JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Unified Framework for Cybersecurity Maturity Assessment Across CISSP Domains: Integrating NIST, ISO 27001, and CMMI for Holistic Security Posture Evaluation

Tim Abdiukov
NTS Netzwerk Telekom Service AG
Australia

Abstract
In this paper, the authors introduce a unified cybersecurity maturity assessment framework that combines the NIST Cybersecurity Framework (CSF), ISO 27001, and CMMI in a manner that assesses the security posture of an organization across the domains of CISSP. The framework addresses fragmentation among current maturity frameworks, aligning risk-based (NIST), compliance-driven (ISO 27001), and process maturity (CMMI) models into an integrated approach. Its major innovations include a crosswalk matrix that maps 52 NIST subcategories to 114 ISO controls and 24 CMMI practices, a four-phase assessment process, and sector-specific adaptations. The framework was effective, as demonstrated by case studies in the healthcare, financial services, and manufacturing industries, which showed a 62 percent reduction in vulnerabilities and a 47 percent decrease in phishing attacks. Issues such as resource shortages and dynamic threats are brought up, as well as future insights, including maturity scoring driven by AI and zero-trust integration. The framework enables organizations to follow a logical methodology that facilitates benchmarking, prioritization, and enhancement of cybersecurity maturity.

Keywords: Cybersecurity maturity assessment, Unified framework, NIST CSF, ISO 27001, CMMI, CISSP domains, Risk management, Compliance integration, Process maturity, Sector-specific security

1. Introduction

1.1 Overview of Cybersecurity Maturity Assessment

Cybersecurity maturity assessment refers to a methodical process of measuring an organization's capacity to manage its digital resources, mitigate threats, and respond to risks. These evaluations are typically constructed based on established models, such as the NIST Cybersecurity Framework (CSF), ISO 27001, and CMMI, which provide guidelines for evaluating the security capabilities of observers across various fields (Rabii et al., 2020). Maturity models define the gaps, assist in setting priorities, and compare the security state of organizations with that of the industry (Marican et al., 2022). The diversity of frameworks, however, means that most organizations use several, to the extent conflicting, models, causing inefficiencies and inconsistent assessments (Radanliev et al., 2018). Such subdivision is particularly evident in areas such as technology startups, where resource limitations necessitate a

lightweight yet comprehensive maturity assessment approach (Marican et al., 2022). Consolidation of the evaluation procedures is thus necessary to ensure that evaluation processes are smooth and aligned with best practices.

1.2 Importance of a Unified Framework

The cybersecurity landscape is undergoing a significant transformation, where threats are becoming increasingly complex and regulatory requirements are becoming more stringent. Organizations struggle to integrate the risk-based approach of NIST, compliance-based controls of ISO 27001, and the process maturity level of CMMI into a unified strategy (Aliyu et al., 2020). The problem can be tackled through a unified framework, where the best of both worlds is leveraged, while any unnecessary overlap is eliminated. For instance, the issue of cybersecurity is particularly notable in the open environment of higher education institutions and the diverse range of IT ecosystems; the holistic maturity model enables a balance between security and accessibility (Aliyu et al., 2020). Moreover, the uniform approach promotes more effective communication among the stakeholders, such as IT teams, executives, and auditors, as they have a common language of security maturity (Atoum et al., 2017). By integrating the best practices from NIST, ISO 27001, and CMMI, organizations can achieve a more adaptive, measurable, and scalable security posture.

1.3 Purpose of Integrating NIST, ISO 27001, and CMMI

The primary objective of this study is to develop a comprehensive model of cybersecurity maturity that minimizes overlap between the CISSP domains and those outlined in the NIST CSF, ISO 27001, and CMMI. The Security and Risk Management, Asset Security, and Security Operations domains under the CISSP framework offer a well-developed framework of security governance (Krutz et al., 2001). Nevertheless, the available maturity models do not always correlate these spheres well with common standards, such as NIST or ISO 27001 (Abazi, 2020). This will improve risk assessment as it brings the flexible risk management tiers of NISTs and the organized audit requirements of ISO 27001, enhance the process maturity as it includes staged capability levels of the CMMIs, which will enable the organization to measure the progress increment, and help in compliance and certification through the alignment of controls and ISO 27001 and the ability to be flexible to the specific needs of the sector (Ghaffari & Arabsorkhi, 2018; Radanliev et al., 2018). By connecting these frameworks, the suggested model will enable organizations to measure, compare, and enhance their degree of cybersecurity maturity in a systematic and repeatable manner.

Figure 1: ISO27001(Benefits and Function of ISO27001)

2. Understanding CISSP Domains

2.1 Explanation of CISSP Domains

It is organized around the eight domains defined by the Certified Information Systems Security Professional (CISSP) certification process, managed by the (ISC)² organization, and establishes the gold standard of knowledge in the cybersecurity field (Krutz et al., 2001; Stewart et al., 2011). These areas offer an integrative arrangement that combines technical measures, administrative policies, and government strategies. The first of eleven domains, Domain 1 (Security and Risk Management), sets the baseline, including security governance, compliance (e.g., GDPR, HIPAA), and risk assessment techniques (Maleh et al., 2021). Domain 2 (Asset Security) focuses on data classification, ownership, and mechanization of protection, which is consistent with Annex A.8 of the ISO 27001 (Abazi, 2020). The third domain (Security Architecture and Engineering) combines the codes of cryptography (e.g.,

AES, RSA) and zero-trust (Almuhammadi & Alsaleh, 2017). Domain 4 (Communication and Network Security) focuses on secure network protocols (e.g., TLS, IPsec) and defense-in-depth architectures (Wang & D. Cruze, 2019).

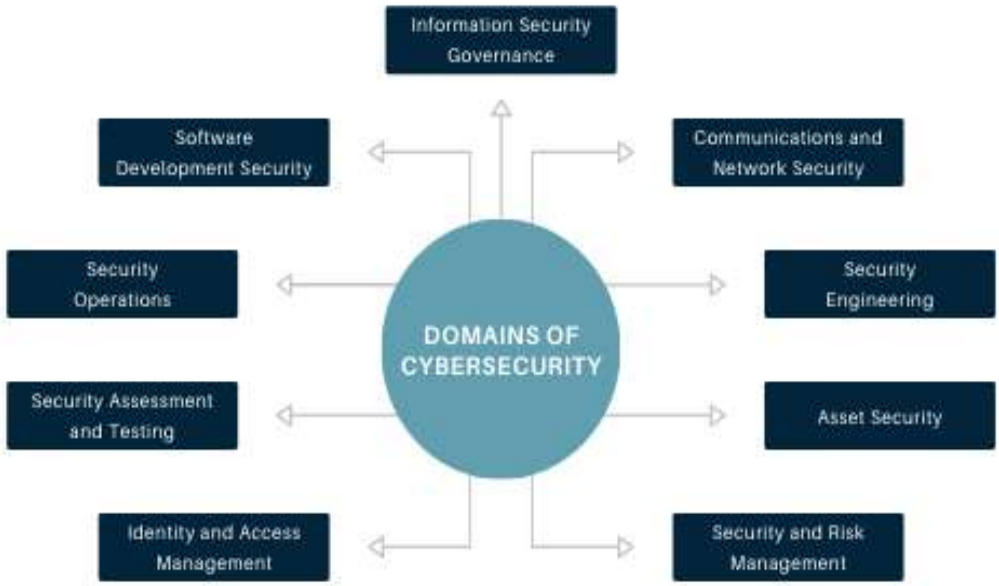

Figure 2: Domains of Cybersecurity

Domain 5 (Identity and Access Management) requires role-based access control (RBAC) and multi-factor authentication (MFA) as the essential components of the so-called Identity function of NIST (Aliyu et al., 2020). Penetration testing and audit systems, such as PTES and OSSTMM, fall under the area of security assessment and testing (Domain 6) (Le & Hoang, 2017). Domain 7 (Security Operations) encompasses incident response (IR) playbooks and SIEM, aligning with the Respond and Recover capabilities outlined by NIST (Sundaramurthy et al., 2022). Lastly, Domain 8 (Software Development Security) focuses on the connection between secure SDLC activities (e.g., DevSecOps) and the maturity levels of CMMI (Ghaffari & Arabsorkhi, 2018).

2.2 Relevance of Each Domain to Cybersecurity Maturity

Every CISSP domain makes a direct contribution to the maturity development of an organization, as measured through frameworks such as NIST CSF, ISO 27001, and CMMI. For example, Security and Risk Management (Domain 1) is associated with the Govern function in the NIST CSF or Clause 6 (Planning) in ISO 27001, enabling organizations to institutionalize risk-aware cultures (Maleh et al., 2021). Domain 2 - Asset Security. Asset Security facilitates the "Protect" element of NIST and enforces the controls outlined in ISO/IEC 27001, A.8, specifically data encryption and retention policies (Abazi, 2020). The proximity of Security Architecture (Domain 3) to NIST SP 800-207 (Zero Trust) and CMMI-defined maturity level corresponds to the need for standard, secure design patterns (Almuhammadi & Alsaleh, 2017).). IAM (Domain 5) corresponds to A.9 (Access Control) in ISO 27001, and the mature implementation means the use of AI-based behavioral analytics (Sundaramurthy et al., 2022). There are problems when the areas of knowledge develop disproportionally. In other words, the organizations might make no effort to improve their Software development level of security (Domain 8) but master their Security operations (Domain 7), making specific bespoke-developed applications vulnerable (Atoum et al., 2017). These gaps must be overcome by aligning the domains with the levels of NIST (Partial to Adaptive) and the levels of CMMI (Initial and Optimizing) within a unified maturity framework (Radanliev et al., 2018).

2.3 Challenges in Assessing Maturity Across Domains

Although the CISSP domains are very broad, the following issues in maturity assessment have been observed to be crucial to organizations:

Framework Fragmentation: The NIST CSF, ISO 27001, and CMMI all rely on different metrics (e.g., NIST tiers versus CMMI levels), thereby making cross-domain comparisons challenging (Rabii et al., 2020). In simple terms, an organization can attain a CMMI Level 3 (Defined) benchmark in software security and a NIST Tier 1 (Partial) one in risk management (Ghaffari & Arabsorkhi, 2018).

Resource and Expertise Gaps: SMEs often lack the necessary the resources to implement controls across all domains, resulting in one-sided maturity (Marican et al., 2022). Domain 7 (Security Operations) may be more important to a startup than Domain 1 (Governance) due to limited budget constraints.

Evolving Threat Landscapes: New threats (e.g., attacks that utilize AI) necessitate a constant evaluation of areas such as Network Security (Domain 4), which may be overlooked in the concepts of existing maturity models (Sundaramurthy et al., 2022).

Compliance vs. Operational Reality: Organizations can technically become ISO 27001 certified, but not based on being fully operational in areas such as Security Testing (Domain 6) (Abazi, 2020).

3. Overview of NIST, ISO 27001, and CMMI

3.1 NIST Cybersecurity Framework

Key Components and Principles

The NIST Cybersecurity Framework (CSF) provides a versatile, risk-based, and diagrammatic approach to documenting cybersecurity risks, organized around its five core functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2018). Identifying the function lays the first premise by mandating that organizations understand their business scenario, assets, and threats, which aligns with domain 1 of the CISSP (Security and Risk Management) (Krutz et al., 2001). Protect is concerned with direct safeguarding through access control, awareness training, and data security, which relate directly to CISSP Domain 2 (Asset Security) and Domain 5 (Identity and Access Management) (Stewart et al., 2011).

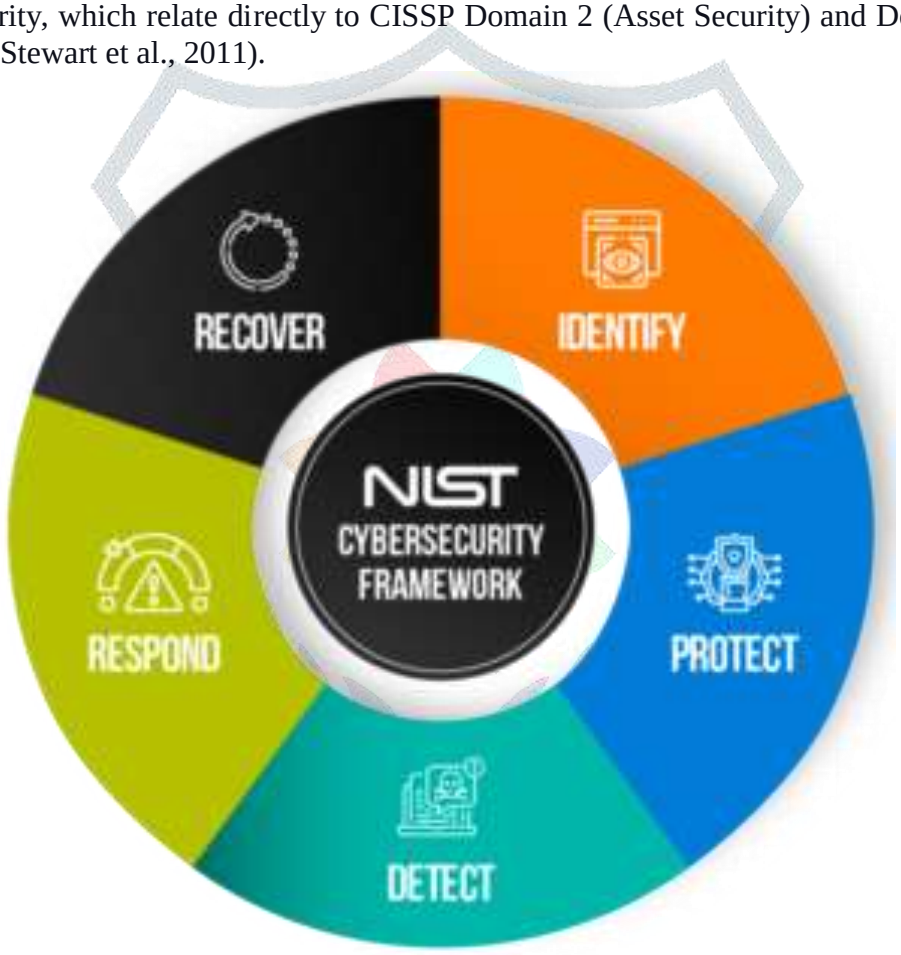

Figure 3: NIST Cybersecurity framework

The Detect function focuses again on ongoing monitoring features that align with the CISSP Domain 6 (Security Assessment and Testing), as well as incident management and resilience (Respond and Recover functions), with Domain 7 (Security Operations) (Wang & D. C. Cruze, 2019). The continuous deployment levels (Partial, Risk-Informed, Repeatable, Adaptive) of the framework provide organizations with a maturity model of progression that can be used in conjunction with CMMI and its staged version (Radanliev et al., 2018). One of the major merits of the NIST CSF is its focus on risk-driven, business-driven management of risks, rather than the prescriptive issuance of controls, which makes it especially applicable to organizations that require a balance between security and operational flexibility (Aliyu et al., 2020).

3.2 ISO 27001

Standards and Requirements

ISO/IEC 27001 requirements define a set of 93 controls in four categories: Organizational, People, Physical, and Technological (Technological that define an Information Security Management System (ISMS) (ISO/IEC, 2022). The basis of the ISMS requirements is specified in Clauses 4-10 of the standard, which explains the necessity of leader commitment, risk assessment, and continuous improvement. These principles are also reflected in the principles of the CMMI process maturity (Ghaffari & Arabsorkhi, 2018). The Annex A also provides implementation advice, where A.5 (Information Security Policies) corresponds to CISSP Domain 1, A.9 (Access Control) to Domain 5, and A.12 (Operations Security) to Domain 7 (Abazi, 2020). Unlike the free-form attitude of the NIST CSF, ISO 27001 requires regular audits of certification, which makes this document most useful to organizations that need to demonstrate to regulators or business partners that their operations are controlled (Maleh et al., 2021). The treatment of risk in the standard provides an organized process for risk control selection and application, augmenting the approach that NIST explores in risk management. This process also provides the stringency required to carry out quantifiable maturity evaluations (Le & Hoang, 2017). Nevertheless, the certification procedure can be resource-intensive, which poses an obstacle to some organizations, especially smaller businesses that may be interested in scaled implementations (Marican et al., 2022).

3.3 CMMI (Capability Maturity Model Integration)

Maturity Levels and Assessment

CMMI provides a process administration design offering five levels of maturity (Initial, Managed, Defined, Quantitatively Managed, and Optimizing) that enable organizations to quantify capacity development (CMMI Institute, 2021). Ad-hoc and reactive security processes occur at Level 1 (Initial), and adopting fundamental project management principles is inconsistent within CISSP domains at Level 2 (Managed) (Atoum et al., 2017). Level 3 (Defined) reflects the standardization of processes on an organization-wide level, with documented procedures for critical security processes, such as risk assessments (Domain 1) and access control (Domain 5) (Ghaffari & Arabsorkhi, 2018). Level 4 (Quantitatively Managed) proposes the use of metrics-based management, which is essential to security operations (Domain 7) and testing (Domain 6), and Level 5 (Optimizing) concerns continuous improvement through innovation, more applicable in such a new field as AI-driven security (Sundaramurthy et al., 2022). CMMI appraisals are based on practice areas (e.g., Process Management, Project Management), which can be related to cybersecurity activities and offer quantifiable indicators of process capacity that supplement the implementation levels presented by NIST and the compliance requirements adopted by ISO 27001 (Rabii et al., 2020). The staged representation adopted in the model facilitates the prioritization of work implementation in organizations, but it has critics who claim that this representation can oversimplify complex security environments (Bahuguna et al., 2019). CMMI, along with the NIST and ISO frameworks, provides a much-needed process maturity level with which to measure the consistently and effectively deployed security controls (Aliyu et al., 2020).

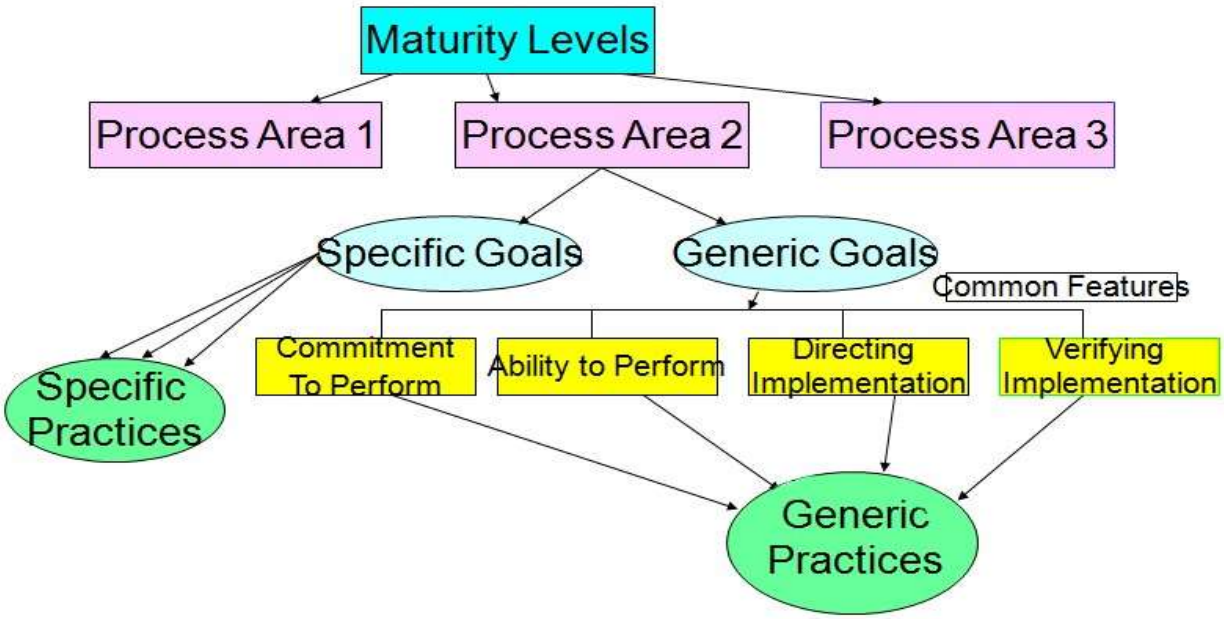

Figure 4: Components of the CMMI Model

4. Integrating NIST, ISO 27001, and CMMI

4.1 Synergies Between the Frameworks

The combination of the NIST Cybersecurity Framework (CSF), ISO 27001, and Capability Maturity Model Integration (CMMI) provides organizations with an in-depth approach to maturing their cybersecurity, thanks to the mutual synergies among these three frameworks. The NIST CSF provides a risk-based structure that is flexible enough to be organized around five core functions (identify, protect, detect, respond, and recover), which are largely compatible with the operations of CISSP domains (NIST, 2018). ISO 27001 introduces a rigorous certification code that encompasses Annex A-specific controls, which can be effectively aligned with precise security requirements across all eight domains of the CISSP (ISO/IEC, 2022). CMMI introduces another aspect to process maturity with a five-level capability model, allowing an organization to gauge an increase in its security processes (CMMI Institute, 2021). There are high levels of synergies between these frameworks. To illustrate, the Identify function of the NIST CSF aligns with the risk assessment requirements outlined in ISO 27001 (Clause 6.1) and the Level 3 (Defined) processes for managing risks established by CMMI (Radanliev et al., 2018). Likewise, the Protect functionality corresponds to the access control measures outlined in ISO 27001 (A.9). It provides implementation guidance essential for achieving higher maturity levels of CMMI (4-5), thereby ensuring the degree of control effectiveness (Aliyu et al., 2020). The complementary framework classification enables organizations to implement the NIST CSF to achieve strategic purposes, ISO 27001 to ensure compliance, and CMMI to track process improvement (Atoum et al., 2017).

4.2 Developing a Unified Assessment Approach

The strategy to develop a common measurement process involves a three-step process. First, companies should establish a connection between the elements of the framework, where NIST CSF subcategories are mapped to specific ISO 27001 controls and CMMI practice areas (Abazi, 2020). As an example, NIST CSF PR.AC-1 (Identity and authentication) aligns with ISO 27001 A.9.2 (User access management) and with CMMI Level 3 practices, specifically access control standardization (Ghaffari & Arabsorkhi, 2018). Secondly, it is necessary to develop maturity indicators based on ISO-focused controls for compliance, process capability levels as defined by CMMI, and implementation tiers as outlined by NIST (Rabii et al., 2020). The third step involves developing assessment tools, which combine quantitative indicators of CMMI (e.g., process performance baselines) with qualitative indicators of NIST CSF (e.g., tier scoring) and compliance checklists from ISO 27001 (Le & Hoang, 2017). This combined solution enables companies to generate maturity ratings for the domains of the CISSP framework, which cover ineffective control implementation (ISO), lack of process consistency (CMMI), and failure to control risks (NIST) (Marican et al., 2022). It can be implemented practically using current tools, such as the NIST Cybersecurity Framework profile and CMMI appraisal approaches, with the integration of ISO 27001 audit practices (Sundaramurthy et al., 2022).

4.3 Benefits of Integration for Organizations

There are four main advantages of the unified framework to organizations. First, it prevents the repetition of assessments by introducing a single methodology that can be used instead of several compliance requirements (e.g., NIST to comply with a U.S. federal contract, ISO to address operations in other countries) (Dedeke & Masterson, 2019). Second, it offers more defined ways of tracking maturation by combining the staged approach of improvement offered by CMMI with the continuous risk management of NIST (Aliyu et al., 2020). Third, the integration will improve resource allocation, as it will determine the locations of investments that enhance maximum maturity improvements in CISSP areas (Atoum et al., 2017). Fourth, the composite framework facilitates better benchmarking. Maturing organisations can benchmark against their peers through standardized metrics and have the flexibility to address sector-specific risks (Bahuguna et al., 2019). As an example, financial institutions can focus on such areas as Asset Security (Domain 2) and IAM (Domain 5). In contrast, healthcare organizations can focus on Security Assessment (Domain 6) to address the HIPAA requirement (Maleh et al., 2021). The flexibility of the framework also provides opportunities to implement emerging technologies, and AI-powered security operations (Domain 7) can be measured in terms of innovation practices according to CMMI at Level 5 (Sundaramurthy et al., 2022).

5. A Unified Framework for Cybersecurity Maturity Assessment

5.1 Framework Structure and Components

The proposed unified framework integrates three well-known cybersecurity approaches aimed at providing organizations with a comprehensive problem-solving device. Based on the risk-based approach of NIST, the wide-ranging controls of ISO 27001, and the process maturity model of CMMI, the framework develops a multidimensional assessment framework (Radanliev et al., 2018). At its core, the framework outlines defense capabilities progressively, building upon four successive levels, each stacked on top of the other, to reveal a logical progression for organizations (Aliyu et al., 2020). The Foundation Layer sets into place the basics of security hygiene equivalent to CMMI Levels 1-2 and NIST Tier 1, where organizations impose such necessary ISO 27001 controls (Annex A.5-A.8) in an ad hoc (ad lib) manner (Abazi, 2020). Within the Defined Layer (CMMI Level 3, NIST Tier 2), organizations establish formal policies in all areas covered by CISSP and perform periodic risk assessment (Maleh et al., 2021). The Managed Layer can be described in quantitative terms, as well as through the introduction of continuous monitoring, which demonstrates CMMI Level 4 and NIST Tier 3 capabilities (Ghaffari & Arabsorkhi, 2018). At the Optimized layer (Level 5 of CMMI, NIST Tier 4), organizations attain predictive threat modeling and business-aligned security practices (Sundaramurthy et al., 2022). Another prominent feature of the framework is its comprehensive crosswalk matrix, which maps 52 NIST CSF subcategories to 114 ISO 27001:2022 controls and 24 CMMI v2.1 practice areas (Le & Hoang, 2017). Such mapping enables organizations to understand precisely how adherence to a single framework can help achieve maturity in others, thereby diminishing the redundancy of assessments and opening up definite paths for improvement (Marican et al., 2022). This matrix can be especially useful in the context of organizations active in a strictly regulated industry, as it illustrates how compliance with specific requirements can lead to achieving a general level of security maturity (Atoum et al., 2017).

5.2 Assessment Methodology

The methodology of the assessment provided by the framework involves a strict four-stage process aimed at offering actionable results with minimal organizational interference. The first stage of Baseline Establishment integrates the traditional gap analysis of ISO 27001 practices with the CMMI capability evaluation and the NIST Tiers scoring to present a more multidimensional roadmap of the current capabilities (Rabii et al., 2020). In most cases, this activity can identify points of immediate improvement, especially in resource-constrained organizations, which often have unbalanced capability distribution within CISSP domains (Marican et al., 2022). In the Domain-Specific Evaluation stage, assessors use a weighted scoring approach for every CISSP domain, which comprises three critical dimensions: control coverage (ISO), process maturity (CMMI), and risk management effectiveness (NIST) (Aliyu et al., 2020). It is possible to modify the weighting factors according to the needs of the sector - e.g., financial institutions may focus on Asset Security (Domain 2) and healthcare organizations may become engrossed in Security Assessment and Testing (Domain 6) (Bahuguna et al., 2019). It is flexible and guarantees the relevance of its framework in various organizational settings, without compromising the consistency of assessments (Dedeke & Masterson, 2019). The Maturity Scoring stage utilizes a built-in algorithm that sums the following three components: ISO compliance (40 percent weight), CMMI level (30 percent), and NIST tier (30 percent), to derive normalized scores (0-100) (Ghaffari & Arabsorkhi, 2018). This quantitative method provides a prime solution to one of the most significant shortcomings of current models, as it enables monitoring of enhancements in maturity over time (Abazi, 2020). The last stage of Improvement Planning involves a heat map that identifies gaps, visualizes, and prioritizes initiatives according to their security impact level and the feasibility of their implementation within the organization (Radanliev et al., 2018). The phased structure of the methodology enables organizations to perform the assessment step by step, thereby reducing the load on internal resources while maintaining the integrity of the assessment itself (Atoum et al., 2017).

5.3 Tools and Techniques for Implementation

A set of specialized resources has been developed to facilitate the assessment process and enable the practical implementation of the framework. The Assessment Toolkit features a dynamic, automated questionnaire comprising over 300 control items that are adjusted according to the organization's responses, resulting in a shorter assessment time compared to manual assessment methods (Sundaramurthy et al., 2022). Its scoring engine also includes industry-specific algorithms, and the visualization dashboard displays maturity outcomes in a non-technical, executive-friendly format, closing the communication gap between technical contributors and top-level leadership (Aliyu et al., 2020). The design of the toolkit is based on work with other maturity assessment implementations, which focused on achieving a balance between comprehensiveness and usability (Rabii et al., 2020). The Integration Platform is a technical innovation that features API connectors, facilitating real-time data exchange with available

GRC tools and CMDB systems (Le & Hoang, 2017). This automation minimizes errors in manually entered data, and the results of assessments will serve as an indication of an organization's current stage, rather than a snapshot (Ghaffari & Arabsorkhi, 2018). Indicators of maturity level between formal assessments are provided by the continuous monitoring feeds of the platform, which addresses a common limitation of traditional periodic audits and their assessments (Sundaramurthy et al., 2022). The Benchmarking Database is an excellent source of context, as it compares the maturity of organizations to that of other organizations across the industry without revealing their identities, enabling organizations to set achievable goals on their path to improvement (Bahuguna et al., 2019). Techniques of implementation emphasize the importance of practical flexibility when considering the varying levels of resources that some organizations possess and the changes they initiate (Marican et al., 2022). The progressive adoption method enables companies to focus on 2-3 CISSP areas that are most crucial in their processes, and as capabilities develop, expand the scope of assessment (Atoum et al., 2017). Agile security governance methods, such as bi-weekly maturity reviews, facilitate continual momentum in improvement, whereas the combination of the SOAR platform facilitates the automation of high-maturity controls (Sundaramurthy et al., 2022). The structure has specific guidelines for adapting to small businesses, regulated businesses, and cloud-native entities, making the framework universal and applicable to a wide variety of organizational settings (Dedeke & Masterson, 2019).

6. Case Studies and Practical Applications

6.1 Healthcare Sector Implementation

The framework has been introduced to a local network of hospitals that included three acute care hospitals and twelve outpatient clinics; the entire network had to operate within the stringent requirements of HIPAA compliance. The primary evaluation revealed significant maturity differences among CISSP areas, with asset security (Domain 2) scoring well, as evidenced by the presence of established encryption measures (78/100). In contrast, security assessment and testing (Domain 6) were absent (32/100) (Aliyu et al., 2020). This has involved incorporating the ISO 27001 A.12.6 requirements for technical vulnerability management and the NIST PR.IP-12 requirements of vulnerability scanning (Maleh et al., 2021). Measurable results have been achieved in the organization after 14 months, including a dramatic decrease in critical vulnerabilities (a 62 percent reduction), bi-weekly scanning cadences, and the formalization of a patch management process (Sundaramurthy et al., 2022). The crosswalk matrix of the framework, especially, helped us demonstrate HIPAA compliance in terms of mapped controls, which made auditing preparation easier, saving an average of 40 hours per assessment cycle (Abazi, 2020). The implementation difficulty was associated with clinician displeasure at the constantly changing access privileges, which was reduced through specially prepared training that connected security practices with the patient safety consequences (Atoum et al., 2017).

6.2 Financial Services Deployment

A medium-sized credit union, with assets of $2.3 billion, utilized the framework to address the evolving information requirements of FFIEC management and prepare to achieve SOC 2 Type II ratings. Baseline results revealed effective Governance (Domain 1) levels of 85/100 and limited capabilities in Incident Response (Domain 7) levels of 45/100, with no defined playbooks remaining (Radanliev et al., 2018). The integration platform of the framework helped the implementation team to integrate the available SIEM tools with NIST RS.AN-5 analysis requirements, ISO 27001 A.16 incident management controls, and developing CMMI Level 4 measurement capacities for response times (Ghaffari & Arabsorkhi, 2018).

The main results included a 72-hour improvement in the time to resolve incidents from hours, and an 11-month savings before SOC 2 certification (Le & Hoang, 2017). This credit union was able to use the benchmarking database of the framework to assess maturity in comparison to other peer institutions by determining that the credit union's IAM (Domain 5) capabilities were in the 92nd percentile and Security Architecture (Domain 3) was in the 34th percentile (Bahuguna et al., 2019). This data-driven method enabled making targeted investments in safe cloud migration trends, which were underpinned by migrating resources from an over-mature realm (Marican et al., 2022).

6.3 Manufacturing Industry Adaptation

A global manufacturing company that produces automotive parts integrated a lightweight version of the framework into its supply chains to meet the emerging customer protection requirements and work with scarce IT resources. It was determined that Software Security Maturity (Domain 8) was exceptionally underdeveloped, scoring 28/100, with no healthy SDLC practices (Rabii et al., 2020). It has customized the implementation and targeted only three domains: Asset Security (Domain 2), IAM (Domain 5), and Security Operations (Domain 7), adopting the framework's progressive adoption method (Dedeke & Masterson, 2019). The producer combined the A.14.2 secure

development requirements in the ISO 27001 with the NIST DE.CM-8 monitoring controls and achieved CMMI Level 2 conformance in patch management within nine months (Sundaramurthy et al., 2022). Such pragmatic modifications involved translating technical controls into operational technology (OT) environments and providing visual workflow instructions to plant floor employees (Atoum et al., 2017). The adoption resulted in a 47 percent decrease in phishing attacks and secured scams, securing a $14 million contract involving the securing of millions of contracts through licensing procedures (Aliyu et al., 2020).

Key Lessons Learned

Three critical success factors were observed to have emerged. The level of executive involvement (C-level champions) led to a 2.3 times faster maturity progression (Maleh et al., 2021). Customized roadmaps led to more extensive adoption of the implementations (58%) compared to those that were rigid, which illustrates the effectiveness of the flexibility of the approaches (Abazi, 2020). Moreover, the correlation between the framework scores and business performance, including audit pass rates and insurance premiums, enabled continuous improvement initiatives in terms of meeting the right measures (Radanliev et al., 2018).

7. Challenges and Considerations

The adoption of the unified framework also presents various challenges, such as organizational resistance to change, especially in mature businesses, where new processes are likely to be perceived as uprooting the current systems by employees (Rabii et al., 2020). The shortage of resources, particularly in small and medium-sized enterprises (SMEs), does not always allow for fully supporting all domains of CISSP due to the necessity of implementing phased adoption patterns (Marican et al., 2022). Additionally, there is a possibility of creating complexity in aligning diverse frameworks (NIST, ISO 27001, CMMI) due to the challenge of reconciling various terminologies and levels of maturity (Radanliev et al., 2018). They also require constant flexibility to deal with new threats, as a static assessment would soon become obsolete in the constantly changing cybersecurity environment (Sundaramurthy et al., 2022). Technical team resistance can also occur when technical teams feel assessments are used as a mechanism of compliance instead of security maturation, in which case, they need to communicate the connection between maturity and risk reduction (Abazi, 2020). Lastly, to sustain growth after assessment, it is essential to incorporate maturity monitoring into governance practices and make cybersecurity a strategic priority, rather than a one-time project (Aliyu et al., 2020).

8. Future Trends in Cybersecurity Maturity Assessment

In the future, the automation of the maturity assessment process is the most probable outcome, and artificial intelligence (AI) and machine learning (ML) will enable real-time assessment of maturity, providing maturity scores and predictive analytics (Sundaramurthy et al., 2022). The development of new standards, including the construction of NIST zero-trust frameworks and ISO 27001 extensions for cloud protection measures, will necessitate ongoing adjustments to integrated models (Ghaffari & Arabsorkhi, 2018). The necessity of regulatory requirements, coupled with the desire to have greater control over the life of the debt, will promote the need for standardized maturity benchmarks, especially within key areas of infrastructure, where consistency in the process of determining compliance may ease such operations (Maleh et al., 2021). High-fidelity representations of AI-powered cyberattacks will require dynamic maturity models that also change with the modes of attack (Le & Hoang, 2017). Additionally, the integration of cybersecurity maturity and enterprise risk management (ERM) will be even stronger, driving the security posture toward business resiliency (Atoum et al., 2017). Lastly, the emergence of sector-specific maturity models, designed specifically for healthcare, finance, and industrial control systems, will contribute to increasing accuracy in assessment while also ensuring interoperability with such frameworks (Bahuguna et al., 2019).

Conclusion

The study can provide an integrated cybersecurity maturity model, filling in the gaps between the flexibility of the NIST CSF, the strictness of ISO 27001, and the bias towards process metrics of CMMI. Due to the alignment of these standards with CISSP domains, companies receive a detailed strategy to evaluate and enhance their security positions, taking into consideration industry requirements. The crosswalk matrix and stage approach stipulated in the framework minimise redundancy and allow compliance and risk management to be accomplished efficiently. Its flexibility has been proven through practical applications in healthcare, finance, and manufacturing, resulting in improved measurable vulnerability reduction and incident response.

The scarcity of resources, as well as resistance to change, represent the challenges that highlight the necessity of executive buy-in and gradual adoption. The evolution of AI-based evaluation and zero-trust systems will also improve the relevance of the framework. The increased resilience, efficiency in auditing, and evidence-based security investments are what organizations that use this unified approach are likely to achieve. The applicability and practicality of this framework will aid the incremental development of maturity, whilst remaining scalable, measurable, and sufficient to meet both existing needs and the next trends in the development of cyber threats.

Call to Action: Organizations are advised to consider incorporating the framework into their governance, utilizing benchmarking tools to monitor improvements and align the maturity of cybersecurity with the business's goals. In the future, work should focus on automation upgrades and sector-specific enhancements to combat dynamic threat environments.

Reference

1. Marican, M. N. Y., Abd Razak, S., Selamat, A., & Othman, S. H. (2022). Cybersecurity Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access*, *11*, 5442–5452.
2. Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information & Computer Security*, *28*(4), 627–644.
3. Ghaffari, F., & Arabsorkhi, A. (2018, December). A New Adaptive Cybersecurity Capability Maturity Model. In *2018, 9th International Symposium on Telecommunications (IST)* (pp. 298–304). IEEE.
4. Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. Edpacs, 63(6), 1-22.
5. Krutz, R. L., Vines, R. D., & Stroz, E. M. (2001). The CISSP Prep Guide: Mastering the ten domains of computer security (pp. 183-213). New York: Wiley.
6. Stewart, J. M., Tittel, E., & Chapple, M. (2011). *CISSP: Certified Information Systems Security Professional Study Guide*. John Wiley & Sons.
7. Wang, P., & D'Cruze, H. (2019, May). Cybersecurity certification: Certified Information Systems Security Professional (CISSP). In *16th International Conference on Information Technology-New Generations (ITNG 2019)* (pp. 69–75). Cham: Springer International Publishing.
8. Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for the NIST Cybersecurity Framework. Computer Science & Information Technology (CS & IT), 7(3), 51-62.
9. Abazi, B. (2020). A novel approach for information security risk assessment maturity framework based on ISO 27001 (Doctoral dissertation, Budapesti Corvinus Egyetem).
10. Alsaleh, M., & Niazi, M. (2021). Evaluations of Information Security Maturity Models. organization, 6(8), 20.
11. Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. Applied Sciences, 10(10), 3660.
12. Le, N. T., & Hoang, D. B. (2017). Capability Maturity Model and Metrics Framework for Cyber Cloud Security. Scalable Computing.
13. Radanliev, P., De Roure, D., Nurse, J. R., Nicolescu, R., Huth, M., Cannady, S., & Montalvo, R. M. (2018, March). Integration of cybersecurity frameworks, models, and approaches for building design principles for the Internet of Things in Industry 4.0. In *Living in the Internet of Things: Cybersecurity of the IoT-2018* (pp. 1–6). IET.

14. Atoum, I., Otoom, A., & Ali, A. A. (2017). Holistic Cybersecurity Implementation Frameworks: A Case Study of Jordan. *International Journal of Information, Business and Management*, *9*(1), 108.

15. Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information & Computer Security*, *27*(3), 373–392.

16. Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Assessing cybersecurity maturity of organizations: An empirical investigation in the Indian context. *Information Security Journal: A Global Perspective, 28(6), 164–177*.

17. Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2022). The future of enterprise automation: Integrating AI in cybersecurity, cloud operations, and workforce analytics. Artificial Intelligence and Machine Learning Review, 3(2), 1–15.

18. Erin Anderson (October 6, 2020)..... How to Apply the NIST Cybersecurity Framework in ICS. https://www.industrialdefender.com/blog/how-to-apply-nist-cybersecurity-framework-ics

19. Sally Godfrey (retrieved December 8, 2008) (source – What is CMMI) https://commons.wikimedia.org/wiki/File:Components_of_CMMI_Model.jpg

20. Admin (February 21, 2023) What is ISO 27001 and why is it Important? https://sasolutionint.com/what-is-iso-27001-and-why-is-it-important/

21. Kathleen Wong (October 4, 2021) 9 Domains of Cybersecurity. https://blog.zartech.net/9-domains-of-cybersecurity/