future internet

MDPI

Article

Leveraging Taxonomical Engineering for Security Baseline Compliance in International Regulatory Frameworks

Šarūnas Grigaliūnas [1,*,†], Michael Schmidt [2,†], Rasa Brūzgienė [1,†], Panayiota Smyrli [3,†] and Vladislav Bidikov [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, Germany; michael.schmidt@lrz.de
[3] Cyprus Research & Academic Network, 33 Neas Egkomis, Egkomi, Nicosia 2409, Cyprus; yiota.smyrli@cynet.ac.cy,
[4] Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University in Skopje, "Rugjer Boshkovikj" 16, P.O. Box 393, 1000 Skopje, North Macedonia; vladislav.bidikov@finki.ukim.mk
* Correspondence: sarunas.grigaliunas@ktu.lt
† These authors contributed equally to this work.

Abstract: A surge in successful Information Security (IS) breaches targeting Research and Education (R&E) institutions highlights a pressing need for enhanced protection. Addressing this, a consortium of European National Research and Education Network (NREN) organizations has developed a unified IS framework. This paper aims to introduce the Security Baseline for NRENs and a security maturity model tailored for R&E entities, derived from established security best practices to meet the specific needs of NRENs, universities, and various research institutions. The models currently in existence do not possess a system to smoothly correlate varying requirement tiers with distinct user groups or scenarios, baseline standards, and existing legislative actions. This segmentation poses a significant hurdle to the community's capacity to guarantee consistency, congruency, and thorough compliance with a cohesive array of security standards and regulations. By employing taxonomical engineering principles, a mapping of baseline requirements to other security frameworks and regulations has been established. This reveals a correlation across most regulations impacting R&E institutions and uncovers an overlap in the high-level requirements, which is beneficial for the implementation of multiple standards. Consequently, organizations can systematically compare diverse security requirements, pinpoint gaps in their strategy, and formulate a roadmap to bolster their security initiatives.

Keywords: information security management; security maturity model; research and education; taxonomy; security baseline

Citation: 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. https://doi.org/10.3390/fi15100330

Academic Editors: Weizhi Meng and Christian D. Jensen

Received: 6 September 2023
Revised: 1 October 2023
Accepted: 2 October 2023
Published: 7 October 2023

1. Introduction

Dealing with information securely is a key issue for organizations of all sizes and across all industries. Due to the greatly increased media attention triggered by security incidents that have been made public, the subject of Information Security (IS) has become an important part of many organizations. As a result of these media events, many executives have become more aware of the issue, and their interest in preventing security incidents has increased.

Information Security Management (ISM) is no longer viewed solely as a cost factor; instead, it has emerged as a key discipline for gaining competitive advantage and is pivotal in securing organizational assets and intellectual property. Furthermore, national and international regulations, such as the General Data Protection Regulation (GDPR) [1] or the Network and Information Security (NIS) Directive [2], impose a strict legal framework that gives organizations an additional incentive to protect their data. In this evolving landscape,

the role of cryptography has become indispensable, serving as a fundamental layer in the multifaceted approach toward robust Information Security. Cryptography, which encompasses techniques such as encryption and hashing, is instrumental in ensuring the confidentiality, integrity, and authenticity of data, thereby mitigating the risks associated with unauthorized access and data breaches. The application of cryptographic measures is especially vital in the context of data privacy [3], where the safeguarding of sensitive information is paramount.

The above-mentioned regulations not only necessitate the implementation of strong cryptographic controls but also emphasize the importance of maintaining a balance between data accessibility and security, underscoring the significance of cryptography in achieving compliance. The GDPR, for instance, explicitly requires the encryption of personal data [4] in transit and at rest, thereby illustrating the integral role cryptography plays in protecting individuals' privacy [5].

Beyond simply meeting regulatory requirements, the strategic use of cryptography boosts an organization's credibility and trust among stakeholders, clients, and partners. With the rise in data breaches and cyber threats, businesses that showcase dedication to data privacy with strong cryptographic measures are more apt to cultivate trust and loyalty. This can result in a lasting competitive edge. The proactive adaptation and integration of advanced cryptographic solutions also enable organizations to stay ahead of emerging threats, thereby reinforcing their security posture and ensuring the resilience of their information systems.

Within the broader IS context, the Research and Education (R&E) sector is not exempt. Universities and research institutions have increasingly come under the scanner of cyber threats. Therefore, it is necessary to address ISM in higher education as well and provide guidance to R&E service and infrastructure providers on how to implement a security program. National Research and Education Networks (NREN) are at the center of scientific IT infrastructure. They connect the higher education facilities in their country and provide them with networks, basic infrastructure, and other IT services. Consequently, they not only need to protect themselves but also play a central role in securing their constituents. European NRENs collaborate under the umbrella of the GÉANT Project [6], a joint venture funded by the European Union Horizon Framework Partnership Agreement. In this project, the organizations not only develop and operate shared services, including R&E core services such as eduGAIN, eduroam, and eduVPN, but also work jointly on common IS challenges. This collaboration puts the NRENs in the perfect position to establish a common security architecture and support each other in implementing necessary measures.

Since 2019, the GÉANT project has also been working more closely in the area of ISM in order to standardize and improve many security aspects within the community. As a result of this initiative, the Security Baseline (SB) for NRENs [7] and the S7 Business Continuity Framework [8] were created. Both are security frameworks that are specifically tailored to the needs of NRENs and other R&E organizations. They are designed to ensure the community's compliance with current security standards and regulations. The SB is a security maturity model to measure and improve the security level of an organization focusing on organizational controls. The S7 framework expands on this and provides practical guidelines to implement a security program and comply with many of the SB requirements.

The original goal of the SB was to define a common Security Baseline for the R&E community. However, it soon became apparent that the organizations in question were too heterogeneous. The GÉANT community alone comprises 39 organizations in 44 countries, and each NREN serves many universities and research institutions. Defining a baseline applicable to all of these organizations thus proved to be a major challenge. Furthermore, there exists no governance authority between these organizations, i.e. there is no way to enforce compliance with certain policies. Thus, all policies would have to be made appropriately attractive so that participants would voluntarily choose to comply. If a baseline were to be established under these conditions, there are two possibilities: defining

high- or low-security requirements. High requirements would force a high level of security, but to comply with them would be too difficult for many organizations. The expected adoption rate would be very low. Low requirements would mean that a majority of organizations could meet them, which would result in a very high adoption rate. However, there would then be no need for action for many organizations, and the baseline would not positively influence the security level of the community.

It was decided to solve this problem by creating several levels of requirements and combining them to create a maturity model. This makes it possible to define different levels for different user groups or use cases. While organizations with weak ISM can still try to reach the baseline level, very mature organizations still have a way to improve their security level. This is already a great advantage compared to common security standards, which usually only allow a binary distinction between compliant and non-compliant. Furthermore, different levels enable organizations to compare their performances with each other. It is anticipated that the emerging peer pressure will trigger some competition, which will lead to a long-term increase in security maturity in the community.

Although other security frameworks already offer security maturity models, they are usually lacking in the proper characteristics. For example, the NIST Cyber Security Framework (CSF) provides a multi-TIER model, but it is explicitly not a maturity model and only considers risk management. The Capability Maturity Model Integration (CMMI) is a very commonly used industry model, but it is mainly used to evaluate processes and not the maturity of security controls. Other maturity models, such as the Cybersecurity Capability Maturity Model (C2M2) [9], are comprehensive but very complex in their design and just contain the general requirements for all sectors. This is why it was decided to create a new maturity model with the SB tailored to the needs of the R&E community.

Ultimately, a maturity model also provides the ability to match different requirements and maturity levels to other standards and regulations. However, this requires a very formal evaluation and mapping of the various documents. An approach to this is described in this article. The main aim of this work is to establish a universal security foundation tailored for the R&E community by introducing Security Baseline requirements. The intention is to foster a holistic security maturity model that not only aligns various requirement tiers with corresponding user groups or scenarios but also integrates these baseline standards, ensuring a comprehensive security framework. The main contributions presented by the authors of this paper are as follows:

- The authors have introduced a unique methodology for a security maturity model. This approach combines maturity levels with Security Baseline requirements;
- The authors have contributed by developing taxonomies that emphasize a compliance framework. This framework is centered around the Security Baseline and is meticulously mapped to various legal regulations prevalent in the cybersecurity domain.

Within the R&E community, there is a discernible gap in the presence of a consolidated security maturity model that takes into account Security Baseline requirements. The existing models lack a mechanism to seamlessly align diverse requirement levels for various user groups or scenarios with both the baseline standards and existing legislative measures. This fragmentation challenges the community's ability to ensure uniformity, compatibility, and comprehensive adherence to an integrated set of security standards and regulations.

The remainder of this article is structured as follows: Section 2 describes an overview of the Security Baseline and security maturity model. Section 3 discusses the relevant literature and other works related to the compliance of different legislation. Section 4 presents the different requirements from regulatory frameworks that were analyzed and transformed into individual taxonomies, which highlight a compliance framework. Section 5 analyzes the results of the harmonization of multiple regulations and the derived correlation matrix and discusses how it can be used to support ISM using the mapping of security requirements. Sections 6 and 7 wrap up the findings, results, and future works.

2. Overview of the Security Baseline

The SB emphasizes the organizational capability of the NREN, arranges requirements by maturity level, and provides references to the ISO/IEC 27001 standard for easier integration [10]. The SB consists of four areas, which were found to be essential for the security level of each organization. These areas are very similar to the recently published revision of ISO/IEC 27001 [11]. The four areas are split into 15 modules; each module contains three maturity levels, and each level contains three requirements.

A security area consists of two parts: a specific domain that covers one particular security subject and security requirements split into three maturity levels. Each maturity level contains the same number of requirements, i.e. three for level one, two for level two, and two for level three. An organization that wants to achieve a higher maturity level needs to comply with all requirements from this and the lower levels. In order to illustrate this, a taxonomy was created for each of these areas that shows the connection between a domain and its requirements per maturity level.

Figure 1 displays the Policy, the foremost security area in the SB, encompassing four domains. This section addresses leadership and the coordination of IS, divided into four modules. Engaging top management to enforce essential regulations is pivotal for the successful implementation of ISM. These regulations should be articulated as policies, clearly defining expected conduct and forbidden actions. From the top-level IS policy, more specific policies should be formulated to oversee the management of information and technologies. In the end, it is imperative for an organization to establish and adhere to not only its policies but also to external regulations.

The section Management Commitment and Mandate outlines requirements to ensure organizational leaders support the ISM strategy. This is deemed the most crucial step in initiating and maintaining a successful security program. As a result, an organization must appoint a designated security official, establish a top-tier policy, and allocate a budget to uphold it. Subsequently, the active involvement of top management in communication, reporting, and decision-making is essential to continuously enhance security efforts.

The Internal Security Policy comprises multiple policies delineating both organizational and technical security measures. Each organization must meticulously consider the behaviors they wish to permit and the directives they aim to establish. These directives pertain to services, systems, or any devices and influence how they are utilized in daily operations. It is vital to not only articulate and document these policies but also to vigilantly monitor and enforce them.

An organization must extract an Acceptable Use Policy from its main security policy. This policy sets rules for the organization's information systems, guiding users on their appropriate use. The content should encompass areas such as the use of networks, hardware, emails, and general information. No individual should be permitted to use any system within the organization without first being familiar with and agreeing to the acceptable use policy.

The Regulatory and Privacy elements are paramount for all organizations to consider. Within the EU, the General Data Protection Regulation (GDPR) primarily addresses these aspects. Regardless of this particular regulation, it is in the interest of every organization to ensure a foundational level of data protection. This necessitates designating a responsible individual for data protection and privacy, who will then enact measures to secure personal data and facilitate communication with users and regulatory bodies.

This domain is tripartite in nature. To foster and adhere to secure processes that preclude IS incidents, both staff and external entities must be adequately informed and trained. Equally crucial is ensuring security protocols are referenced during hiring, with new hires receiving proper orientation. In the end, not just the internal workforce, but also external vendors, must be engaged to cultivate a secure collaborative framework.

The subsequent area, People, depicted in Figure 2, pertains to the most vital component of ISM: the individuals within and outside the organization.

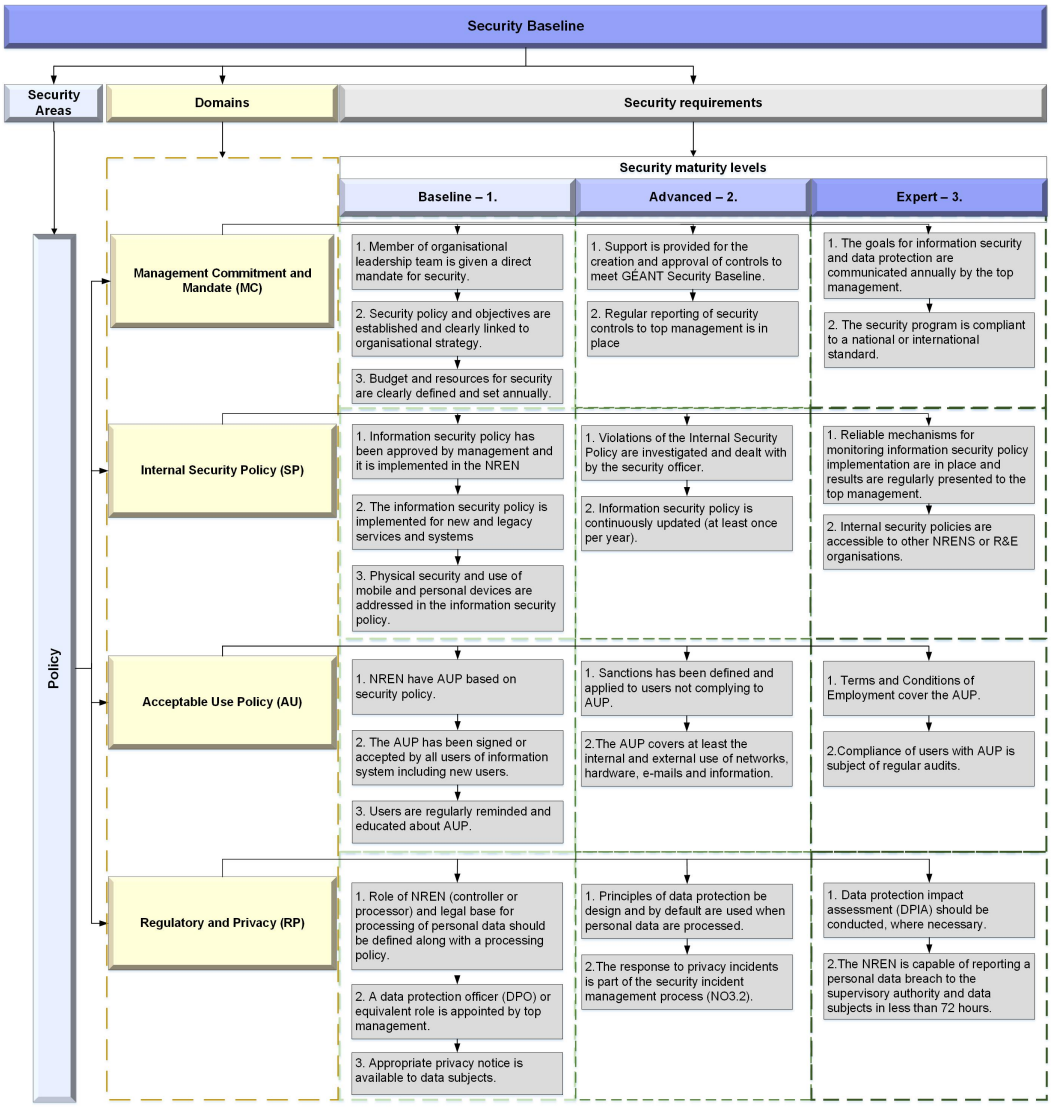

Figure 1. Taxonomy of Security Baseline requirements for policy area.

The first initiative an organization needs to implement in the area of people is a suitable Training and Awareness program. While simple awareness training for all staff is sufficient in the beginning, in the long term, this should be transformed into role-specific coaching, in which efficiency is verified regularly. Again, it is very important to involve the top management in order to motivate the employees through a positive example and proper communication within the company.

Personnel Management should consider security aspects before, during, and after the termination of employment. HR needs to think about clear (security) requirements for jobs that need to be done by internal as well as external employees. Employees must be informed of their duties with respect to IS and be bound by contracts or Non-Disclosure Agreements (NDA). Ultimately, it is important that HR reacts quickly when employees leave the company (in bad faith), and it should be ensured in advance that this does not have a negative impact on operations.

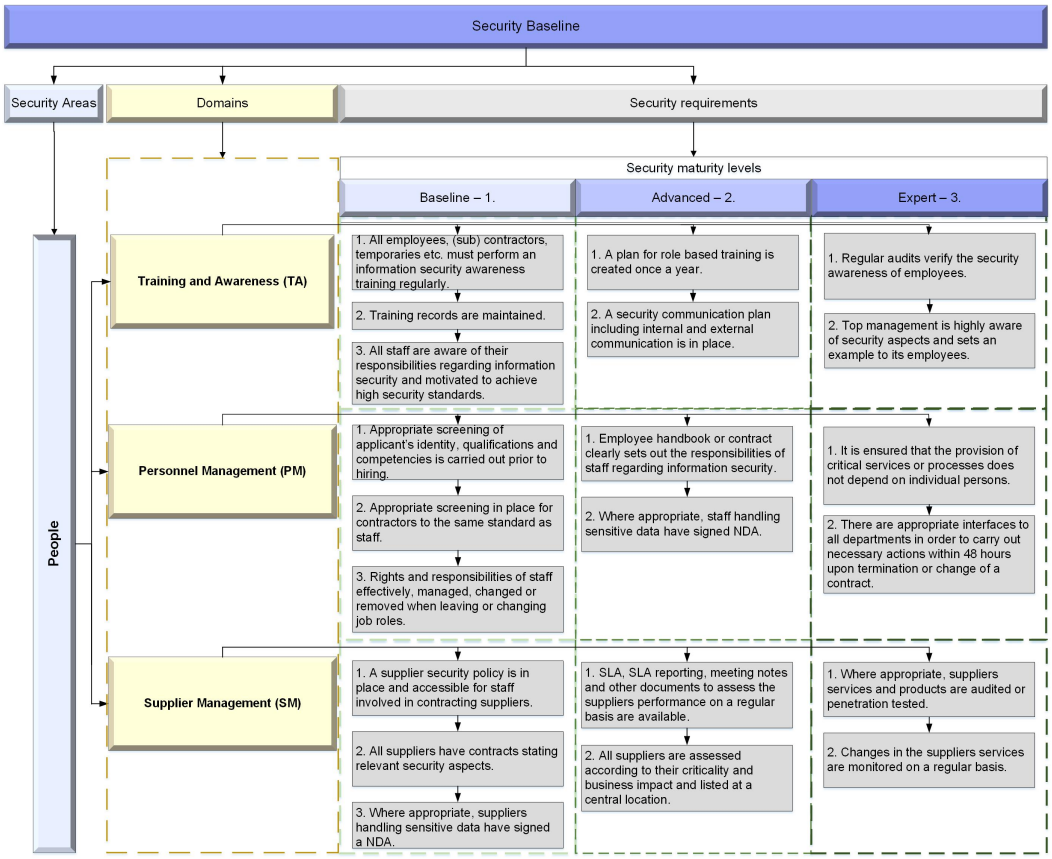

Figure 2. Taxonomy of Security Baseline requirements for people area.

In addition to covering the security requirements for its staff, an organization needs to establish effective Supplier Management to handle their contractors. This starts with a security policy for suppliers that covers at least all aspects of the internal security policy. Suppliers must be held accountable for compliance, which must be supplemented by further NDAs if required. Every organization therefore needs an overview of its suppliers, should assess their criticality, and regularly review the security of particularly important suppliers. Figure 3 shows the third area Threats containing the comprehensive scope of all types of threats to the organization. Of course, internal Information Security Risk Management (ISRM) is at the center of this and must ensure that the organization is able to identify risks and deal with them. If a risk nevertheless materializes, then the organization must ensure rapid and effective handling of the resulting incidents. Ultimately, the organization must also be prepared for critical incidents and be able to continue its business operations.

Risk Management is a key process in ISM that should drive every major decision. There are multiple national and international frameworks for implementing IS risk management. An organization should always pick one of these standard processes and assign a senior person to be in charge of IS risk. The organization should select all of their security measures based on a previous risk assessment that considers its assets and common threats. While, at the beginning, only common threats are considered, later on, the organization should assess its specific threat situation and its consequence.

Since not all risks can be prevented by security measures, the organization needs to have an Incident Management process in place to handle security incidents. This requires the design of a process that enables fast response times to security incidents and their handling by a Cyber Security Incident Response Team (CSIRT). It should use common communication protocols and inform interested parties of relevant incidents. The team should be continuously expanded so that at any time people are available to process security events.

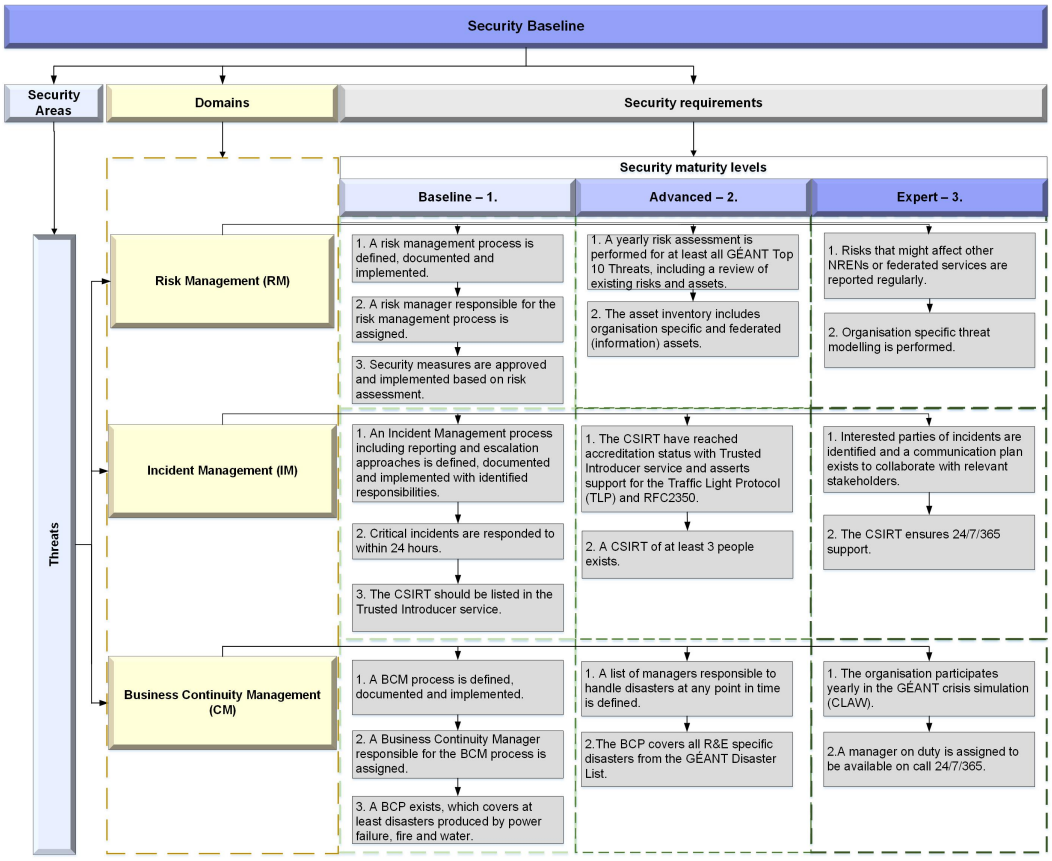

Figure 3. Taxonomy of Security Baseline requirements for threats area.

An incident with a critical impact on the organization is considered a disaster that needs to be handled via Business Continuity Management. The organization needs a responsible person who prepares a business continuity plan that covers at least common (natural) disasters. These plans should be continuously improved and tested, preferably together with other organizations, in order to test emergency communications. It is necessary to have access to senior personnel at all times who are able to take control in the event of a disaster.

Finally, the fourth area, Operations, deals with the operation of the organization, in particular, the technology required for it. Figure 4 shows its five security domains. Basically, the organization must be able to adequately secure its own infrastructure. A wide variety of cryptographic measures can help to protect data at rest and in transit. It is also important to configure access to all systems in such a way that unauthorized access is prevented. These and other security measures are only effective if the software used is always up to date and patches are applied promptly. In turn, it is essential that the organization has established a procedure for identifying and quickly removing new vulnerabilities.

All software Tools used within operations need to be secured and managed by the organization. This requires an overview of all available software of company devices and an approval flow. Common security measures, such as antivirus software, firewalls, virtual private networks, network segregation, intrusion detection, and denial of service protection, should be implemented as the security program matures.

It is important to have a policy on Cryptography within the organization that handles encryption of sensitive data. This policy must define the kind of data that should be protected and the cryptographic means to do that. The functions and algorithms used need to be improved, and, in the long term, only those recommended by international standards should be used.

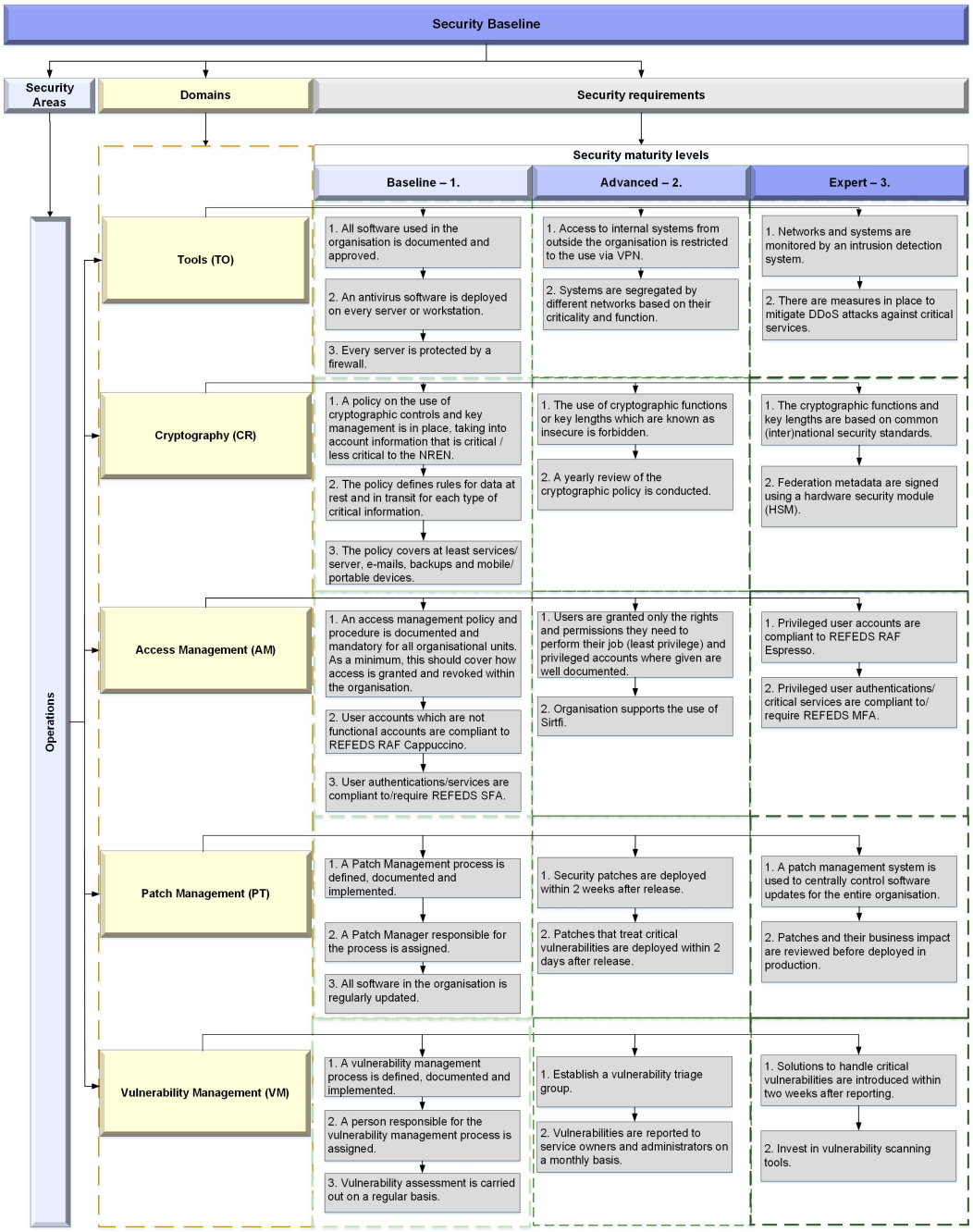

Figure 4. Taxonomy of Security Baseline requirements for operations area.

Access management covers how users access information systems and data. The organization needs a procedure to assign access to users and needs to protect these user accounts using suitable authentication. Common principles, such as need-to-know and least privilege, should be considered. The goal is that at some point all accounts are tied to one person (identity assurance) and are protected by multi-factor authentication.

Patch management is a proactive process to keep all software in the organization up to date. The person responsible must ensure that the defined process will identify unpatched software in the organization and update it regularly. More mature organizations aim for very short time frames until a security patch is applied to a system. A patch management system and a connection to risk management practices can help to improve the process.

A well-designed vulnerability management ensures that vulnerabilities in software products are fixed before they are exploited. In parallel with proactive patch management, the organization needs to regularly check their (self-developed) software for vulnerabilities.

Security experts should assess new vulnerabilities and report them to the person responsible for a system, who fixes them as fast as possible. Scanning tools can help to support or automate the identification of vulnerabilities.

3. Related Works

Adopting a cybersecurity framework can be seen as a best practice, effectively showing that an organization has taken a robust duty of care. However, in today's digital transformation era, this is insufficient. The constantly evolving threat landscape presents new challenges, necessitating tailored and innovative solutions to prevent malicious actions and disruptions. Consequently, organizations need to establish, apply, and uphold various controls from diverse regulatory frameworks. Over the past few years, many researchers have evaluated the EU's cybersecurity environment, considering the increasing scale and sophistication of present cyber threats. They have also conducted studies comparing the relationships or correlations among existing regulatory frameworks. The research mainly centers on manual techniques or security ontologies to develop security standard mappings. This section aims to delve into these studies, illustrating that various legal regulations in the cybersecurity age can be effectively compared using generalized requirements.

In 2019, the authors in [12] examined the interplay between the GDPR and NIS Directive focusing mainly on the incident notification obligations and their enforcement, while demonstrating that the two instruments represent a cross-sectorial approach. They also stated that any overlap of two instruments may only occur with respect to the operators and providers encompassed by the NIS Directive. They concluded that various legal uncertainties remain that are hard to translate into deterministic requirements for software design, and the choice of the instrument for a Directive adds to this dilemma. Moreover, the interplay between the NIS Directive and the GDPR is unclear where similar obligations exist, running the risk of the double jeopardy of non-compliance.

In 2020, Prameet P. Roy [13] provided a high-level comparison between the National Institute of Standards and Technology's (NIST) Cyber Security Framework (CSF), which is closely aligned to the NIS Directive and the ISO 27001 Security Standard. The pros, cons, and benefits of each risk management framework have been examined, particularly when choosing between the NIST CSF and ISO 27001. A thorough comparison was made on how major security control frameworks/guidelines, such as NIST SP 800-53 [14], CIS Top-20, and ISO 27002, align with one another. Both ISO 27001 and NIST CSF offer guidelines, policies, and procedures to establish a comprehensive Information Security Management System (ISMS). They can be enhanced with other guidelines. It was concluded that the optimal strategy to prevent unforeseen disasters is to integrate the strengths and recommendations of both frameworks.

In the same year, Andrea Mussmann et al. [15] provided an overview of research focused on mapping security standards (e.g., ISO 27001, ISO 27002, ITIL, COBIT, NIST SP800-53, GDPR). They explored methodologies formulated for these mappings and delved into tools, such as mapping tables, that support the process. Mussmann noted that the mapping between standards is not comprehensive but rather focuses on subsets of standard controls or on a more general mapping. She asserted that fully automating this mapping process is crucial, and future research on security standard mappings should embrace Natural Language Processing (NLP) methods, potentially combined with existing security ontologies and manual comparison techniques.

Enescu in [16] has carried out a comparative analysis of the cybersecurity strategies of the EU members taking into account the NCSS documents published by EU and European countries. Even if they benefit from the same guidelines, the documentation that makes them up is different from one state to another, based on a preliminary analysis of each national cyber framework. This has the effect of promoting diverse approaches in terms of priorities, objectives, set of measures, and their corresponding fields of action. A key concern of the above strategies is to find efficient ways to integrate cybersecurity into the education system, as a measure aimed at strengthening the level of its cybersecurity culture.

Sulistyowati et al. in [17] conducted an analysis of security standards, including NIST, ISO 27002, COBIT, and PCI DSS, employed by the ABC organization. This organization is a government agency overseeing critical infrastructure and the digital economy in Indonesia. They developed an integrated framework concept aimed at enhancing ICT management performance. Furthermore, their analysis informed the creation of a cybersecurity maturity framework designed to bolster existing software processes and other procedures. This is achieved by assessing an organization's cybersecurity capabilities and positioning it on a scale reflective of its current state. This framework encompasses twenty-one integrated cybersecurity categories, serving as a foundation for mapping the progression of ABC's organizational maturity capabilities.

Aliyu A. et al. in [18] introduced a comprehensive Cybersecurity Maturity Assessment Framework. This framework consolidates the various privacy regulations and security best practices to which Higher Education Institutes (HEI) should adhere. Moreover, this user-friendly web-based tool can serve as a self-assessment instrument or a cybersecurity audit mechanism, enabling organizations to undertake gap analyses and obtain automated compliance reports, along with visual depictions of their security stance. The study meticulously evaluated the synergies, redundancies, and challenges presented by security and data protection mandates, integrating them into a maturity model. Throughout this research, the necessary technical security measures, as informed by the GDPR and NISD's best practices, among others, were pinpointed and combined.

Najmudin Saqib et al. in [19] embarked on mapping the GDPR and NISD. Their study delved into the sections of these regulations most commonly considered by organizations during implementation, the underlying principles and intentions behind these regulations, and their influence on security requirements. Najmudin Saqib et al. provided a comparative analysis between these two European initiatives, illustrating the disparities in tabular form. Their research effectively complements the study in [18], as it predominantly centers on organizational, policy-making, and practical concerns rather than purely technical aspects.

In their work, Syed Wasif Abbas Hamdani et al. [20] conducted an extensive literature review, meticulously analyzing various cybersecurity frameworks and presenting statistics related to cyber-attacks on operating systems (OS). They also provided a detailed comparison of the available standards, frameworks, tools, and software for OS compliance testing. Additionally, they deeply explored the software solutions frequently utilized to ensure compliance with specific cybersecurity mandates. Concluding their study, they proposed a comprehensive set of foundational security-related requirements pertaining to OS hardening, grounded in the examined cybersecurity standards.

Mùrino G. et al. in [21] showcased the primary attributes of CSFTool, an encompassing web-based application aimed at heightening awareness regarding IT/OT cybersecurity. The tool strives to equip end-users, particularly those in SMEs, with hands-on knowledge about standards, regulations, and legislation tied to the protection of critical infrastructure. CSFTool aids in the enactment of the "National Framework for Cybersecurity & Data Protection" and a set of "Essential Cybersecurity Controls". The authors expounded on the foundational reasoning behind the project and furnished details concerning the design and realization of a proof-of-concept prototype for the entire system. They also described its architectural layout and highlighted some core functionalities, including a visual sitemap of the tool.

Meryem Ammi et al. in [22] delivered a comprehensive overview of prevailing CTI-based ontologies, taxonomies, and knowledge graphs. They carried out a comparative review of different CTI enumeration and sharing standards and identified diverse metrics essential for shaping standard CTI taxonomies. Given the hurdles observed with popular cybersecurity taxonomies—such as limited integration and a lack of connections between taxonomies and ontologies—the authors introduced a standardized framework. This framework consolidates various taxonomies, aiming to bolster efficient vulnerability assessment capabilities and augment CTI efficacy. The suggested framework encompasses multiple stages, namely discover, prioritize, continuous evaluation, reporting, and remediation. In

line with their approach, they also touched upon the anticipated growth in the importance of CTI knowledge graphs stemming from the standardization process.

Venizelos C. in [23] conducted a mapping of the controls from ISO/IEC 27002:2013, ISO/IEC 27002:2022, the NIS Directive, and the GDPR. The primary aim was to guide organizations in properly implementing these regulations, pinpointing potential security concerns, and formulating new security strategies.

Wicklund Lindroth in [24] formulated and showcased a security ontology delineating the connections among vulnerabilities, standards, and legal as well as regulatory mandates. This created resource can bolster the resilience of organizational assets and enhance security mitigation. The detailed relationships illustrate the manner and specific controls that address existing vulnerabilities while concurrently adhering to legal and regulatory stipulations.

Dominguez-Dorado M. et al. in [25] introduced the CyberTOMP framework, a comprehensive tool that equips organizations with resources for holistic cybersecurity management on both tactical and operational fronts. A significant component of this framework is the Unified List of Expected Outcomes (ULEO), which offers a consistent listing of cybersecurity measures required to safeguard specific assets. Additionally, ULEO presents a set of metrics that, when combined, can assess the current cybersecurity status of assets, trace their progression over time, or set cybersecurity goals at various organizational levels. Notably, this proposition emphasizes procedural and methodological approaches rather than purely technical solutions.

Marwan Alshar'e in [26] conducted a comparison between the NIST CSF and ISO 27001 cybersecurity frameworks, primarily examining their suitability and selection criteria. The study suggests that organizations should evaluate and adopt specific frameworks based on factors such as their risk maturity level, certification requirements, and a cost-benefit analysis.

The authors in [27] introduced an automated technique that furthers ontology engineering and development to accurately depict security directives for automated verification. Impressively, the method ingeniously merges methodologies and tools from two recognized domains of informatics: Natural Language Processing (NLP) for POS tagging and ontology creation. This method is demonstrated through a tangible challenge: creating an automated representation of directives as ontologies, specifically for the latest European directive on cybersecurity, the NIS 2. The developed NIS 2 ontology followed a waterfall methodology, adhering to a set sequence of stages ranging from specification and implementation to evaluation, akin to traditional software development.

Gianpietro Castiglione et al. in [28] introduced an ontological approach for the characterization of security directives. The proposed structural solution supports the case that semantic representation of the NIS 2 Directive provides an effective method for compliance verification. The approach meets the FAIR principles and the NIS ONTOLOGY as it is termed may help security analysts to quickly verify the status of the institutions' compliance, resulting in an efficient search engine for security measures. The development of the model is currently ongoing toward a more complete coverage of the NIS 2 Directive, as its current version only covers articles 7 and 10 of the NIS 2.

Mierzwa S. et al. in [29] showcased a study offering small- to medium-sized enterprises a methodology for exploring accessible frameworks, along with a complimentary toolbox to assist in swiftly addressing cyber risks and threat evaluations. The report further details an assortment of audit strategies and cyber risk assessment guidelines, empowering these businesses to draw inspiration and devise their unique strategies by integrating various solutions.

Djebbar F. and Nordstrom K. in [30] undertook a comparison to pinpoint commonalities in security requisites and differences among three widely recognized domain-specific cybersecurity standards: ETSI EN 303 645 v2.1.1, ETSI EN 303 645 v2.1.1, and ISO/IEC 27001:2022. The study aims to confront the challenges of crafting and complying with numerous security standards, regardless of their distinct operational contexts. By highlighting

the shared elements in industrial standards' security controls, the compliance pathway can be more efficient for organizations grappling with the task of meeting several standards at once. Their research reveals a considerable concurrence between the standards, potentially leading to conserving resources, minimizing repetition, and enhancing the efficacy of a firm's cybersecurity deployment.

Previous studies have substantially enhanced our comprehension of the adoption and execution of security frameworks, including the interrelation and convergence of security controls and standards. However, a gap remains in streamlining compliance efforts with the appropriate attributes. By identifying congruences and mapping regulatory standards with cybersecurity frameworks, organizations can mitigate redundant actions and streamline the compliance journey. This can notably decrease the time for implementation and enhance the cost efficiency of adhering to the full spectrum of security prerequisites. The existence of a thorough comparative overlap among these standards further simplifies the selection procedure. The primary goal of this endeavor is to establish a universal security foundation for the R&E community. This involves crafting various requirement tiers for diverse user groups or scenarios and amalgamating them to formulate a security maturity model. This model facilitates the alignment of different prerequisites and maturity stages with other legal measures and standards.

4. Framework for Security Baseline Compliance

To address the challenge of ensuring compliance with Security Baseline requirements across various ISO standards or EU directives, such as the NIS 2, GDPR, and CIS, a methodological approach based on taxonomical engineering principles was developed. Taxonomies, which were created for the Security Baseline requirements in Section 2, present the conceptualizations of the knowledge in a security maturity model, and they can be used as a key in mapping those requirements with the complexities of different standards and directives. The mapping process included aligning similar concepts and relationships between the Security Baseline requirements and appropriate legislation. The methodology was developed based on the recommendations and insights of experts who are members of the GÉANT project group. The taxonomies presented below in this section highlight a compliance framework for the Security Baseline mapped with different law regulations in the cybersecurity area.

Figures 5–8 present the Security Baseline requirements for four security areas mapped by the ISO/IEC 27001:2013 and ISO/IEC 27001:2022 standards. Through its numerous annexes, ISO/IEC 27001:2022 emphasizes the critical role of leadership in supporting Information Security. Due to this, the requirements of the MC domain (on all security maturity levels) fully cover ISO/IEC 27001:2022, while the SP domain on the expert level covers it only partly.

Annex A.5.1 asserts senior management's leadership in aligning Information Security with organizational strategy. A.5.2 emphasizes creating a security policy in line with organizational goals, requiring senior management endorsement. A.5.3 focuses on clear communication of security roles and responsibilities. A.5.4 discusses operational planning, including risk management, requiring leadership oversight. A.5.5 ensures management's commitment to providing the necessary ISM resources. A.5.6 underscores leadership's role in evaluating the ISM's performance. A.5.8 pertains to the executive review of the ISMS, promoting continuous improvement. A.5.22 mandates integrating security policies and objectives with organizational processes, emphasizing leadership's strategic alignment.

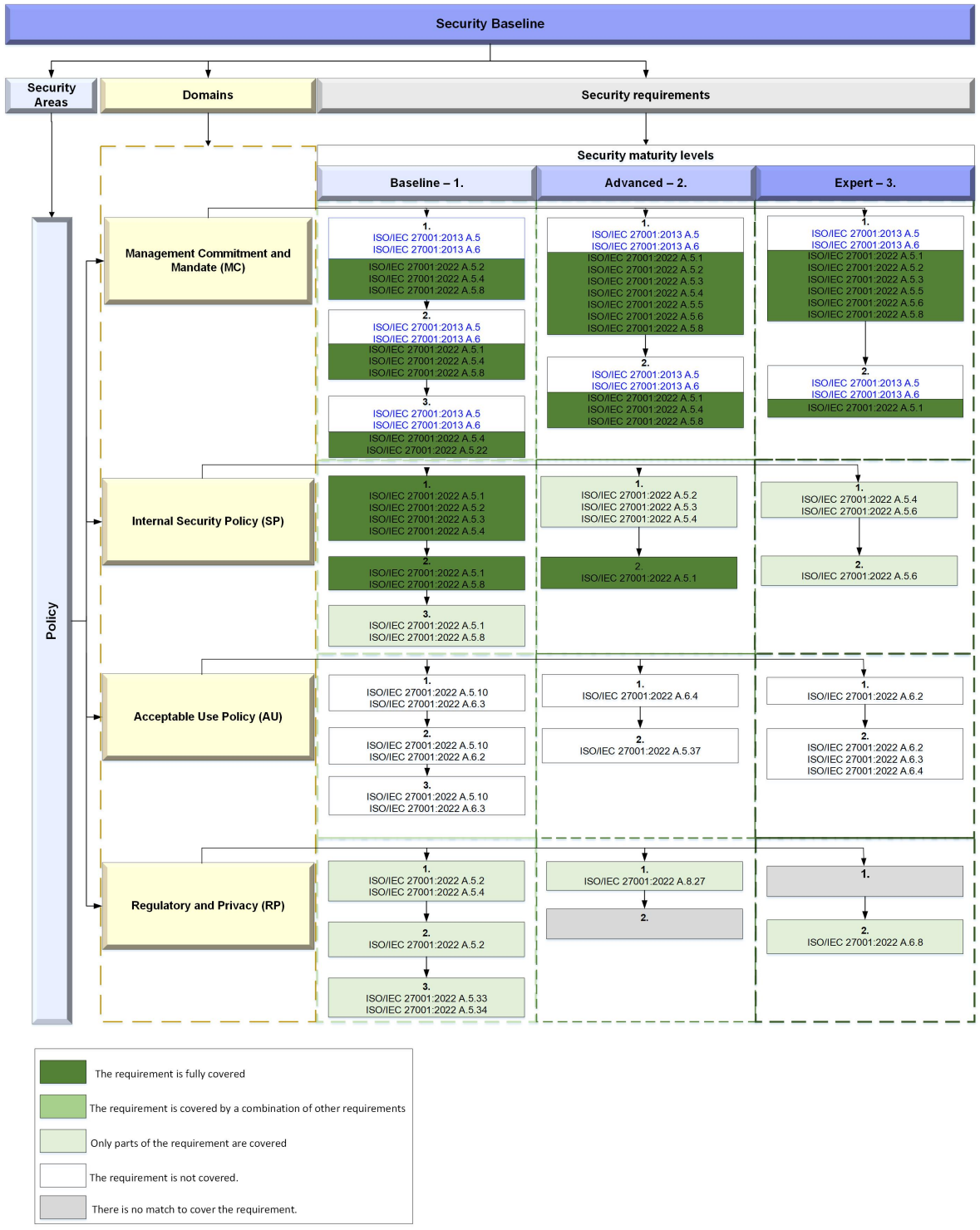

Figure 5. Taxonomy of Security Baseline requirements for policy area mapped by different ISO standards.

In a hypothetical scenario, the ISO/IEC 27001:2022 standard could encompass explicit provisions for an Acceptable Use Policy within annexes A.5.10, A.6.2–A.6.4, and A.5.37. These annexes might be designated to delineate the parameters and specifications for developing, implementing, and maintaining an Acceptable Use Policy, outlining user responsibilities, access controls, and operational procedures, along with other relevant domains of Information Security.

In contrast, the SB for the policy area does not completely cover the requirements given in A.5 and A.6 of the ISO/IEC 27001:2013 standard. ISO/IEC 27001:2013 does not prescribe specific leadership requirements but provides a framework that allows organizations to define their own leadership structures and commitments within the context of Information Security. The emphasis is on flexibility, global applicability, and continuous improvement, while leadership commitment is implied throughout the standard's requirements.

In the TA domain (see Figure 6), for advanced and expert security maturity levels, as well as for PM.1.2 and PM.3.1, there is no match in the ISO standards to cover these requirements. The majority of the requirements for the baseline security level are covered by both of the ISO standards. Both ISO/IEC 27001:2013 and ISO/IEC 27001:2022 address the requirements for people inside and outside organizations with a focus on roles, responsibilities, awareness, and training. The 2022 version enhances the explicit consideration of roles and responsibilities, making it even clearer that these requirements should be addressed to ensure the effective implementation of an ISM.

Supplier management is a critical aspect of Information Security, as suppliers can pose various risks to an organization's information assets. Both ISO 27001 versions address supplier management through a dedicated sections in their annexes. The controls in the A.15 domain aim to ensure the protection of an organization's assets that are accessible by suppliers and to maintain the integrity and security of the organization's information and systems. A.13.2.4 is relevant to supplier management in the context of protecting information shared between an organization and its suppliers. The use of confidentiality or non-disclosure agreements can be a measure that ensures suppliers understand their responsibilities regarding the handling of sensitive information and are legally bound to protect it. Such agreements are integral to managing supplier relationships and mitigating the risks associated with information disclosure.

ISO 27001:2002 A.5.19 focuses on the responsibility of an organization to ensure that when utilizing products and services from suppliers, including cloud service providers, they carefully assess the inherent risks associated with using external systems. This evaluation should also take into account the potential impact on the organization's adherence to Information Security measures. An effective policy encompasses the delineation, choice, administration, and termination of suppliers, as well as the regulation of information assets pertaining to suppliers, with the aim of mitigating related risks while facilitating the attainment of corporate goals and objectives. Intelligent organizations will include their Information Security strategy for suppliers into a comprehensive relationship framework, rather than only focusing on security alone. They will also consider other relevant issues in order to provide a well-rounded approach. According to A.5.22, it is recommended that organizations engage in consistent monitoring, evaluating, and auditing of their supplier service delivery procedures. The type of contract that has been signed and whether or not the organization has its own legal department should both be considered when deciding whether or not A.5.20 should be implemented.

An effective control is one that allows for the management of any changes to supply chain policies, procedures, and controls, as well as the maintenance and improvement of already existing Information Security policies, processes, and controls. This is established by taking into account the significance of the business information, the nature of the change, the type(s) of suppliers that are impacted, the processes and systems that are involved, and reevaluating the risk factors. When deciding to modify the services that a supplier delivers, it is important to take into account the closeness of the connection as well as the organization's capacity to either influence or manage the change.

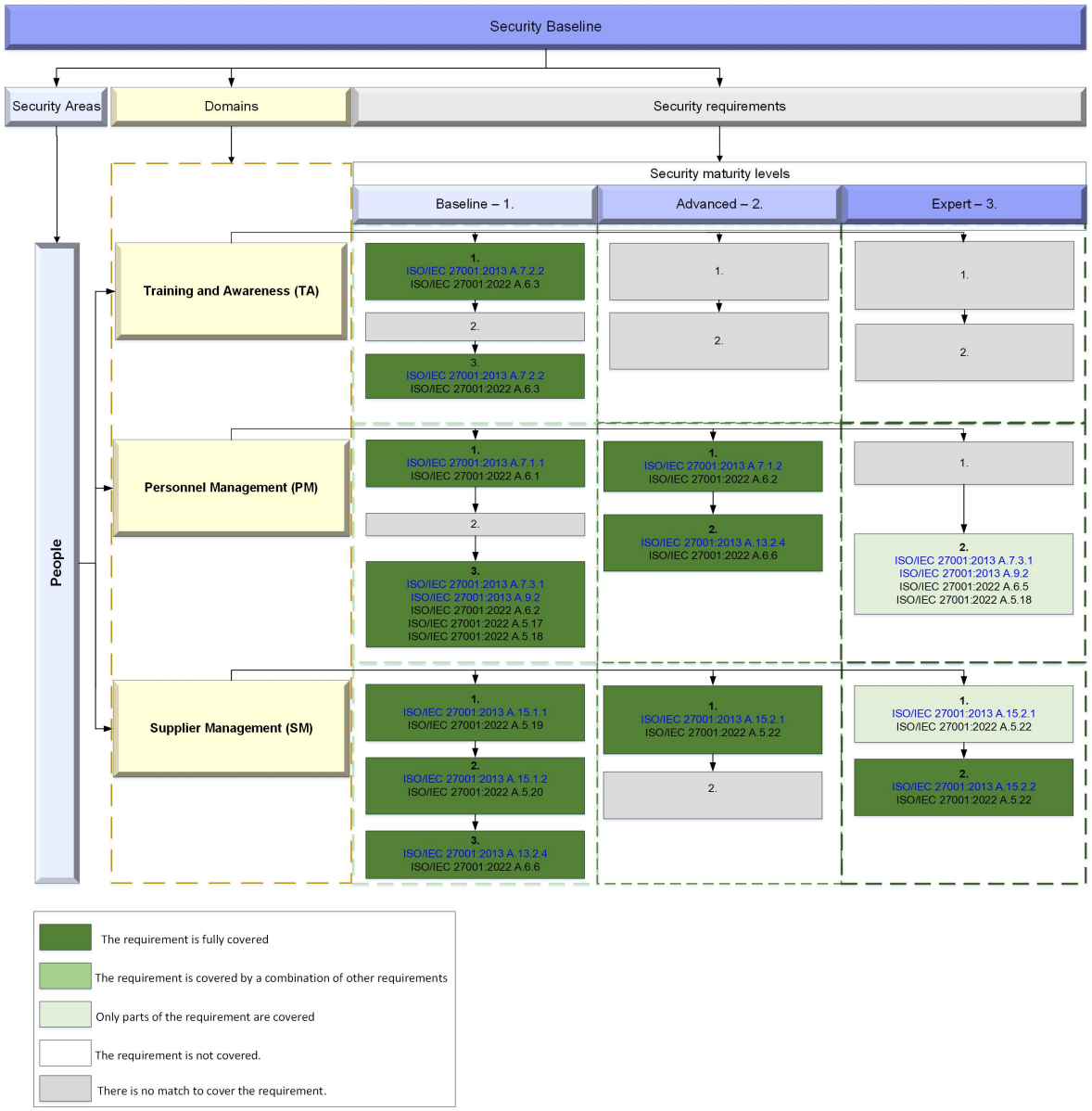

Figure 6. Taxonomy of Security Baseline requirements for people area mapped by different ISO standards.

Both ISO/IEC 27001:2013 and ISO/IEC 27001:2022 emphasize the requirements for dealing with threats (Figure 7). ISO/IEC 27001:2013 requires organizations to assess Information Security risks; identify assets, threats, and vulnerabilities; and assess the likelihood and impact of incidents. It specifies the need for a risk treatment plan to address identified risks and provides controls and guidelines for managing Information Security risks. ISO/IEC 27001:2022 introduces dedicated annexes on risk management, aligning with the ISO 31000 standard for a broader risk management perspective. It emphasizes the establishment of a risk management process within the organization and provides more detailed requirements for risk assessment and treatment.

ISO/IEC 27001:2013 includes a dedicated annex, 16, emphasizing the importance of managing and responding to Information Security incidents. Moreover, it provides control A.16.1.5, which specifies the requirements for reporting security incidents and ensuring proper documentation, analysis, and response to incidents. ISO/IEC 27001:2022 features a specific annex, 8, emphasizing the importance of a systematic and proactive method for handling Information Security incidents.

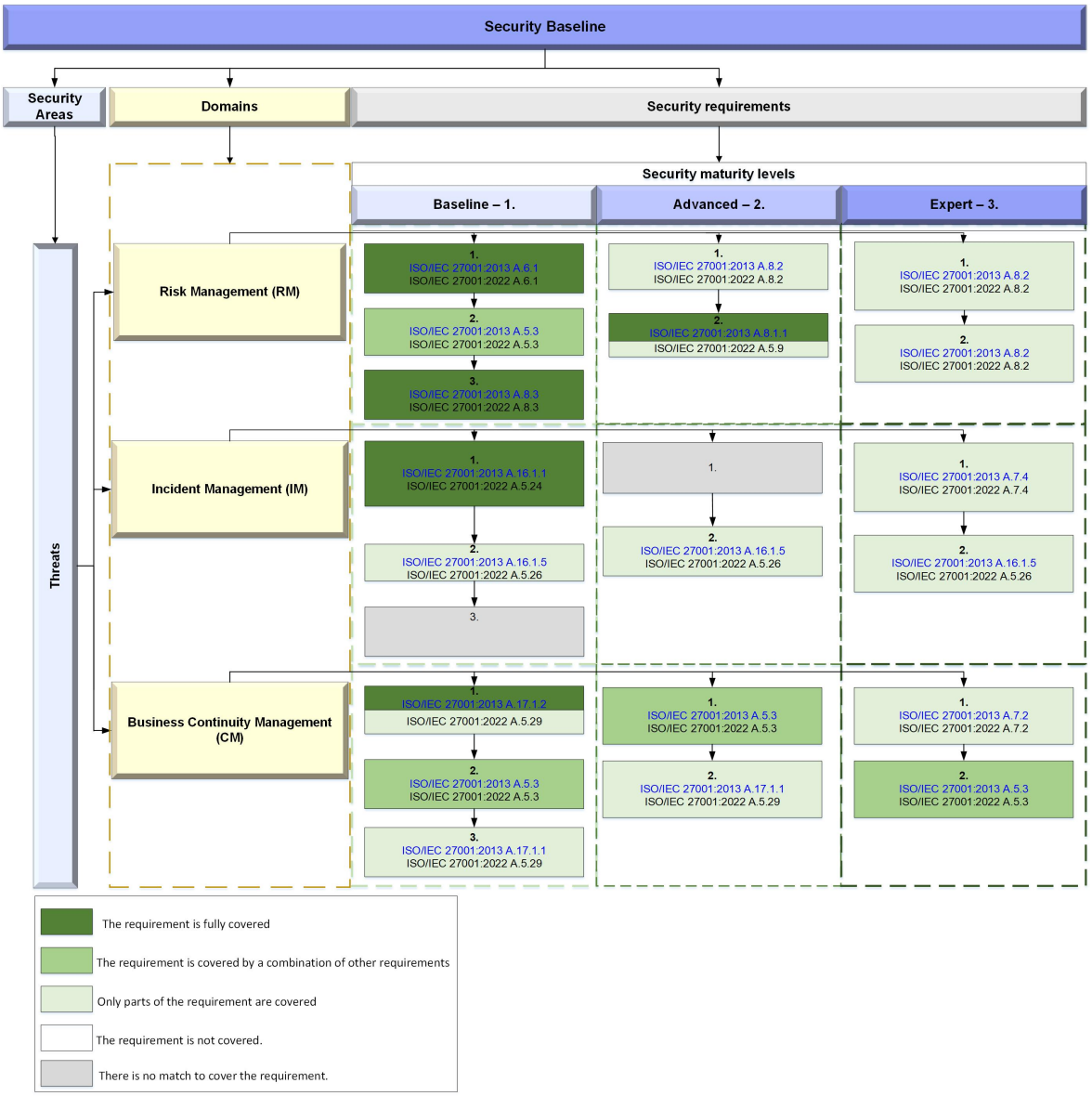

Figure 7. Taxonomy of Security Baseline requirements for threats area mapped by different ISO standards.

Both ISO/IEC 27001 include access management requirements (Figure 8), but they are intentionally high-level and flexible to accommodate a wide range of organizational needs and to align with more specialized standards and frameworks that provide detailed guidance on access control. Organizations are expected to tailor their access management controls based on their unique circumstances and risks.

The security requirements in the domain Cryptography are almost fully covered by the ISO/IEC 27001:2013 and ISO/IEC 27001:2022 standards. Only CR requirements 2.2 and 3.2 are missing matches. Control A.10.1.2, known as "Key Management", under the ISO/IEC 27001:2013 standard, is within the area of cryptography and serves as a crucial element in fortifying operational security by implementing effective cryptographic key management practices. The purpose of this control is to ensure the protection of cryptographic keys against any unauthorized modifications, disclosures, or losses. Implementing secure procedures during all stages of the key's life—including its creation, exchange, storage, change, retirement, archiving, and recovery—achieves this. A.10.1.2 is closely connected to operational security and plays a crucial role in ensuring the confidentiality, authenticity, and integrity of encrypted data. It serves as a fundamental component for establishing

secure business processes and transactions, with a particular emphasis on cryptographic features. The careful administration of cryptographic keys, as described in A.10.1.2, plays a crucial role in strengthening the security measures and resilience of an organization's information systems and data. By using cryptography in the right way, organizations may protect the availability, integrity, authenticity, and confidentiality of their information assets in accordance with the requirements of ISO 27001:2022, Annex A 8.24.

Security requirements for access management mostly do not have a match in the ISO/IEC 27001 standards. Controls A.9.1.2, A.9.1.1, A.9.2.1, and A9.2.3 all belong to the "Access Control" subdomain of the A.9 domain in ISO/IEC 27001:2013. This subdomain is labeled "Access Control". These controls lay forth the rules and principles that must be followed in order to effectively manage and limit access to information and information processing facilities.

In ISO 27001:2022, the procedures for obtaining access are extensively detailed in Annex A 5.15. This control acts as a preventative measure, aiding organizations in managing risk by enhancing their intrinsic ability to limit access to information and assets. A.5.15 explicitly stipulates that access permissions and any subsequent alterations thereof should adhere to a predefined set of business and Information Security standards.

As can be seen from Figure 9, just the requirements for MC 1.2 and MC 2.2 are fully covered by NIS 2 articles 7 and 20. The rest of the requirements for the security policy management commitment and mandate are not covered at all or cover only parts of it (i.e., MC 3.2). It is important to note that the majority of the requirements in the Regulatory and Privacy domain are fully or partly covered by various GDPR articles.

The Critical Entities Resilience Directive (CER) article 15 provides a description of the specific oversight arrangements that are applicable to critical entities of particular significance to Europe. However, CER.15 does not match the requirements in the Regulatory and Privacy domain.

NIS 2 articles 25, 21, and 33 fully cover the requirements for baseline training and awareness (TA 1.1), partly for TA 2.1 and SM 2.1, while the rest of the requirements are not covered at all (Figure 10). The Critical Entities Resilience (CER) Directive, also known as the European Union (EU) Directive 2018/1148 on the resilience of critical entities, addresses people-related requirements just in the context of enhancing the overall resilience of critical infrastructure and services. That is why the requirements for the people area are not covered by this directive.

Requirements for risk management (Figure 11) are covered partly by NIS 2 articles 21 and 22 (RM 1.2, RM 2.1, RM 2.2, and RM 3.2), while just RM 3.1 is covered in combination with other requirements. Only the majority of incident management (IM) requirements are covered fully by NIS 2's various parts. However, NIS 2 articles 9 and 16 cover only parts of the requirements for business continuity management (CM 1.1 and CM 2.2), while the rest of these requirements are not covered.

Article 9 of NIS 2 focuses on incident response and recovery capabilities. Operators of essential services and digital service providers are mandated to develop and sustain incident response and recovery capabilities. Business continuity is implicitly linked to incident response and recovery in NIS 2 article 9 because the ability to recover from incidents and maintain service continuity is a core aspect of business continuity management. Organizations subject to NIS 2 must have plans and measures in place to respond to incidents effectively, mitigate their impact, and ensure the continuity of their essential services or digital services.

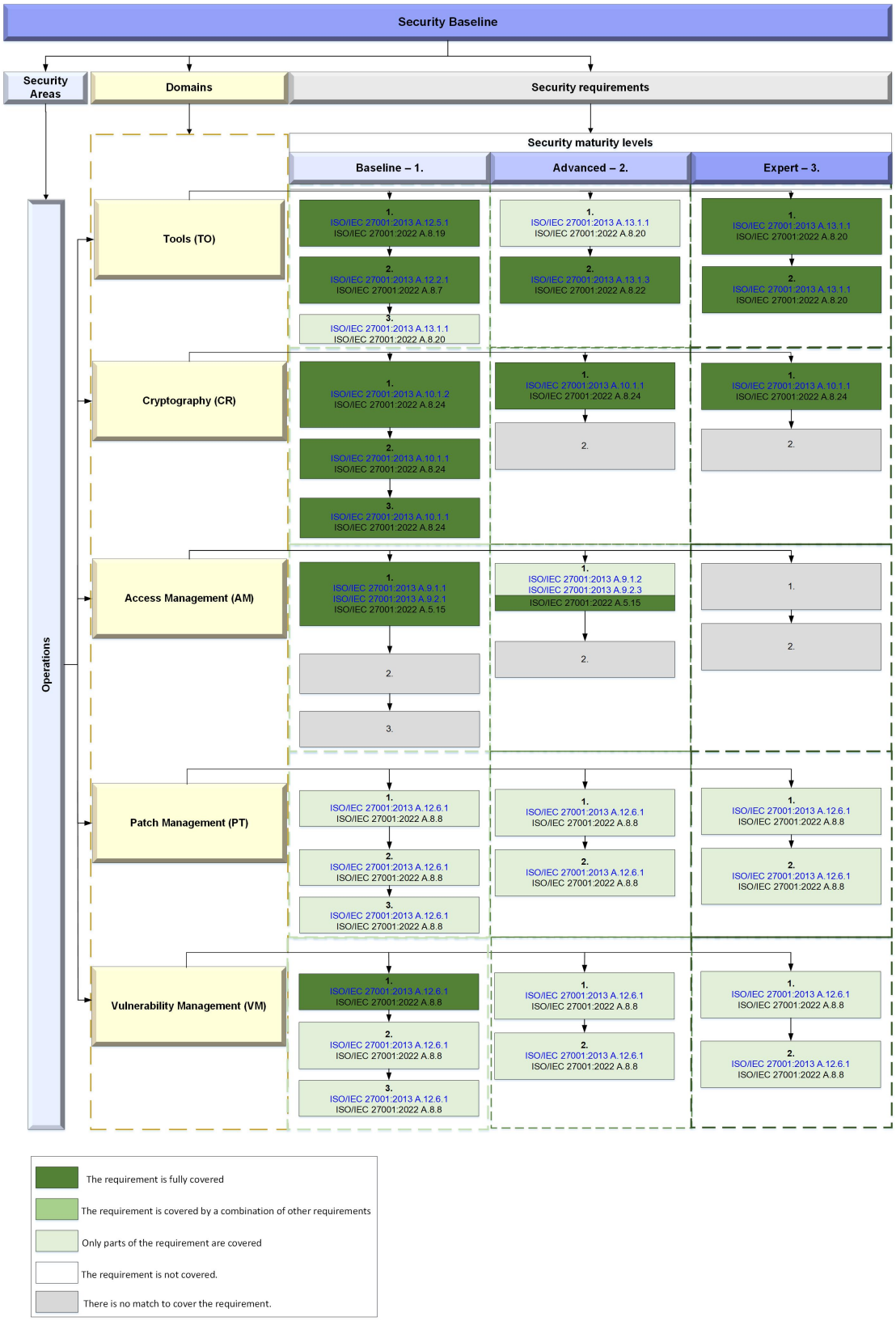

Figure 8. Taxonomy of Security Baseline requirements for operations area mapped by different ISO standards.

Figure 9. Taxonomy of Security Baseline requirements for policy area mapped by different legislation.

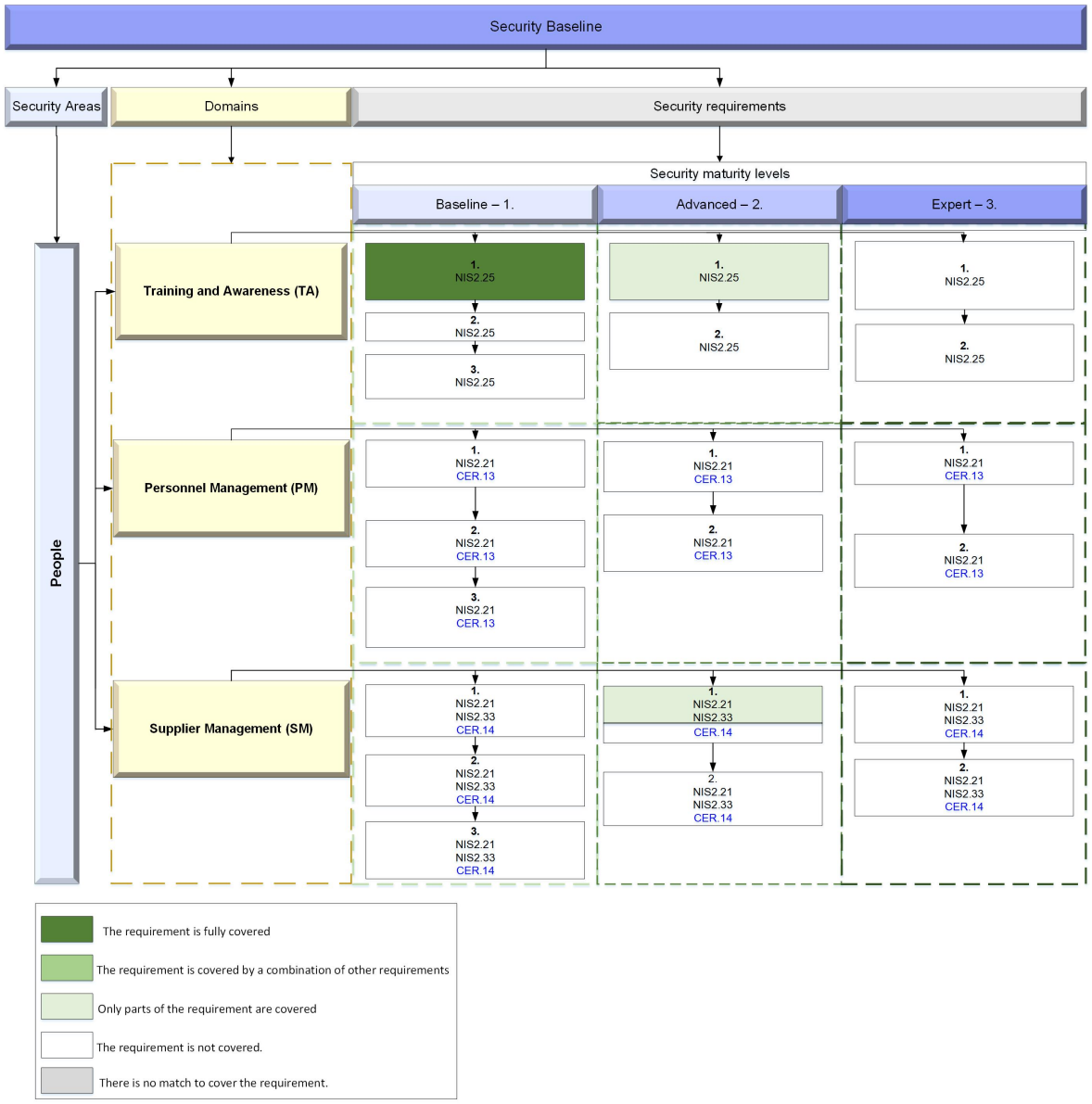

Figure 10. Taxonomy of Security Baseline requirements for people area mapped by different legislation.

Article 16 of NIS 2 outlines specific security requirements for digital service providers. They must take appropriate and proportionate security measures to manage risks to the security of their services, including risks to their systems and data. It covers not just incident prevention but also strategies to guarantee the continuity and availability of digital services. It also reinforces the importance of including continuity planning within the broader context of cybersecurity measures taken by digital service providers to protect their services.

The security area for operations lacks coverage of the security requirements across security legislation (Figure 12). Only requirements such as AM 1.1 for access management, PT 1.1 for patch management, and VM 1.2 for vulnerability management are fully covered by NIS 2 articles 21 and 12, while the rest of the requirements are not covered or are covered only partly. It is worth mentioning that requirement CR 1.1 for cryptography is covered partly by the GDPR article 32, which underscores the importance of implementing security measures to protect personal data and cryptography, specifically data encryption.

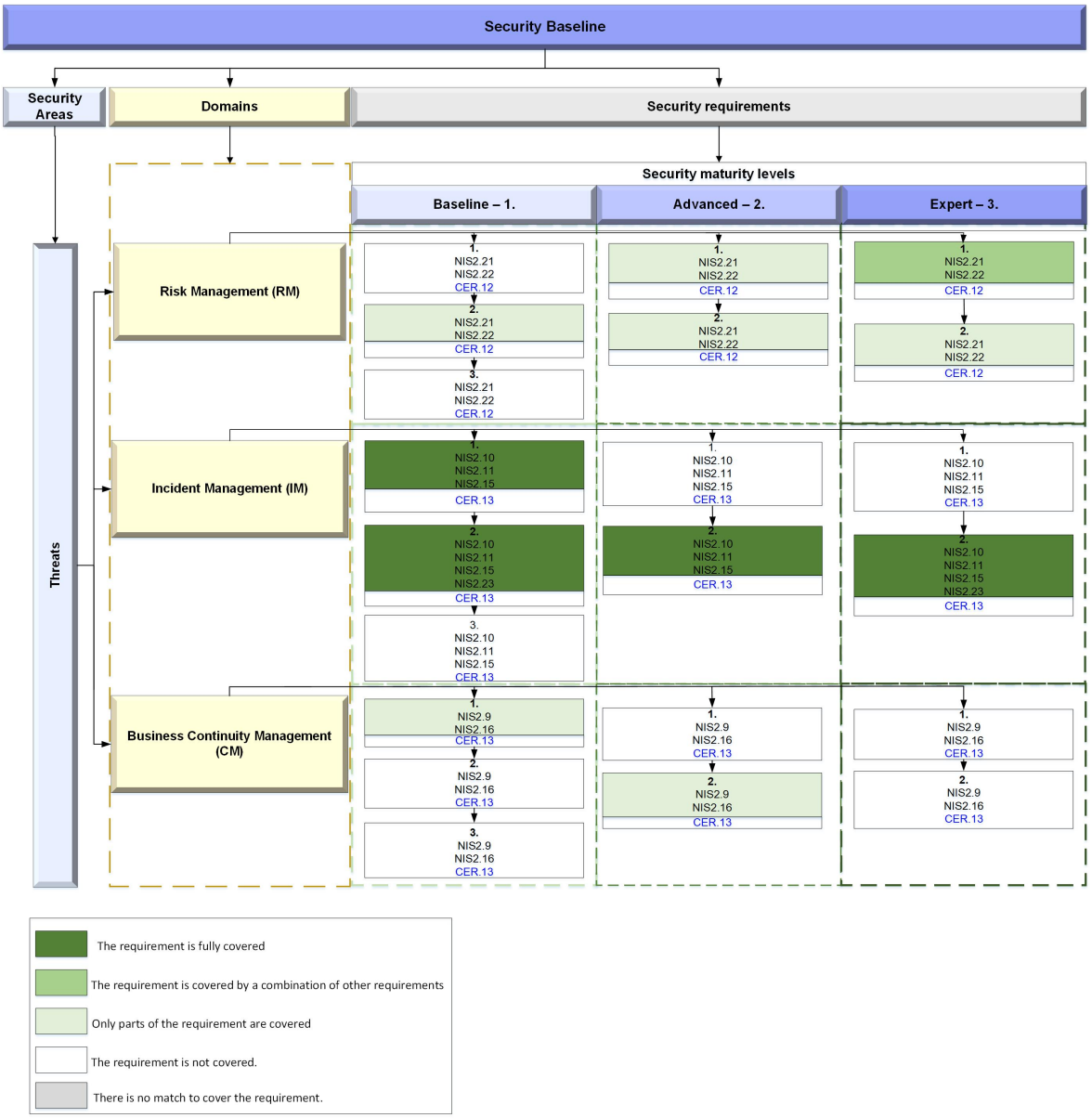

Figure 11. Taxonomy of Security Baseline requirements for threats area mapped by different legislation.

The Center for Internet Security (CIS) Controls, often referred to as the Critical Security Controls, offers a collection of best practices and recommendations to bolster an organization's defense against cyber threats. These guidelines are tailored to assist organizations in safeguarding their digital assets and data. Specifically, CIS Control 3.7 delivers detailed technical advice on securing email and web browser systems. This control can serve as a valuable resource for organizations to refine their security protocols, guaranteeing robust defenses against email and web-related vulnerabilities. By aligning their policies with the control, organizations can establish a strong defense against cyberattacks targeting these attack vectors. Due to this, only the SP 1.1 and SP 2.2 requirements (see Figure 13) are fully covered by CIS 3.7, while the majority of the requirements for the security policy area are not covered at all.

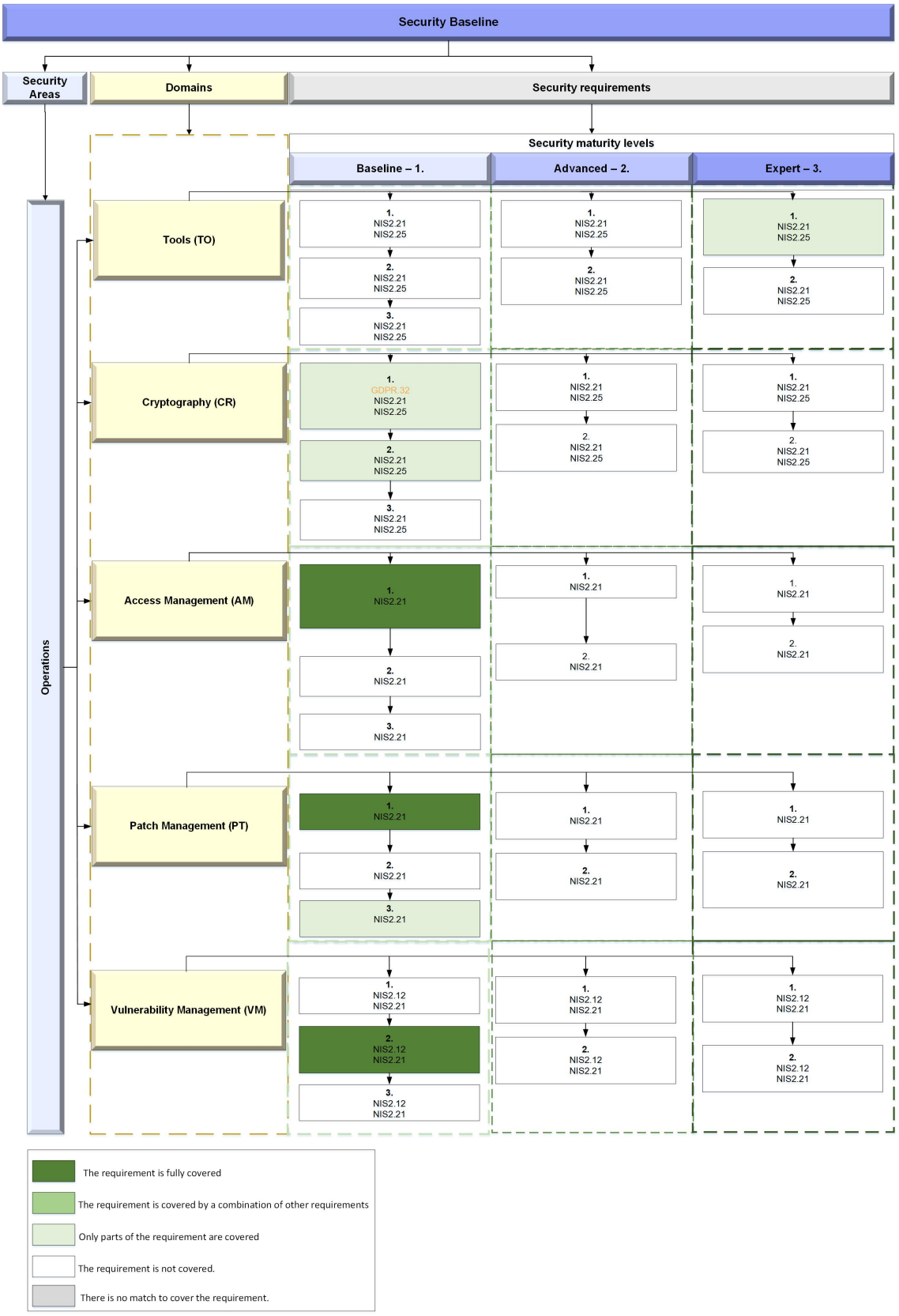

Figure 12. Taxonomy of Security Baseline requirements for operations area mapped by different legislation.

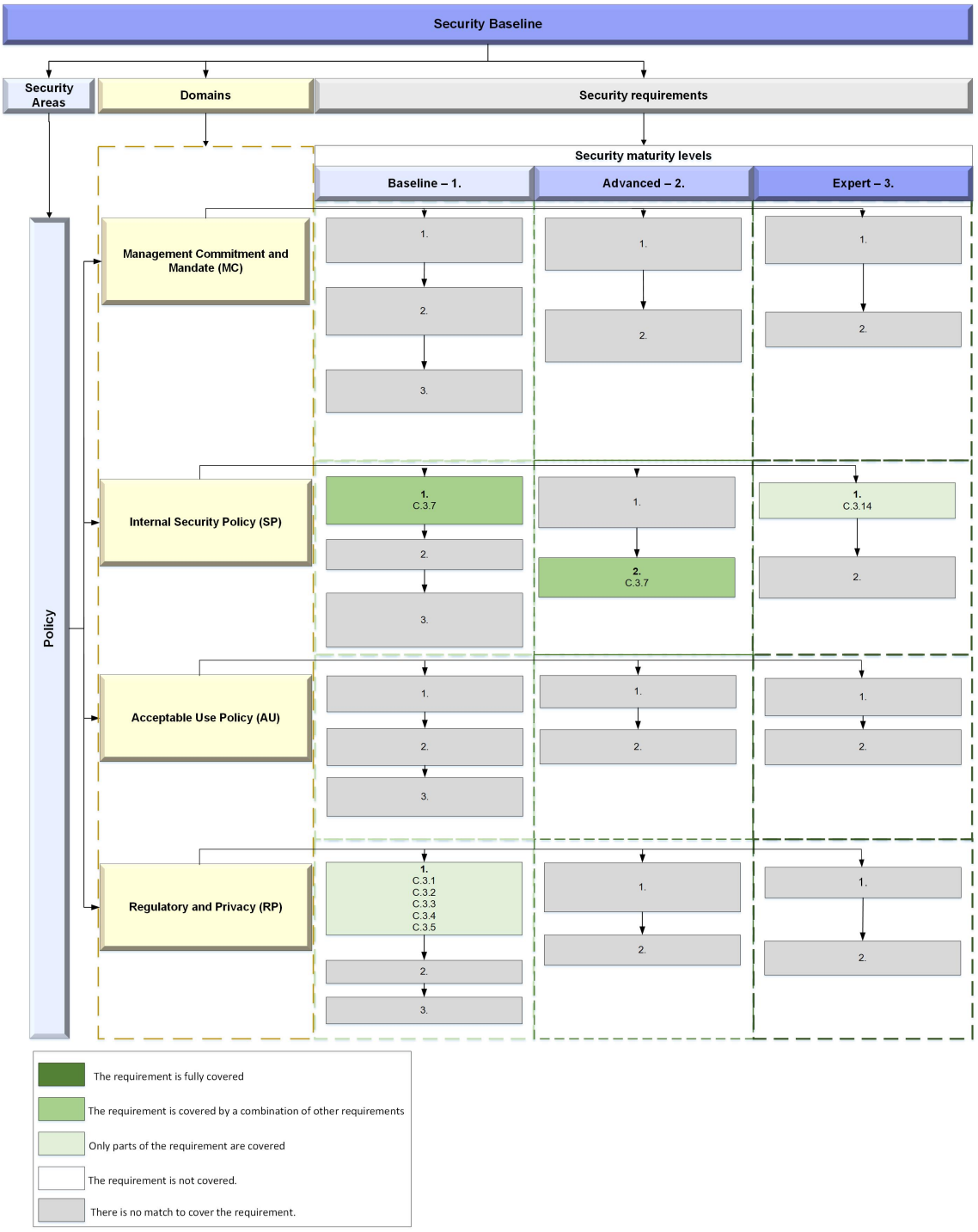

Figure 13. Taxonomy of Security Baseline requirements for policy area mapped by critical security controls.

CIS Control 14, also known as "Security Awareness and Training", focuses on the importance of educating and training personnel to be aware of and respond effectively to cybersecurity risks and threats. This control emphasizes the human element in cybersecurity and the role of people in defending against cyberattacks (Figure 14). Other requirements for the people lack security controls or even do not have any match from this point of view.

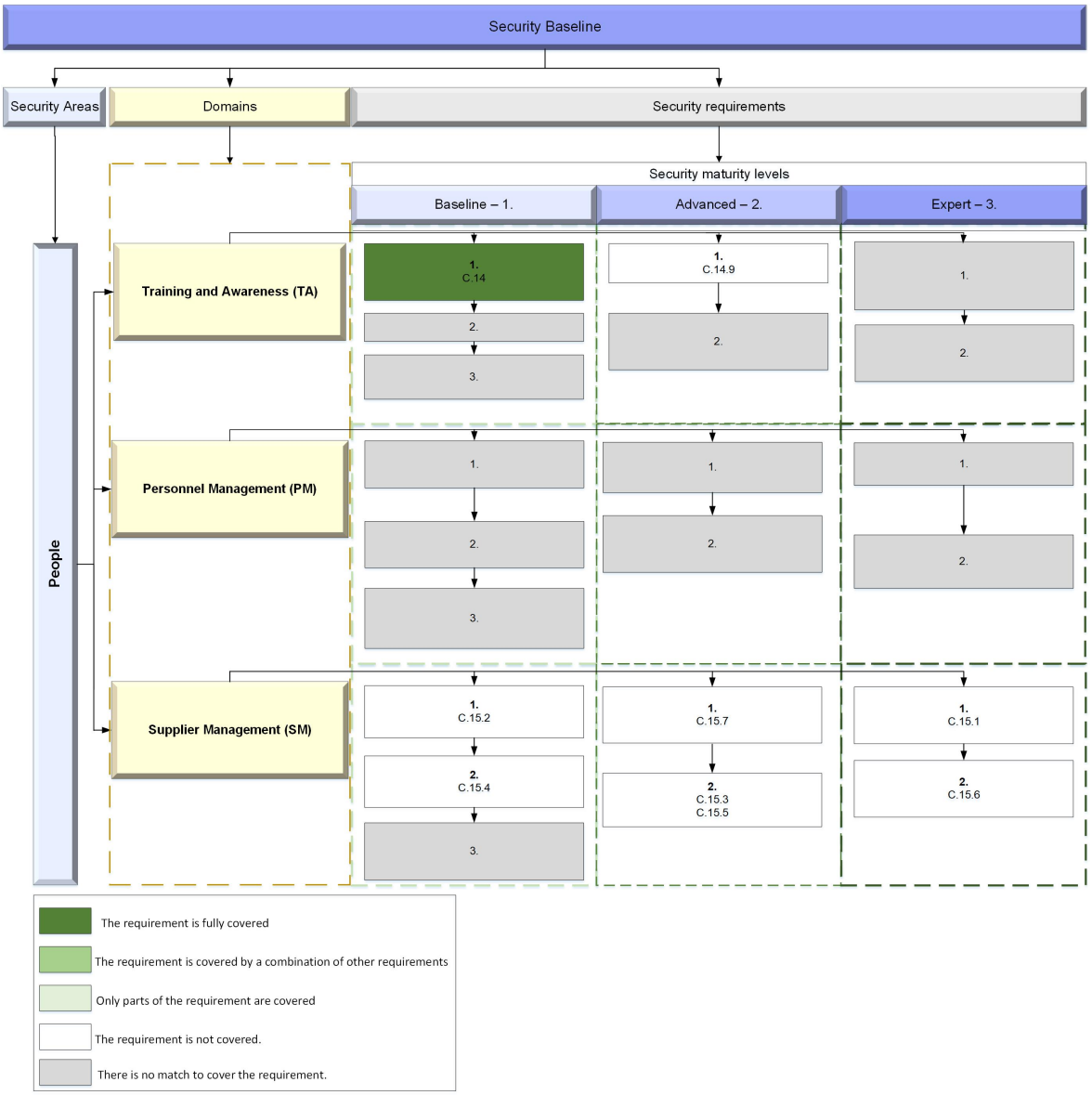

Figure 14. Taxonomy of Security Baseline requirements for people area mapped by critical security controls.

Looking at Figure 15, it is very clear that there is a wide gap in security controls for threat management. Only parts of the RM 2.1, 2.2; IM 1.1, 2.1, 2.2; and CM 1.3, as well as CM 3.1, requirements are covered by several CIS controls. CIS Controls 1.1 through 1.5 are foundational controls that are closely related to risk management in cybersecurity. They help organizations identify and mitigate risks associated with devices, software, configurations, vulnerabilities, and administrative privileges. CIS Control 17 (and its parts 17.1 and 17.6) is closely related to incident management within the broader context of cybersecurity. It provides guidance on establishing an effective incident response plan, detecting and classifying incidents, and executing response actions such as containment, eradication, recovery, and forensics analysis. CIS Control 11 primarily focuses on the security of network devices, and its implementation directly contributes to business continuity by reducing the risk of network outages, DoS attacks, unauthorized access, and other disruptions.

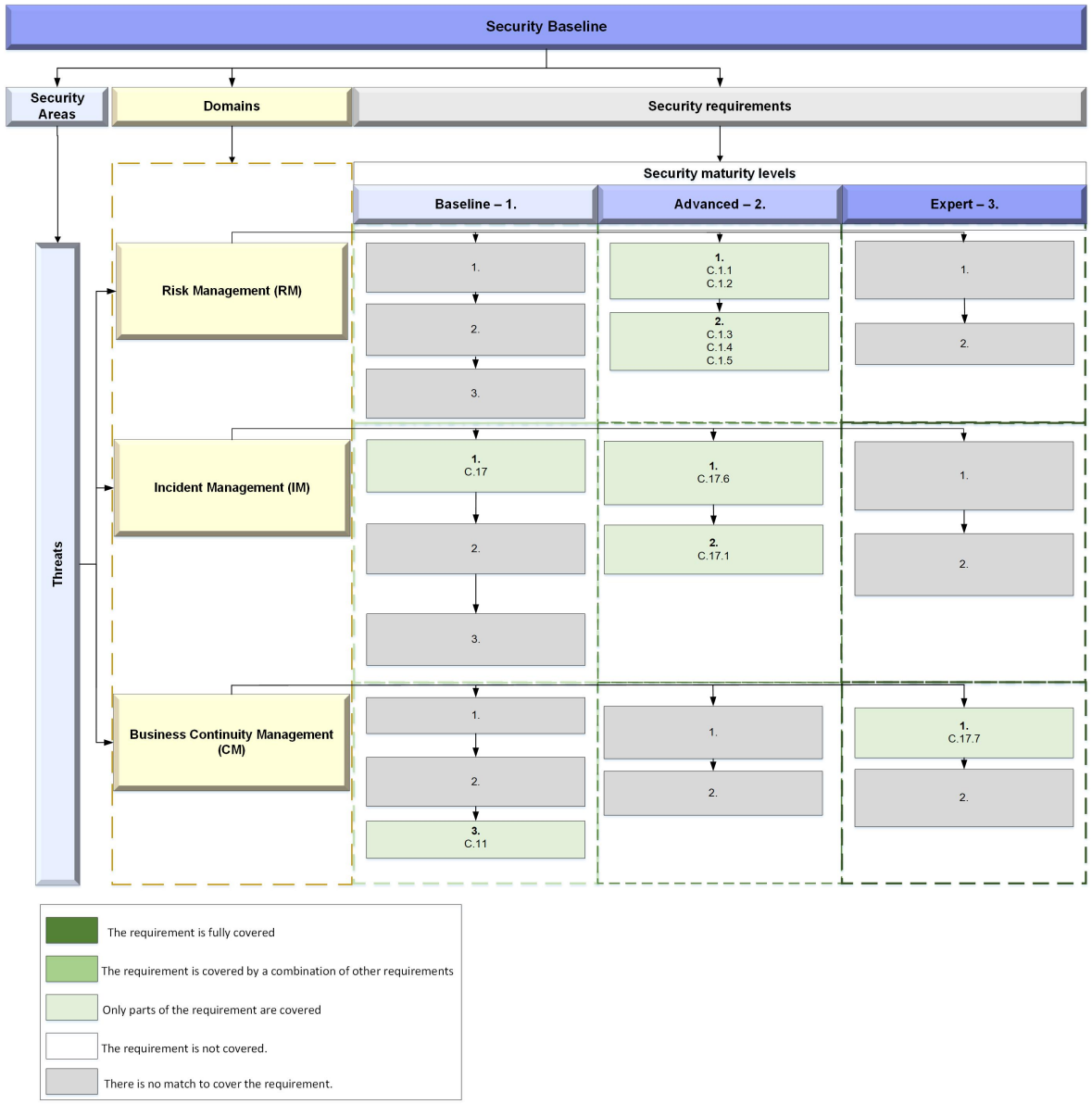

Figure 15. Taxonomy of Security Baseline requirements for threats area mapped by critical security controls.

CIS Controls 2.1–2.7 and Control 12.7 highlight the importance of using security tools and technologies to support security operations (Figure 16). These tools help security teams manage hardware and software assets, continuously assess vulnerabilities, control administrative privileges, maintain secure configurations, monitor audit logs, protect email and web browsers, and secure software applications. Other requirements for the operations security area are covered partly or do not have a match at all.

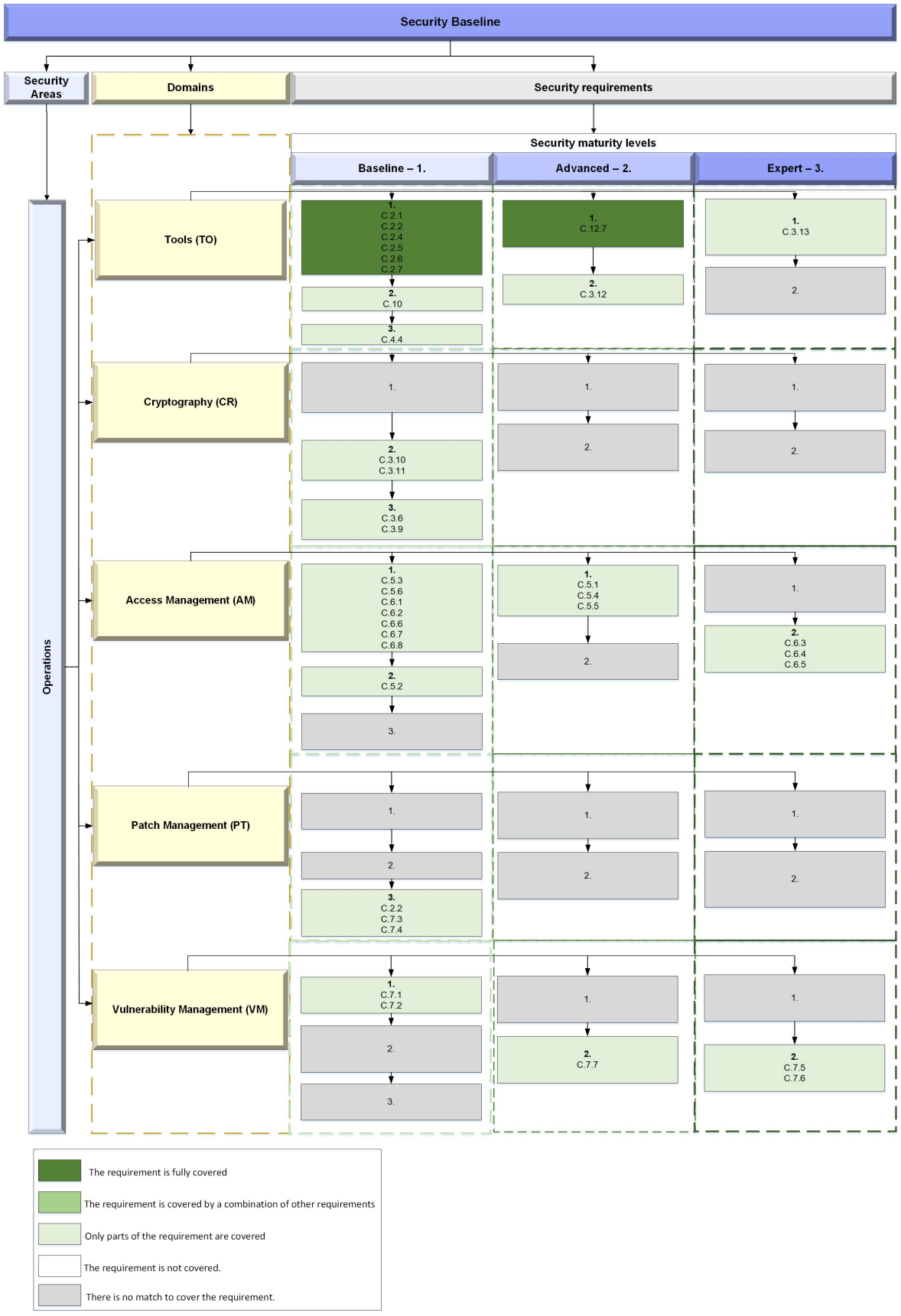

Figure 16. Taxonomy of Security Baseline requirements for operations area mapped by critical security controls.

5. Analysis of the Results

The data set, which was used during the process of methodological mapping, has undergone a restructuring process aimed at optimizing its suitability for subsequent analytical endeavors. Figure 17 shows the distribution of the coverage across various legislation for cybersecurity. The term "coverage" is employed to convey the extent to which each requirement is addressed, utilizing a scale that ranges from '0' to '3', where '0' signifies no coverage, '1' denotes partial coverage, '2' indicates combined coverage, and '3' represents full coverage.

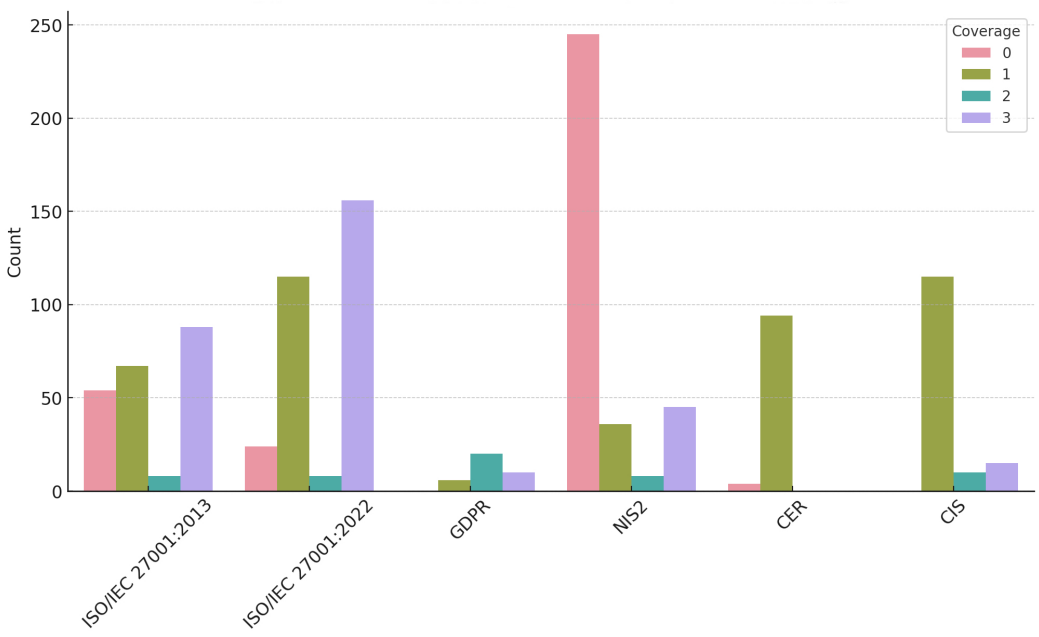

Figure 17. Distribution of coverage across different standards, directives, and regulations.

Figure 17 shows the distribution of coverage across various legislation for cybersecurity, using a qualitative score from 0 to 3, where 0 signifies no coverage, 1 denotes partial coverage, 2 indicates combined coverage, and 3 represents full coverage. Taking the average of a qualitative score is a common practice in research, particularly in the field of cybersecurity. This is because it can be difficult to quantify the effectiveness of cybersecurity legislation, and qualitative scores provide a way to compare different pieces of legislation on a common scale. When taking the average of a qualitative score, it is important to consider the following:

- The reliability of the scoring system. The scoring system should be well-defined and consistently applied.
- The number of items being scored. The average will be more representative if there are a large number of items being scored.
- The variability of the scores. If the scores are highly variable, the average may not be a good measure of central tendency.

In the case of Figure 17, the qualitative score is based on a well-defined scoring system and is applied to a large number of items (i.e., the different requirements in each piece of legislation). Additionally, the scores are not highly variable, as most pieces of legislation have a coverage score of one or two. Therefore, it is reasonable to take the average of the qualitative scores in Figure 17. The summary statistics provide a comprehensive overview of the results:

- NIS 2 is the most common standard, appearing 334 times in the compliance framework of the Security Baseline;

- The coverage has values ranging from 0 to 3, with an average of approximately 1.31. This suggests that the average requirement is partly covered in the Security Baseline;
- NIS 2 article 21 appeared most frequently (128 times) in coverage of the requirements;
- NIS 2 standard has a high frequency of full coverage (3) and also a considerable number of requirements that are not covered at all (0);
- The ISO/IEC 27001:2022 standard has a significant number of fully covered requirements (3) and very few that are not covered (0);
- Certain compliance levels, such as 'RP1.1', 'RP1.2', and 'MC1.1', have a considerable number of requirements that are fully covered (3), while others, such as 'MC1.3' and 'MC1.2', have a significant number of requirements that are not covered at all (0).

The average coverage for each of the analyzed security legislation is as follows: GDPR-2.11; ISO/IEC 27001:2022—1.98; ISO/IEC 27001:2013—1.60; CIS—1.29; CER—0.96; and NIS 2—0.56. This suggests that, on average, the GDPR standard has the highest coverage, while the NIS 2 standard has the lowest coverage.

When looking at the average coverage for each compliance level, a wide range of values can be seen. Some compliance levels, such as 'TA1.1' and 'AM1.1', have high average coverages, while others, such as 'CR3.2' and 'TA2.2', have an average coverage of 0, indicating that they do not meet any of the requirements. These insights can be useful for identifying which standards and compliance levels are best at meeting the requirements and where improvements may be needed.

Figure 18 presents the list of the Security Baseline requirements according to their coverage.

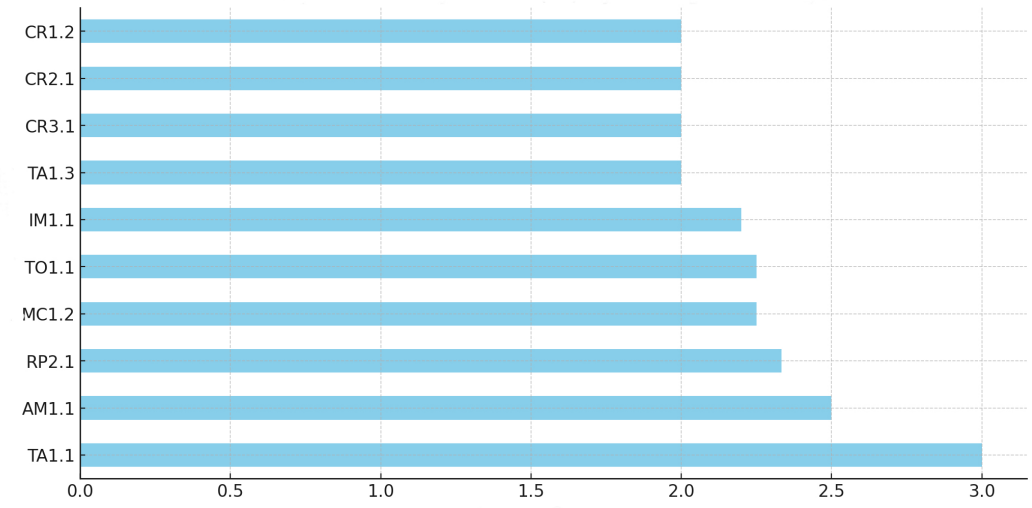

Figure 18. Top 10 Security Baseline requirements by their coverage.

These results highlight which security requirements tend to have high coverage (such as 'TA1.1' and 'AM1.1') and which ones tend to have low coverage (such as 'CR3.2' and 'TA2.2'). Figure 18 shows the average qualitative score for each cybersecurity requirement, where a higher score indicates better coverage. The results show that the following requirements have high coverage:

- TA1.1: Implement a vulnerability management program.
- AM1.1: Use access control mechanisms to control access to systems and data.
- MC1.2: Monitor information systems and networks for security events.
- TA1.3: Respond to security incidents in a timely and effective manner.

The following requirements have low coverage:

- CR2.1: Conduct risk assessments to identify and prioritize cybersecurity risks.
- CR3.2: Implement a security awareness and training program.

- TA2.2: Implement and maintain a configuration management program.
- RP2.1: Regularly review and update security policies and procedures.

As explained above, taking the average of a qualitative score is a common practice in research, particularly in the field of cybersecurity. This is because it can be difficult to quantify the effectiveness of cybersecurity legislation, and qualitative scores provide a way to compare different pieces of legislation on a common scale. These requirements are covered mostly in comparison with other requirements by the standards, directives, or regulations that are presented in Figure 19.

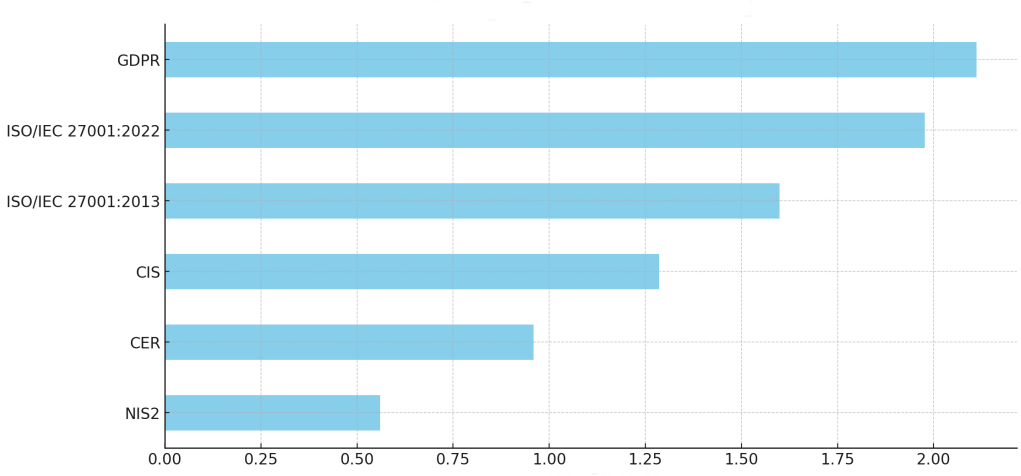

Figure 19. Distribution of coverage per different legislation.

It is clear that GDPR has the highest average coverage, indicating that it tends to fully meet the requirements, while NIS 2 has the lowest average coverage, suggesting that it often does not meet the requirements or only partially meets them. This analysis can be beneficial for organizations to understand which standards and compliance levels are best suited to their needs and where they might need to focus their efforts to improve their security practices.

ISO/IEC 27001:2022 is a standard for Information Security Management (ISMS), while the General Data Protection Regulation (GDPR) is a regulation in the European Union (EU) that sets out rules on the protection of personal data. Although ISO/IEC 27001:2022 and the GDPR are different in nature, there is a significant overlap between the two frameworks. Both frameworks require organizations to implement a number of measures to protect data, such as:

- Conducting risk assessments to identify and prioritize security risks;
- Implementing appropriate security controls to mitigate those risks;
- Monitoring and reviewing security controls on an ongoing basis;
- Providing training on security awareness to employees.

Both ISO/IEC 27001:2022 and the GDPR require organizations to have a process in place for responding to security incidents. The following are some specific examples of the overlap between ISO/IEC 27001:2022 and the GDPR:

- ISO/IEC 27001:2022 Control A.12.6.1 requires organizations to implement access control mechanisms to control access to information systems and data. This is similar to article 25 of the GDPR, which requires organizations to implement appropriate technical and organizational measures to protect personal data.
- ISO/IEC 27001:2022 control A.13.1.1 requires organizations to implement measures to detect and report security incidents. This is similar to article 33 of the GDPR, which requires organizations to notify the supervisory authority within 72 h of becoming aware of a personal data breach.

- ISO/IEC 27001:2022 control A.8.2.1 requires organizations to implement measures to protect the confidentiality of information. This is similar to article 32 of the GDPR, which requires organizations to implement appropriate technical and organizational measures to protect the confidentiality of personal data.

The overlap between ISO/IEC 27001:2022 and the GDPR makes it logical to compare the two frameworks. By understanding the similarities and differences between the two frameworks, organizations can develop more effective compliance strategies. In addition to the above reasons, there are a number of other reasons why it is useful to compare ISO/IEC 27001:2022 and the GDPR:

- Many organizations are subject to both ISO/IEC 27001:2022 certification and GDPR compliance. By comparing the two frameworks, organizations can streamline their compliance efforts.
- Organizations that are not subject to the GDPR can still benefit from implementing ISO/IEC 27001:2022. ISO/IEC 27001:2022 is a comprehensive framework for managing Information Security risks, and it can help organizations to protect their data from a wide range of threats.
- Comparing ISO/IEC 27001:2022 and the GDPR can help organizations to identify areas where they can improve their security posture. For example, organizations may find that they need to implement additional security controls in order to meet the requirements of the GDPR.

It is worth noting that this is a high-level analysis and further in-depth analysis could provide more specific insights. For example, one could look at the coverage of specific requirements across different standards and compliance levels or analyze the data at a more granular level, such as examining coverage for individual mapping codes. Instead, the examination of the co-occurrence of full coverage (3) in different standards were performed. This can give an idea of how often different standards are fully meeting the requirements together (Figure 20).

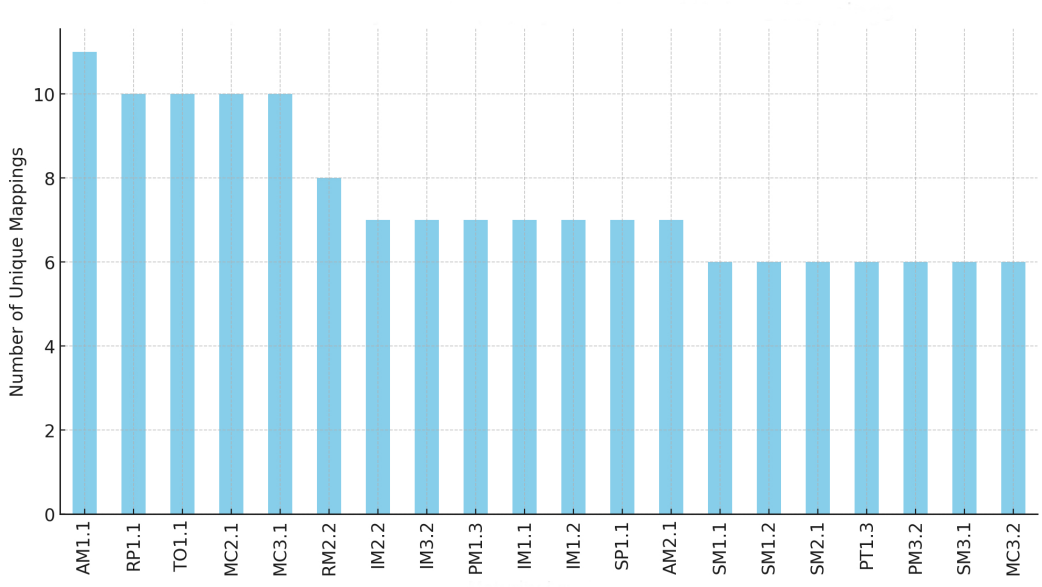

Figure 20. Top 20 Security Baseline requirements by the number of unique mappings associated with legislation.

The results in Figure 20 provide the list of the Security Baseline requirements by the number of their unique mappings associated with the various legislation. This provides an idea of which maturity levels are associated with a wider variety of requirements. For example, 'MC1.1', 'MC1.2', and 'MC1.3' are associated with a large number of unique mappings, suggesting that these maturity levels have a wide range of requirements. Conversely,

requirements such as 'PT1.1' and 'PT1.2' correlate with fewer distinct mappings, suggesting a more limited scope of requirements. Such insights are valuable for organizations as they shed light on the complexities of different compliance levels, allowing them to strategize their efforts more effectively.

Going deeper, the correlation matrix of the coverage levels for different legislation has been analyzed (Figure 21). A correlation matrix will serve as a key to understanding how often different legislation has full coverage or another level of coverage together with each other. The programming language called Python with a popular library in it named *pandas* was used during this research. This software was useful for further data analysis and manipulation.

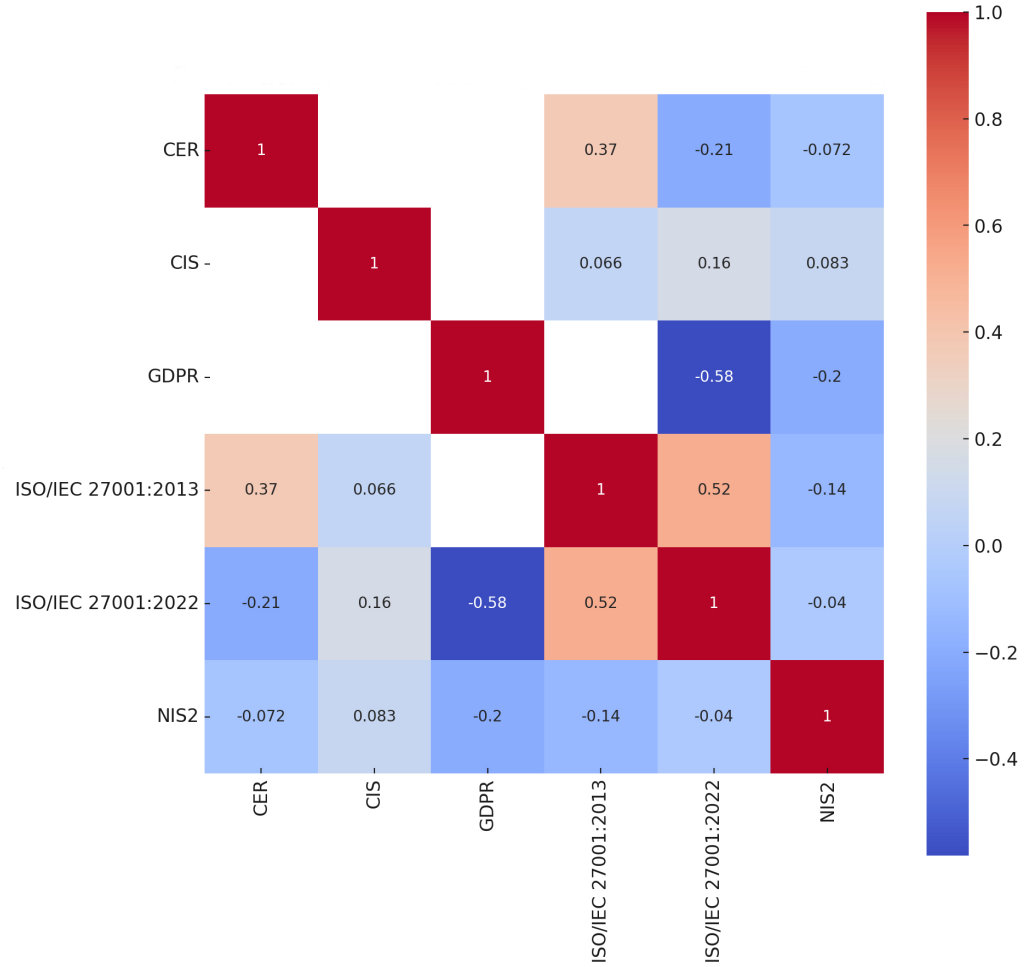

Figure 21. Correlation matrix of the coverage levels for different legislation.

The analysis and mapping were done using the "Matrix working on model.csv" as a CSV (comma-separated values) document prepared by the expert assessment of the GEANT SIG-ISM group members.

```
#importing data
import pandas as pd
df = pd.read_csv('Matrix_working_on_model.csv')
df.head()
```

Python was also used to analyze the data from the experiment and create figures and tables to visualize the results. This helped to communicate the results of the experiment in a clear and concise way. The following piece of the programming code describes how to

create a list called mapping columns. If the word 'Mapping' is in the column name, it is added to the list. Similarly, using the index, the name of the 'coverage' column that has the highest value is defined. Some columns in this table are about "Mapping", and some are about "Coverage". Such code will precisely find out which "Coverage" column has the highest value and the name of that "Coverage" column and its corresponding "Mapping" column.

```
mapping_columns = [col for col in df.columns if 'Mapping' in col]
max_coverage_values = [df[col].max() for col in coverage_columns]
max_coverage_index = max_coverage_values.index(max(max_coverage_values))
max_mapping_column = mapping_columns[max_coverage_index]
max_coverage_column = coverage_columns[max_coverage_index]
max_mapping_column, max_coverage_column
```

After that, the rearrangement (pivoting) of the data from the restructured data table has been done. In this new format (pivot data), each unique value in the ID (requirement) column of the original table becomes a row. Each unique value in the Standard column of the original table becomes a new column in pivot data.

```
# Pivot the data
pivot_data = restructured_data.pivot_table(index='ID', columns='Standard',
values='Coverage', aggfunc='mean')
# Creating correlation matrix
correlation_matrix = pivot_data.corr()
# Ploting
plt.figure(figsize=(10, 10))
sns.heatmap(correlation_matrix, annot=True, cmap='coolwarm', square=True)
plt.title('Correlation Matrix of Coverage Levels for Different Standards')
plt.show()
```

A creation of the heatmap using the sns (which typically stands for Seaborn, which is a visualization library) has been completed. A heatmap is a grid where each cell's color represents a value, and, here, the values are the correlation values from the correlation matrix. The proposed model reorganizes some data to see how "Coverage" values vary for different "Standards" for each "ID". It then checks how each "Standard" relates to every other "Standard" and displays these relationships as a colorful heatmap.

Two Python libraries, networkx (abbreviated as nx), which helps in creating, manipulating, and studying networks and graphs, and itertools, which provides tools to create iterators for efficient looping, were included as well. The mappings string, splitting it by commas, and then generating all possible pairs (combinations) of these split values were initialized. For example, if mappings were "A,B,C", then the pairs would be ("A", "B"), ("A", "C"), and ("B", "C"). The proposed model defines a function to create a network/graph from a table (dataframe). For each row in the table, it checks the 'Mapping' and 'Coverage' columns. If the 'Mapping' value is valid, and the 'Coverage' is greater than zero, it adds connections (edges) to the graph between the items in 'Mapping', weighted by the 'Coverage' value.

```
import networkx as nx
import itertools

def create_graph(df, mapping_col, coverage_col):
    G = nx.Graph()
    for _, row in df.iterrows():
        mappings = row[mapping_col]
        coverage = row[coverage_col]
        if pd.notna(mappings) and coverage > 0:
            for pair in itertools.combinations(mappings.split(','), 2):
                if G.has_edge(*pair):
                    G.edges[pair]['weight'] += coverage
                else:
                    G.add_edge(*pair, weight=coverage)
    return G
G = create_graph(df, 'Mapping', 'Coverage')
nx.draw(G, with_labels=True)
```

After creating the graph, the code visualizes it (see Figure 21).

The heatmap shows the correlation matrix of the coverage levels for different standards. Each cell in the matrix represents the correlation coefficient between two standards. The correlation coefficient is a value between -1 and 1 that represents the degree to which two variables are linearly related. Mathematically, the correlation coefficient is derived from the covariance of the two variables, normalized by the product of their standard deviations. This normalization ensures that the correlation coefficient is dimensionless and bounded between -1 (a perfect negative linear relationship) and 1 (a perfect positive linear relationship). A value of 0 indicates no linear correlation. The bounds of -1 and 1 arise because the correlation coefficient essentially measures the quality of the linear approximation to the data; any data set perfectly aligned along a line (either ascending or descending) will achieve these extremal values, while data sets that do not exhibit a linear trend will result in values closer to 0. In this context, a positive correlation indicates that when one standard has a high coverage level, the other standard also tends to have a high coverage level. A negative correlation, on the other hand, indicates that when one standard has a high coverage level, the other standard tends to have a low coverage level. Looking at the heatmap, we can see some interesting patterns:

- Figure 21 shows a correlation coefficient of -0.58, which indicates a moderately negative correlation between the GDPR and ISO/IEC 27001:2022. This means that organizations that are certified to ISO/IEC 27001:2022 are slightly less likely to be compliant with the GDPR. It is important to note that correlation does not equal causation. Just because there is a negative correlation between the GDPR and ISO/IEC 27001:2022 does not mean that ISO/IEC 27001:2022 certification causes organizations to be less compliant with the GDPR. There are a number of other factors that could explain the negative correlation. For example, it is possible that organizations that are certified with ISO/IEC 27001:2022 are more likely to be in industries that are subject to stricter GDPR requirements. This could mean that they are more likely to be audited by GDPR regulators and, as a result, be more likely to be found to be non-compliant.
- There is also a strong positive correlation between ISO/IEC 27001:2013 and ISO/IEC 27001:2022, suggesting that these two standards often meet the requirements together as well.
- There is a moderate negative correlation between NIS 2 and other standards, such as ISO/IEC 27001:2013, ISO/IEC 27001:2022, and the GDPR. This could suggest that when NIS 2 has a high coverage level, these other standards tend to have a low coverage level, and vice versa.

The GDPR has the highest average coverage; other standards also have significant coverage and might be more relevant depending on the context. For example, ISO/IEC 27001:2022 also has high average coverage and might be more suitable for organizations that are more focused on Information Security Management Systems.

Finally, it is worth noting that the best approach to ensure compliance is often to adhere to multiple standards, as different standards cover different aspects of security and privacy. A combination of standards can provide a more holistic coverage of the Security Baseline requirements.

6. Discussion

It is worth noting that this is a high-level analysis, and further in-depth analysis that could provide more specific insights into compliance with the various legislation and requirements for cybersecurity. For example, one could look at the coverage of specific requirements across different standards (ISO/IEC 27001:2013, ISO/IEC 27001:2022, the GDPR, CER, CIS, NIS 2) and compliance levels, or analyze the data at a more granular level, such as examining coverage for individual mapping codes. The authors' work that has been completed generates research questions such as:

- How can organizations develop tailored compliance roadmaps that consider their unique needs and the identified correlations between standards?
- How can organizations streamline their compliance efforts by understanding which parts of different legislation and standards often meet requirements together?
- How can organizations overcome the challenges and costs of integrating multiple cybersecurity standards?

The correlations found between standards might reflect broader industry or regulatory shifts. Engaging with stakeholders—such as policymakers, industry experts, and compliance officers—could elucidate the practical implications and perceptions of these correlations. Based on the findings, future endeavors could focus on developing tailored compliance roadmaps for organizations, considering their unique needs and the identified correlations between standards.

This paper would help organizations understand how well the Security Baseline covers the requirements of the existing standards, and it would also help organizations identify any gaps in the Security Baseline. This is because the Security Baseline is based on expert judgment and uses the NREN as the main assumption. However, the Security Baseline is a valuable tool for organizations that are trying to improve their security posture.

The research questions could be used to develop a more in-depth analysis of the issues and proposed solutions. For example, the researchers could conduct interviews with policymakers, industry experts, and compliance officers to understand the practical implications and perceptions of the correlations between standards. The researchers could also develop a case study of an organization that has successfully integrated multiple cybersecurity standards.

Given the moderate negative correlation between NIS 2 and other standards, it would be valuable to investigate why this standard is distinct. Does NIS 2 have fundamentally different requirements, or does its application diverge in certain industry contexts? Even when the relevance of standards varies depending on the context? The organization could be segmented in the future by size, industry, or region to assess if correlations persist or if new patterns emerge.

7. Conclusions and Future Work

The results highlighted strong and moderate correlations between certain standards for security. Future studies could delve deeper into the reasons for these correlations. Understanding the overlapping principles and requirements between these standards could provide insights into how and why they complement or oppose each other. Our analysis provides a snapshot of the correlation matrix at a certain time. However, standards evolve, and it would be insightful to observe how these correlations change over time,

especially as updates to standards are released. A granular breakdown of the requirements for each standard could shed light on specific areas of overlap or divergence. For example, understanding which parts of the legislation, such as the GDPR and ISO/IEC 27001:2022, often meet requirements together can help organizations streamline their compliance efforts.

This study investigated the correlations between different cybersecurity standards and their Security Baselines. Our findings suggest that some standards are more compatible than others and that adhering to multiple standards can provide more holistic coverage of security requirements. However, there are also challenges and costs associated with integrating multiple standards, especially those with negative correlations. The findings of this study have implications for organizations that are trying to comply with multiple cybersecurity standards. Organizations should carefully consider the correlations between different standards when developing their compliance strategies. Organizations should be aware of the challenges and costs associated with integrating multiple standards.

The current research sheds light on the correlations between different standards; there is a vast landscape of potential explorations. Ensuring compliance is an evolving challenge, and understanding the dynamics between different standards can provide invaluable insights to navigate this complex domain.

Future research could explore these challenges and costs in more detail, as well as empirically test the effectiveness of adhering to multiple standards in reducing security breaches or non-compliance penalties. Moreover the engagement with industry experts, regulatory bodies, and organizations to gather insights on practical challenges and best practices in standard compliance, while also evaluating how emerging technologies, such as AI and blockchain, impact the adherence to and evolution of cybersecurity standards, ensuring organizations remain at the forefront of compliance innovation. Additionally, future studies could delve deeper into the reasons for the correlations observed in this study. Understanding the overlapping principles and requirements between these standards could provide insights into how and why they complement or oppose each other.

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

Funding: This research received no external funding.

Data Availability Statement: The data presented in this paper are available on request from the corresponding author. The data are not publicly available due to the project not being completed.

Acknowledgments: © 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.

Conflicts of Interest: The authors declare no conflict 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 2023).
2. European Commission. Network and Information Security Directive. Nis2 Directive, 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 10 August 2023).

3. Wang, L.; Near, J.P.; Somani, N.; Gao, P.; Low, A.; Dao, D.; Song, D. Data capsule: A new paradigm for automatic compliance with data privacy regulations. In Proceedings of the Heterogeneous Data Management, Polystores, and Analytics for Healthcare: VLDB 2019 Workshops, Poly and DMAH, Los Angeles, CA, USA, 30 August 2019; Revised Selected Papers 5; Springer: Cham, Switzerland, 2019; pp. 3–23.
4. Caruccio, L.; Desiato, D.; Polese, G.; Tortora, G. GDPR compliant information confidentiality preservation in big data processing. *IEEE Access* **2020**, *8*, 205034–205050. [CrossRef]
5. Renaud, K.; Shepherd, L.A. How to make privacy policies both GDPR-compliant and usable. In Proceedings of the 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), Glasgow, UK, 11–12 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–8.
6. GÉANT Association. GÉANT Projects. Available online: https://geant.org/projects/ (accessed on 10 August 2023).
7. Harris, N.; Janmaat, I.; Pribolsan, V.; Schmidt, M.; Ziegler, J. Deliverable D8.2 Security Baseline for NRENs. Available online: https://geant.org/projects/gn4-3-deliverables/ (accessed on 7 March 2020).
8. Mishev, A.; Bidikov, V.; Gerdes, M.; Lauter, D.; Kahl, C.; Grigaliunas, S. Deliverable D8.12 GÉANT Community Requirements for Business Continuity Planning. Available online: https://geant.org/projects/gn4-3-deliverables/ (accessed on 7 May 2021).
9. Office of Cybersecurity, Energy Security, and Emergency Response. Cybersecurity Capability Maturity Model (C2M2). Technical Report 2.1, U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, June 2022. Available online: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2 (accessed on 12 August 2023).
10. Nicole Harris, Ivar Janmaat, Vlado Pribolsan, Michael Schmidt, Jule Ziegler. Security Baseline. A Security Maturity Model for NRENs. Available online: https://security.geant.org/baseline/ (accessed on 1 March 2021).
11. ISO/IEC JTC 1/SC 27. ISO/IEC 27001:2022 Information Security Management Systems— Requirements. Standard 3, International Organization for Standardization, October 2022. Available online: https://www.iso.org/standard/27001 (accessed on 13 August 2023).
12. Cole, M.D.; Schmitz, S. The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape. Available online:. (accessed on 12 August 2023). [CrossRef]
13. Roy, P.P. A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. In Proceedings of the 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), Durgapur, India, 7–8 February 2020; pp. 1–3. [CrossRef]
14. National Institute of Standards and Technology. Standard. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations. Available online: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (accessed on 12 August 2023).
15. Mussmann, A.; Brunner, M.; Breu, R. Mapping the State of Security Standards Mappings. In *Wirtschaftsinformatik (Zentrale Tracks)*; University of Innsbruck: Innsbruck, Austria, 2020; pp. 1309–1324. [CrossRef]
16. Enescu, S. A Comparative Study on European Cyber Security Strategies. *Redefining Community Intercult. Context* **2020**, *9*, 277–282.
17. Sulistyowati, D.; Handayani, F.; Suryanto, Y. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *JOIV Int. J. Inform. Vis.* **2020**, *4*, 225–230. [CrossRef]
18. Aliyu, A.; Maglaras, L.; He, Y.; Yevseyeva, I.; Boiten, E.; Cook, A.; Janicke, H. A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Appl. Sci.* **2020**, *10*, 3660. [CrossRef]
19. Saqib, N.; Germanos, V.; Zeng, W.; Maglaras, L. Mapping of the Security Requirements of GDPR and NISD. *EAI Endorsed Trans. Secur. Saf.* **2020**, *7*, 1–18. [CrossRef]
20. Hamdani, S.W.A.; Abbas, H.; Janjua, A.R.; Shahid, W.B.; Amjad, M.F.; Malik, J.; Murtaza, M.H.; Atiquzzaman, M.; Khan, A.W. Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons. *ACM Comput. Surv.* **2021**, *54*, 57:1–57:36. [CrossRef]
21. Murino, G.; Ribaudo, M.; Romano, S.P.; Tacchella, A.; Armando, A.; Colajanni, M. OT Cyber Security Frameworks Comparison Tool (CSFCTool). In Proceedings of the ITASEC, Rome, Italy, 20–24 June 2021; pp. 9–22.
22. Ammi, M.; Adedugbe, O.; Alharby, F.; Benkhelifa, E. Taxonomical Challenges for Cyber Incident Response Threat Intelligence: A Review. *Int. J. Cloud Appl. Comput.* **2022**, *12*, 1–14. [CrossRef]
23. Venizelos, C. Security Controls and Security Standards: Correlations and Synergies—ProQuest. Available online: https://www.proquest.com/openview/41c8b8bb54909ad0d09d4667ba0ec93d/1?pq-origsite=gscholar&cbl=2026366&diss=y (accessed on 9 August 2023).
24. Wicklund Lindroth, O. *Cybersecurity Ontology—The Relationship between Vulnerabilities, Standards, Legal and Regulatory Requirements*; Stockholm University: Stockholm, Sweden, 2022.
25. Domínguez-Dorado, M.; Cortés-Polo, D.; Carmona-Murillo, J.; Rodríguez-Pérez, F.J.; Galeano-Brajones, J. Fast, Lightweight, and Efficient Cybersecurity Optimization for Tactical–Operational Management. *Appl. Sci.* **2023**, *13*, 6327. [CrossRef]
26. Alshar'e, M. Cyber Security Framework Selection: Comparision of NIST and ISO27001. *Appl. Comput. J.* **2023**, *3*, 245–255. [CrossRef]
27. Bella, G.; Castiglione, G.; Santamaria, D.F. An automated method for the ontological representation of security directives. *arXiv* **2023**, arXiv:2307.01211.
28. Castiglione, G.; Santamaria, D.F.; Bella, G. An ontological approach to compliance verification of the NIS 2 directive. *arXiv* **2023**, arXiv:2306.17494.

29. Mierzwa, S.; Klepacka, A. Practical Approaches and Guidance to Small Business Organization Cyber Risk and Threat Assessments. *J. Strateg. Innov. Sustain.* **2023**, *18*, 29.
30. Djebbar, F.; Nordström, K. A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access* **2023**, *11*, 85315–85332. [CrossRef]