International Journal of Information Security (2026) 25:173
https://doi.org/10.1007/s10207-026-01329-8

REGULAR CONTRIBUTION

Exploratory empirical evaluation of the cyber-resistivity maturity and scoring framework (CRMSF): a multi-sector pilot study

Konstantinos Papachristofis[1] · Georgios Vardoulias[2] · Konstantinos Vavousis[3] · Costas Iordanou[1] · Yianna Danidou[4]

Received: 14 March 2026 / Accepted: 29 August 2026
© The Author(s) 2026

Abstract

Cybersecurity maturity models are widely used to assess and improve organizational security posture. However, many existing frameworks remain control-centric, static, and insufficiently adaptive to organizational scale and sector-specific constraints. These limitations are particularly evident in small and medium-sized enterprises and public-sector environments, where resource and governance challenges hinder effective implementation. The Cyber-Resistivity Maturity and Scoring Framework (CRMSF) is developed as a modular, scalable, and business-aligned framework that integrates maturity progression with explicit weighting, complexity, criticality, and benchmarking mechanisms. It combines technical and organizational practices within a unified self-assessment and scoring architecture designed to support risk-informed and actionable decision-making. This paper presents an initial empirical evaluation of CRMSF through a mixed-methods pilot study involving 26 cybersecurity professionals from multiple industry sectors. Data were collected through structured self-assessments across seven domains and twenty-four security categories, supplemented by surveys and expert interviews. Both quantitative and qualitative data were collected to evaluate usability, completeness, and contextual relevance. Based on structured practitioner evaluations, the results indicate meaningful perceived relationships between cybersecurity and cyber-resilience domains and suggest that practitioners regarded the framework as supportive for prioritizing initiatives and informing strategic investment decisions, while complementing established standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. The findings suggest strong perceived coherence and practical applicability of the framework, while identifying opportunities for refinement and further evaluation of scalability. The results provide initial, exploratory evidence that CRMSF is perceived as supporting adaptive, context-aware cybersecurity maturity assessment aligned with strategic governance and operational realities.

Keywords Cybersecurity maturity model · Cyber-resistivity · Security assessment · Cyber-resilience · Risk-based cybersecurity framework · Security capability prioritization · Cybersecurity governance

1 Introduction

As the global digital ecosystem continues to expand in complexity, interdependence, and scale, the cybersecurity threat landscape has become increasingly volatile. Modern organizations, regardless of size or sector, are required to adopt mature, adaptive, and context-aware approaches to managing cyber risk. The widespread adoption of cloud computing, remote work models, Internet of Things (IoT) technologies,

✉ Yianna Danidou
Yianna.danidou@cut.ac.cy

Konstantinos Papachristofis
kp222608@students.euc.ac.cy

Georgios Vardoulias
gvardoulias@hna.gr

Konstantinos Vavousis
kvavousis@acg.edu

Costas Iordanou
c.iordanou@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, American College of Greece, 6 Gravias Str., 15342 Ag. Paraskevi, Greece

[4] Department of Communication and Internet Studies, Cyprus University of Technology, Tsakkistos Building, Marathonos & Argyrou Drousioti corner, 3041 Limassol, Cyprus

Published online: 09 October 2026

and AI-enabled services has further eroded traditional network boundaries and increased exposure to advanced and persistent cyber threats [9, 20].

Over the past two decades, a wide range of cybersecurity maturity models (CMMs) have emerged to support the systematic development of information security capabilities. Among the most widely adopted are the NIST Cybersecurity Framework, now in version 2.0 [18], the Cybersecurity Capability Maturity Model (C2M2), and international standards such as ISO/IEC 27001 [12]. These frameworks provide structured mechanisms for assessing security posture, defining controls, and demonstrating regulatory compliance. However, existing studies highlight notable limitations: most maturity models remain largely control-centric and descriptive, assume uniform importance across security domains, and provide limited mechanisms for prioritization, weighting, or contextual adaptation based on organizational scale, sector, or risk appetite [2].

These limitations are especially pronounced in small and medium-sized enterprises (SMEs) and public-sector organizations, where cybersecurity resources, specialized expertise, and executive-level cyber literacy are often limited. Empirical evidence suggests that while frameworks such as NIST CSF and ISO/IEC 27001 are comprehensive, their implementation can be challenging for organizations lacking mature governance structures or dedicated security teams, resulting in fragmented adoption and limited strategic impact [1, 9]. Moreover, many existing CMMs do not explicitly distinguish between technical and organizational control layers, hindering effective prioritization, capability planning, and governance alignment [2].

The increasing complexity and interdependence of digital infrastructures have exposed significant limitations in existing cybersecurity maturity frameworks. In particular, there is a lack of empirically validated, weighted assessment models that explicitly connect preventive cybersecurity capabilities with cyber-resilience requirements across diverse organizational contexts [7, 19]. Although cybersecurity maturity models have provided structured guidance, they remain largely descriptive in nature and offer limited support for prioritization, weighting, and contextual adaptation, thereby constraining their practical decision-making value [22].

To address these challenges, the CRMSF has been developed as a holistic and modular alternative to traditional cybersecurity maturity models. As introduced in prior conceptual work [17], CRMSF is structured around four integrated modules:

1. A foundational maturity model comprising two sections, seven domains, and twenty-four security categories that explicitly differentiate organizational and technical practices;
2. A security grading mechanism defining Baseline, Advanced, and Maximal maturity levels;
3. A significance module that incorporates explicit weighting, criticality, and complexity dimensions; and
4. A scoring module that consolidates maturity data into actionable scores and dashboards.

Unlike static compliance-oriented frameworks, CRMSF emphasizes progressive adaptation and prescriptive guidance that are aligned with organizational and business contexts. The framework is designed to support self-assessment while accounting for sector-specific conditions, operational maturity, and available resources. By translating maturity outcomes into Cyber-Resistivity Security Classes, CRMSF aims to bridge the interpretive gap between technical security specialists and non-technical stakeholders. In this way, it supports informed strategic planning and cybersecurity governance [2, 17].

Central to the framework is the construct of cyber-resistivity. Building on the definition established in prior work [17], cyber-resistivity denotes an organization's capability to withstand, absorb, and adapt to evolving cyber threats, integrating both cybersecurity (preventive and defensive) and cyber-resilience (response, recovery, and adaptation) perspectives within a single construct. This construct is deliberately broader than several adjacent concepts. It differs from cybersecurity maturity, which characterizes the developmental state of preventive controls, and from cyber resilience, which emphasizes response and recovery; cyber-resistivity spans both. It extends beyond cyber robustness, the capacity to resist disruption without necessarily adapting, and beyond cyber readiness, a point-in-time state of preparedness, by incorporating an explicit adaptive and evolutionary dimension. Finally, in contrast to a general notion of organizational cyber capability, cyber-resistivity is operationalized as a structured, weighted, and prioritizable assessment construct. Conceptually, it is grounded in maturity-model theory [4] and is informed by socio-technical systems thinking, resilience-engineering principles, and the organizational-capability perspective, which jointly motivate its integrated treatment of organizational and technical capabilities across prevention, response, and adaptation. Table 1 summarizes how cyber-resistivity relates to and differs from these adjacent concepts, clarifying the specific construct evaluated in this study.

This paper presents the first empirical evaluation of CRMSF. While previous publications focused on the conceptual foundations and architectural design of the framework [17], the present paper evaluates its perceived usability, completeness, and contextual relevance across a diverse set of organizational environments. A multi-participant pilot study was conducted using a structured self-assessment survey comprising fifty-five items distributed across the seven

Table 1 Cyber-resistivity in relation to adjacent cybersecurity constructs

Concept	Brief description and relation to cyber-resistivity
Cyber-resistivity *(this framework)*	An organization's capability to withstand, absorb, and adapt to evolving cyber threats, integrating cybersecurity (prevention, defense) and cyber-resilience (response, recovery, adaptation) within a single, structured, weighted, and prioritizable assessment construct. Deliberately spans prevention through adaptation
Cybersecurity maturity	The developmental state of an organization's preventive and defensive controls. Narrower than cyber-resistivity, which extends beyond prevention to encompass response, recovery, and adaptation
Cyber resilience	The capacity to respond to, recover from, and adapt after disruptive cyber events. Complementary but partial: cyber-resistivity incorporates resilience while also covering the preventive dimension
Cyber robustness	The capacity to resist and absorb disruption without necessarily adapting. Cyber-resistivity subsumes robustness but adds an explicit adaptive and evolutionary dimension
Cyber readiness	A point-in-time state of preparedness against anticipated threats. Cyber-resistivity is a broader, developmental construct rather than a static snapshot of preparedness
Organizational cyber capability	A general notion of an organization's cyber-related abilities. Cyber-resistivity differs by being operationalized as a structured, weighted, and prioritizable assessment construct rather than a generic capability descriptor
Adaptation *(as a dimension)*	The ability to learn from events and evolve controls and posture over time. Not a standalone construct here but an integral dimension of cyber-resistivity, distinguishing it from robustness and readiness

CRMSF domains. The survey collected both quantitative (Likert-scale) and qualitative (open-ended) data addressing the framework's comprehensiveness, practicality, and strategic alignment.

The empirical objectives of this study are threefold:

1. To assess the perceived structural completeness and adequacy of the CRMSF, as evaluated by cybersecurity professionals across multiple industry sectors;
2. To examine the perceived functional value and distinctiveness of the Resistivity Evaluation Attributes (REAs) namely the maturity, weighting, criticality, complexity and benchmarking that underpin the framework's scoring logic;
3. To collect practitioner-driven improvement insights to support future refinement and further evaluation of the framework across regulatory, educational, and operational contexts.

CRMSF is positioned as a socio-technical maturity model, that is, a model that treats organizational and human factors (governance, culture, awareness, processes, and roles) and technical factors (controls, architectures, and tooling) as interdependent dimensions of capability, rather than assessing technical controls in isolation as predominantly control-centric maturity models tend to do. This characterization is reflected in the framework's structure, which explicitly distinguishes and jointly assesses organizational and technical practices within each security category and combines human-centric domains (such as Strategy and Awareness & Training) with technical domains. In doing so, this paper contributes to the growing body of literature advocating adaptive, stakeholder-aligned approaches to cybersecurity assessment [1, 2]. To address these objectives, the study adopts a mixed-methods research design combining quantitative survey analysis with qualitative expert feedback, examining practitioner perceptions and assessment outcomes across multiple sectors to provide initial evidence regarding the practical applicability, feasibility, and decision-support value of the CRMSF.

The present paper contributes to the literature on cybersecurity maturity assessment and cyber-resilience frameworks in several ways. First, it provides the initial empirical evaluation of the CRMSF, examining its usability, structural coherence, and contextual applicability across multiple industry sectors. Second, the research provides practitioner-based insights into the applicability of a prescriptive and modular cybersecurity maturity framework across organizations of different sizes, sectors, and regulatory environments. Third, the paper empirically examines the Resistivity Evaluation Attributes REAs, that underpin the framework's scoring logic, providing initial evidence of their functional distinctiveness and perceived value for context-aware prioritization of cybersecurity practices. Of these (REAs), maturity, weighting, criticality, and complexity are mandatory and jointly modulate the weighted aggregation at every level

of the hierarchy, whereas benchmarking is optional: it is operationalized through the Risk Adjustment Factor (RAF), which leaves the cumulative score unchanged when set to 1 and adjusts it for sector- and context-specific exposure when assigned any other value within its defined range.

Finally, the findings contribute empirical evidence regarding the practical value of integrating cybersecurity and cyber-resilience capabilities within a unified maturity and scoring architecture.

2 Materials and methods

2.1 Research questions formulation

This paper empirically evaluates the CRMSF, a modular, risk-based cybersecurity framework integrating distinctive factors such as weighting, criticality, complexity, maturity levels, and benchmarking, following established empirical evaluation and design science research principles [8, 10].

Guided by the overarching research objective to determine whether CRMSF provides a scalable, business-aligned, and empirically grounded mechanism to assess organizational cyber-resistivity, this investigation addresses five research questions consistent with best practices for empirical framework evaluation studies [4, 8].

RQ1: How can cybersecurity maturity and cyber-resilience be integrated within a unified assessment framework that reflects organizational context and operational complexity?

RQ2: How can qualitative cybersecurity practices be transformed into a consistent quantitative scoring mechanism that supports prioritization and benchmarking?

RQ3: Which evaluation attributes are required to capture the relative criticality, complexity, and importance of cybersecurity capabilities across organizational environments and especially for small and medium organizations?

RQ4: To what extent does the CRMSF enable the classification of organizational and technical cybersecurity practices while remaining scalable and vendor-neutral across organizations of different sizes and regulatory environments?

RQ5: To what extent does CRMSF provide improved assessment granularity, interpretability, and practical value compared to existing frameworks and maturity models (e.g. NIST CSF, ISO 27001)?

While these research questions articulate the broader design aspirations of the CRMSF, the present pilot study addresses them within the bounds of a perception-based exploratory evaluation. Accordingly, questions concerning the scoring mechanism (RQ2), scalability and vendor-neutrality (RQ4), and comparison with established frameworks (RQ5) are examined here through practitioners' perceived usability, applicability, granularity, and decision-support value, rather than through validation of the scoring computation, demonstrated scalability, or measured comparative performance, which remain the subject of dedicated future work.

These research questions guide the empirical evaluation of the CRMSF, focusing on the applicability, perceived effectiveness, and structural coherence of its design, weighting logic, and overall usability. Through a modular development approach combined with empirical data collection from practitioner evaluation, the study examines practitioners' perceptions of the framework's applicability across organizations of different sizes and sectors, its perceived support for risk-based resource prioritization, its perceived contribution to strengthening organizational cybersecurity posture, and its adaptability to an evolving threat landscape. The findings aim to contribute not only to academic research on cybersecurity maturity and scoring models, but also to the practical enhancement of cybersecurity decision-making and resilience across diverse sizes and industries.

Each research question is explicitly mapped to specific components of the empirical design, data collection instruments, and analytical procedures, ensuring methodological traceability between the theoretical foundations of the CRMSF and its empirical evaluation.

By addressing these research questions, this study establishes the conceptual and methodological foundations for the development and empirical evaluation of the CRMSF.

The broader CRMSF research program pursued a set of framework-development objectives, namely, the systematic analysis of existing maturity models and identification of structural gaps; the design of a modular, vendor-neutral framework integrating cybersecurity and cyber-resilience; the definition and formalization of the Resistivity Evaluation Attributes (REAs); the development of a risk-based scoring mechanism; and the operationalization of the framework through a self-assessment tool. These development objectives were addressed in the preceding conceptual and architectural publications of this doctoral research series [17] and are summarized here only to situate the present study; they are not the subject of this paper.

Building on that foundation, the present paper pursues the three empirical evaluation objectives stated in the Introduction: to assess the perceived structural completeness and adequacy of the CRMSF; to examine the perceived functional value and distinctiveness of the REAs that underpin its scoring logic; and to collect practitioner-driven improvement insights. Accordingly, this study constitutes the empirical evaluation stage of the research program, distinct from the development stages reported previously.

Consistent with the exploratory, perception-based design of this pilot study, the following evaluation propositions (EP) were formulated to guide the interpretation of practitioner feedback. They are not subjected to confirmatory statistical testing; rather, they structure the qualitative and descriptive

examination of how practitioners perceived the framework, and they are revisited in Sect. 4.8 in terms of the evidence the pilot can and cannot provide. Where a proposition extends beyond what an exploratory pilot can establish, this is stated explicitly within the proposition itself.

EP1: Practitioners perceive a multi-dimensional, risk-driven framework as providing greater assessment granularity and interpretability than traditional single-axis maturity models.

EP2: Practitioners perceive that the integration of weighted evaluation attributes supports the prioritization of cybersecurity practices and investments in relation to organizational risk exposure.

EP3: Practitioners perceive that integrating cybersecurity and cyber-resilience within a single prescriptive framework helps align security-posture improvements with operational continuity objectives.

EP4: A modular framework architecture is expected to facilitate scalable adoption across organizations of different sizes, sectors, and regulatory environments. The present pilot examines this proposition partially, through practitioner perceptions across a multi-sector sample; its full assessment requires larger-scale validation beyond the scope of this study.

EP5: Relative to existing frameworks, the proposed approach is expected to yield more consistent and actionable assessment outcomes. This pilot addresses EP5 only at the level of perceived comparative value reported by practitioners; a confirmatory comparative claim would require a dedicated comparative design and is therefore not established here.

This pilot study evaluates three aspects of the CRMSF: (i) the perceived structural completeness and adequacy of its sections, domains and security categories; (ii) its perceived usability, clarity, and decision-support value; and (iii) the functional distinctiveness and perceived value of the Resistivity Evaluation Attributes (REAs) that underpin the scoring logic. It does not constitute a validation of the underlying mathematical scoring model, nor a demonstration of performance superiority over established frameworks. These aspects, namely the formal validation of the scoring computation and controlled comparative evaluation, are deliberately deferred to dedicated subsequent studies. This delineation ensures that the conclusions drawn remain commensurate with the exploratory, perception-based design of the study.

Operationally, cyber-resistivity maturity is represented in this study through the CRMSF structure together with the Resistivity Evaluation Attributes. Consistent with the unit of analysis defined in Sect. 2.2.2, what this study evaluates is the practitioners' assessment of this operationalized construct, the perceived relevance, adequacy, and applicability of these domains, categories, and attributes, rather than a direct measurement of organizational cyber-resistivity levels.

2.2 Data collection

Following established principles in empirical information security and mixed-methods research, the study adopted a two-phase methodological approach comprising a theoretical phase and an empirical evaluation phase [8, 21].

2.2.1 Theoretical study

The theoretical phase consolidated the findings of the first two studies in this doctoral research series, which collectively established the conceptual foundations and internal coherence of the CRMSF.

The first paper developed the conceptual rationale and literature-based justification for a resistivity-oriented cybersecurity maturity model, identifying structural limitations in universal maturity models and compliance-driven frameworks, particularly with respect to contextual adaptation, prioritization, and risk sensitivity [16]. The second paper introduced the complete CRMSF architecture, formally defining its four integrated modules (Foundation, Security Grades, Significance, and Scoring) and operationalizing the Resistivity Evaluation Attributes (REAs) of maturity, weighting, complexity, and criticality [17].

This theoretical consolidation phase ensured conceptual rigor and internal consistency prior to empirical field validation, in line with design science research principles for artifact evaluation [10].

2.2.2 Empirical study

The empirical phase evaluated the usability, completeness, and contextual relevance of CRMSF through a structured multi-participant pilot study conducted across multiple industry sectors.

Data collection instruments were specifically developed for this study and comprised:

1. The CRMSF Self-Assessment Tool (SA-Tool), a digital instrument that operationalizes the seven domains and 24 security categories of the framework through weighted organizational and technical practices;
2. A structured CRMSF Evaluation Questionnaire, consisting of 55 items combining five-point Likert-scale measures with open-ended qualitative questions;
3. The peer-reviewed publication "Developing Cyber-Resistivity Maturity and Scoring Framework (CRMSF) for Any Size of Organization", which served as a foundational conceptual instrument, providing the theoretical grounding, domain structure, scoring logic, and weighting principles upon which the empirical instruments were designed and validated.

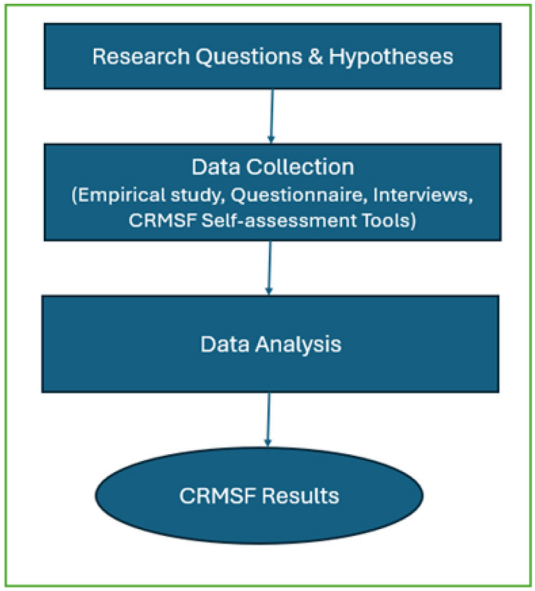


Fig. 1 Empirical phase design

The 55 evaluation items, together with their mapping to the CRMSF sections, domains, categories, evaluation attributes, and research questions, are provided in Appendix B (Table 14).

Together, these instruments enabled the systematic capture of both quantitative assessments and qualitative expert judgments, consistent with best practices in mixed-methods cybersecurity research [8]. Figure 1, depicts the empirical phase design.

(a) Sampling design A purposive sampling strategy was employed to recruit cybersecurity professionals and subject-matter experts with demonstrated practical experience in cybersecurity governance, implementation, or assurance. Participants included Chief Information Security Officers (CISOs), Information Security Managers (ISMs), auditors, and technical cybersecurity practitioners from a diverse range of sectors, including financial services and banking, manufacturing, technology and SaaS, education, retail and eCommerce, maritime, internet services, legal (law) services, and gambling.

In total, 34 professionals were invited to participate, of whom 26 completed the study, yielding a response rate of approximately 76%. Beyond the minimum eligibility criteria stated below, purposive selection deliberately sought diversity across professional roles, depth of cybersecurity expertise, industry sectors, and organization sizes (small, medium, and large) so that the framework could be evaluated across heterogeneous organizational contexts.

The minimum inclusion criteria were that all participants possessed a minimum of three years of professional cybersecurity experience and were actively involved in strategic or operational cybersecurity decision-making. The final sample comprised 26 participants (n = 26), of whom seven were identified as senior expert reviewers based on their roles and extensive professional experience. Given the exploratory and pilot nature of the study, the sample size is consistent with empirical framework validation studies involving expert participants, where the focus is on practitioner insight and interpretive evaluation rather than statistical generalization. In terms of organizational location, 24 participants were based in organizations headquartered in Greece, one in Cyprus, and one in the Netherlands. Organizational reach, however, extended well beyond the country of headquarters: 19 of the 26 participants belonged to organizations with an international presence, predominantly across other European countries. This distinction between headquarters location and operational reach supports evaluation of the framework across both national and cross-border operational contexts, while the geographic concentration of headquarters is acknowledged as a limitation (Sect. 2.6). Although the participant group reflects multiple industry sectors and includes professionals with experience in multinational environments, the sample size remains limited and a substantial portion of participants originate from a specific geographic region. Consequently, the findings should be interpreted as indicative insights derived from expert practitioners rather than as statistically representative of the broader cybersecurity practitioner population. Table 2 outlined the participants' profiles.

(b) Instruments and protocol

Prior to active participation, all respondents received the CRMSF Presentation to Participants slide deck summarizing the framework structure, study objectives, and confidentiality terms. Participants then attended one of five scheduled online group briefing sessions (approximately 60 min each) to ensure a shared understanding of the CRMSF framework, the self-assessment process, and the evaluation objectives. Following informed consent and signed participation forms, formal invitations were issued and participants proceeded to complete the SA-Tool and the Evaluation Questionnaire independently.

Participants were instructed to perform the SA-Tool assessments across the relevant organizational domains, adjust weighting or complexity factors where applicable, and submit their evaluations through the online Evaluation Form. The data collection phase lasted approximately two months, allowing participants sufficient time to review supporting materials and reflect on their organizational context.

Participants were provided with working access to the SA-Tool for approximately two months. Larger organizations, and several medium-sized organizations, were granted dedicated SA-Tool workspaces, whereas smaller organizations were given shared workspace access (two to three

participants per workspace), reflecting their intent to explore the framework's logic across selected domains rather than to conduct an exhaustive organizational assessment. Due to confidentiality constraints, the organizational scores and improvement actions generated during SA-Tool use were neither collected nor disclosed; the empirical analysis therefore focuses on structured practitioner evaluation of the framework rather than on the disclosure of organizational assessment results.

The evaluation instrument was structured into five sections aligned with the study's research questions:

(A) Demographic and organizational context (role, sector, organization size, implemented frameworks);
(B) Evaluation of CRMSF domains and security categories in terms of conceptual completeness and practical adequacy;
(C) Weighting and prioritization mechanisms, including simulated prioritization and resource allocation exercises;
(D) Overall framework usability and comparative assessment against established frameworks (e.g., NIST CSF, ISO/IEC 27001, CIS, C2M2); and
(E) Open qualitative feedback on adoption challenges, contextual requirements, and improvement opportunities.

NIST CSF and ISO/IEC 27001 were used as the primary comparative reference points in the evaluation instrument. These were selected because they are the most widely adopted instruments in practice, reflected in their incorporation, directly or in adapted form, into EU member-state implementations of the NIS2 Directive, and because the subject-matter experts were most familiar with them, making them the most meaningful anchors for practitioner comparison. A comprehensive structural comparison of these and other models (CMM, COBIT, C2M2) was conducted in a prior study in this research series [16] and is not repeated here. It is acknowledged that these instruments differ in nature. ISO/IEC 27001:2022 is a governance and compliance standard that does not define maturity levels. The NIST CSF, by contrast, defines four Implementation Tiers that characterize the degree to which an organization's cybersecurity risk-management practices are formalized and integrated, and these tiers are widely used in practice as maturity levels, including in NIST-based self-assessment tools. The CSF is therefore frequently applied as a maturity model, even though, unlike dedicated maturity models, it was not originally structured around a comprehensive maturity-scoring scheme. These distinctions inform the comparative positioning of the CRMSF rather than diminishing the established value of either instrument.

The instrument combined structured Likert-scale measurements with prioritization exercises and qualitative feedback to capture both measurable practitioner perceptions and expert reasoning. Conceptually, the CRMSF assessment process follows a structured progression from section-level and domain-level evaluation to security category assessment, maturity level assignment, and weighted scoring, ultimately producing an aggregated cyber-resistivity assessment outcome.

The unit of analysis in this study is the structured practitioner evaluation of the CRMSF and its Resistivity Evaluation Attributes (REAs), as captured through the 55-item Evaluation Questionnaire and informed by hands-on use of the SA-Tool. The reported scores represent expert practitioners' assessments of the framework's structural completeness, usability, clarity, functional differentiation, and perceived applicability. They do not represent measured maturity levels of the participants' organizations, nor direct comparative measurements against other frameworks. Although participants applied the SA-Tool within their own organizational context during the evaluation period, the resulting organizational scores and improvement actions were intentionally not collected, for the confidentiality reasons noted above.

These seven senior experts, identified on the basis of their roles and extensive professional experience, contributed in two ways: they completed the SA-Tool and Evaluation Questionnaire as participants, and they additionally took part in the expert-review meetings, where they validated the interpretation of the aggregated results, helped refine the emergent qualitative themes, and assessed whether any evaluation dimension was missing. Their input thus served a triangulation and interpretive-validation function rather than contributing additional quantitative observations. These sessions were used to validate interpretation of the results and refine analytical insights derived from the survey responses.

(c) Data analysis and validation procedures

Following data collection, quantitative responses were analyzed to assess consistency, interpretability, and prioritization patterns, while qualitative responses were subjected to thematic analysis to identify recurring insights and contextual considerations. To enhance methodological rigor and validity, a triangulation approach was applied through multiple expert review sessions involving senior participants. These sessions supported interpretation alignment, validation of findings, and refinement of conclusions, contributing to the robustness and credibility of the empirical results [14].

All responses were anonymized prior to analysis, and qualitative feedback was used to complement quantitative findings and inform iterative refinement of the CRMSF structure and scoring logic.

2.3 Contextual and descriptive data characterization

The demographic and contextual characteristics of participants and organizations are presented to support transparent interpretation of the empirical findings, since maturity and scoring outcomes must be read in light of professional expertise, organizational context, governance environment, and resource constraints [3, 4].

These descriptive tables document the heterogeneity of the sample and the contexts from which practitioner evaluations were drawn. Several role, sector, and role-by-size combinations are represented by a single participant; such single-case entries are reported solely to characterize sample diversity and should not be interpreted as evidence of sectoral, role-specific, or size-specific applicability or generalizability of the framework.

Table 2 summarizes the professional profiles of participants, including organizational roles, experience, and educational background. The distribution of senior and operational roles (CISOs, information security managers, auditors, and technical implementers), combined with extensive experience and relevant qualifications, establishes the expertise-based nature of the sample.

Table 3 presents the organizational context of participating entities by industry type, organizational size, sector of operation, and organizational scope. The table shows substantial heterogeneity across private and public organizations, national and multinational entities, and a wide range of industry sectors. This diversity is essential for evaluating whether the CRMSF can be meaningfully applied across different organizational structures, operational scales, and sectoral conditions, rather than being tailored to a single industry profile.

For the purposes of classification consistency across all subsequent tables, organizational size is defined according to employee count as follows: Small (<50 employees), Medium (50−249 employees), and Large (>=250 employees). These standardized thresholds are applied uniformly throughout the paper to ensure terminological clarity and analytical coherence.

Table 4 combines organizational size with reported availability of cybersecurity resources (personnel, time, and budget). The observed variation highlights real-world constraints that directly influence the implementation and effectiveness of controls.

Table 5 outlines the frameworks, standards, certifications, and regulatory instruments implemented by participating organizations (e.g., ISO/IEC 27001, NIST, CIS, GDPR, NIS2, PCI DSS, DORA), illustrating the governance and compliance landscape within which participants operate and which shapes their cybersecurity priorities and investment decisions.

Table 6 examines the alignment between participants' roles and their organizational environments, combining position with organization size and industry type. This clarifies the decision-making level from which CRMSF inputs were provided, indicating that the framework was primarily evaluated by roles with strategic or governance-level responsibility across organizations of varying scale.

Collectively, these data establish the empirical boundary conditions of the study, ensuring that the findings are interpreted within realistic operational contexts rather than as decontextualized metrics.

2.4 Data analysis

The data analysis followed a mixed-methods research design, integrating quantitative statistical analysis of Likert-scale responses with qualitative thematic analysis of open-ended feedback. This approach enabled methodological triangulation between numerical assessment outcomes and expert perceptions, enhancing interpretive robustness and analytical credibility in the empirical evaluation of the CRMSF [8].

The quantitative analysis focused on evaluating descriptive patterns, internal consistency, and relational coherence across CRMSF domains and evaluation attributes, while remaining aligned with the exploratory and pilot-oriented nature of the study.

2.4.1 Quantitative analysis

Quantitative data were derived from the CRMSF Evaluation Questionnaire completed by twenty-six (n = 26) cybersecurity professionals representing diverse organizational roles and industry sectors. All closed-ended items were measured using a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree).

Of the 26 participants, three did not complete the Likert component of the Evaluation Questionnaire and are therefore excluded from the quantitative analyses, which are based on an analytic sample of n = 23; these three respondents are retained in the demographic, contextual, and qualitative analyses, so that the full sample (n = 26) is preserved for those purposes. For a small number of individual items, some respondents elected not to answer questions outside their immediate area of responsibility. When asked, these respondents indicated that their assessment for such items fell between 4 and 5 but preferred not to commit to a specific value; their answered items were, in 85–100% of cases, within the 4–5 range. Accordingly, these sporadic item-level gaps were handled by midpoint imputation at 4.5. A sensitivity analysis comparing this approach with pairwise-available computation (no imputation) confirmed that the results are substantively identical, with a maximum divergence in category means of 0.019 across all 24 categories.

Table 2 Participant professional profile and expertise

Position	Experience	Education level
CISO (n = 8)	Years in current role: median 2.5 (range 1−11), mean 4.2	Master (n = 5); Bachelor (n = 2); PhD (Doctorate) (n = 1)
	Total professional experience: median 22.5 (range 15−40), mean 23.8	
IT Manager (n = 5)	Years in current role: median 5 (range 2−19), mean 8.2	Master (n = 2); Bachelor (n = 1); PhD (Doctorate) (n = 1); Diploma (n = 1)
	Total professional experience: median 24 (range 11−28), mean 21	
Security implementer/engineer (n = 4)	Years in current role: median 4 (range 4−6), mean 4.5	Bachelor (n = 3); Diploma (n = 1)
	Total professional experience: median 23 (range 17−26), mean 22.2	
ISM (n = 4)	Years in current role: median 4 (range 1.5−12), mean 5.4	Master (n = 3); Bachelor (n = 1)
	Total professional experience: median 20 (range 12−26), mean 19.5	
System administrator (n = 2)	Years in current role: median 6.5 (range 5−8), mean 6.5	Bachelor (n = 1); Diploma (n = 1)
	Total professional experience: median 19 (range 18−20), mean 19	
Digital risk insurance broker (n = 1)	Years in current role: median 12 (range 12−12), mean 12	Master (n = 1)
	Total professional experience: median 15 (range 15−15), mean 15	
General director (n = 1)	Years in current role: median 1 (range 1−1), mean 1	PhD (Doctorate) (n = 1)
	Total professional experience: median 30 (range 30−30), mean 30	
ICT & Digital learning administrator (n = 1)	Years in current role: median 1 (range 1−1), mean 1	Master (n = 1)
	Total professional experience: median 20 (range 20−20), mean 20	

Unless otherwise stated, the descriptive, reliability, and correlation statistics reported below are based on this analytic sample. Where specific items were mandatory and therefore completed by all 26 participants, notably the weighting items reported in Sect. 3, analyses of those items are based on the full sample ($n = 26$), as indicated in the corresponding tables.

Analyses were conducted at both domain and security category levels, consistent with the hierarchical design of the CRMSF. Descriptive statistics were used to summarize central tendency and dispersion, while reliability and correlation analyses were applied to assess internal consistency and relational patterns among maturity, criticality, and complexity attributes.

Internal consistency was evaluated using Cronbach's α, adopting a threshold of $\alpha \geq 0.70$ as indicative of acceptable reliability for exploratory and validation-oriented studies [15]. Given the ordinal nature of Likert-scale data and the moderate sample size, non-parametric correlation analysis was performed using Spearman's rank-order correlation coefficient, which does not assume normality and is appropriate for monotonic associations in ordinal datasets [13].

2.4.1.2 Scoring architecture: functional overview To make the present evaluation self-contained, this subsection summarizes the functional logic of the CRMSF scoring architecture, that is, how an assessment is structured and how the Resistivity Evaluation Attributes (REAs) participate in it. The complete mathematical specification of the scoring computation, including its normative parameters, constitutes a separate methodological contribution and is therefore described here

Table 3 Organizational context and structural characteristics of participating entities

Industry type	Organization size	Sector of operation	Type of organization
Financial services/banking (n = 7)	Large (n = 4)	Private sector: (n = 7)	National: (n = 4)
	Small (n = 2)		Multinational: (n = 3)
	Medium (n = 1)		
Manufacturing/industrial (n = 6)	Large (n = 6)	Private sector: (n = 6)	Multinational: (n = 5)
			National: (n = 1)
Technology and SaaS (n = 3)	Medium (n = 1)	Private sector: (n = 3)	Multinational: (n = 2)
	Small (n = 1)		National: (n = 1)
	Large (n = 1)		
Education (n=3)	Medium (n = 2)	Private sector: (n = 2)	National: (n = 2)
	Large (n = 1)	Public sector: (n = 1)	Multinational: (n = 1)
Retail & eCommerce (n = 2)	Large (n = 2)	Private sector: (n = 2)	Multinational: (n = 1)
			National: (n = 1)
Maritime (n = 2)	Large (n = 1)	Private sector: (n = 2)	National: (n = 1)
	Small (n = 1)		Multinational: (n = 1)
Internet service provider (n = 1)	Medium (n = 1)	Private sector: (n = 1)	National: (n = 1)
Law (n=1)	Medium (n = 1)	Private sector: (n = 1)	National: (n = 1)
Gambling (n = 1)	Large (n = 1)	Private sector: (n = 1)	Multinational: (n = 1)

Table 4 Organizational cybersecurity resource availability and capability context

Organization size	Available cybersecurity resources	Industry type
Large (n = 16)	Moderate: (n = 11)	Manufacturing/industrial (n = 6)
	High: (n = 3)	Financial Services/Banking (n = 4)
	Low: (n = 2)	Retail & eCommerce (n = 2)
		Education (n = 1)
		Maritime (n = 1)
		Technology & SaaS (n = 1)
		Gambling (n = 1)
Medium (n = 6)	Moderate: (n = 5)	Education (n = 2)
	High: (n = 1)	Financial Services/Banking (n=1)
		Internet Service Provider (n = 1)
		Technology & SaaS (n = 1)
		Law (n = 1)
Small (n = 4)	Low: (n = 3)	Financial Services/Banking (n = 2)
	Moderate: (n = 1)	Technology & SaaS (n = 1)
		Maritime (n = 1)

at the functional level required to interpret the present results, rather than in full formal detail.

The CRMSF organizes cybersecurity capabilities hierarchically: individual practices are grouped into security categories, categories into domains, and domains into two sections (cybersecurity and cyber-resilience). Each practice is assessed against a maturity structure defined by three security grades (Baseline, Advanced, and Maximal) with maturity status expressed on a normalized scale to enable comparison across heterogeneous practices.

Assessment outcomes are aggregated upward through a weighted roll-up: practice- and category-level evaluations are combined into domain-level scores, which are in turn consolidated into section- and framework-level outcomes. Within this aggregation, the REAs perform distinct functions. Maturity captures the assessed implementation status of a practice; weighting expresses the relative importance assigned to a component within its parent level; criticality reflects the consequence of a capability gap for the organization; and complexity reflects the implementation effort and

Table 5 Implemented cybersecurity frameworks, certifications, and regulatory requirements

Implemented frameworks/certifications/regulations	Industry type	Sector of operation
GDPR (n = 19)	Financial services/banking (n = 6)	Private sector (n = 18)
	Education (n = 3)	Public Sector (n = 1)
	Retail & eCommerce (n = 2)	
	Maritime (n = 2)	
	Manufacturing/industrial (n = 2)	
	Internet service provider (n = 1)	
	Law (n = 1)	
	Technology & SaaS (n = 1)	
	Gambling (n = 1)	
ISO 27001 (n = 15)	Manufacturing/industrial (n = 5)	Private sector (n = 15)
	Financial services/banking (n = 4)	
	Technology & SaaS (n = 3)	
	Internet Service Provider (n = 1)	
	Retail & eCommerce (n = 1)	
	Gambling (n = 1)	
NIS2 (n = 9)	Manufacturing/industrial (n = 4)	Private sector (n = 9)
	Financial services/banking (n = 2)	
	Internet service provider (n = 1)	
	Maritime (n = 1)	
	Technology & SaaS (n = 1)	
PCI DSS (n=6)	Financial services/banking (n = 4)	Private sector (n = 6)
	Manufacturing/industrial (n=1)	
	Gambling (n = 1)	
DORA (n=6)	Financial services/banking (n = 4)	Private sector (n = 6)
	Manufacturing/industrial (n = 1)	
	Technology & SaaS (n=1)	
NIST (n = 4)	Manufacturing/industrial (n = 2)	Private sector (n = 4)
	Financial services/banking (n=1)	
	Technology & SaaS (n = 1)	
CIS (n = 2)	Financial services/banking (n = 2)	Private sector (n = 2)
None (n = 1)	Manufacturing/industrial (n = 1)	Private sector (n = 1)
Other (n = 1)	Education (n = 1)	Private sector (n = 1)

difficulty associated with a capability. These attributes jointly modulate the relative contribution of each component to the aggregated outcome, so that the assessment reflects not only whether practices are present, but their relative importance and feasibility within a given organizational context.

Assessment proceeds hierarchically from individual practices to the framework-level Cyber-Resistivity Security Class. The Resistivity Evaluation Attributes modulate the weighted aggregation at each level. The specific weighting, and complexity values are sector- and context-adjustable rather than fixed. Figure 2 summarizes this functional flow, in which assessment proceeds hierarchically from individual practices to the framework-level Cyber-Resistivity Security Class, the REAs modulate the weighted aggregation at each level, and benchmarking via the Risk Adjustment Factor provides an optional context adjustment. The normative parameter values referenced in the figure are part of the framework's separately specified scoring model and are not reproduced here.

The framework also accommodates partial assessment: organizations may pursue selected grade targets (for example, Baseline-only or Baseline-plus-Advanced), in which case non-pursued grades are treated as out of scope for that assessment rather than as failures. Finally, aggregated framework-level outcomes are mapped onto four interpretive bands, namely the Cyber-Resistivity Security Classes, which translates quantitative outcomes into qualitative resilience categories for stakeholder communication.

Table 6 Alignment of professional roles with organizational and industry context

Current position	Organization size	Industry type
CISO (n = 8)	Large (n = 6)	Technology & SaaS (n = 3)
	Medium (n = 1)	Manufacturing/industrial (n = 3)
	Small (n = 1)	Maritime (n = 1)
		Financial services/banking (n = 1)
IT Manager (n = 5)	Medium (n= 2)	Financial services/banking (n = 1)
	Large (n = 2)	Internet service provider (n = 1)
	Small (n = 1)	Education (n=1)
		Maritime (n = 1)
		Gambling (n = 1)
Security implementer/engineer (n = 4)	Large (n = 3)	Retail & eCommerce (n = 2)
	Small (n = 1)	Manufacturing/industrial (n = 1)
		Financial services/banking (n = 1)
ISM (n = 4)	Large (n = 4)	Financial services/banking (n = 3)
		Manufacturing/industrial (n = 1)
System administrator (n = 2)	Large (n = 1)	Manufacturing/industrial (n = 1)
	Medium (n = 1)	Law (n = 1)
Digital risk insurance broker (n = 1)	Small (n = 1)	Financial services/banking (n = 1)
General director (n = 1)	Medium (n = 1)	Education (n = 1)
ICT & Digital learning administrator (n = 1)	Medium (n = 1)	Education (n = 1)

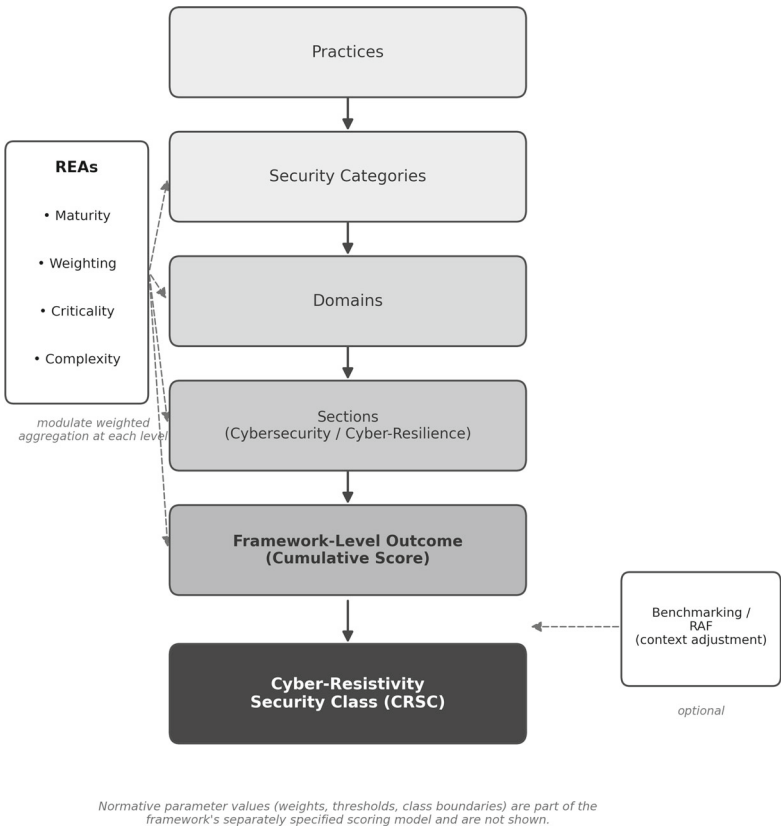


Fig. 2 Functional overview of the CRMSF scoring architecture

It is important to delineate the role of this architecture in the present study. The scoring logic is described here to clarify what the participants evaluated and how the REAs are situated within the framework. This study evaluates the perceived adequacy, usability, and functional distinctiveness of these components; it does not evaluate or validate the numerical scoring computation itself, which together with its normative parameters and the precise boundaries of the Security Classes is the subject of dedicated, separately evaluated work.

2.4.1.2 Descriptive statistics at domain and security category level

Descriptive statistics were computed at both CRMSF domain level and security category level to capture practitioner perceptions regarding the relevance, adequacy, and structural completeness of the proposed framework across heterogeneous organizational contexts.

For each CRMSF domain, composite domain scores were calculated by averaging participant responses across the corresponding domain-level items. Composite domain medians and interquartile ranges were computed from the per-respondent composite domain scores. This aggregation approach reflects the framework's hierarchical structure and supports comparative interpretation across domains. Table 7 and Fig. 3 presents the mean, median, standard deviation, and 95% confidence intervals for each domain.

Across all seven CRMSF domains, mean scores ranged from 4.30 to 4.54, indicating consistently high perceived relevance and adequacy. The relatively narrow confidence intervals suggest strong convergence of expert judgment, while slightly higher variance observed within technically intensive domains (e.g., Fortification) reflects expected heterogeneity arising from differences in infrastructure maturity and resource availability across organizations.

To provide finer analytical granularity, descriptive statistics were also computed at the security category level. Composite category scores were calculated for each category item, directly reflecting practitioner evaluations of specific cybersecurity and cyber-resilience capabilities. Table 8 and Fig. 4 summarizes the corresponding means, standard deviations, and confidence intervals.

The high median values, several of which reach the scale maximum, should be interpreted with caution. In several categories, notably Endpoint Protection and Email Security, approximately 70% of responses were at the maximum value of 5, producing medians of 5 alongside lower means and non-trivial standard deviations. While this pattern is consistent with strong perceived acceptance of the framework, it may also reflect ceiling effects and limited discriminative power of the five-point ordinal instrument. The bounded scale, the small analytic sample, and these ceiling effects should be borne in mind when interpreting the confidence intervals and any subgroup comparisons reported below.

Overall, category-level results indicate that CRMSF security categories were perceived as practically applicable and conceptually coherent, with variation patterns consistent with staged and progressive maturity development rather than structural deficiencies.

2.4.1.3 Reliability and internal consistency analysis

Reliability analysis was conducted to evaluate the internal consistency of CRMSF measurement constructs at the domain level. Cronbach's α values were calculated for each domain based on the associated measurement items, with results summarized in Table 9.

All CRMSF domains met the recommended minimum threshold of 0.70 [15], with α values ranging from 0.722 to 0.945, indicating acceptable to excellent internal consistency. As Cronbach's α is of limited informativeness for two-item scales, the inter-item Spearman correlation and the Spearman–Brown coefficient are reported alongside α for the two-item domains; these confirm satisfactory internal consistency without indicating redundancy. No domain exhibits an α above 0.95, and the multi-item domains (Fortification, $\alpha = 0.945$; Restoration & Evolution, $\alpha = 0.894$) reflect coherent but non-redundant item sets representing closely related operational practices.

These findings are consistent with the use of CRMSF domain constructs for composite scoring and subsequent relational analysis within this exploratory study.

2.4.1.4 Inter-domain and attribute relationship analysis

To examine relationships among CRMSF domains and key evaluation attributes, inter-domain and attribute-level correlation analysis was performed using Spearman's rank-order correlation coefficient. The analysis focused on associations between perceived maturity levels, assigned criticality, assessed complexity, and aggregated domain scores.

Correlation matrices revealed moderate to strong positive associations between practitioners' evaluations of core preventive domains and their evaluations of detection-, containment-, and restoration-oriented domains. Because the underlying data represent practitioner evaluations of the CRMSF domains, these associations indicate that participants tended to evaluate the domains in a mutually consistent manner. Those who assigned relatively higher ratings to one domain tended to assign relatively higher ratings to related domains, and those who rated a domain more conservatively tended to do so across related domains, while meaningful variation across the five-point scale was retained. They are therefore interpreted as evidence of perceived coherence among the domains, a coherent relational structure in how practitioners assessed the framework, rather than as evidence that the underlying organizational cybersecurity capabilities

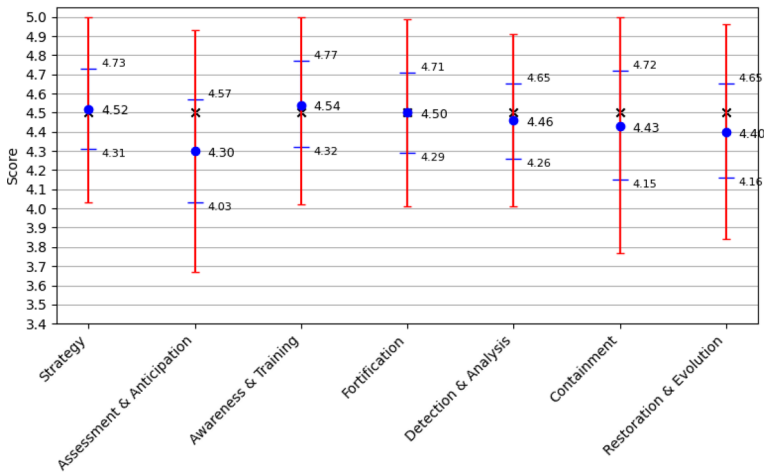


Fig. 3 Statistics of CRMSF domains. Points denote mean scores ($n = 23$), crosses indicate median values. Blue bars represent 95% confidence intervals and red bars indicate $\pm$ one standard deviation. Numerical annotations show the corresponding bounds. Confidence-interval and standard-deviation bounds are capped at the response-scale maximum of 5

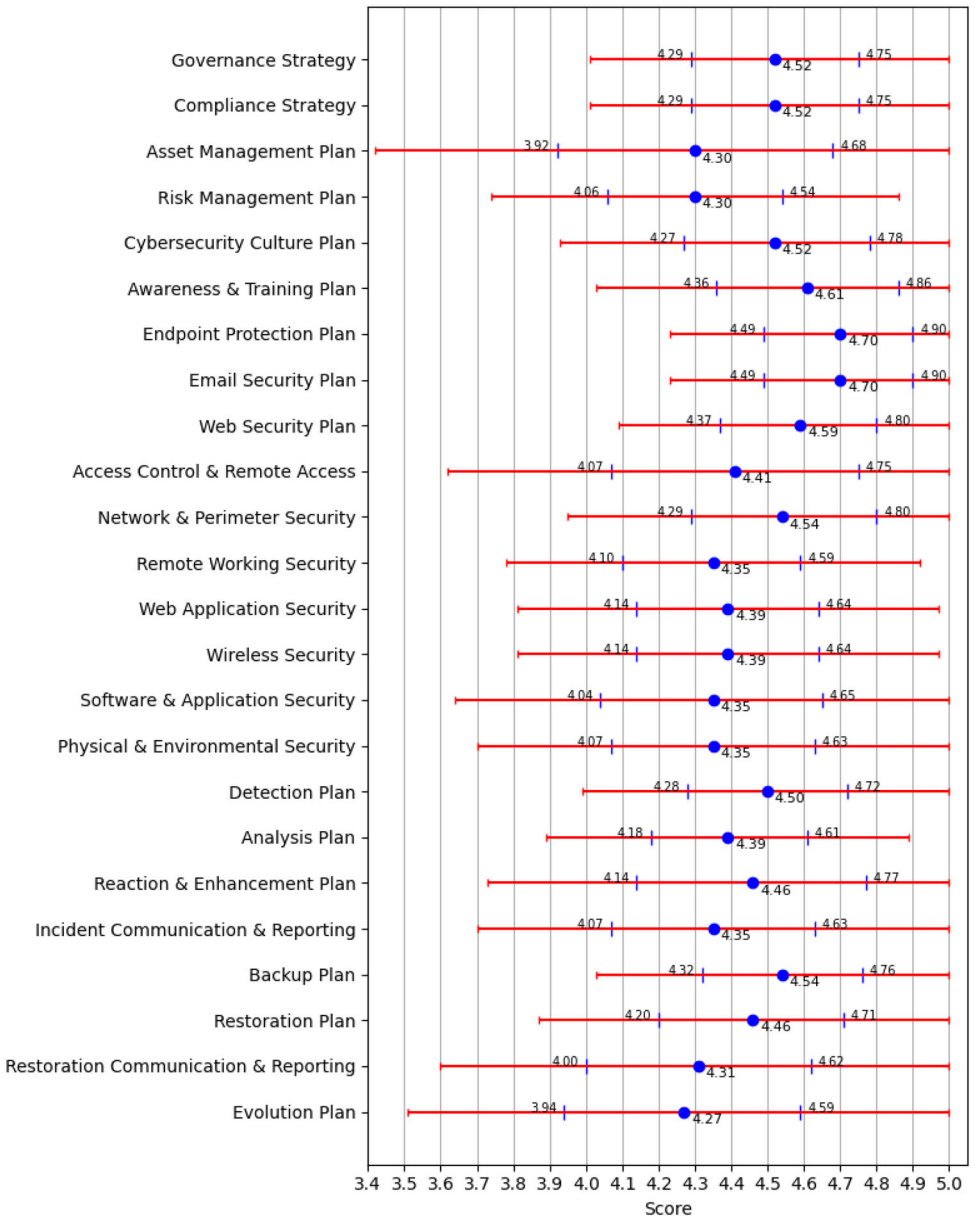


Fig. 4 Statistics per CRMSF Category. Points denote mean scores ($n = 23$). Blue bars represent the reported 95% confidence intervals, while red bars indicate $\pm$ one standard deviation. Numerical annotations show the mean values. Interval bounds are capped at the response-scale maximum of 5

Table 7 Descriptive statistics per CRMSF domain (n = 23)

Domain	Mean	Median	IQR	Std. Dev.	95% CI
Strategy	4.52	4.50	[4.0, 5.0]	0.49	[4.31, 4.73]
Assessment and anticipation	4.30	4.50	[4.0, 5.0]	0.63	[4.03, 4.57]
Awareness and training	4.54	4.50	[4.0, 5.0]	0.52	[4.32, 4.77]
Fortification	4.50	4.50	[4.0, 5.0]	0.49	[4.29, 4.71]
Detection and analysis	4.46	4.50	[4.0, 5.0]	0.45	[4.26, 4.65]
Containment	4.43	4.50	[4.0, 5.0]	0.66	[4.15, 4.72]
Restoration and evolution	4.40	4.50	[4.0, 5.0]	0.56	[4.16, 4.65]

Table 8 Descriptive statistics per CRMSF category (n = 23)

Category	Mean	Median	IQR	Std. Dev.	95% CI
Governance strategy	4.52	5.0	[4.0, 5.0]	0.51	[4.29, 4.75]
Compliance strategy	4.52	5.0	[4.0, 5.0]	0.51	[4.29, 4.75]
Asset management plan	4.30	4.5	[4.0, 5.0]	0.88	[3.92, 4.68]
Risk management plan	4.30	4.0	[4.0, 5.0]	0.56	[4.06, 4.54]
Cybersecurity culture plan	4.52	5.0	[4.0, 5.0]	0.59	[4.27, 4.78]
Awareness and training plan	4.61	5.0	[4.0, 5.0]	0.58	[4.36, 4.86]
Endpoint protection plan	4.70	5.0	[4.5, 5.0]	0.47	[4.49, 4.90]
Email security plan	4.70	5.0	[4.5, 5.0]	0.47	[4.49, 4.90]
Web security plan	4.59	5.0	[4.0, 5.0]	0.50	[4.37, 4.80]
Access control and remote access	4.41	4.5	[4.0, 5.0]	0.79	[4.07, 4.75]
Network and perimeter security	4.54	5.0	[4.0, 5.0]	0.59	[4.29, 4.80]
Remote working security	4.35	4.0	[4.0, 5.0]	0.57	[4.10, 4.59]
Web application security	4.39	4.5	[4.0, 5.0]	0.58	[4.14, 4.64]
Wireless security	4.39	4.5	[4.0, 5.0]	0.58	[4.14, 4.64]
Software and application security	4.35	4.5	[4.0, 5.0]	0.71	[4.04, 4.65]
Physical and environmental security	4.35	4.0	[4.0, 5.0]	0.65	[4.07, 4.63]
Detection plan	4.50	4.5	[4.0, 5.0]	0.51	[4.28, 4.72]
Analysis plan	4.39	4.0	[4.0, 5.0]	0.50	[4.18, 4.61]
Reaction and enhancement plan	4.46	5.0	[4.0, 5.0]	0.73	[4.14, 4.77]
Incident communication and reporting	4.35	4.0	[4.0, 5.0]	0.65	[4.07, 4.63]
Backup plan	4.54	5.0	[4.0, 5.0]	0.51	[4.32, 4.76]
Restoration plan	4.46	4.5	[4.0, 5.0]	0.59	[4.20, 4.71]
Restoration communication and reporting	4.31	4.0	[4.0, 5.0]	0.71	[4.00, 4.62]
Evolution plan	4.27	4.0	[4.0, 5.0]	0.76	[3.94, 4.59]

Table 9 Reliability analysis for domains (n = 23)

CRMSF domain	# Items	Cronbach's α	Inter-item ρ (2-item)	Spearman–Brown (2-item)	Interpre-tation
Strategy	2	0.905	0.826	0.905	Very good
Assessment and anticipation	2	0.831	0.748	0.856	Very good
Awareness and training	2	0.777	0.686	0.814	Acceptable–good
Fortification	10	0.945	–	–	Excellent
Detection and analysis	2	0.722	0.565	0.722	Acceptable
Containment	2	0.901	0.856	0.922	Very good
Restoration and evolution	4	0.894	–	–	Very good

themselves constitute empirically established interdependent clusters.

Interpreted in this way, the observed correlations reflect perceived structural coherence rather than causal dependency, and are consistent with the CRMSF's intended use as a holistic assessment framework without assuming linear or deterministic progression between domains.

Importantly, the observed correlations reflect structural coherence rather than causal dependency, reinforcing the CRMSF's suitability as a holistic assessment framework without assuming linear or deterministic progression between domains.

The complete Spearman rank-order correlation matrix across the seven CRMSF domains, including coefficients, p-values, and sample sizes, is provided in Appendix A (Table 13). All twenty-one inter-domain associations are positive, with coefficients ranging from $\rho = 0.38$ to $\rho = 0.88$. The strongest associations are observed among the detection- and resilience-orientated domains: Containment with Restoration & Evolution ($\rho = 0.88$, $p < 0.001$), Detection & Analysis with Restoration & Evolution ($\rho = 0.85$, $p < 0.001$), and Assessment & Anticipation with Restoration & Evolution ($\rho = 0.84$, $p < 0.001$) together with the association between Fortification and Containment ($\rho = 0.80$, $p < 0.001$). The weakest association, between Awareness & Training and Fortification, is small and not statistically significant ($\rho = 0.38, p = 0.071$). Consistent with the exploratory scope of the study, these coefficients are interpreted as indicative of perceived coherence among the practitioners' domain evaluations rather than as evidence of causal dependency or of empirically established interdependence among organizational capabilities, and they should be read in light of the small analytic sample (n = 23) and the bounded ordinal scale.

2.4.1.5 Perceived weight distribution and prioritization analysis

Beyond maturity-level evaluation, the quantitative analysis examined practitioner perceptions of relative weighting and prioritization, a core design objective of the CRMSF. It is important to note that this analysis represents a comparative judgment exercise rather than a latent measurement model and was therefore analyzed independently from psychometric reliability constructs.

Participants allocated relative importance across two paired dimensions: (i) cybersecurity versus cyber-resilience and (ii) organizational versus technical measures. Individual allocations were normalized such that each paired dimension summed to 100%, preserving interpretability and enabling meaningful aggregation. Mean values and standard deviations were subsequently calculated across participants.

As summarized in Table 10 and Fig. 5, participants assigned, on average, 57−58% of relative weight to cybersecurity and 42−43% to cyber-resilience. This distribution indicates a clear, though not exclusive, prioritization of preventive and protective security capabilities. Importantly, the results are consistent with the CRMSF premise that practitioners regard cyber-resilience as a necessary complementary dimension, rather than a secondary or optional extension to cybersecurity maturity.

Table 10 Perceived weight distribution (practitioner perspective, normalized) (n = 26)

Dimension	Mean (%)	SD (%)
Cybersecurity	57.31	7.10
Cyber-resilience	42.69	7.10
Organizational measures	47.12	8.62
Technical measures	52.88	8.62

Unlike the domain- and category-level Likert analyses, which are based on the analytic sample ($n = 23$), the weighting items were mandatory and were completed by all 26 participants; the perceived weight distribution is therefore reported for the full sample ($n = 26$)

A comparable weighting pattern emerged between technical and organizational measures. Practitioners allocated, on average, 53% weight to technical controls and 47% to organizational measures, reflecting the continued centrality of technical safeguards while simultaneously acknowledging the critical role of governance, culture, training, and process-oriented capabilities. The observed non-trivial variance across both dimensions (SD ≈ 7−9%) suggests context-sensitive adaptation rather than rigid prioritization, suggesting context-sensitive adaptation across heterogeneous organizational environments.

Collectively, these findings provide preliminary support for the inclusion of explicit weighting and criticality mechanisms within cybersecurity maturity assessment models.

The functional logic of the scoring architecture, and the role of the REAs within it are summarised in Sect. 2.4.1.1. The complete mathematical formulation of the scoring computation, including its normative parameters, is a distinct methodological contribution that is the subject of separately evaluated work and is therefore not reproduced here. As delineated in Sect. 2.1, the present study evaluates the perceived adequacy and functional distinctiveness of the framework's components rather than the numerical scoring computation itself.

2.4.1.6 Methodological considerations and validity safeguards

Several methodological safeguards were applied to ensure interpretive rigor. Demographic and contextual variables were used exclusively for contextual interpretation rather than psychometric modeling, while reliability metrics were applied only to multi-item constructs where internal consis-

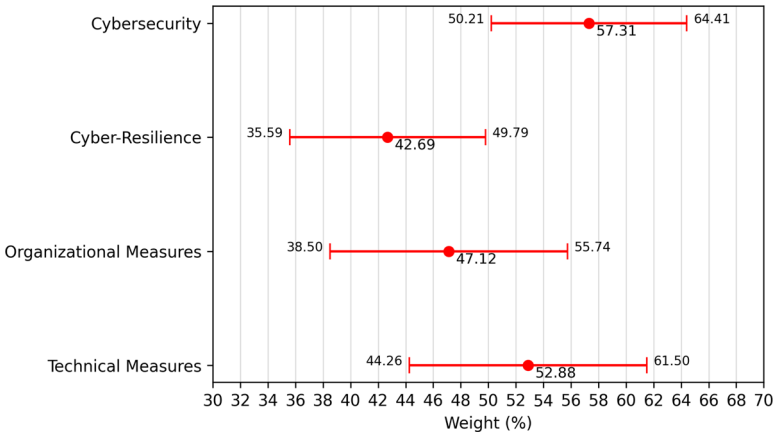


Fig. 5 Perceived weight distribution of cybersecurity and cyber-resilience dimensions (n = 26). Points denote mean weight percentages and horizontal bars represent ± one standard deviation. Numerical annotations show the mean values and SD bounds

tency assumptions were theoretically justified. All analyses were framed within the exploratory scope of the study.

2.4.2 Qualitative analysis

Qualitative data were obtained from open-ended responses collected through the CRMSF Evaluation Questionnaire and complemented by follow-up semi-structured interviews conducted with seven senior cybersecurity professionals. The qualitative analysis was conducted using reflexive thematic analysis, following established methodological principles [5, 6].

The analysis combined inductive and deductive thematic approaches. An inductive orientation enabled themes to emerge organically from participant narratives, capturing authentic practitioner perspectives on the practical applicability, interpretability, and perceived value of the CRMSF. In parallel, a complementary deductive mapping examined qualitative data in relation to the framework's predefined domains, security categories, and design principles, allowing empirical observations to confirm, refine, or critically reflect upon theoretical constructs embedded within the CRMSF.

Coding and theme development were conducted by the primary researcher through an iterative, reflexive process. Open-ended questionnaire responses were first coded inductively; initial codes were then grouped into candidate themes, which were iteratively reviewed against both the data and the CRMSF structure and refined over successive passes until a stable thematic structure was reached. Consistent with the reflexive thematic analysis tradition [6], analysis was performed by a single, reflexively engaged analyst; inter-rater reliability metrics were therefore not computed, as they are not theoretically aligned with this approach. The seven expert interviews were conducted online and, in accordance with participant preference and the study's confidentiality terms, were not audio-recorded; instead, detailed contemporaneous notes were taken and used to contextualize and enrich the interpretation of the questionnaire-based qualitative responses, facilitating deeper exploration of expert reasoning, sector-specific considerations, and implementation contexts. The single-coder nature of the analysis is acknowledged as a limitation in Sect. 2.6.

Through this combined analytical process, four dominant themes were identified:

1. Perceived prescriptiveness and structural clarity: Participants consistently emphasized the CRMSF's prescriptive orientation and stepwise guidance, contrasting it with predominantly descriptive cybersecurity frameworks that offer limited operational direction.
2. Usability and interpretability: Respondents highlighted the framework's clarity and ease of interpretation, particularly its effectiveness in supporting communication and understanding at executive and governance levels.
3. Decision-support and prioritization value: The explicit incorporation of weighting, complexity, and criticality was repeatedly identified as enabling more informed prioritization of cybersecurity initiatives and resource allocation decisions.
4. Refinement and extension opportunities: Suggestions for improvement focused primarily on sector-specific calibration and contextual tailoring, rather than on fundamental structural limitations of the framework.

Table 11 maps each theme to representative anonymized participant quotations and to the CRMSF components to which they relate. Quotations are reproduced verbatim except for the removal of any organization-identifying details.

Findings from the qualitative analysis were systematically triangulated with quantitative survey results to enhance interpretive coherence and methodological robustness. This triangulation reduced method-specific bias and reinforced convergence between numerical assessment outcomes and practitioner perceptions, consistent with established mixed-methods research principles [8].

Table 11 Qualitative themes, representative anonymized quotations, and related CRMSF components

Theme	Representative anonymized quotation	Related CRMSF component
1. Perceived prescriptiveness and structural clarity	"CRMSF's strongest aspect is its clear, modular structure, which brings prevention, detection, response, and recovery together in a coherent way." (P04)	Foundation (two sections, seven domains); modular architecture
	"The four modules allow each organization to follow a structured method to identify its needs." (P21, translated from Greek)	Four modules (Foundation, security grades, significance, scoring)
2. Usability and interpretability	"It enables an organization to measure the current cybersecurity maturity, share this information with Senior Management, monitor improvements and have a holistic view." (P14)	SA-Tool; Scoring → executive communication
	"CRMSF creates a shared language and structure that makes it easier to compare domains, justify budgets, and show leadership a clear 'where we are vs. where we need to be' improvement path." (P09)	Scoring; Cyber-Resistivity Security Classes
3. Decision-support and prioritization value	"The strongest aspect is the risk evaluation based on weight, criticality, complexity and maturity." (P02)	REAs (weighting, criticality, complexity, maturity)
	"These three consistently deliver the highest reduction of real-world cyber risk when building defenses from scratch." (P11)	Significance module; criticality-driven prioritization
4. Refinement and extension opportunities	"It does not provide a benchmark or industry average." (P24)	Benchmarking / RAF
	"Sector-specific overlays or profiles … would increase applicability across industries." (P08)	Sector adaptation; future refinement

2.4.3 Summary of data analysis

Together, the quantitative and qualitative analyses provide a coherent basis for evaluating the CRMSF, enabling triangulation between numerical outcomes and practitioner perspectives. This integrated foundation informs the Results and Discussion sections, where the findings are examined in direct relation to the study's research questions and evaluation propositions.

2.5 Ethical considerations

All participants provided informed consent prior to participation. Data collection and processing were conducted in accordance with the General Data Protection Regulation (GDPR, 2018) and the Research Ethics Guidelines of the European University Cyprus. Participation was voluntary, confidentiality was maintained throughout the study, and no personally identifiable information is disclosed in any publication outputs.

2.6 Study limitations

As an exploratory pilot evaluation study, the findings are based on expert and practitioner perspectives rather than on a statistically representative sample. While the multi-sector composition of participants enhances external relevance, the sample size limits the generalizability of the results. Accordingly, the findings should be interpreted as indicative of framework feasibility and perceived value rather than as confirmatory evidence, motivating future large-scale and longitudinal validation studies.

Relatedly, several role, sector, and role-by-size combinations in the descriptive tables are represented by single participants; as noted in Sect. 2.3, these entries characterize sample diversity and do not support sector-, role-, or size-specific generalization.

In addition, the qualitative analysis was conducted by a single analyst. While this is consistent with the reflexive thematic analysis approach adopted, the absence of multiple independent coders should be borne in mind when interpreting the qualitative findings.

Furthermore, the participating organizations were predominantly headquartered in Greece (24 of 26), with one each in Cyprus and the Netherlands; although the majority (19 of 26) operated within organizations having an international presence, the concentration of headquarters in a single country remains a source of potential regional bias. Nevertheless, the geographic distribution of respondents should be considered when interpreting the external evaluation of the findings, as cybersecurity governance practices, regulatory environments, and organizational risk management approaches may vary across regions.

Finally, several potential sources of bias inherent in perception-based evaluation should be acknowledged. Because participants received a structured introduction to the CRMSF before completing their evaluations, the responses may be subject to social desirability bias, whereby participants rate a newly presented framework more favorably than they might in fully independent use; the consistently high ratings reported in Sect. 3 should be interpreted with this possibility, and the related ceiling effects, in mind. The purposive recruitment of cybersecurity professionals who agreed to participate may also introduce self-selection bias, as respondents with a prior interest in maturity assessment or in novel frameworks may be over-represented relative to the broader practitioner population. In addition, a subset of the senior experts contributed both as respondents and to the subsequent interpretation of the findings; while this supported triangulation, it may introduce a degree of confirmation bias, as the same individuals were involved in evaluating and in interpreting the framework. These biases do not invalidate the exploratory findings, but they reinforce the need for the independent, larger-scale, and longitudinal validation identified above, in which evaluation and interpretation are more fully separated and participants are drawn from a broader population.

3 Results

3.1 Overview of empirical findings

This section summarizes the empirical findings across domains, security categories, weighting mechanisms, and practitioner perceptions, serving as a roadmap for the detailed analyses that follow.

Overall, the empirical results indicate consistently high evaluations of the CRMSF across domains and security categories, accompanied by meaningful variation reflecting differences in organizational context, technical maturity, and resource availability. Quantitative findings indicate strong internal consistency and coherent domain-level patterns, while qualitative feedback highlights perceived clarity, usability, and decision-support value.

The results further reveal differentiated prioritization patterns between cybersecurity and cyber-resilience capabilities, as well as between technical and organizational measures, indicating context-sensitive weighting rather than uniform assessment. In addition, relational patterns across preventive, detective, and resilience-oriented domains suggest that participants perceive these capabilities as interrelated components of a unified assessment structure.

The following subsections examine these findings in greater detail, presenting domain-level and category-level results, perceived weighting and prioritization effects, and the integration of quantitative and qualitative insights.

3.2 Domain-level results and interpretation

This subsection presents empirical findings at the CRMSF domain level, reporting descriptive statistics, reliability outcomes, and observed inter-domain relationships across the seven framework domains.

Across all CRMSF domains, mean scores were consistently high (all exceeding 4.30), reflecting strong practitioner agreement on domain relevance and adequacy, with acceptable to excellent internal consistency (Cronbach's $\alpha \geq 0.77$).

The Strategy domain achieved high mean values with very good internal consistency. Positive associations were observed between Strategy and both preventive and resilience-oriented domains, indicating concurrent high evaluations across governance, protection, and recovery-related capabilities.

The Assessment & Anticipation domain also exhibited high mean scores and low dispersion. Correlation patterns indicate alignment between anticipatory capabilities and both preventive (Fortification) and detection-oriented domains.

The Awareness & Training domain demonstrated strong internal consistency and high perceived adequacy. Observed associations with Strategy and Fortification domains indicate concurrent evaluations of human-centric and technical capability areas.

Within the Fortification domain, slightly higher variance was observed alongside excellent internal consistency. Strong associations were identified between Fortification and downstream domains, including Detection & Analysis and Containment.

The Detection & Analysis, Containment, and Restoration & Evolution domains all achieved high mean scores and acceptable to excellent reliability. Moderate to strong associations were observed among these domains, indicating concurrent evaluations across detection, response, and recovery capability areas.

3.3 Category-level insights and assessment granularity

This subsection reports empirical findings at the CRMSF security category level, presenting descriptive patterns that illustrate variation and differentiation within and across framework domains.

Descriptive statistics indicate consistently high mean scores across both strategic and technical security categories, accompanied by meaningful variation within and between domains. This pattern reflects differentiated practitioner evaluations across specific capability areas rather than uniform assessments at the aggregate level.

Strategic and organizational categories, including governance strategy, compliance strategy, cybersecurity culture, and awareness and training, exhibit high mean values with relatively low dispersion. In contrast, technical implementation categories, such as endpoint protection, network security, access control, and detection mechanisms, demonstrate higher variance, reflecting differences in technical maturity, infrastructure complexity, and resource availability across organizations.

Additional differentiation is observed between preventive-oriented categories and resilience-oriented categories. Preventive categories generally display high mean scores with moderate dispersion, while resilience-related categories, including detection, incident response, backup, restoration, and evolution planning, exhibit comparatively higher variance across participants.

At the category level, the results indicate that security capabilities are not evaluated uniformly, but vary according to organizational context, technical complexity, and maturity stage. These patterns provide granular insight into the distribution of perceived capability adequacy across the CRMSF structure.

3.4 Weighting, criticality, complexity and prioritization effects

This subsection reports empirical findings related to perceived weighting, criticality, complexity, and prioritization patterns observed during the CRMSF evaluation.

Results indicate that participants did not assign uniform importance across cybersecurity capabilities. Instead, differentiated weighting patterns were observed across key dimensions. On average, cybersecurity capabilities were weighted more heavily than cyber-resilience capabilities, while technical measures received higher relative importance than organizational measures. At the same time, observed variability across participants indicates that weighting decisions were context-sensitive rather than fixed.

The distribution of perceived weights reflects differentiated prioritization across preventive and resilience-oriented capability areas. Preventive cybersecurity capabilities generally received higher relative importance, while resilience-oriented capabilities, including response and recovery-related categories, were weighted with greater variability.

In addition to weighting, participants explicitly considered complexity and criticality when prioritizing capabilities. Capabilities perceived as both critical and complex were consistently highlighted as priority areas, indicating that assessment outcomes were influenced not only by maturity scores but also by perceived operational impact and implementation difficulty.

Overall, the results indicate that practitioners apply differentiated and adaptive prioritization logic, with weighting, criticality, and complexity jointly influencing perceived importance across the CRMSF structure, supporting the design principle that capability assessment should incorporate explicit weighting and contextual prioritization rather than uniform maturity scoring alone.

3.5 SME-focused evaluation of CRMSF (Small vs medium organizations)

An exploratory subgroup analysis was conducted to examine CRMSF evaluation patterns among Small (<50 employees, $n = 4$) and Medium (50−249 employees, $n = 6$) organizations. The analysis focused on practitioner evaluations of key CRMSF design elements, including structural clarity, prescriptive guidance, security grades, criticality and complexity attributes, scoring interpretability, self-assessment tool utility, executive communication support, and ease of understanding. Given the very small subgroup sizes (Small n = 4; Medium n = 6), these results are strictly exploratory and descriptive; they characterize patterns within this sample and are not intended to support statistical generalization to small or medium-sized organizations more broadly.

Given the ordinal nature of Likert-scale responses and the limited subgroup sizes, results are reported using descriptive statistics and complemented by non-parametric Mann−Whitney U tests with Cliff's δ effect sizes to assess practical differences without assuming normality [11, 13].

Across all evaluated CRMSF elements, both Small and Medium organizations reported high mean scores, indicating positive evaluations of framework clarity, usability, and decision-support features. No statistically significant differences were observed between the two subgroups after correction for multiple comparisons. However, examination of mean patterns and effect sizes provides additional descriptive insight.

Small organizations exhibited higher mean scores on items related to ease of understanding and structural clarity, while Medium organizations showed slightly higher evaluations for criticality and complexity mechanisms and executive-level communication support. Both subgroups rated the scoring model and self-assessment tool highly, indicating consistent perceived usability across SME contexts. Detailed subgroup results are summarized in Table 12.

4 Discussion

Rather than treating the evaluation propositions as isolated claims to be individually confirmed, the discussion interprets the empirical findings holistically in relation to the research questions and the overarching design objectives of the CRMSF.

Table 12 CRMSF element ratings by organization size

CRMSF element	Small			Medium			Mann – Whitney p	Cliff's δ
	n	Mean (SD)	95% CI	n	Mean (SD)	95% CI		
CRMSF structure	4	4.75 (0.50)	[3.95, 5.00]	6	4.33 (0.82)	[3.48, 5.00]	0.464	0.292
Prescriptive guidance	4	4.50 (0.58)	[3.58, 5.00]	6	4.17 (0.75)	[3.38, 4.96]	0.556	0.250
Security grades	4	4.50 (0.58)	[3.58, 5.00]	6	4.33 (0.82)	[3.48, 5.00]	0.906	0.083
Criticality and complexity	4	4.50 (0.58)	[3.58, 5.00]	6	4.67 (0.52)	[4.12, 5.00]	0.708	− 0.167
Scoring model	4	4.50 (0.58)	[3.58, 5.00]	6	4.50 (0.84)	[3.62, 5.00]	0.903	− 0.083
Self-assessment tool (composite)	4	4.50 (0.79)	[3.24, 5.00]	6	4.67 (0.52)	[4.12, 5.00]	0.718	− 0.167
Communication to top management	4	4.50 (0.58)	[3.58, 5.00]	6	4.67 (0.52)	[4.12, 5.00]	0.708	− 0.167
Easy to understand	4	4.75 (0.50)	[3.95, 5.00]	6	3.83 (1.17)	[2.61, 5.00]	0.205	0.500
Comparisons vs frameworks (composite)	4	4.54 (0.63)	[3.54, 5.00]	6	4.43 (0.89)	[3.50, 5.00]	1.000	0.042

4.1 Integrated interpretation of empirical findings

Taken together, the empirical findings suggest that cybersecurity maturity assessment benefits from a shift away from single-axis, descriptive models toward multi-dimensional and prescriptive evaluation architectures. Rather than producing uniform maturity classifications, the CRMSF enabled practitioners to reason about capability adequacy, priority, and interdependence in a context-sensitive manner.

The convergence of quantitative dispersion patterns and qualitative narratives indicates that observed variability reflects real-world heterogeneity in organizational maturity and resource constraints, rather than structural ambiguity. This supports the interpretation of CRMSF as an adaptive framework capable of accommodating diverse operational environments without compromising internal coherence.

Importantly, the findings indicate that maturity assessment is most meaningful when explicitly linked to prioritization logic. The integration of weighting, criticality, and complexity attributes allows assessment outcomes to function as decision-support inputs rather than static maturity labels. In this respect, CRMSF reframes maturity evaluation as a governance-relevant process aligned with operational continuity and strategic planning objectives.

4.2 Interpretation of domain-level findings

The domain-level findings indicate that the CRMSF's modular architecture supports integrated and interpretable assessment of cybersecurity maturity and cyber-resilience. Rather than being evaluated as isolated control groupings, the seven domains were perceived by practitioners as interrelated components of a unified assessment structure.

More importantly, the observed relational patterns highlight the foundational role of strategic and anticipatory capabilities. Governance, risk assessment, and anticipation are interpreted not as compliance-driven activities, but as enabling mechanisms that influence both preventive and resilience-oriented domains.

The integration of awareness and training with strategic and technical domains further reinforces the socio-technical nature of cybersecurity maturity. This socio-technical interpretation is further supported empirically by the practitioners' distinct weighting of organizational versus technical measures (Table 10), in which both dimensions received substantial and non-trivial weight (organizational $\approx$ 47%, technical $\approx$ 53%), indicating that participants treated them as complementary rather than as a single technical axis. Human-centric capabilities are perceived as embedded enablers rather than supplementary controls. Similarly, the resilience-oriented domains (detection, containment, and restoration) are interpreted as interdependent mechanisms, reflecting a

coordinated resilience logic rather than a linear incident lifecycle.

Overall, the domain-level interpretation indicates that CRMSF was perceived as supporting context-aware reasoning about capability interdependencies, enabling maturity assessment to inform governance and prioritization decisions across heterogeneous organizational environments.

4.3 Interpretation of category-level findings and assessment granularity

Category-level interpretation reveals the primary source of CRMSF's diagnostic depth. By disaggregating domains into operational security categories, the framework enables practitioners to reason about specific capability strengths and gaps that remain obscured in aggregated maturity models.

Strategic and organizational categories are interpreted as foundational and broadly applicable across contexts, exhibiting high consensus regardless of organizational size or sector. In contrast, technical implementation categories show greater variability, reflecting differences in infrastructure complexity, technological maturity, and resource availability. This distinction highlights the value of category-level analysis in capturing context-sensitive maturity patterns.

The contrast between preventive and resilience-oriented categories further reinforces CRMSF's staged maturity logic. Preventive controls are widely recognized and implemented, while recovery and continuous improvement capabilities exhibit greater dispersion, indicating higher maturity thresholds. This supports the interpretation of cyber-resilience as a progressive extension of cybersecurity maturity rather than a parallel construct.

By enabling fine-grained differentiation across strategic, technical, preventive, and resilience-oriented capabilities, category-level granularity allows assessment outcomes to be directly linked to prioritization and improvement planning, addressing a key limitation of aggregated maturity models. In this respect, CRMSF extends the interpretive resolution of maturity assessment beyond classification, supporting actionable decision-making across heterogeneous organizational environments.

4.4 Interpretation of weighting, criticality, and prioritization effects

The interpretation of weighting, criticality, and complexity effects underscores CRMSF's shift from descriptive maturity classification toward decision-oriented assessment. Practitioner evaluations indicate that cybersecurity capabilities are not perceived as uniformly important, nor is maturity understood as a linear progression across domains or controls.

Participants naturally differentiated between preventive and resilience-oriented capabilities, as well as between technical and organizational measures. While preventive and technical controls often received greater emphasis, the observed variability reflects adaptive judgment shaped by organizational context rather than fixed prioritization rules. This finding reinforces the premise that meaningful maturity assessment must accommodate contextual risk exposure, operational constraints, and implementation effort.

The explicit incorporation of criticality and complexity enhances the interpretive value of maturity assessment by aligning evaluation outcomes with operational impact and organizational feasibility. Rather than optimizing maturity scores in isolation, practitioners interpreted weighted outcomes as guidance for balancing short-term protection needs with longer-term resilience objectives. In this sense, weighting mechanisms support phased improvement planning and reduce the risk of over-investment in low-impact controls.

In contrast to established frameworks that rely on implicit or post-hoc prioritization, CRMSF embeds weighting, criticality, and complexity directly within the assessment logic. Practitioners interpreted this integration as enabling actionable prioritization rather than descriptive classification, reinforcing the framework's role as a governance-relevant decision-support instrument.

4.5 Integration of quantitative and qualitative evidence

The convergence of quantitative and qualitative evidence strengthens the interpretive validity of the CRMSF evaluation. Numerical assessment patterns are consistently reinforced by expert narratives, indicating alignment between statistical coherence and practitioner reasoning.

High domain- and category-level evaluations are interpreted alongside qualitative emphasis on prescriptiveness and structural clarity, suggesting that CRMSF translates analytical complexity into usable guidance. Variability observed in technically intensive and resilience-oriented areas is best understood through qualitative insights highlighting sectoral constraints, phased adoption, and resource sensitivity.

The qualitative evidence both supports and qualifies the quantitative findings. On the supporting side, the high ratings for structural clarity and prescriptiveness are echoed in recurrent practitioner statements describing the framework's modular structure and its capacity to provide a shared language for technical and executive stakeholders. On the qualifying side, several participants noted that effective use of the framework requires non-trivial adoption effort, expertise to perform a reliable self-assessment, and careful integration with standards already in use (for example, ISO/IEC 27001, NIS2, and DORA). These observations contextualize the high but more variable ratings observed in technically intensive and resilience-oriented categories, indicating that the dispersion reflects real differences in organizational

resources and adoption readiness rather than ambiguity in the framework itself.

The alignment between quantitative prioritization patterns and qualitative perceptions of decision-support value further indicates that weighting and criticality attributes function as interpretive bridges between assessment and action. Collectively, this triangulation suggests that CRMSF operates as an integrated interpretive framework rather than a purely measurement-oriented instrument.

4.6 Comparative interpretation with existing frameworks

Comparative interpretation positions CRMSF as a complementary extension to established cybersecurity frameworks rather than a replacement. While frameworks such as NIST CSF and ISO/IEC 27001 provide comprehensive control taxonomies, they remain largely descriptive and rely on implicit prioritization.

The findings indicate three areas, supported by perception-based practitioner evaluation, in which CRMSF is regarded as extending the interpretive and decision-support capabilities of existing frameworks. First, category-level granularity enables interpretive differentiation beyond aggregated maturity scores. Second, the integration of weighting, criticality, and complexity embeds prioritization directly within assessment logic, transforming maturity evaluation into a decision-support process. Third, the unified treatment of cybersecurity and cyber-resilience reflects practitioner perceptions of prevention, detection, response, and recovery as interdependent capabilities.

By translating control coverage into actionable, context-aware insights, CRMSF enhances the practical utility of existing frameworks and supports more consistent, governance-relevant maturity interpretation across diverse organizational environment.

A detailed structural comparison of CRMSF's design space against established models (CMM, COBIT, NIST CSF, C2M2, and ISO/IEC 27001) was the subject of a dedicated prior study in this research series [16], which compares these models along their main characteristics (origin, maturity levels and domains, prescriptive versus descriptive orientation, organizational environment, organization size, and field applicability—its Table 1), and identifies the specific gaps that motivate CRMSF, namely the absence of an integrated self-assessment tool, explicit prioritization, treatment of practice complexity, weighting, and combined organizational and technical coverage in a single size-agnostic, prescriptive framework (its Table 2). That analysis showed that COBIT, although a maturity-capable model, is confined to IT governance, whereas NIST CSF and ISO/IEC 27001 though the most widely adopted instruments were not designed to provide this holistic, prescriptive, size-agnostic coverage. The present study builds on that structural analysis and contributes the complementary, perception-based finding that practitioners regarded CRMSF as offering greater assessment granularity, prioritization support, and interpretive value than the frameworks they currently use. We emphasize that this is a perceived comparative utility reported by experienced practitioners, not a demonstrated performance superiority; establishing the latter would require a controlled comparative design in which CRMSF and other frameworks are applied to the same organizations or assessment tasks, which we identify as future work.

4.7 Implications for research and practice

The empirical evaluation of the CRMSF yields important implications for both cybersecurity maturity research and organizational practice. From a theoretical perspective, the findings challenge the sufficiency of traditional single-axis, descriptive maturity models and provide empirical support for multi-dimensional, weighted, and risk-informed assessment architectures. The results indicate that maturity assessment benefits from explicit differentiation across capabilities, criticality, and complexity, suggesting that future research should move toward capability-based and resilience-integrated maturity constructs rather than linear progression logics.

The unified treatment of cybersecurity and cyber-resilience further advances maturity theory by operationalizing resilience as an intrinsic component of maturity assessment rather than as an implicit outcome or parallel concern. The convergence of quantitative and qualitative evidence provides a validated foundation for future research on resilience-oriented maturity modeling and highlights the methodological value of mixed-methods approaches in evaluating complex socio-technical frameworks.

From a practical standpoint, practitioners perceived clear decision-support value in CRMSF beyond compliance-oriented frameworks. Its combination of domain- and category-level granularity with weighting and prioritization mechanisms enables organizations to align cybersecurity investments with risk exposure, operational impact, and resource constraints. This capability was perceived as particularly relevant for small and medium-sized enterprises, where incremental, prescriptive adoption is essential. At the same time, participants regarded the framework as applicable to larger organizations and as supporting clearer communication between technical teams and executive stakeholders. Although the empirical evaluation was conducted with a pilot sample of cybersecurity professionals, the diversity of organizational contexts represented in the paper provides indicative evidence that the CRMSF can be meaningfully applied across heterogeneous organizational environments. Overall, the findings position CRMSF as a decision-oriented

maturity and cyber-resilience framework that effectively bridges assessment, prioritization, and actionable improvement across diverse organizational contexts.

While the empirical findings provide strong initial support for the CRMSF, the results should be interpreted in light of the study's exploratory scope. The reliance on expert and practitioner perception, combined with a pilot-scale sample, positions the findings as indicative rather than confirmatory. Future research should therefore focus on large-scale validation, longitudinal adoption studies, and integration with automated assessment mechanisms to further examine stability, sensitivity, and longitudinal impact. Future work should also examine inter-rater consistency and longitudinal stability of CRMSF scoring outcomes to further strengthen empirical generalizability.

4.8 Addressing the research questions

The empirical findings presented in this paper provide evidence addressing the research questions formulated for the evaluation of the CRMSF.

RQ1 is addressed through the conceptual integration of cybersecurity and cyber-resilience within the unified CRMSF architecture, which organizes preventive, detective, and resilience-oriented capabilities into a coherent multi-domain assessment structure. The empirical evaluation indicates that practitioners perceived these sections as interrelated components of a unified assessment structure that jointly inform the evaluation of organizational cybersecurity posture.

RQ2 concerns the transformation of qualitative cybersecurity practices into a consistent quantitative scoring mechanism. Within the scope of this pilot, the evaluation addresses practitioners' perceptions of this mechanism. Participants regarded the integration of maturity levels with weighting, criticality, and complexity attributes as supporting consistent, prioritization-oriented assessment across security sections, domains, and categories. The validation of the scoring computation itself was not undertaken in this study and remains the subject of dedicated future work.

RQ3 is addressed through the definition and empirical evaluation of the Resistivity Evaluation Attributes (REAs), which capture the relative criticality, complexity, and importance of cybersecurity capabilities. The results indicate that practitioners naturally apply differentiated prioritization logic when evaluating cybersecurity controls, supporting the relevance of these attributes within maturity assessment.

RQ4 concerns the framework's capacity to classify organizational and technical practices while remaining scalable and vendor-neutral. Within the scope of this pilot, the results indicate that practitioners perceived CRMSF as supporting the classification of organizational and technical practices across organizations of varying sizes and regulatory contexts. Its scalability and vendor-neutrality as demonstrated properties remain to be examined in larger-scale validation and are therefore not claimed here.

RQ5 concerns the comparative granularity, interpretability, and practical value of CRMSF relative to existing frameworks. Within the scope of this pilot, comparative practitioner evaluations and qualitative feedback indicate that participants perceived CRMSF as offering enhanced assessment granularity, interpretability, and decision-support value compared with frameworks they currently use. This reflects perceived comparative utility rather than demonstrated comparative performance; the latter would require a controlled comparative design in which CRMSF and other frameworks are applied to the same organizations or assessment tasks.

The evaluation propositions are addressed as follows. EP1–EP3, which concern perceived granularity, prioritization support, and the integration of cybersecurity with cyber-resilience, are supported by the convergence of the descriptive patterns (Sects. 3.2, 3.3 and 3.4) and the qualitative themes (Sect. 2.4.2), which indicate that practitioners perceived these properties in the framework. EP4 (scalable adoption across sizes, sectors, and regulatory environments) and EP5 (more consistent and actionable outcomes relative to existing frameworks) are only partially and indirectly informed by the present pilot: the multi-sector composition of the sample and the perception-based comparative feedback are consistent with these expectations, but neither proposition can be confirmed within an exploratory design of this scale. Both are therefore retained as expectations to be examined through larger-scale and explicitly comparative studies.

5 Conclusions

This paper presented the initial empirical evaluation of the CRMSF, a modular and prescriptive framework designed to support integrated assessment of cybersecurity maturity and cyber-resilience across diverse organizational contexts. Addressing limitations of existing compliance-oriented and predominantly descriptive maturity models, CRMSF introduces a multi-dimensional assessment architecture, that combines domain- and category-level granularity with explicit weighting, criticality, and complexity mechanisms.

The mixed-methods evaluation provides convergent initial evidence regarding the framework's perceived coherence, interpretability, and practical relevance. Quantitative analysis indicated strong internal consistency across domains and meaningful variation at both domain and category levels, suggesting that practitioners were able to differentiate capability adequacy and maturity in a nuanced and context-sensitive manner. Qualitative findings reinforced these results by highlighting the framework's prescriptive clarity, usability, and decision-support value, particularly in translating

Table 13 Spearman rank-order correlation matrix of CRMSF domains ($n = 23$)

Domain	(1)	(2)	(3)	(4)	(5)	(6)	(7)
(1) Strategy	1.00						
(2) Assessment and anticipation	0.77***	1.00					
(3) Awareness and training	0.42*	0.45*	1.00				
(4) Fortification	0.71***	0.60**	0.38	1.00			
(5) Detection and analysis	0.73***	0.67***	0.58**	0.76***	1.00		
(6) Containment	0.57**	0.66***	0.45*	0.80***	0.78***	1.00	
(7) Restoration and evolution	0.71***	0.84***	0.49*	0.77***	0.85***	0.88***	1.00

Coefficients are Spearman's rank-order correlations (ρ) computed on per-respondent composite domain scores; $n = 23$ for all pairs. Numbers in column headers correspond to the numbered domains in the first column. $^{*}p < 0.05$; $^{**}p < 0.01$; $^{***}p < 0.001$ (two-tailed). All associations are positive ($\rho = 0.38$–0.88)

maturity assessment into actionable prioritization and planning insights.

A central contribution of the study lies in the initial empirical evaluation of the Resistivity Evaluation Attributes that underpin CRMSF's weighted scoring logic. The findings indicate that practitioners did not perceive cybersecurity capabilities as uniformly important, but rather as context-dependent and differentiated across preventive, detective, and resilience-oriented dimensions. By embedding prioritization directly into the assessment process, CRMSF shifts maturity evaluation from a static classification exercise toward a risk-informed, decision-oriented approach aligned with real-world operational and governance needs.

The results further indicate that practitioners perceived CRMSF as applicable across organizations of varying size, sector, and regulatory exposure. Exploratory SME-focused analysis suggests that the framework's modular structure and ease of interpretation were perceived as supporting incremental adoption in resource-constrained environments, while being regarded as suitable for more complex organizational settings. Demonstrated scalability across organizational scales remains to be established in larger-scale validation.

Despite these contributions, the results should be interpreted in light of the study's exploratory scope and pilot-scale empirical evaluation, including sample size limitations, reliance on practitioner perception, and potential regional bias due to the geographic concentration of participants. Future research should extend validation across larger and more diverse populations, examine longitudinal adoption effects, and explore integration of CRMSF with regulatory, educational, and automated assessment contexts.

Overall, the paper provides initial empirical evidence positioning CRMSF as an interpretable and decision-oriented framework with promising potential for both research and practice in cybersecurity maturity and cyber-resilience assessment.

Appendix A Spearman rank-order correlation matrix of CRMSF domains

This appendix presents the complete Spearman rank-order correlation matrix across the seven CRMSF domains, supporting the relational analysis summarized in Section 2.4.1. Correlations were computed on per-respondent composite domain scores for the analytic sample ($n = 23$). All twenty-one inter-domain associations are positive, ranging from $\rho = 0.38$ to $\rho = 0.88$. The strongest associations are observed among the detection- and resilience-oriented domains—Containment with Restoration & Evolution ($\rho = 0.88$), Detection & Analysis with Restoration & Evolution ($\rho = 0.85$), and Assessment & Anticipation with Restoration & Evolution ($\rho = 0.84$)—together with Fortification and Containment ($\rho = 0.80$). The weakest association, between Awareness & Training and Fortification, is small and not statistically significant ($\rho = 0.38$, $p = 0.071$). Consistent with the exploratory scope of the study, these coefficients are interpreted as indicative of structural coherence among capability clusters rather than as evidence of causal dependency, and they should be read in light of the small analytic sample and the bounded ordinal scale.

Appendix B Evaluation questionnaire structure and item mapping

This appendix documents the structure of the 55-item Evaluation Questionnaire used in the study and maps its items to the CRMSF structure, the evaluation attributes, and the research questions. The instrument was administered as a structured online form organized into five sections (A–E). Section A

Table 14 Mapping of evaluation items to CRMSF structure, attributes, and research questions

Section	Items (form no.)	CRMSF domain/category	Evaluation attribute	RQ
A—Demographics and Context	1–13	Contextual (role, experience, sector, organization size, resources, implemented frameworks)	–	–
B—Domain and category evaluation	14–15 (domain-level)	All seven domains	Structural completeness/adequacy	RQ1, RQ3
	17, 19, 21, 23, 25, 27, 29	Twenty-four security categories across the seven domains	Structural completeness/adequacy	RQ1, RQ3
	16, 18, 20, 22, 24, 26, 28, 30 (open)	Cross-cutting, per domain	Refinement/adequacy	RQ3
C—Weights and Prioritizations	31–32	Cybersecurity vs. Cyber-Resilience sections	Weighting	RQ2, RQ3
	33–34	Organizational vs. Technical practices	Weighting	RQ2, RQ3
	35–40	Domains within each section	Prioritization (criticality, complexity)	RQ2, RQ4
D—Framework evaluation	41 (Structural)	Foundation: structure, coverage, clarity	Usability / interpretability	RQ4
	43 (Functional)	SA-Tool; Significance (REAs); Security Grades	Functional value	RQ2, RQ4
	44 (Utility)	Scoring; executive communication; scalability	Decision-support	RQ4, RQ5
	45 (Comparative)	Comparison vs. NIST CSF, CIS, C2M2, ISO/IEC 27001	Perceived comparative utility	RQ5
	46 (Overall)	Whole framework	Overall acceptance	RQ4, RQ5
	42, 47, 48 (open)	Cross-cutting	Refinement/adoption	RQ3, RQ5
E—Open feedback	49–53	Cross-cutting	Adoption barriers/refinement/recommendation	RQ3, RQ5

Item numbers follow the questionnaire form. Closed-ended (rating) items used a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree); open-ended items provided qualitative evidence. Section D comprised five rating blocks—Structural Evaluation, Functional Effectiveness, Framework Utility, Comparative Assessment, and Overall Evaluation. Form items 54–55 concerned follow-up review consent and the participant declaration, respectively, and are not part of the analytic instrument. RQ = research question (RQ1–RQ5, as defined in Section 2.1)

captured demographic and organizational context. Section B assessed the perceived relevance, completeness, and practical adequacy of the CRMSF foundation—its seven domains and twenty-four security categories—at both domain and category level. Section C elicited weighting and prioritization judgments, including the distribution of emphasis between the cybersecurity and cyber-resilience sections and between organizational and technical practices, together with constrained-budget prioritization exercises. Section D evaluated the framework's structural coherence, functional effectiveness, utility, comparative positioning, and overall acceptance. Section E gathered open-ended reflective feedback. Closed-ended items used a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree); open-ended items provided the qualitative evidence analyzed in Sect. 2.4.2. The complete item wording is available as a supplementary file. Table 14 summarizes the mapping of questionnaire items to the CRMSF structure, evaluation attributes, and research questions.

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

Author Contributions K.P. conceived the paper, developed the CRMSF framework, designed the methodology, conducted the data collection (survey and interviews), performed the statistical analysis, and wrote the main manuscript text. G.V. improved the presentation of the tables and prepared all figures and diagrams. K.V. supervised the research process. All authors reviewed and approved the final manuscript.

Funding Open access funding provided by the Cyprus Libraries Consortium (CLC). This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability The datasets generated and analysed during this study are not publicly available due to participant confidentiality agreements. However an anonymised version may be made available by the corresponding author upon reasonable request.

Declarations

Conflict of interest The authors declare no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, 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 changes were made. 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/4.0/.

References

1. Ahmad, A., Desouza, K.C., Maynard, S.B., et al.: How integration of cybersecurity management and incident response enables organizational resilience. Computers & Security **104**, 102190 (2021). https://doi.org/10.1016/j.cose.2021.102190
2. Alshaikh, M.: Cybersecurity maturity model: a systematic review of models and their adoption in organizations. Computers & Security **93**, 101788 (2020). https://doi.org/10.1016/j.cose.2020.101788
3. Alshaikh, M.: Developing cybersecurity culture to influence employee behavior: a practice perspective. Computers & Security **98**, 102003 (2020). https://doi.org/10.1016/j.cose.2020.102003
4. Becker, J., Knackstedt, R., Pöppelbuß, J.: Developing maturity models for it management. Business Inform. Syst. Eng. **1**(3), 213–222 (2009)
5. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qual. Res. Psychol. **3**(2), 77–101 (2006)
6. Braun, V., Clarke, V.: Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health **11**(4), 589–597 (2019)
7. Carías, J.F.: Cyber resilience progression model. Appl. Sci. **10**(21), 7393 (2020). https://doi.org/10.3390/app10217393
8. Creswell, J.W., Clark, P., V.L.: Designing and conducting mixed methods research, SAGE Publications (2018). (3rd edn)
9. European Union Agency for Cybersecurity (ENISA): enisa threat landscape 2023. (2023) https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
10. Hevner, A.R., March, S.T., Park, J., et al.: Design science in information systems research. MIS Q. **28**(1), 75–105 (2004)
11. Holm, S.: A simple sequentially rejective multiple test procedure. Scand. J. Stat. **6**(2), 65–70 (1979). https://doi.org/10.2307/2335832
12. ISO/IEC: iso/iec 27001:2022 — information security, cybersecurity and privacy protection.(2022) https://www.iso.org/standard/82875.html
13. Jamieson, S.: Likert scales: how to (ab)use them. Med. Educ. **38**(12), 1217–1218 (2004)
14. Kitchenham, B., Pfleeger, S.L., Pickard, L.M., et al.: Preliminary guidelines for empirical research in software engineering. IEEE Trans. Software Eng. **28**(8), 721–734 (2002)
15. Nunnally, J.C., Bernstein, I.H.: Psychometric theory, McGraw-Hill (1994). (3rd edn)
16. Papachristofis, K., Vardoulias, G., Vavousis, K.: Comparative evaluation of cybersecurity maturity models and frameworks. (2025). https://doi.org/10.1007/978-3-031-81325-2_12
17. Papachristofis, K., Vardoulias, G., Vavousis, K., et al.: Developing cyber-resistivity maturity and scoring framework (CRMSF) for any size of organization. Int. J. Inf. Secur. **24**, 242 (2025). https://doi.org/10.1007/s10207-025-01154-5
18. Pascoe, C., Quinn, S., Scarfone, K.: The nist cybersecurity framework (csf) 2.0. NIST Cybersecurity White Paper NIST CSWP 29. Gaithersburg, MD (). https://doi.org/10.6028/NIST.CSWP.29
19. Sharkov, G.: Assessing the maturity of national cybersecurity and resilience. Connections: Quarterly J. **19**(4), 5–24 (2020). https://doi.org/10.11610/Connections.19.4.01
20. Verizon: Data breach investigations report (DBIR), (2024). https://www.verizon.com/business/resources/reports/dbir/
21. Zammani, M., Razali, R.: An empirical study of information security management success factors. Int. J. Adv. Sci. Eng. Inform. Tech. **6**(6), 904–912 (2016). https://doi.org/10.18517/ijaseit.6.6.1371

22. Zammani, M., Razali, R., Singh, D.: Organisational information security management maturity model. Int. J. Adv. Comput. Sci. Appl. (2021). https://doi.org/10.14569/IJACSA.2021.0120974

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