says-tesla-repelled-serious-ransomware-attack-a-14907 (accessed on 28 August 2020).
31. Magaña, J.; Olvera, C.I.; Lous, P. How can we improve security against DDoS attacks? A case study: The DyN Attack in 2016. *Cybersecurity* **2019.** [CrossRef]
32. Hughes, M. GitLab Suffers Massive Backup Failure Due to a Fat Finger. Available online: https://thenextweb.com/news/massive-ddos-attack-dyn-dns-causing-havoc-online (accessed on 21 October 2016).
33. Google. Incident Affecting Google Cloud Storage. Available online: https://status.cloud.google.com/incidents/vLsxuKoRvykNHW3nnhsJ (accessed on 14 July 2022).
34. Jones, T. Capital One Data Breach—2019. Available online: https://medium.com/nerd-for-tech/capital-one-data-breach-2019-f85a259eaa60 (accessed on 4 December 2022).
35. Confessore, N. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. Available online: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (accessed on 4 April 2018).

36. Ponomarev, A. Deploy Gone Wrong: The Knight Capital Story. Available online: https://medium.com/engineering-managers-journal/deploy-gone-wrong-the-knight-capital-story-984b72eafbf1 (accessed on 26 October 2023).
37. Cisco. System Error Messages for Cisco Unified Communications Manager 12.5(1). Available online: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/err_msgs/12_x/ccmalarms1251.html (accessed on 18 July 2019).