International Journal of Information Security (2025) 24:242
https://doi.org/10.1007/s10207-025-01154-5

REGULAR CONTRIBUTION

Developing cyber-resistivity maturity and scoring framework (CRMSF) for any size of organization

Konstantinos Papachristofis[1] · Georgios Vardoulias[2] · Konstantinos Vavousis[3] · Costas Iordanou[1] · Yianna Danidou[1]

Received: 22 July 2025 / Accepted: 26 October 2025 / Published online: 20 November 2025
© The Author(s) 2025

Abstract

Cybersecurity is essential for organizations of all sizes, as cyber threats can jeopardize their data, operations, reputation, and competitiveness. Consequently, a one-size-fits-all cybersecurity framework, especially one based solely on maturity levels, is neither practical nor effective, as acknowledged in recent literature critiquing universal maturity models (Liyanage et al. in Sok: identifying limitations and bridging gaps of cybersecurity capability maturity models (ccmms). arXiv preprint arXiv:240816140, https://arxiv.org/abs/2408.16140, 2024). Instead, organizations require a scalable and adaptive framework that allows them to assess their current cybersecurity posture, identify gaps and risks, and implement targeted measures to enhance their cybersecurity maturity in a timely and practical manner. Maintaining continuous awareness of their cybersecurity status and understanding the degree of necessary improvement is critical. In response to these challenges and to address the limitations of existing capability models and frameworks, this paper proposes a novel framework, the Cyber-Resistivity Maturity and Scoring Framework (CRMSF). It emphasizes distinct capability evaluation attributes, including the use of weight factors, criticality and complexity analysis, benchmarking, and maturity levels.

Keywords Cybersecurity framework · Cybersecurity maturity models · Cyber resilience frameworks

1 Introduction

Cyberattacks, as well as cyber threats, have been growing exponentially day by day, driven by the rapid expansion of the digital landscape and the increasing interconnectivity of systems. This digital evolution introduces new technologies, services, and endpoints, which in turn broaden the attack surface—defined as the sum of all possible entry points, or attack vectors, where an unauthorized user might attempt to access a system or extract data. As a result, the growing complexity and dynamism of modern IT infrastructures significantly amplify the risk landscape. Therefore, organizations must constantly monitor their attack surface to identify and block potential threats as quickly as possible, as rapid detection enables immediate containment, limits the time attackers remain undetected within systems, and prevents escalation into major breaches. Timely intervention minimizes data loss, financial damage, and reputational harm, while preserving forensic evidence. It also strengthens regulatory compliance by reducing legal exposure, operational disruption, and the cost of recovery through early, effective incident handling. Technologies and applications like social, mobility, analytics, cloud, Internet-of-Things (IoT), Artificial Intelligence (AI) and Operational Technology (OT) have made a paradigm shift in the information technology space.

✉ Konstantinos Papachristofis
kp222608@students.euc.ac.cy

Georgios Vardoulias
gvardoulias@hna.gr

Konstantinos Vavousis
kvavousis@acg.edu

Costas Iordanou
c.iordanou@euc.ac.cy

Yianna Danidou
y.danidou@euc.ac.cy

[1] Department of Computer Science and Engineering, European University Cyprus, 6 Diogenis Str., 2404 Nicosia, Cyprus

[2] Hellenic Naval Academy, Hadjikyriakou Avenue, 18539 Piraeus, Greece

[3] Department of Information Technology, Cybersecurity and Computer Science, School of Science and Technology, DEREE - The American College of Greece, 6 Gravias Street, 15342 – Ag. Paraskevi, Athens, Greece

Threats are dynamic and organizations must be updated on the practices they should adopt to protect critical assets.

A 2022 IBM report [16], highlights the growing prevalence of cybersecurity incidents. The report indicates that 83% of the organizations surveyed, experienced more than one data breach, reflecting the increasing frequency of security incidents. Another analysis by Cybersecurity Ventures (Cybersecurity [8]), supports this trend, estimating that 66% of small and medium-sized businesses had experienced at least one cyber incident during the period 2021–2022.[1] In 2024, IBM reports[2] that the average global cost of a data breach has increased to $4.88 million, marking a 10% increase from the previous year. Statista [34] projects that the total cost of cybercrime will increase from $6.4 trillion between 2024 and 2029, reaching a staggering $15.63 trillion by the end of this period. This projection reflects the cumulative economic impact of cybercrime globally, including direct and indirect losses from data breaches, ransomware, business disruption, and reputational damage.

Information systems entail risks that are not only complex but also difficult to quantify, as their consequences can directly impact an organization's objectives [41]. Security measures must therefore be selected based on their cost-efficiency, considering the extent of risk reduction they offer and the potential losses that breaches could cause [31]. Furthermore, these practices should align with the principle of proportionality, as articulated in the Network and Information Systems Directive (NIS2) Directive,[3] ensuring that security measures are commensurate with the nature, scale, and potential impact of the associated risks [13].

The Cyber-Resistivity Maturity and Scoring Framework (CRMSF) is introduced in this article as a novel approach that combines maturity assessment with additional evaluation attributes, namely weight, complexity, criticality and benchmarking. Unlike existing frameworks, CRMSF is designed not only to help strengthen an organization's cybersecurity posture, but also to provide a scoring mechanism that reflects both technical and organizational measures in a balanced and quantifiable manner. The detailed structure and methodology of CRMSF are presented in later sections.

One of the main motivations for developing a novel framework is the widespread realization that "one-size-fits-all" cybersecurity frameworks are often inefficient and unsuitable, particularly for SMEs. Larger organizations may have the resources to implement complex models, but smaller businesses typically lack the capacity to do so. The proposed framework is highly adaptable and can be effectively applied across various sectors, including healthcare, manufacturing, public services, and retail, while also supporting organizations subject to the NIS2 Directive.

Frameworks play a critical role in guiding and supporting organizations in establishing an Information Security Management System (ISMS) that encompasses people, processes, and technology. An ISMS typically consists of a structured set of policies, procedures, standards, guidelines, and controls designed to safeguard the Confidentiality, Integrity, and Availability (CIA) of information assets [25]. However, implementing an ISMS poses significant challenges, particularly for SMEs, such as limited financial and human resources, lack of specialized expertise, and difficulty adapting standardized requirements to their specific operational contexts. These challenges become more pronounced and costly as organizational size grows [36].

To address the increasing complexity of cyber threats, organizations need structured approaches that enable informed decisions and sustainable risk management. In this context, two key approaches emerge:

- A compliance-oriented cybersecurity approach focuses on adhering to predefined rules and standards set by regulations such as Health Insurance Portability and Accountability Act (HIPAA) [39] and Payment Card Industry Data Security Standard (PCI-DSS) [30]. Organizations implement minimum safeguards to meet these requirements and avoid non-compliance risks, often treating compliance as a "check-the-box" task. This method tends to address known and specific threats, but can lack flexibility to deal with evolving cyber risks.
- In contrast, a risk-oriented approach prioritizes identifying and mitigating risks based on the likelihood and impact of potential threats. By focusing on the severity of risks and deploying controls accordingly, this approach ensures more comprehensive and adaptable cybersecurity. Risk-oriented cybersecurity offers a more robust approach than compliance-based models, as it proactively addresses evolving threats and operational vulnerabilities, thereby enhancing the protection of an organization's mission, reputation, and critical assets [9].

A persistent challenge in cybersecurity is bridging the communication gap between technical experts and decision-makers. Existing models often generate outputs that are too technical for non-experts, making it difficult for leadership to make informed choices. The proposed novel framework will address this issue by offering a business-driven, multi-dimensional scoring system that is comprehensible to both cybersecurity professionals and business executives.

[1] While this data refers to incidents from several years ago, it illustrates the ongoing exposure of SMEs to evolving cyber threats.

[2] https://www.ibm.com/reports/data-breach.

[3] The principle of proportionality refers to the requirement that the security measures, obligations, and regulatory interventions imposed on entities should be proportionate to the level of risk, size, type, and importance of the entity, as well as the criticality of the services they provide.

To address these challenges, the "Cyber-Resistivity Maturity and Scoring Framework (CRMSF)" is proposed. The term reflects a novel construct introduced in this paper. "Cyber-resistivity" denotes an organization's capability to withstand, absorb, and adapt to evolving cyber threats, integrating both cybersecurity and cyber resilience perspectives. The use of "maturity" and "framework" underscores its hybrid character: providing structured guidance (framework) and evaluating execution capability over time (maturity). "Scoring" facilitates self-assessment and promotes continuous improvement through weighted, risk-based capability metrics.

This novel framework is distinguished by its focus on flexibility and tailored implementation. CRMSF organizes security practices into distinct security grades, enabling organizations to customize their cybersecurity strategies based on specific needs and maturity levels. Unlike traditional models that may require 4 to 5 years to reach full maturity, CRMSF allows organizations—especially medium-sized ones—to attain intermediate security grades within 1 to 2 years. This accelerated progression is made possible through its modular design, emphasis on progressive improvements, and the use of a weighted scoring mechanism that prioritizes critical and achievable measures. This approach emphasizes incremental achievements (security grades) rather than an all-or-nothing approach.

CRMSF offers prescriptive and progressive guidance to help organizations develop and enhance their cybersecurity posture. It incorporates assessment methods that provide actionable insights for improving security posture and clearly define responsibility for information management [32]. The framework's organizational and technical practices are precise, technically grounded, and vendor-agnostic, making it applicable across diverse structures, industries, and sizes.

While descriptive frameworks illustrate the current state, CRMSF's prescriptive nature supports the development of targeted improvement roadmaps that can add measurable value to business processes. It also enables benchmarking across industries or regions through a comparative model.

Given the evolving threat landscape and expanding digital footprint of modern organizations, a continuous improvement approach to cybersecurity is essential. Maturity models and frameworks are widely used to assess an organization's level of preparedness. CRMSF aims to serve organizations of all sectors and sizes —government, industry, and academia alike—by integrating existing cybersecurity best practices and initiatives into a unified, practical model. This alignment with related work, further discussed in Sect. 2, ensures that the framework remains relevant and beneficial to stakeholders by incorporating proven practices and existing cybersecurity initiatives.

To be truly effective, organizations require a practical framework that is scalable, actionable, and adaptable to their infrastructure maturity level. This paper presents the core concepts and rationale behind CRMSF, along with an in-depth analysis of its components. It discusses the key considerations that guided its development, highlights its advantages, and shares findings from initial implementation and management efforts. It also presents the development and structure of the proposed CRMSF, which was designed to address gaps identified in existing cybersecurity maturity models.

The primary aim is to articulate the framework's conceptual design, internal logic, and modular architecture. While this work does not include empirical validation, a pilot evaluation is planned as part of a future research phase, as described in Sect. 5. The current version of CRMSF reflects a stable design structure, with potential refinements limited to the technical and organizational control definitions per category. Section 2 of this paper reviews existing frameworks and maturity models, along with prevailing trends and ideas. Section 3 introduces the proposed cyber-resistivity framework. Section 4 outlines the benefits of CRMSF. Section 5 presents the methodological approach for upcoming pilot tests, and Sect. 6 concludes with key takeaways.

2 Related work

A structured set of principles and best practices called a cybersecurity framework is intended to assist organizations in regulating and reducing cybersecurity risk [20]. Its primary objective is to help organizations understand their cybersecurity posture by giving stakeholders a uniform language and methodical approach, as well as to make communication easier. Notable cybersecurity-related frameworks (compliance- or risk-oriented) include Control Objectives for Information and Related Technologies (COBIT) [17], which—although originally developed as an IT governance framework—now incorporates elements of cybersecurity risk management; Factor Analysis of Information Risk (FAIR) [11], a quantitative model for cyber risk analysis; and PCI-DSS, a compliance-focused standard aimed at protecting payment card data.

Cybersecurity maturity models seek to create a standardized assessment to evaluate the level of information security within an organization, facilitating the achievement of specified security objectives. Since these maturity levels are progressive, as the maturity levels increase, so do the applied measures. These levels are capabilities for assessing the security of the organizations that need to be examined, as well as the security of third-party companies that the organizations deal with. There are some notable cybersecurity maturity models like Cybersecurity Capability Maturity Model (C2M2) [38] and Capability Maturity Model Integration (CMMI) [18].

Below are some of the most widely recognized frameworks, models and tools, each offering specific guidance tailored to different organizational needs.

2.1 Compliance-oriented cybersecurity frameworks

Notable compliance- and policy-oriented frameworks include:

ISO/IEC 27001 is an international standard for establishing, implementing, maintaining, and continually improving an ISMS. The 2022 version emphasizes risk management and the PDCA (Plan-Do-Check-Act) cycle, making it adaptable to organizations of all sizes by offering scalable practices. It helps organizations systematically manage sensitive information and strengthen resilience against cyber threats by focusing on continuous improvement [24].

NIST Cybersecurity Framework (CSF) v2.0 has been developed by the U.S. National Institute of Standards and Technology (NIST) [27]. The Cybersecurity Framework (CSF) provides a policy framework of cybersecurity activities and outcomes. The newly updated v2.0 incorporates greater alignment with other standards and is designed to be flexible and applicable to organizations of any size, from small businesses to large enterprises. Its six core functions—Govern, Identify, Protect, Detect, Respond, and Recover—make it an essential guide for improving organizational cybersecurity resilience [15].

Network and Information Security Directive (NIS2) is a European Union directive focused on improving cybersecurity resilience across the following mid-size and large sectors, including energy; transport; banking; financial market infrastructures; health; drinking water; wastewater; digital infrastructure; ICT service management (business-to-business); public administration; space; postal and courier services; waste management; manufacture, production, and distribution of chemicals; production, processing, and distribution of food; manufacturing; digital providers; and research. It emphasizes harmonized approaches across member states, ensuring that organizations of all sizes, especially in critical industries, adopt a proactive approach to cyber threats [1, 33].

2.2 Capability and maturity-oriented models

These models assess the maturity of cybersecurity implementations and facilitate capability development within organisations:

The Cybersecurity Capability Maturity Model (C2M2) is a voluntary, free-to-use model developed by the U.S. Department of Energy to evaluate and improve cybersecurity capabilities. Its maturity levels offer a structured approach for organizations to measure their cybersecurity performance, making it especially relevant for organizations seeking to understand their current security capabilities and plan improvements. It enables organizations—regardless of size or sector—to perform self-assessments, benchmark maturity levels, and prioritize improvements [6].

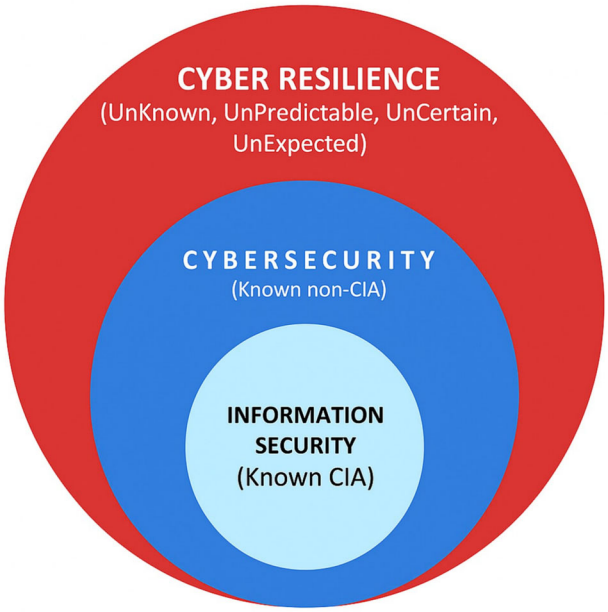


Fig. 1 Information security forum (ISF) levels—1 [4]

The CIS Controls version 8 (Center for Internet Security Critical Security) provides 18 critical security practices to safeguard systems and data. It is widely used across various industries and is particularly beneficial for small and medium-sized organizations due to its focus on practical, implementable steps. CIS emphasizes a prioritized approach that addresses the most critical cybersecurity risks [2].

2.3 Standards, assessment and self-evaluation tools

These are practical, often lightweight tools, standards or structured methodologies that support internal evaluations of security posture and resilience:

Information Security Forum (ISF) standards and tools, such as the Standard of Good Practice for Information Security (SOGP), provide actionable guidelines for managing cybersecurity risks. This global organization delivers adaptable and scalable resources to help organizations implement risk-based security frameworks suitable for enterprises of varying sizes. ISF has structured cybersecurity threats and corresponding countermeasures into three distinct levels, depicted in Fig. 1 [4].

The SysAdmin, Audit, Network, and Security (SANS) Institute[4] offers extensive training and research in cybersecurity, making it a key resource for organizations seeking to bolster their internal security capabilities. While it does not provide a specific framework, its research-driven approach offers critical insights into cybersecurity best practices and incident response strategies, particularly for sectors with advanced threat landscapes.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) developed the Stop Ransomware Guide, a self-assessment tool specifically aimed at helping U.S. state, local, tribal, and territorial governments enhance their resilience to ransomware attacks. The guide is designed to be used by small to mid-sized organizations with limited resources and offers practical, easy-to-implement recommendations [7].

Cyber Security Resilience Self-Assessment Handbook offers organizations a comprehensive guide to evaluating their cybersecurity resilience through a structured self-assessment. It focuses on risk management, preparedness, and the capacity to recover from cyber incidents, making it valuable for organizations that aim to benchmark their resilience maturity levels [19].

2.4 Identified gaps

The maturity models and frameworks, developed primarily with large organizations and their associated structures in mind, that have been presented have proven to be unsuccessful when implemented within small and medium-sized businesses [36]. This limitation arises from their resource-intensive requirements and lack of scalable evaluation mechanisms. CRMSF addresses these challenges by incorporating security grades which enable proportional adaptation to the size, resources, and risk profile of SMEs. Unlike traditional frameworks that often impose a uniform set of requirements irrespective of organizational capacity, the graded structure of CRMSF ensures that smaller entities can focus on fulfilling baseline measures as a minimum standard, while selectively adopting advanced or maximal practices when resources allow or regulatory obligations require it. This scalability reduces the burden of compliance and allows for gradual improvement without overwhelming limited budgets or personnel. Moreover, by embedding attributes of complexity and criticality, the framework assists SMEs in prioritizing controls that yield the highest security impact relative to effort, thereby maximizing the efficiency of their cybersecurity investments. The result is a practical roadmap that highlights both essential requirements and achievable quick wins, fostering continuous improvement in a manner that is both realistic and sustainable for SMEs. As a result, CRMSF offers a more practical and feasible approach for smaller organizations to assess and enhance their cybersecurity posture.

The preliminary findings, as reported in [29], highlight notable limitations across existing models (CMM, COBIT, NIST CSF, C2M2, and ISO/IEC 27001), including a lack of complexity, insufficient use of weight factors, and limited evaluation attributes to quantify maturity. These gaps suggest that current frameworks often fail to holistically represent an organization's cybersecurity posture. A more detailed comparative analysis of these limitations, supported by quantitative indicators and case-based evidence, is presented in [29]. This earlier work provides the empirical foundation upon which the current study builds, while the present review remains concise to align with the scope of this paper.

The authors observe that maturity models alone may not adequately reflect an organization's actual security posture. While such models provide insights into the implementation level of specific controls or practices, they often fall short in offering a comprehensive perspective across broader security domains. In response to this limitation, the proposed CRMSF introduces a more granular assessment mechanism, which incorporates weighting factors alongside maturity levels to better capture the contextual significance and effectiveness of individual measures. The stated framework CRMSF includes concepts by Eloff and Eloff [12] and the C2M2, suggesting implementation and progressive control. However, it implements other evaluation attributes and security grades. Specifically, the latter allows the organizations to adapt progressively, methodically, and properly. While cybersecurity frameworks and capability models are vital in bolstering an organization's cybersecurity efforts, they serve different purposes. CRMSF combines maturity and other evaluation attributes into one framework.

3 The cyber-resistivity maturity and scoring framework (CRMSF)

3.1 Overview of CRMSF

Various cybersecurity standards, frameworks, and maturity models were considered in the development of the proposed CRMSF, as they are crucial in helping organizations of all sizes assess and improve their security posture.

CRMSF is a comprehensive model designed to assist organizations in improving their cybersecurity posture through continuous development and risk-based practices. CRMSF provides organizations with a robust and flexible framework to assess and improve their cybersecurity posture. It stands apart from existing maturity models due to its prescriptive nature and progressive approach, emphasizing a practical approach to enhance cybersecurity capabilities. CRMSF introduces unique features, such as security grades,

[4] https://www.sans.org/.

weights, complexity, criticality, and benchmarking, making it a flexible and scalable tool for organizations of all sizes. The framework empowers organizations to tailor their security practices to their unique needs, while ensuring long-term resilience against evolving cyber threats.

CRMSF is a business-driven, prescriptive, technology-driven, risk-based and vendor neutral framework, with modular approach and consists of four (4) primary modules: "Foundation", "Security Grades", "Security Significance" and "Security Scoring". These modules, while interconnected, address different facets of cybersecurity management to provide a holistic view. Table 1 summarizes the entire framework architecture, which is further elaborated upon in the following subsections.

3.2 Foundation module

The Foundation module establishes a dynamic and continuously evolving security framework that adapts to the ever-changing threat landscape. The foundational aspect focuses on three stages: Adaptive Preparation, Active Resistance, and Rapid Regain and Evolution. This module is built around a "continuous resistivity cycle," emphasizing the need for real-time threat detection and response.

- *Adaptive preparation*: This stage builds a long-term, adaptable cybersecurity strategy that anticipates risks and allows organizations to evolve their security measures as new threats emerge. By leveraging advanced risk intelligence, organizations can stay ahead of potential disruptions.
- *Active resistance*: Organizations are encouraged to implement adaptive defenses and containment measures that can limit the impact of cybersecurity incidents in real time. This stage integrates cybersecurity and resilience, ensuring that defenses are not only reactive but also proactive.
- *Rapid regain and evolution*: In the event of an attack, this stage ensures the organization's ability to recover quickly, reinforce weak points, and prevent future attacks through continuous improvement.

The Foundation is the module comprising three elements: Sections, Domains and Security Categories. Each security category consists of Structural Categories (organizational and technical). It is essential that organizational practices be purposefully kept apart from technical (security) practices. Sections consist of two (2) elements, cybersecurity and cyber resilience. Domains consist of seven (7) elements:

- *Strategy*: Understanding business needs is vital in focusing and prioritising efforts on risk management strategy, governance, and compliance.
- *Assessment and anticipation*: Discovering, inventorying, understanding, and prioritizing assets, risks, and vulnerabilities are essential. This activity emphasizes evaluating or determining the state of an organization's environment and risks.
- *Awareness and training*: Establishing and maintaining policies, procedures, and practices creating a cyber security culture and ensuring the ongoing suitability of personnel to respond to threats against critical infrastructure and organizational objectives.
- *Fortification*: Developing and implementing safeguards (organizational and security practices) to protect critical assets.
- *Detection and analysis*: Establishing and maintaining mechanisms aimed at identifying and analyzing potential threats and security incidents. Detection focuses on identifying potential security threats in real-time, while analysis involves a deeper examination of these threats to understand their nature, impact, and origin.
- *Containment*: Developing and implementing actions and practices to address and mitigate the impact of a cybersecurity incident including containment, eradication, and practices to prevent future incidents.
- *Restoration and evolution*: Developing and implementing actions and practices to restore and resume critical operations.

The domains are categorized based on security section and event-driven approach as shown in Table 2 and Fig. 2.

Each Domain consists of several Security Categories, representing areas of cybersecurity activities. Figure 3 presents a subset of the overall framework and illustrates each domain's security category. The CRMSF assigns a distinct color to each of its seven domains, following the sequence of the rainbow spectrum. The seven domains—Strategy (Red), Assessment and Anticipation (Orange), Awareness and Training (Yellow), Fortification (Green), Detection and Analysis (Blue), Containment (Indigo), and Restoration & Evolution (Violet)—are color-coded based on the natural rainbow spectrum to support intuitive visual association. This visual structure enhances clarity and recognition, with each domain adopting its corresponding position in the spectrum.

The Foundation module encourages businesses to take a proactive and holistic approach, ensuring long-term sustainability and security resilience.

3.3 Security grades module

The CRMSF provides security grades which are levels of security that organizational or technical practices fall under. This will be the heart of the framework and will be designed to provide a common language for cybersecurity activities, which contain guidelines, best practices, and standards that

Table 1 Cyber-resistivity maturity and scoring framework (CRMSF)

SECURITY SCORING Module	Cumulative Cyber-Resistivity Maturity & Score		
	Benchmarking (Risk Adjustment)		
	Cyber-Resitivity Security Classes		
	Metrics		
SECURITY SIGNIFICANCE Module	Complexity, Criticality, Weights		
SECURITY GRADES Module	Baseline	Advanced	Maximal
FOUNDATION Module	Organizational Practices	Technical Practices	
	Categories (24)		
	Domains (7)		
	Sections (2)		

Table 2 Sections, phases and domains of CRMSF

Section	Phase	Domains	Description
Cyber-security	Pre-event	Strategy, assessment and anticipation, awareness and training, fortification	Refers to the period before a security incident occurs. It involves proactive practices like risk assessment, planning, training, awareness, and implementation of security practices
Cyber-resilience	During-event	Detection and analysis	Refers to the occurrence of a security incident. It involves immediate response, containment, and threat analysis
	Post-event	Containment, restoration and evolution	Activities after the incident: recovery, root cause analysis, reporting, and improvement planning

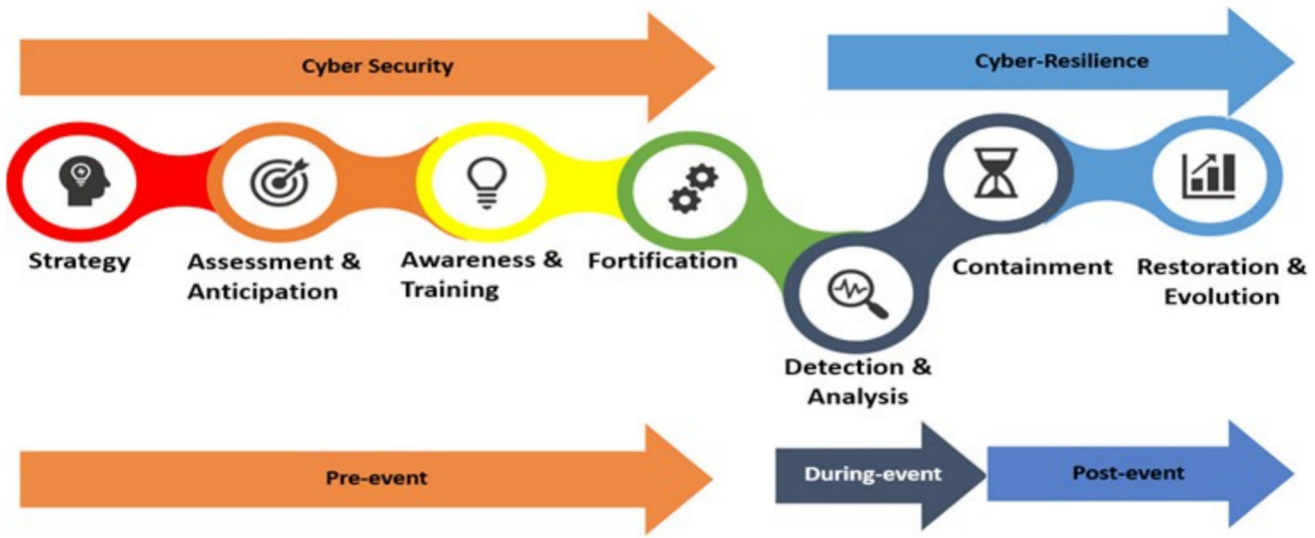


Fig. 2 Sections, phases and domains of CRMSF

Stages	Adaptive Preparation			Active Resistance			Rapid Regain and Evolution
Sections	CYBERSECURITY				CYBER RESILIENCE		
Phases	Pre-event				During-event	Post-event	
Domains	STRATEGY	ASSESSMENT & ANTICIPATION	AWARENESS & TRAINING	FORTIFICATION	DETECTION & ANALYSIS	CONTAINMENT	RESTORATION & EVOLUTION
Categories	Develop Governance Strategy	Develop Asset Management Plan	Develop Cybersecurity Culture Plan	Develop Endpoint Protection Plan Develop Email Security Plan Develop Web Security Plan Develop Access Control & Remote Admin Plan Develop Network & Perimeter Security Plan	Develop Detection Plan	Develop Reaction & Enhancement Plan	Develop Backup Plan Develop Recovery Plan
	Develop Compliance Strategy	Develop Risk Management Plan	Develop Cybersecurity Awareness Training Plan	Develop Remote Working Security Plan Develop Web Application Security Plan Develop Wireless Security Plan Develop Software and Application Security Plan Develop Physical & Environmental Security Plan	Develop Analysis Plan	Develop Communication & Reporting Plan	Develop Communication & Reporting Plan Develop Enhancement Plan

Fig. 3 CRMSF: domains and categories (rainbow spectrum)

help organizations manage and improve their cybersecurity posture.

The proposed security grade according to the type of organization, takes into account how the EU NIS2 classifies organizations according to their size. It is possible that some organizations would like to apply a higher level of security grade, which is best practice in cases where certifications they must obtain (e.g., ISO27K) or compliance with some regulatory frameworks (General Data Protection Regulation (GDPR), NIS, NIS2, etc.) impose. This framework allows flexibility in choosing the desired maturity level and the appropriate weight factor to achieve the desired result. Figure 4 summarizes the Foundation and Security Grades modules of the CRMSF.

The framework defines three (3) Security Grades, —Baseline, Advanced, and Maximal—offering a practical approach to defining security measures based on organizational needs. By categorizing practices in this way, organizations can make informed decisions about which security practices are most appropriate for their specific needs and threat landscapes.

- *Baseline*: This represents the foundational level of security, focusing on essential practices that every organization must implement to safeguard its critical assets.
- *Advanced*: Building on the Baseline level, this grade includes additional measures, it addresses more sophisticated threats and enhances organizational resilience.
- *Maximal*: The highest grade, which incorporates cutting-edge practices, continuous monitoring, and advanced security automation. Organizations adopting this grade are highly resistant to cyber threats and capable of responding to the most advanced threats.

This grading system allows organizations to adopt cybersecurity measures at their own pace while ensuring that their practices evolve in line with changing threats and regulatory requirements.

An organization using this model may be operating at different security grades in different security categories and domains. For example, an organization could operate at Baseline in one domain, Advanced in another domain, and use the same logic for security categories. An organization must perform all practices at a specific grade in all its security categories to earn a specific security grade (e.g., Advanced) in a given domain. If an organization sets its goal for the cybersecurity section to achieve an advanced security grade, this means that all domains in that section should earn the same grade. Likewise, for the cyber-resilience section. Practice performance and security grade achievement must be aligned with business objectives, business cybersecurity program strategy, and risk appetite.

Achieving the highest security grade in all domains may not be optimal. Organizations should evaluate the costs of attaining a specific security grade versus its potential benefits. However, the model is designed so that organizations, regardless of size, should be able to achieve Baseline across all domains.

3.4 Security significance module

The Security Significance module introduces the concepts of weight, complexity, and criticality, which determines the importance of specific cybersecurity practices. By incorporating these factors, CRMSF offers organizations a more nuanced understanding of their security practices and helps prioritize security efforts.

- *Weight*: This is used to assign importance to each security category. Weight values are crucial for determining how resources should be allocated across the organization's cybersecurity efforts. The weight values can be

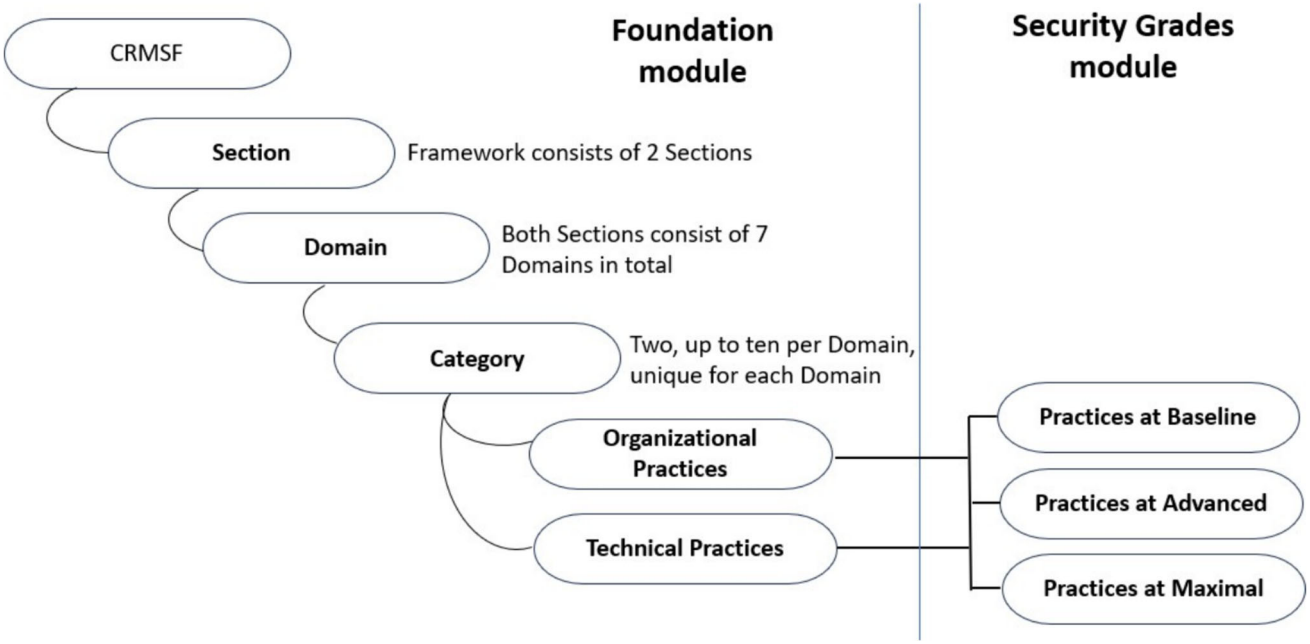


Fig. 4 CRMSF foundation and security grades modules

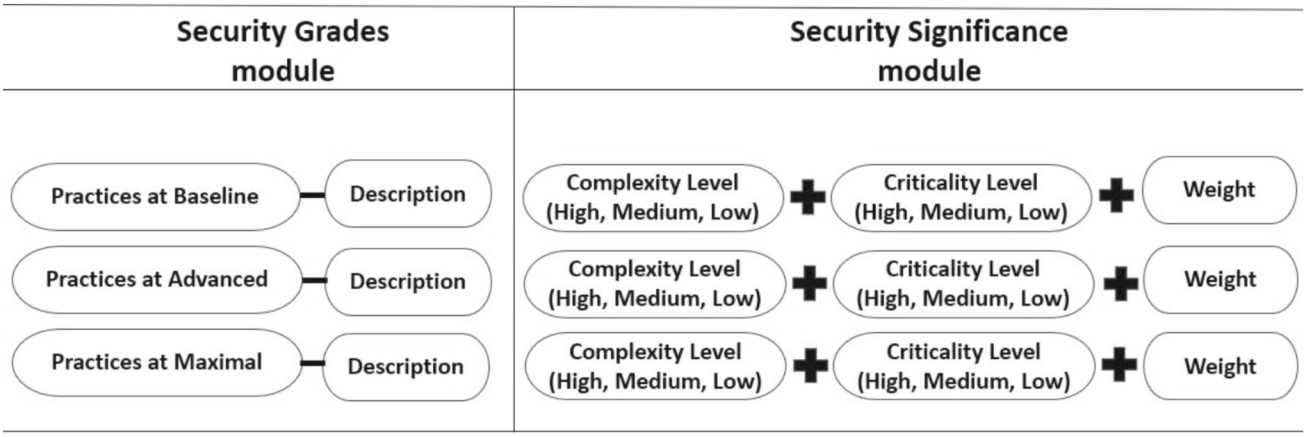


Fig. 5 CRMSF security significance module

assigned per Section, and then divided appropriately into Domains, Security Categories, and reach down to structural categories (Organizational or Technical). For example, organizational practices may not carry the same weight as technical ones.

- *Complexity*: Security practices are classified according to their technical and procedural complexity. Achieving maturity levels within security grades may be of low, medium, or high in complexity, with higher complexity indicating more sophisticated security measures that require greater effort and expertise.
- *Criticality*: This factor assesses the importance of a given security practice in the organization's overall security posture. Critical practices address vulnerabilities that could have severe consequences for the organization.

Together, these values allow organizations to balance their security efforts, ensuring that resources are directed towards the most critical and impactful measures. Figure 5 presents the elements of the CRMSF Security Significance module.

3.5 Security scoring module

The last module, Security Scoring, combines the concepts of maturity levels, weights, risk adjustment, complexity and benchmarking to provide a comprehensive self-assessment tool (Fig. 6). Organizations can use this tool to measure their current security posture, identify gaps, and track their progress over time. The framework uses three (3) maturity levels (ML-1, ML-2, ML-3) per security grade, using in calculations the current (MCL) and desired (MDL) maturity

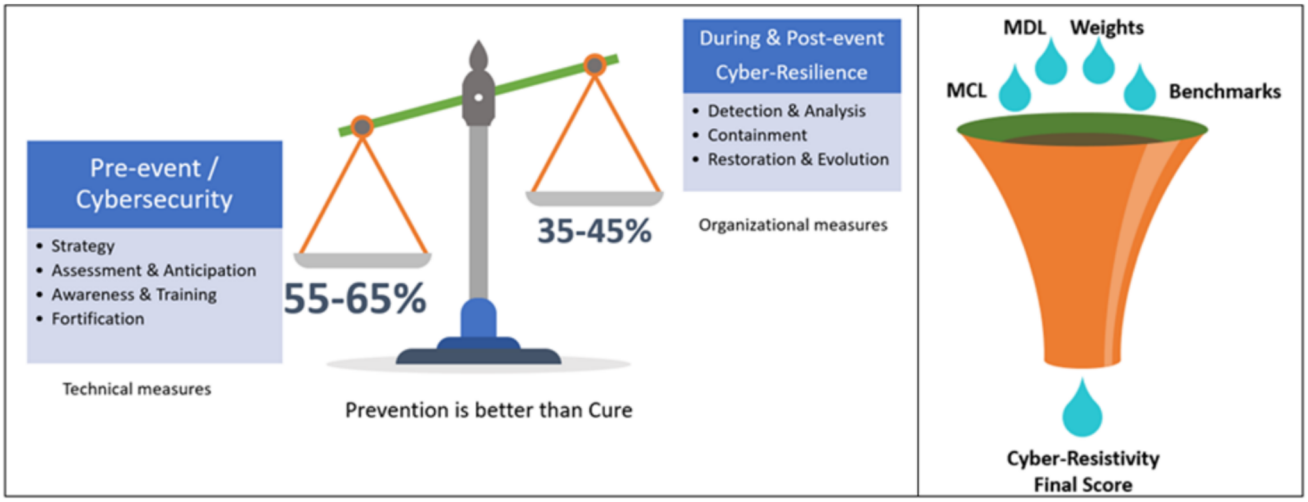


Fig. 6 Security scoring and concepts

level, to assess the organization's readiness, allowing for incremental improvements. Additionally, organizations can benchmark their performance against industry standards to ensure that their practices are in line with the best in the field. This module is essential for continuous improvement, enabling organizations to refine their security practices based on real-time data and evolving risks.

To analyze and compare an organization's Cyber-Resistivity profile, final scores are grouped into a four-band scale called the Cyber-Resistivity Security Class (CRSC), illustrated in Table 3. CRSC provides a mechanism for a single view and visualization of the degree of resistivity of the organization. This comparative tool can also compare the organization's performance at different intervals.

4 The benefits of cyber-resistivity maturity and scoring framework (CRMSF)

Unfortunately, putting well-known frameworks like NIST or ISO 27001 into practice can be difficult for a lot of organizations, as these require time-consuming processes, specialized auditing, and consulting effort. Moreover, they assume the presence of internal IT governance structures and trained personnel—resources that are often unavailable in SMEs—making these frameworks overly complex and costly without significant adaptation [3]. Other researchers, have also pointed out that the controls and requirements outlined in frameworks like ISO 27001 may be seen as overwhelming for SMEs, further complicating their practical implementation [40]. Measuring the organizational implementation's level of readiness, document preparation, and different information security scenarios and strategies are some of the challenges. Certain critical controls can be difficult to comprehend, measure, and implement, presenting significant challenges for organizations [35]. Organizations may face both internal and external challenges when implementing information security, and without proper preparation, various obstacles can hinder the success of these efforts [21].

CRMSF will help organizations achieve their goals methodically, effectively, and efficiently. It will help them adhere to a clear plan of action (roadmap), deliverables, and rules to achieve specific objectives. This framework has enough flexibility to let organizations use the same model in different ways by customizing capability values to achieve their own distinct goals. One of the main benefits of CRMSF is that it recognizes the diversity of each organization—even among those in the same industry. It supports and encourages customization, enabling each entity to develop a maturity strategy aligned with its specific risk appetite, tolerance, and strategic objectives. This adaptability is further detailed in the design principles and scoring methodology described in Sects. 3.3 and 3.4, which emphasize modularity, capability weighting, and contextual alignment.

The existing cybersecurity frameworks, even the well-known ones, lack an objective scoring system and a substantial prescriptive approach. Existing tools for cybersecurity risk assessment often fail to cover all necessary stages, leading to ineffective implementation. Their proposal highlights the absence of comprehensive scoring systems in existing frameworks like NIST or ISO (International Organization for Standardization), as described in S´anchez-Garc´ıa et al. [37].

Any implementation of a cybersecurity program is a journey rather than a one-time task. Organizations need to be able to record and keep an eye on their present and future states. A scoring scheme that enables an organization to compare

Table 3 The cyber-resistivity security class table

Class	Final score	Description
A-Secure	860–1200	Optimal resistivity achieved based on **best practices** and comprehensive implementation of cybersecurity measures. Baseline and advanced practices are fully implemented
B-Protected	730–859	High resistivity from structured but inconsistent implementation. Some elements are missing, but baseline practices are fully applied
C-Insecure	440–729	Moderate resistivity from inconsistent and unstructured application. Many essential practices are missing, including low scores in baseline practices
D-Exposed	0–439	Deficient level of cyber-resistivity

its present situation with its ideal future state could be used to track progress.

What is desirable for all companies is to know the security posture in cybersecurity and cyber resilience. These are two different things. Cybersecurity measures primarily focus on protecting assets from attacks, whereas cyber resilience encompasses the ability to adapt, recover, and continue operations after a breach or attack. This approach recognizes the inevitability of breaches and prepares organizations to respond swiftly to limit damage and recover as soon as possible [26]. CRMSF is a framework that helps organizations evaluate and improve their cybersecurity capabilities and cyber resilience.

Implementing capability evaluation attributes like weighting factors, criticality, complexity, and benchmarks in the framework gives us the real score for an organization. This score can easily be communicated to senior executives and the individual measures in which the most significant deviations can be explained to shield the organization. Also, when all these capability evaluation attributes are present, it is straightforward to identify quick wins. Quick wins are practices with high priority for the organization and low complexity. Starting with them, an organization can be shielded very quickly. In addition, organizations should prioritize business services based on risk assessment and then implement the most essential controls for the highest-risk services [14].

The framework targets decision-makers, leaders, practitioners, and facilitators with different responsibilities and perspectives on cybersecurity. It can also be used by organizations that carry out cybersecurity audits and by organizations that carry out insurance coverage in the field of cybersecurity.

CRMSF provides several key benefits to organizations. It allows organizations to systematically assess their cybersecurity maturity, prioritize investments, and implement necessary changes. Some of the main benefits include:

- *Scalability*: CRMSF can be applied to organizations of any size, offering flexible levels of security practices that align with organizational needs.
- *Customizability*: The framework is adaptable to various industries, ensuring that specific risks and regulatory requirements are addressed.
- *Continuous improvement*: By incorporating a self-assessment tool, organizations can track their progress and continuously enhance their security posture.
- *Holistic approach*: The framework integrates cybersecurity and resilience, offering a comprehensive approach to managing and mitigating cyber risks.

While no single framework fits every context, CRMSF can serve as a foundational layer upon which more specialized frameworks can be built—especially in highly regulated sectors such as energy or healthcare. Larger organizations in industries like manufacturing, retail and wholesale, education, public administration, transport, food production, and maritime services can also adopt it.

These anticipated benefits are derived from the architectural principles and internal logic of the framework, as detailed in Sects. 3.3 and 3.4. While practical validation will be conducted in the upcoming pilot phase (Sect. 5), the modular design, scoring methodology, and self-assessment structure already provide strong theoretical grounding for the expected advantages.

The framework begins with the identification of organizational and technical practices (see Fig. 7), which are systematically structured into 24 Categories, grouped under 7 Domains, and further classified within two (2) overarching Sections. Each practice is subsequently assigned to a Security Grade (Baseline, Advanced, or Maximal) and further refined into three Maturity Levels (ML-1, ML-2, ML-3). At this stage, the resistivity evaluation attributes of Complexity and Criticality are also defined, ensuring that the evaluation captures both the effort required for implementation and the relative importance of each measure.

The assessment process is facilitated through a self-assessment tool, where organizations record the percentage of completion of a Maturity level which contains a group of practices. The tool applies the predefined or customized weights to these inputs and calculates the resulting score.

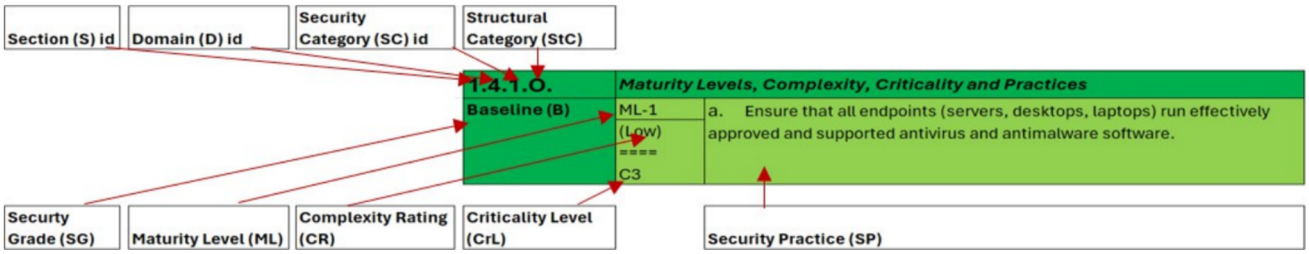


Fig. 7 CRMSF security practices

This process produces the CRMSF Score, the corresponding Cyber-Resistivity Security Class (CRSC), and a set of dashboards that provide analytical insights. The dashboards include results per Section, Domain, Category, and Security Grade, as well as Quick Wins that highlight measures requiring immediate attention. A feedback loop ensures that the framework operates as a continuous and iterative cycle. The outputs feed back into the system, allowing organizations to refine their implementation, adjust priorities, and monitor progress over time. This cyclical nature reflects the dynamic approach of CRMSF and supports its applicability as a living, adaptable model for improving cybersecurity maturity and resilience.

The overall process of the CRMSF is summarized in Fig. 8. The figure illustrates the system flow of CRMSF, highlighting the interplay between inputs, the assessment process, outputs, and the feedback loop.

5 Methodological approach for upcoming pilot tests

The development of the CRMSF follows a methodological approach to ensure that it addresses the critical gaps in existing cybersecurity frameworks and models. By combining comparative analysis, modular development, empirical data collection, and real-world validation, CRMSF provides organizations with a practical prescriptive, and scalable framework that helps them prioritize resources, improve their cybersecurity posture, and adapt to an evolving threat landscape. The comparative model allows for benchmarking within industries or regions [10]. This research will contribute not only to academic knowledge but also to the practical improvement of cybersecurity practices across various industries. Benchmarking and weightage are useful factors that help to quantify the degree of maturity. The practice maturity (technical descriptive measures) evaluation will attempt to assess how mature the actual operational practices are. References [5, 22] explain how one can introduce such values in maturity models.

Interviews with Chief Information Security Officers (CISOs) and cybersecurity professionals will be conducted to assess the accuracy and suitability of the proposed framework. Based on the reviews, the proposed model will be finalized. To validate the functionality of each modular unit, pilot testing will be conducted with industry partners. Pilot testing will involve 6–8 organizations from sectors such as critical infrastructure, healthcare, retail, maritime, and financial services.

The selection of pilot participants is a critical aspect of the validation phase to ensure that the CRMSF's scalability, adaptability, and effectiveness are thoroughly tested. Participants will be chosen based on key factors such as industry type, organization size, and available resources. This deliberate diversity ensures that the framework is evaluated in a variety of operational contexts, from highly regulated industries like healthcare and finance to less-regulated sectors such as retail and education. Including organizations of different sizes—from small-to-medium enterprises to large-scale enterprises—will allow the pilot to test the CRMSF's modular design and its capacity to adapt to varying levels of complexity and resource availability. Additionally, focusing on industries with distinct cybersecurity challenges, such as critical infrastructure and customer-facing businesses, will provide valuable insights into the framework's flexibility and applicability.

The pilot tests will assess the ease of implementation for each modular unit, the accuracy of the scoring model, based on real-world data from participating organizations and the effectiveness of the framework's prescriptive guidance in improving the cybersecurity posture of the organization. Feedback from these tests will be used to refine the framework, ensuring that it meets the practical needs of organisations while maintaining a focus on risk prioritization and adaptability.

The effectiveness of the CRMSF will be evaluated based on several key criteria. If the framework is easy to understand and implement and if both technical staff and executives use the framework's guidance (usability). If the framework is adaptable for organizations of different sizes, and if the modular units can be scaled up or down as needed (scalability). If the framework's scoring model accurately reflects an organization's cybersecurity posture and how well it integrates additional capabilities (accuracy of scoring). If

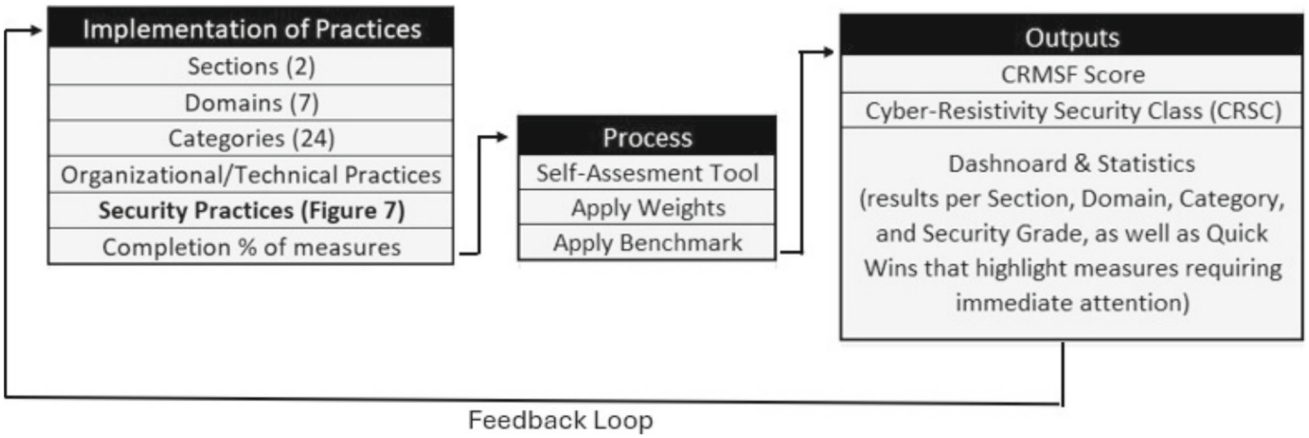


Fig. 8 Interplay of modules within the CRMSF

Table 4 Evaluation criteria and methods for validating the CRMSF

Evaluation criterion	Action/evaluation method	Target metric/output
Usability	Interviews and surveys with technical staff and executives	Clarity, ease of use, adoption rate of framework components
Scalability	Application of the framework in organizations of various sizes	Number of modules used, adaptation effort, user satisfaction
Accuracy of scoring	Comparison of scoring outcomes with expert assessments	Alignment rate between CRMSF score and expert judgment
Prescriptive guidance	Case-based walkthroughs and scenario testing	Clarity of steps, success in applying recommendations

the framework offers actionable, clear, step-by-step guidance, organizations can follow to improve their cybersecurity posture (prescriptive guidance). If the framework works in conjunction with existing industry regulations (e.g., GDPR, NIS2), it can be used as a first-level framework that integrates compliance with risk management (compliance integration). The evaluation process is structured around five main criteria, each linked to specific methods and target metrics, as summarized in Table 4.

The validation process will demonstrate the practical applicability of the CRMSF, ensuring that it provides both an accurate assessment of an organization's security posture and a roadmap for continuous improvement.

To further validate the CRMSF, the framework will be benchmarked against existing cybersecurity models. This involves testing the framework's scoring system using real-world data from organizations and comparing it to the results of other frameworks (e.g., how organizations score on NIST vs. CRMSF). The benchmarking will determine the accuracy of the CRMSF's scoring model in reflecting an organization's actual cybersecurity posture. It will compare the prescriptive guidance of the CRMSF to that of other models to assess improvements in clarity and implementation. It will analyze the effectiveness of the CRMSF in enabling better decision-making at both the technical and executive levels.

The framework will include a versatile online self-assessment scoring platform that will support the methodology through dynamic workflows. The platform will feature dashboards tailored for executive, managerial, or operational audiences.

6 Conclusions

This paper presented the Cyber-Resistivity Maturity and Scoring Framework (CRMSF), a novel framework designed to address limitations observed in traditional frameworks and models. CRMSF offers a modular and context-aware structure that enables organizations of varying sizes and sectors to evaluate and enhance their cybersecurity posture through a unified scoring mechanism and structured security classification.

A key contribution of the proposed framework lies in its ability to combine adaptability, risk prioritization, and prescriptive guidance, supporting both strategic and operational needs. Emphasis has been placed on inclusiveness, enabling

organizations—particularly SMEs—to tailor their cybersecurity development according to specific goals, risk profiles, and compliance requirements.

Existing maturity models have proven ineffective, particularly for small and medium enterprises (SMEs), which face distinct challenges in implementing cybersecurity management systems. Many current standards fail to address the unique needs of SMEs, often overlooking their roles and requirements within the broader digital ecosystem. This highlights the need for more inclusive and adaptable assessment models that recognize the diversity of organizational contexts [28].

The proposed framework adopts a prescriptive, technology-driven, risk-based and vendor-agnostic approach, classifying measures into organizational and technical categories. It incorporates a comprehensive self-assessment tool that generates nuanced scores in individual sections and domains, assigns security grades, and evaluates overall security posture, offering a clearer view of the cybersecurity achievements of an organization.

The primary objective of the work presented here is to support organizations in strengthening their cybersecurity posture, particularly across Information Technology (IT), OT, and IoT environments, through a prescriptive and progressive approach that effectively identifies and evaluates the specific strengths and weaknesses within these domains. This work contributes to the ongoing discourse on cybersecurity maturity models by offering a context-aware and scalable approach that responds to the limitations of traditional models. It argues that cybersecurity effectiveness can be significantly enhanced through a multidisciplinary and integrated strategy: one that balances defensive and offensive, passive and active measures. The paper further illustrates how this framework can be tailored to meet the diverse needs of organizations in both the public and private sectors.

Although empirical validation is part of the ongoing research process, this paper focuses on the theoretical formulation, architectural components, and anticipated benefits of the proposed framework.

Although empirical evaluation has not yet been conducted, the framework's structure and design principles have been clearly defined. A pilot phase is planned to validate and refine specific control measures, without altering the core architecture. As such, the current version establishes a robust foundation for scalable, practical, and measurable cybersecurity maturity management.

Acknowledgements The authors would like to thank their affiliated institutions for academic support. No additional acknowledgements are applicable.

Author contributions KP conceived and developed the core research idea, designed the cybersecurity framework (CRMSF), conducted the analysis, and wrote the manuscript. GV contributed to refining the academic tone and structure of the paper. KV, CI, and YD supervised the research, provided academic guidance throughout the process, and reviewed the manuscript. All authors reviewed and approved the final version of the manuscript.

Funding This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Availability of data and materials No datasets were generated or analysed during the current study. The proposed framework is based on conceptual synthesis and literature review.

Declaration

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

References

1. Advisera: Who does nis2 apply to? (2023). https://advisera.com/articles/who-does-nis2-apply-to/. Accessed 11 May 2025
2. Ambika, P.H., Sujatha, G.: System hardening using cis benchmarks. In: Proceedings of the IEEE International Conference on Advanced Computing and Artificial Intelligence (ACCAI). IEEE (2024). https://doi.org/10.1109/ACCAI61061.2024.10602274
3. Antunes, M., Maximiano, M., Gomes, R.: Information security and cybersecurity management: a case study with SMEs in Portugal. J. Cybersecur. Privacy **1**(2), 12 (2021). https://doi.org/10.3390/jcp1020012
4. Baikloy, E., Praneetpolgrang, P., Jirawichitchai, N.: Development of cyber resilient capability maturity model for cloud computing services. CEEOL (Central and Eastern European Online Library) (2020). https://www.ceeol.com/search/article-detail?id=894538. Accessed 11 May 2025
5. Bodeau, D.J., Graubart, R.D., McQuaid, R.M.: Cyber resiliency metrics, measures of effectiveness, and scoring. Technical report, MITRE Corporation (2018). https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf. Accessed 11 May 2025
6. Curtis, P.D., Mehravari, N.: Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. In: 2015 IEEE International Symposium on Technologies for Homeland Security (HST) (2015). https://doi.org/10.1109/THS.2015.7225323. https://www.researchgate.net/publication/308829669
7. Cybersecurity and Infrastructure Security Agency (CISA): Stop ransomware guide (2025). https://www.cisa.gov/resources-tools/resources/stopransomware-guide. Accessed 11 May 2025

8. Cybersecurity Ventures: Cybersecurity almanac 2022 (2022). https://cybersecurityventures.com/cybersecurity-almanac-2022/. Accessed 11 May 2025
9. Dedeke, A.: Cybersecurity framework adoption: using capability levels for implementation tiers and profiles. IEEE Xplore (2017). https://ieeexplore.ieee.org/abstract/document/8055684/. Accessed 11 May 2025
10. Dube, D., Mohanty, R.: Towards development of a cyber security capability matu- rity model. Int. J. Bus. Inf. Syst. **34**(1), 104–127 (2020). https://doi.org/10.1504/IJBIS.2020.106800
11. Elasticito: Using the fair model to quantify cyber risk. Pdf, Elasticito (2020). https://elasticito.com/wp-content/uploads/2020/02/Cyber-Risk-Quantification-Using-FAIR.pdf
12. Eloff, J., Eloff, M.: Information security management—a new paradigm. Information Security Management (2003). http://www.sis.pitt.edu/jjoshi/courses/is2621/SecManParadigm2.pdf. Accessed 11 May 2025
13. European Parliament and Council: Directive (EU) 2022/2555 of the European parliament and of the council of 14 December 2022 on measures for a high common level of cybersecurity across the union (nis2 directive) (2022). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555. Accessed 11 May 2025
14. Gary, T.: Portland uses the cybersecurity framework and critical security controls aligns business risk and security (2016). https://www.tenable.com/blog/portland-uses-the-cybersecurity-framework-and-critical-security-controls. Accessed 11 May 2025
15. Gourisetti, S., Mylrea, M., Patangia, H.: Cybersecurity vulnerability mitigation framework through empirical paradigm (cyfer): prioritized gap analysis. IEEE Syst. J. (2020). https://doi.org/10.1109/JSYST.2019.2913141
16. IBM Newsroom: IBM report: consumers pay the price as data breach costs reach all-time high (2022). https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High. Accessed 11 May 2025
17. ISACA: Cobit® 2019 framework: introduction and methodology. Pdf, ISACA (2019). https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodologyreseng1118.pdf
18. ISACA & CMMI Institute: Building cybersecurity capability, maturity, resilience: CMMI cyber security capability assessment. Technical report, ISACA & CMMI Institute (2017). https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/TueAM22CMMI.pdf
19. Keinonen, M.: The concept of comprehensive security as a tool for cyber deterrence. In: Proceedings of the European Conference on Cyber Warfare and Security (ECCWS). Academic Conferences International Limited (2023). https://doi.org/10.34190/eccws.22.1.1254
20. Khan, S., et al.: Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. Electronics (2022). https://doi.org/10.3390/electronics11142181
21. Kosutic, D.: ISO 27001 and bs 25999 (2010). http://blog.iso27001standard.com. Accessed 11 May 2025
22. Kulugh, V.E., Mbanaso, U.M., Chukwudebe, G.: Cybersecurity resilience maturity assessment model for critical national information infrastructure. SN Comput. Sci. (2022). https://doi.org/10.1007/s42979-022-01108-x
23. Liyanage, L., Arachchilage, N.A.G., Russello, G.: Sok: identifying limitations and bridging gaps of cybersecurity capability maturity models (ccmms) (2024). arXiv preprint arXiv:240816140. https://arxiv.org/abs/2408.16140, preprint
24. Malatji, M.: Management of enterprise cyber security: a review of ISO/IEC 27001:2022. In: Proceedings of the IEEE International Conference on Cyber Management and Engineering (CyMaEn). IEEE (2023). https://doi.org/10.1109/CyMaEn57228.2023.10051114
25. Moyo, M., Abdullah, H., Nienaber, R.C.: Information security risk management in small-scale organisations: a case study of secondary schools computerised information systems. In: Proceedings of the IEEE Information Security for South Africa (ISSA) Conference, pp 14–16 . IEEE Press (2013). https://ieeexplore.ieee.org/abstract/document/6641062/. Accessed 11 May 2025
26. National Institute of Standards and Technology (NIST): Developing cyberresilient systems: a systems security engineering approach. Technical report, NIST SP 800-160, Vol. 2 Rev. 1, U.S. Department of Commerce (2021). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf. Accessed 11 May 2025
27. National Institute of Standards and Technology (NIST): NIST special publications: Nist sp 800-53, nist sp 800-46, nist sp 800-73, nist sp 800-76, nist sp 800-78, nist sp 800-116. Technical report, U.S. Department of Commerce (2025). https://csrc.nist.gov/publications/sp. Accessed 11 May 2025
28. Ozkan, B.Y., Spruit, M.: Assessing and improving cybersecurity maturity for SMEs: standardization aspects (2020). arXiv preprint arXiv:200701751. https://doi.org/10.48550/arXiv.2007.01751
29. Papachristofis, K., Vardoulias, G., Vavousis, K.: Comparative evaluation of cybersecurity maturity models and frameworks. In: Springer Lecture Notes in Computer Science. Springer (2024). https://doi.org/10.1007/978-3-031-81325-2_12. Accessed 11 May 2025
30. PCI Security Standards Council: Payment card industry data security standard (PCI-DSS) requirements and testing procedures, version 4.0. Technical standard, PCI SSC (2022). https://www.commerce.uwo.ca/pdf/PCI-DSS-v40.pdf
31. Peltier, T.R.: Preparing for ISO 17799. Inf. Syst. Secur. **11**(6), 21–28 (2003). https://doi.org/10.1201/1086/43324.11.6.20030101/40428.5
32. Simonsson, M., Johnson, P.: The IT organization modeling and assessment tool: correlating it governance maturity with the effect of it. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS), pp. 1–10. IEEE Press (2008). https://ieeexplore.ieee.org/abstract/document/4439136/. Accessed 11 May 2025
33. Singh, C.: The European approach to cybersecurity in 2023: a review of the changes brought in by the network and information security2 (nis2) directive 2022/2555. Int. Company Commer. Law Rev. **5**, 251–261 (2023). https://doi.org/10.1108/JFC-01-2023-0011
34. Statista Research Department: Cost of cybercrime worldwide from 2016 to 2028 (in trillion U.S. dollars) (2025). https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide. Accessed 24 June 2025
35. Susanto, H., Almunawar, M.N., Tuan, Y.C.: Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. Academia (2012). https://www.academia.edu/download/38094740/36585913256483.pdf. Accessed 11 May 2025
36. S´anchez, L.E., Villafranca, D., Fern´andez-Medina, E., et al.: Developing a maturity model for information system security management within small and medium size enterprises. In: Proceedings of the International Conference on Information Systems Security (ICISS) (2006)
37. Sánchez-García, I., Mejía, J., San Feliu Gilabert, T.: Cybersecurity risk assessment: a systematic mapping review, proposal, and validation. Appl. Sci. **13**(1), 395 (2023). https://doi.org/10.3390/app13010395

38. U.S. Department of Energy: Cybersecurity capability maturity model (c2m2) version 2.1. Technical report, U.S. Department of Energy (2022). https://www.energy.gov/ceser/c2m2-cybersecurity-capability-maturity-model. Accessed 11 May 2025
39. U.S. Department of Health & Human Services: Summary of the hipaa privacy rule. Pdf summary, HHS Office for Civil Rights (2000). https://www.hhs.gov/sites/default/files/privacysummary.pdf
40. Valdevit, T., Mayer, N., Barafort, B.: Tailoring ISO/IEC 27001 for SMEs: a guide to implement an information security management system in small settings. In: Communications in Computer and Information Science. Springer (2009). https://doi.org/10.1007/978-3-642-04133-4_17
41. Zhang, J., Yuan, W., Qi, W.: Research on security management and control system of information system in it governance. In: Proceedings of the IEEE International Conference on Computer Science and Service System (CSSS), pp. 668–673. IEEE Press (2011). https://ieeexplore.ieee.org/abstract/document/5974703/. Accessed 11 May 2025

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.