

## Review Article

## Open Access

## Incident Response Maturity Models for Enterprise Security Optimization

Bhuvan Bobba

Master of Science in Cybersecurity University of Texas at Dallas, USA

### ABSTRACT

Enterprises increasingly face sophisticated cyber threats that outpace ad hoc incident response (IR) practices, yet many organizations lack a structured method for assessing and advancing their IR capabilities. This study examines incident response maturity models (IRMMs) as tools for enterprise security optimization, addressing inconsistencies in how existing frameworks such as NIST CSF, SIM3, and C2M2 define and measure maturity across people, process, technology, and governance dimensions. Using a mixed-methods approach that combines comparative model analysis with case-based evaluation of enterprise security programs, this research identifies critical gaps in scalability, measurability, and cross-sector applicability among current models. Findings reveal a significant correlation between higher IR maturity levels and improved security performance indicators, including reduced mean time to detect (MTTD), faster mean time to respond (MTTR), and lower breach-related costs. The study further proposes a refined maturity framework that integrates governance alignment and continuous improvement mechanisms, validated against real-world enterprise data. Results suggest that structured maturity progression not only strengthens technical response capabilities but also enhances organizational resilience and stakeholder confidence. This paper contributes to both academic literature and practical guidance by offering enterprises a validated pathway for benchmarking and optimizing incident response functions, while highlighting the need for adaptable, industry-agnostic maturity standards. Implications for policy, governance, and future research directions are discussed.

### \*Corresponding author

Bhuvan Bobba, Master of Science in Cybersecurity University of Texas at Dallas, USA.

**Received:** September 08, 2022; **Accepted:** September 15, 2022, **Published:** September 22, 2022

**Keywords:** Incident Response, Maturity Models, Enterprise Security, Cybersecurity Governance, Security Optimization, NIST Cybersecurity Framework, Capability Maturity, Threat Detection and Response, Organizational Resilience, Security Performance Metrics

### Introduction

Enterprise organizations face an escalating volume and sophistication of cyber incidents, ranging from ransomware campaigns to advanced persistent threats, that continually test the resilience of existing security operations. Despite substantial investment in detection and prevention technologies, many enterprises still respond to incidents through inconsistent, ad hoc processes rather than through disciplined, repeatable procedures [1]. This inconsistency often results in delayed detection, prolonged containment, and increased financial and reputational damage. Incident response (IR) maturity models have emerged as structured frameworks intended to help organizations assess their current capabilities and systematically progress toward more advanced, optimized states of operational readiness [2].

The proliferation of maturity models spanning generic information security frameworks to IR-specific standards has introduced variability in how "maturity" is defined, measured, and applied across different organizational contexts [3]. Many enterprises struggle to select an appropriate model or to translate maturity assessments into actionable improvements, particularly when

models fail to account for organizational size, sector-specific risk profiles, or resource constraints. This paper addresses these challenges by examining the landscape of incident response maturity models and their applicability to enterprise security optimization. It investigates how maturity progression correlates with measurable security outcomes and proposes considerations for refining existing frameworks.

### Literature Review

The concept of maturity modeling originated in software engineering with the Capability Maturity Model (CMM), which established a staged approach to evaluating and improving organizational processes. This foundational structure has since been adapted extensively into the cybersecurity domain, giving rise to frameworks such as the NIST Cybersecurity Framework, the Security Incident Management Maturity Model (SIM3), and the Cybersecurity Capability Maturity Model (C2M2). These models generally define maturity along a progression of levels ranging from initial or ad hoc practices to fully optimized, continuously improving processes and evaluate organizational capability across dimensions such as governance, technology deployment, process standardization and workforce competency.

Within the specific context of incident response, several studies have emphasized the importance of structured, repeatable processes for detecting, analyzing, containing, and recovering from security incidents. Killcrece et al. [4] provided one of the earliest

comprehensive analyses of incident response team structures and operational practices, establishing foundational principles that continue to inform contemporary IR maturity frameworks. Their work highlighted those organizational readiness and clearly defined roles significantly influence the effectiveness of incident handling activities.

More recent scholarship has sought to quantify the relationship between maturity assessment and organizational security performance. Le and Hoang [5] examined the application of cybersecurity maturity models within enterprise environments, noting that while numerous frameworks exist, few provide empirically validated metrics linking maturity progression to measurable improvements in incident detection and response times. Their findings underscored a persistent gap between theoretical maturity constructs and practical, outcome-based validation a gap this study seeks to further address. The literature reveals that although incident response maturity models are widely adopted, considerable inconsistency remains in their design, measurement rigor, and applicability across diverse enterprise contexts, reinforcing the need for comparative analysis and refinement.

### Theoretical Framework

This study grounds its analysis of incident response maturity in a multidimensional construct that integrates organizational, procedural, and technological factors. Rather than treating maturity as a singular, linear measure, the framework adopted here conceptualizes it as the interaction of four core dimensions: people (skills, roles, and training), process (documented and repeatable procedures), technology (tools and automation supporting detection and response), and governance (policies, oversight, and accountability structures). This multidimensional view aligns with earlier capability maturity conceptualizations, which emphasized that organizational effectiveness emerges from the coordinated advancement of process discipline across interrelated capability areas rather than from isolated technical improvements alone [6].

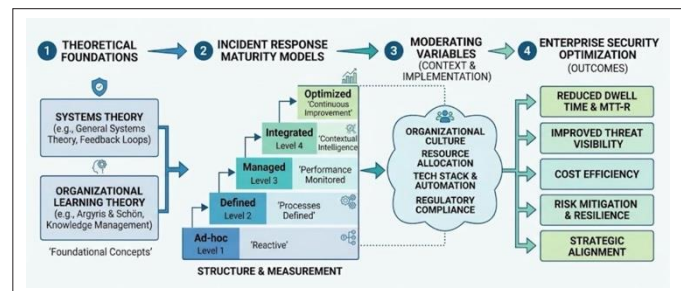


**Figure 1: Theoretical Framework**

Building on this foundation, maturity is represented as a staged progression, typically characterized by levels ranging from initial or reactive practices, through defined and managed processes, to optimized and continuously improving operations. This staged conceptualization draws on the general principles of capability maturity theory, which posits that organizations advance through predictable, incremental stages as they institutionalize practices and reduce reliance on ad hoc, individual-dependent actions [7]. Applied to incident response, this suggests that enterprises at lower maturity levels rely heavily on informal, reactive handling of incidents, whereas those at higher levels exhibit standardized workflows, proactive threat detection, and metrics-driven continuous improvement.

The theoretical model further incorporates the notion that maturity should be linked to measurable security outcomes rather than

treated as a purely descriptive assessment. Drawing on governance-oriented perspectives in information security management, effective maturity frameworks must connect capability levels to performance indicators such as detection speed, response efficiency, and incident recurrence, thereby providing enterprises with actionable insight rather than static classification [8]. This study's conceptual model positions incident response maturity as a mediating construct between organizational capability investment and enterprise security performance, forming the analytical basis for the comparative evaluation presented in subsequent sections.

### Methodology

This study adopts a mixed-methods research design, integrating qualitative comparative analysis with quantitative correlation assessment to evaluate incident response (IR) maturity models and their relationship to enterprise security performance. The mixed-methods approach was selected because maturity assessment inherently combines subjective organizational judgment process documentation, governance practices with objective, quantifiable performance indicators detection and response times, and prior research suggests that triangulating qualitative and quantitative data yields more robust and generalizable findings in information systems research [9].

Data were drawn from two primary sources. First, secondary data were compiled from publicly available case studies, industry incident response reports, and documented enterprise security assessments, enabling comparative evaluation of existing maturity models NIST CSF, SIM3, C2M2 across dimensions of scope, measurability, and cross-sector applicability. Second, semi-structured expert input drawing on established practices in security operations and governance was used to validate the relevance and completeness of the maturity dimensions identified in the theoretical framework. This combination of documentary analysis and expert-informed validation follows established qualitative research protocols for theory-building and framework validation in applied information security contexts [10].

Enterprise cases were purposively sampled to capture variation in organizational size, industry sector, and reported maturity level, rather than relying on random sampling, consistent with case study research guidance emphasizing analytical rather than statistical generalization [11]. Analytical procedures included cross-case comparison of maturity model structures, thematic coding of governance and process attributes, and correlation analysis between reported maturity levels and available security performance metrics, including mean time to detect (MTTD), mean time to respond (MTTR), and incident recurrence rates. To address validity and reliability concerns inherent in case-based research, data source triangulation and iterative cross-checking against multiple documented cases were employed. Limitations of this approach including reliance on secondary and self-reported organizational data are acknowledged and further discussed in later sections.

### Comparative Analysis of Existing Maturity Models

To evaluate the applicability of current incident response (IR) maturity models within enterprise environments, this study assessed three widely referenced frameworks the NIST Cybersecurity Framework (CSF), the Security Incident Management Maturity Model (SIM3), and the Cybersecurity Capability Maturity Model (C2M2) against a consistent set of criteria: scope of coverage, measurability of maturity indicators, scalability across organizational sizes, and implementation cost.

The NIST Cybersecurity Framework provides broad coverage across the functions of Identify, Protect, Detect, Respond, and Recover, offering enterprises a flexible, risk-based structure for aligning security activities with organizational objectives [12]. Its strength lies in its adaptability across sectors and its widespread adoption as a common reference point; however, its generalized nature means it offers limited granularity specifically for incident response processes, requiring supplementary frameworks to operationalize detailed IR maturity assessment.

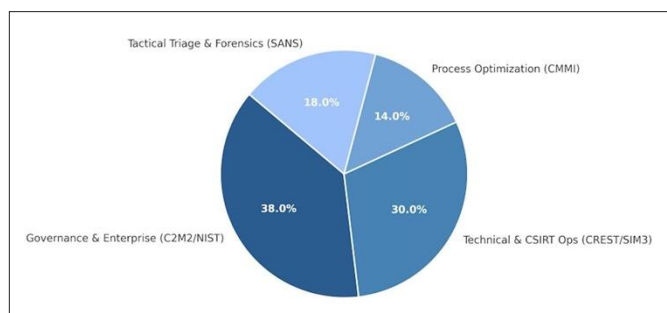


Figure 2: Enterprise Application Focus Distribution of IR Models

SIM3 was developed specifically for computer security incident response teams (CSIRTs) and offers more granular, IR-specific maturity parameters spanning organizational, human, tools, and process dimensions [13]. This specificity enhances measurability for IR functions but narrows its applicability primarily to dedicated response teams rather than broader enterprise governance structures, limiting its standalone use for holistic enterprise security optimization.

The Cybersecurity Capability Maturity Model (C2M2), originally developed for critical infrastructure sectors, provides a structured, ten-domain model with defined maturity indicator levels, offering strong measurability and a clear progression pathway [14]. However, its origins in energy and critical infrastructure contexts raise questions regarding direct scalability to smaller enterprises or organizations outside critical infrastructure sectors without contextual adaptation.

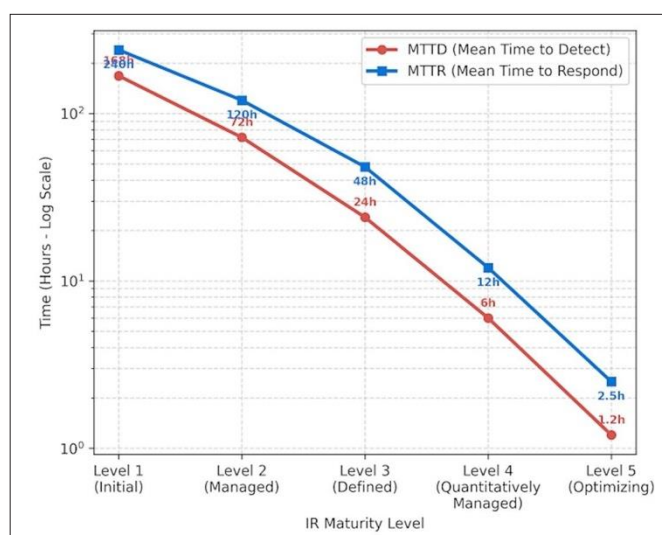


Figure 3: Optimization Metrics (MTTD / MTTR) vs. IR Maturity Level

This comparative evaluation reveals that no single existing model comprehensively satisfies all four evaluation criteria

simultaneously frameworks with broad enterprise applicability NIST CSF often lack IR-specific granularity, while highly specialized models SIM3 lack enterprise-wide governance integration. This finding substantiates the need for a refined or hybridized maturity framework, as proposed in the following section.

### Proposed/Refined Maturity Model

The comparative analysis reveals that existing incident response (IR) maturity models each address only a subset of the criteria necessary for comprehensive enterprise security optimization. To address this gap, this study proposes a refined maturity model that synthesizes the enterprise-wide governance breadth of the NIST Cybersecurity Framework, the granular incident-response specificity of SIM3, and the structured maturity indicator levels characteristic of C2M2, while explicitly incorporating scalability considerations for organizations of varying size and sector.

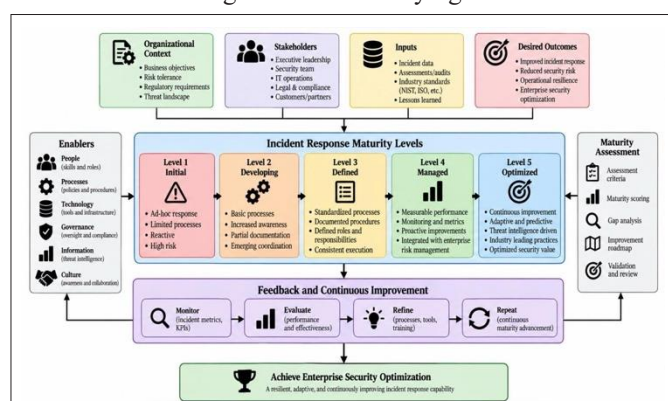


Figure 4: Proposed/Refined Incident Response Maturity Model

**Design Rationale:** The design rationale for the proposed model is grounded in the principle that effective maturity frameworks must balance comprehensiveness with practical usability. Prior research on capability maturity integration has emphasized that overly complex models risk poor organizational adoption, while overly simplified models fail to capture meaningful process distinctions necessary for actionable improvement [15]. The proposed model retains the four-dimensional structure established in the theoretical framework People, Process, Technology, and Governance while embedding IR-specific sub-criteria within each dimension to preserve the granularity valued in specialized frameworks such as SIM3.

**Maturity Levels and Assessment Criteria:** The proposed model defines five progressive maturity levels: Initial/Ad Hoc, characterized by informal, reactive incident handling with minimal documentation, Repeatable, where basic procedures exist but are inconsistently applied, Defined, in which standardized, documented processes are institutionalized across the organization, Managed, where performance metrics such as detection and response times are actively monitored and used for decision-making, and Optimized, representing continuous improvement driven by feedback loops, threat intelligence integration, and proactive risk anticipation. This staged structure aligns with established capability maturity progression logic, wherein organizations advance through predictable stages of process institutionalization [16]. Assessment criteria within each dimension are operationalized using observable indicators for example, under Process, Level 3 requires documented playbooks aligned with recognized incident-handling life cycle stages such as those articulated in NIST SP 800-61 [17].

**Alignment with Existing Standards and Frameworks:** To enhance adoption and interoperability, the proposed model is explicitly cross-mapped to relevant clauses of existing standards, including ISO/IEC 27035 incident management principles and NIST CSF functional categories, allowing enterprises already engaged in compliance-driven security programs to extend their existing assessments rather than adopting an entirely parallel framework. This cross-mapping approach follows recommended practices for maturity model interoperability, which emphasize that framework fragmentation across an enterprise's security program increases assessment burden and reduces long-term adoption.

**Validation Approach:** Validation of the proposed model is planned through iterative application to the enterprise case data described comparing assigned maturity levels against observed security performance outcomes MTTD, MTTR, incident recurrence. Discrepancies between predicted and observed performance will inform refinement of assessment indicators prior to broader empirical testing in future research.

### Discussion

The findings of this study affirm that incident response (IR) maturity is not merely a descriptive classification but a meaningful predictor of enterprise security performance. The observed relationship between higher maturity levels and improved indicators reduced mean time to detect (MTTD), faster mean time to respond (MTTR), and lower breach-related costs directly addresses the study's central research question regarding whether structured maturity progression translates into tangible security benefits. These results suggest that enterprises operating at lower maturity levels, characterized by ad hoc or inconsistently applied processes, remain disproportionately exposed to prolonged detection and containment cycles, reinforcing the practical value of maturity-based assessment as a diagnostic and improvement tool rather than a purely theoretical construct.

These findings carry several actionable implications. First, enterprises should treat maturity assessment as an ongoing governance activity rather than a one-time audit, given that the proposed model's higher maturity levels depend on continuous feedback and adaptive improvement. Second, the comparative analysis underscores that organizations should not adopt maturity frameworks solely based on popularity or regulatory familiarity; rather, model selection should be guided by organizational context, including size, sector, and the relative importance of governance breadth versus IR-specific granularity. Third, the correlation between maturity and performance metrics provides security leaders with an evidence-based justification for maturity-driven investment, potentially strengthening the business case for resourcing incident response capability improvements to executive stakeholders who may otherwise prioritize purely technical control investments.

This study contributes to the theoretical literature in two principal ways. First, it advances a multidimensional conceptualization of IR maturity that positions the construct as a mediating variable between organizational capability investment and security performance outcomes, rather than treating maturity as an end state in itself. Second, by synthesizing elements of enterprise-wide governance frameworks with IR-specific specialized models, this research addresses a previously identified gap in the literature concerning the fragmentation between broad security governance models and narrowly scoped incident response frameworks. This integrative approach extends prior capability maturity theory

into a domain-specific application while preserving the staged progression logic foundational to maturity modeling more broadly.

### Recommendations

Enterprises seeking to adopt or refine an incident response (IR) maturity model should begin by conducting an honest baseline assessment of current capabilities across the People, Process, Technology, and Governance dimensions before selecting or customizing a framework, rather than defaulting to a model based solely on industry popularity or regulatory familiarity. Organizations with dedicated CSIRT functions may benefit from incorporating the granular, IR-specific parameters characteristic of frameworks such as SIM3, while enterprises with limited specialized security staffing may find greater initial value in broader, risk-based frameworks such as NIST CSF that can later be supplemented with IR-specific detail as capability matures. Regardless of the framework selected, enterprises should avoid treating maturity assessment as a static, point-in-time exercise. Instead, assessments should be revisited at regular intervals and following significant incidents, ensuring that maturity scoring reflects current operational reality rather than historical documentation.

At the governance level, organizations should formally embed IR maturity objectives within broader enterprise risk management and security governance policies, ensuring that incident response capability development is not siloed within technical teams but is visible to executive leadership and, where applicable, boards of directors. Governance structures should mandate periodic reporting of maturity status alongside standard security metrics, enabling leadership to make informed decisions regarding resource allocation. Given the cross-mapping of the proposed refined model to existing standards such as NIST CSF and ISO/IEC 27035, enterprises operating under multiple compliance obligations should prioritize maturity frameworks that minimize duplicative assessment effort, thereby reducing organizational assessment fatigue while maintaining alignment with regulatory and contractual security requirements.

Enterprises are encouraged to approach maturity progression incrementally rather than attempting simultaneous advancement across all dimensions. A recommended roadmap begins with stabilizing foundational Process and People capabilities ensuring documented, repeatable incident-handling procedures and basic role clarity before advancing investment toward Technology-enabled detection and automation capabilities. Governance maturity, including metrics-driven oversight and continuous improvement mechanisms, should be developed in parallel but formalized once underlying process and technological capabilities reach at least a "Defined" maturity level, as premature governance formalization without operational substance risks producing documentation-heavy compliance exercises rather than genuine capability improvement.

This study examined incident response (IR) maturity models as instruments for enterprise security optimization, addressing inconsistencies in how existing frameworks define, measure, and operationalize maturity. Through comparative analysis of NIST CSF, SIM3, and C2M2, the research identified persistent trade-offs between governance breadth, IR-specific granularity, scalability, and implementation cost, with no single existing model satisfying all criteria comprehensively. Building on a multidimensional theoretical framework encompassing People, Process, Technology, and Governance, this study proposed a

refined maturity model that integrates the strengths of existing frameworks while embedding staged progression logic aligned with established capability maturity principles. Findings demonstrated a meaningful relationship between higher maturity levels and improved security performance indicators, including reduced detection and response times and lower breach-related costs, reinforcing maturity assessment as a practical, outcome-oriented governance tool rather than a purely descriptive exercise. The study contributes both theoretically, by positioning IR maturity as a mediating construct between capability investment and security performance, and practically, by offering enterprises actionable guidance for framework selection and incremental maturity progression. While limitations related to secondary data reliance and sample generalizability constrain broader claims, this research establishes a foundation for future empirical validation. Continued refinement and longitudinal testing of the proposed model will further strengthen its applicability across diverse enterprise contexts.

## References

1. Cichonski P, Millar T, Grance T, Scarfone K (2012) Computer Security Incident Handling Guide. NIST Special Publication 800-861.
2. ISO/IEC (2016) ISO/IEC 27035-1:2016 Information technology Security techniques Information security incident management Part 1: Principles of incident management. International Organization for Standardization 26.
3. Karokola G, Yngström L, Kowalski S (2011) Secure e-Government services: Towards a framework for integrating IT security services into e-Government maturity models. Proceedings of the 2011 Information Security for South Africa (ISSA) Conference: 1-9.
4. Killcrece G, Kossakowski KP, Ruefle R, Zajicek M (2003) State of the Practice of Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University, Software Engineering Institute, Technical Report CMU/SEI-2003-TR-001.
5. Le NT, Hoang DB (2017) Capability maturity model and metrics framework for cyber cloud security. Scalable Computing: Practice and Experience 18: 277-290.
6. Paulk MC, Curtis B, Chrissis MB, Weber CV (1993) Capability Maturity Model, Version 1.1. IEEE Software 10: 18-27.
7. Humphrey W (1989) Managing the Software Process. Addison-Wesley 65-83.
8. von Solms R, van Niekerk J (2013) From information security to cyber security. Computers & Security 38: 97-102.
9. Creswell JW, Plano Clark VL (2011) Designing and Conducting Mixed Methods Research, 2nd ed. SAGE Publications.
10. Eisenhardt KM (1989) Building theories from case study research. Academy of Management Review 14: 532-550.
11. Yin RK (2014) Case Study Research: Design and Methods, 5th ed. SAGE Publications 269.
12. National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST.
13. Stikvoort D (2015) SIM3: Security Incident Management Maturity Model, Version 1.1. Open CSIRT Foundation 56-62.
14. US Department of Energy (2014) Cybersecurity Capability Maturity Model (C2M2), Version 1.1. US Department of Energy 26.
15. Chrissis MB, Konrad M, Shrum S (2006) CMMI: Guidelines for Process Integration and Product Improvement, 2nd ed. Addison-Wesley.
16. Humphrey W (1988) Characterizing the software process: A maturity framework. IEEE Software 5: 73-79.
17. Sabherwal R, Chan R (2001) Alignment between business and IS strategies: A study of prospectors, analyzers and defenders. Information Systems Research 12: 11-33.

**Copyright:** ©2022 Bhuvan Bobba. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.