Black Sea Journal of Engineering and Science
doi: 10.34248/bsengineering.1729927

Open Access Journal
e-ISSN: 2619 – 8991

Research Article
Volume 9 - Issue 1: 158-179 / January 2026

A MULTI-CRITERIA EVALUATION OF CYBERSECURITY INCIDENT MANAGEMENT FRAMEWORKS: INTEGRATING AHP, CMMI AND SWOT

Hasan Caglar AGAR[1]*, Baris CELIKTAS[1]

[1]*Işık University, Institute of Graduate Students, Department of Computer Science Engineering, 34398, İstanbul, Türkiye*

Abstract: With the growing complexity and frequency of cybersecurity incidents, the selection of an appropriate incident management framework has emerged as a strategic imperative and a nontrivial decision-making problem for organizations operating across diverse sectors. This study presents a multi-dimensional evaluation of four globally recognized frameworks and standards—ISO 27035, NIST 800-61, ITIL v4, and PCI DSS—to determine their effectiveness across 10 rigorously selected key performance parameters. The initial stage of the study involved the identification of 20 preliminary parameters through expert input and literature synthesis. These were then evaluated by 70 cybersecurity professionals using a hybrid decision-making model combining Likert scale scoring, standard deviation filtering, CV score, Z-score normalization and the Analytic Hierarchy Process (AHP) for pairwise comparisons. The top 10 key parameters were derived based on calculated priority weights. To assess each framework, we applied the Capability Maturity Model Integration (CMMI) and visualized results via radar charts and heatmaps, offering comparative insights into operational maturity. Additionally, SWOT analysis was conducted to examine strategic positioning and identify opportunities for improvement. The outcomes not only provide a practical benchmarking guide for practitioners but also introduce a replicable, evidence-based methodology for academic and industry adoption. This work offers a novel and structured lens to evaluate incident management maturity, addressing the pressing need for strategic alignment, automation integration, and adaptive resilience in cybersecurity operations.

Keywords: Incident management, Framework comparison, Evaluation criteria, Maturity model, Analytic hierarchy process, SWOT analysis

***Corresponding author:** Işık University, Institute of Graduate Students, Department of Computer Science Engineering, 34398, İstanbul, Türkiye
E mail: 24sibe5003@isik.edu.tr (H.C. AGAR)
Hasan Caglar AGAR https://orcid.org/0009-0005-4549-3376
Baris CELIKTAS https://orcid.org/0000-0003-2865-6370

Received: June 30, 2025
Accepted: November 22, 2025
Published: January 15, 2026

Cite as: Agar, H. C., & Celiktas, B. (2026). A multi-criteria evaluation of cybersecurity incident management frameworks: Integrating AHP, CMMI and SWOT. *Black Sea Journal of Engineering Science, 9*(1), 158–179.

1. Introduction

In the field of cybersecurity, conceptual clarity is of critical importance for the effective execution of Incident Management Process (IMP). According to ITIL 4 (Agutter, 2020) event refers to any system state (positive or negative) that may be significant relative to normal operations, typically detected through monitoring mechanisms. An incident is defined by both ISO 27035 (International Organization for Standardization, 2016) and Cichonski et al. (2012) as an adverse event such as unauthorized access or data leakage that threatens or has the potential to threaten information security. A problem, as described in ITIL 4, represents the root cause of one or more incidents and typically requires a permanent solution. Meanwhile, a disaster, as outlined in ISO 22301 (International Organization for Standardization, 2019) and Cichonski et al. (2012) frameworks; refers to large-scale, systemic incidents that severely threaten an organization's business continuity. While these concepts are often used interchangeably in the industry, they in fact represent distinctly different processes.

In today's highly interconnected and digital environment, the importance of a well-defined IMP has become substantial. Organizations are exposed to a wide range of incidents that can disrupt operations, compromise data security, and damage reputation. These incidents span from cyberattacks and data breaches to natural disasters, operational errors, and service outages.

Incident management encompasses a structured series of activities designed to detect, analyze, and remediate service disruptions. It provides a systematic approach for identifying, mitigating, and resolving unanticipated events that may compromise the confidentiality, integrity, or availability of critical information assets. If not properly managed, coordinating incident responses and analyzing relevant resources can demand significant time and internal effort.

Leading regulatory and standards bodies (such as ISO, NIST, ITIL and PCI DSS) commonly define five core stages necessary for effective incident management: (1) Planning and Preparation (establishing organizational policies, trained teams, and logging procedures); (2)

Detection and Reporting (identifying and documenting potential incidents); (3) Incident Analysis (categorizing incidents by impact and urgency); (4) Incident Response (executing mitigation and containment actions); and (5) Incident Closure (conducting final reviews and formally closing the incident).

This study focuses exclusively on cybersecurity incident management and is structured accordingly. Its primary objective is to conduct an in-depth examination of the phases established by these regulatory bodies, and to provide a comprehensive comparative analysis of the incident management frameworks and standards they have developed, namely ISO 27035, NIST SP 800-61 Rev.2 (2012), ITIL 4, and PCI DSS.

Through this comparative assessment, the strengths and limitations of each framework and standard have been identified. Building upon these findings, the study proposes best practices and outlines areas for future research, aiming to contribute practical guidance for practitioners and researchers in the field.

This study contributes to the academic and professional field on cybersecurity by proposing a structured, data-driven methodology for evaluating incident management frameworks. Unlike previous works that rely primarily on qualitative comparisons, this work integrates expert input through Likert-scale evaluations and Analytic Hierarchy Process (AHP)-based pairwise comparisons. Standard deviation filtering is applied to enhance statistical reliability in the selection of key evaluation parameters. By synthesizing results from Capability Maturity Model Integration (CMMI) scoring, radar chart visualizations, and SWOT (Strengths, Weaknesses, Opportunities and Threats) analyses, the study provides multi-dimensional insights into the operational, strategic, and technological maturity of four globally recognized frameworks and standards. Furthermore, the study introduces a key parameter–driven comparison model, which enhances the relevance of framework or standard selection based on sectoral needs such as energy, finance, defense, manufacturing and health. This holistic approach not only supports organizations in choosing or customizing frameworks or standards more effectively but also lays a foundation for future studies exploring hybrid or AI-enhanced incident response strategies.

This study provides the following main contributions:

- A structured multi-criteria evaluation model combining Likert scoring, CV score, Z-score normalization, AHP, and standard deviation filtering.
- A comparative assessment of frameworks and standards using CMMI scoring and visual tools.
- A parameter-driven benchmarking approach for sector-specific framework or standard selection.
- Integration of visual decision support, including radar charts and heatmaps.
- Recommendations for hybrid adoption and the use of AI and automation in incident management.

The rest of this paper is organized as described below. Section II offers a review of previous literature and critiques its influence on business practice and establishes the new contributions of this research. Section III describes the process to choose the first 20 preliminary parameters of evaluation and the system for reducing them to the final 10 essential factors using Likert scoring, AHP matrices, and weighted scoring methods. Section IV presents a comparative analysis of the four core incident management frameworks and standards based on a systematic approach rooted in CMMI. Section V formulates the above analysis to find strengths and weaknesses through SWOT matrices. Section VI takes into account the research's limitations and challenges. Section VII evaluates the findings and considers the integration with future technologies such as artificial intelligence, threat intelligence, and automation. Finally, Section VIII provides sector-specific recommendations and assesses framework applicability for small and medium-sized enterprises (SMEs) and large-scale organizations.

1.2. Literature Review

Incident management has become a focal point of cybersecurity research, particularly as threat landscapes grow in complexity and scale. Numerous scholars have examined frameworks and methodologies for responding to security incidents across diverse organizational and technological contexts. For instance, Reuben-Owoh and Haig (2025) conducted a comprehensive comparative evaluation of NIST and ISO-based response strategies, emphasizing the importance of early detection and decision latency in response orchestration. Jäntti (2009) offered a systematic review of incident response models and noted the fragmentation of standards and lack of interoperability as major challenges in unified implementation. Similarly, Aguiar et al. (2018) proposed a taxonomy to classify incident handling models by maturity, adaptability, and traceability, yet acknowledged that practical deployment of such taxonomies remains limited in sector-specific use.

Recent literature has also begun exploring the integration of AI and SOAR (Security Orchestration, Automation, and Response) into traditional frameworks. For example, Bin Ibrahim et al. (2023) highlight how automation-enhanced models reduce incident dwell time, although their work does not include a comprehensive multi-framework comparison. Additionally, Ahmad et al. (2020) stress the organizational impact of incident frameworks, calling for performance benchmarking across scalability, compliance, and recovery efficiency. Despite these advances, many existing studies still treat frameworks or standards in isolation or rely mainly on qualitative methods, offering limited attention to quantified, criteria-driven comparisons across established frameworks and standards.

This study aims to address this critical gap by offering a quantitative, expert-informed, and multi-phased comparative analysis of four globally recognized incident management frameworks and standards. The research begins by identifying and ranking 20 preliminary

parameters through Likert scale surveys and AHP-based pairwise comparisons collected from experienced cybersecurity professionals. This dual-stage prioritization yields a validated set of 10 key parameters, which are then used to assess each framework and standard using CMMI-based maturity scoring, radar chart visualization, and SWOT analysis. By combining quantitative techniques with visual and strategic assessment tools, the study not only compares the frameworks and standards but also surfaces actionable insights for practitioners, especially in high-risk sectors such as finance, transportation, health, defense, and manufacturing.

What distinguishes this research is its emphasis on methodological integration, expert-driven metrics, and cross-framework benchmarking. Unlike previous works that rely solely on qualitative evaluation or single-framework optimization, our approach offers a replicable, scalable model that aligns with real-world organizational decision-making processes. Furthermore, the inclusion of a heatmap matrix and sector-oriented insights introduces a layer of practical applicability often missing in abstract framework and standard comparisons. The proposed methodology can serve as a strategic decision-making tool, guiding stakeholders not only in framework or standard selection, but also in hybrid model development and customization based on key operational needs.

Table 1 provides a structured summary of these and other key studies, highlighting their objectives, methodologies, and contributions to the field.

Table 1. Comparative summary of related work on incident management frameworks and standards

Related Study	Summary	Contribution
Aguiar et al. (2018)	This study proposes an incident management maturity model that eliminates overlaps between multiple frameworks (ITIL, COBIT, CMMI-SVC), enabling organizations to assess and improve their incident management capabilities more systematically and consistently.	The model provides organizations with a unified tool to benchmark and enhance incident management processes across different frameworks, supporting better integration, compliance, and operational efficiency in incident management.
Pirta-Dreimane et al. (2025)	This paper presents a technology-enhanced educational approach, named esCAPE, designed to simulate cybersecurity incidents	The study contributes to workforce development by offering interactive training methods that enhance practical incident response capabilities
Grobauer and Schreck (2019)	This paper analyzes the unique challenges of incident handling in cloud environments and discusses potential approaches to effectively detect, manage, and respond to security incidents.	The study provides cloud service providers and enterprises with guidance for designing robust cloud incident response strategies
Gnanasekaran et al. (2025)	This paper introduces a comprehensive role taxonomy for security and safety incident response, categorizing responsibilities and interactions to clarify roles during incident handling and improve coordination among response teams.	By defining clear roles and responsibilities, the taxonomy helps organizations streamline incident response operations, reduce confusion during critical events, and enhance both security and safety outcomes in complex IT and industrial environments.
Ahmad et al. (2020)	This study investigates how integrating cybersecurity management with incident response processes fosters organizational learning, emphasizing knowledge capture from security incidents to improve future resilience.	The findings support organizations in establishing feedback loops between incident response and cybersecurity governance, enabling continuous improvement, enhanced threat awareness, and more informed decision-making in managing cybersecurity risks.
Onwubiko and Ouazzane (2022)	This study presents SOTER, a structured playbook for managing cybersecurity incidents, detailing processes and best practices.	The playbook provides organizations with a practical framework to improve incident handling efficiency and enhance overall cybersecurity resilience.
Naseer et al. (2021)	This paper examines the concept of analytical information processing capability within cybersecurity incident response, highlighting how organizations analyze, interpret, and act on incident data to improve decision-making and response effectiveness.	By clarifying how analytical capabilities influence incident response performance, the study guides organizations in developing data-driven response strategies, optimizing resource allocation, and enhancing overall cybersecurity resilience.

Table 1. Comparative summary of related work on incident management frameworks and standards (continuing)

Related Study	Summary	Contribution
Dykstra et al. (2022)	Dykstra et al. (2022) discuss the risks of "action bias" in cybersecurity incident response, emphasizing that impulsive actions can worsen incidents.	The paper encourages organizations to adopt more measured and deliberate incident response strategies, reducing errors and improving overall security posture.
Munteanu et al. (2014)	This paper examines the challenges of incident management in cloud environments, proposes research directions, and outlines an architectural approach to improve detection, response, and recovery processes in cloud infrastructures.	The study aids cloud service providers and enterprises in designing more robust cloud incident management frameworks, addressing scalability, complexity, and operational efficiency issues while enhancing overall service reliability and security.
Almashaqbeh and Almomani (2023)	This study aims to enhance the effectiveness of SOAR platforms by utilizing AI-assisted playbook recommendations.	Within the scope of the study, similarity learning and open-source SOAR platform integration methods were employed.
Alevizos (2025)	This paper explores an automated approach to cybersecurity compliance and threat response by leveraging AI, blockchain, and smart contracts, aiming to enhance real-time monitoring, enforcement, and incident handling.	The study provides a framework for organizations to implement automated, trustable, and auditable cybersecurity processes, reducing manual intervention, improving compliance adherence, and enabling faster, more reliable responses to emerging threats.
McLaughlin (2023)	This article explores the integration of Artificial Intelligence (AI) with the Cybersecurity Mesh framework, analyzing how this combined approach strengthens modern digital defense strategies and enhances adaptive, distributed cybersecurity capabilities.	The study provides practical insights for organizations aiming to implement AI-driven, mesh-based cybersecurity architectures, promoting more resilient, scalable, and proactive defense mechanisms against evolving cyber threats.
Lourens et al. (2022)	This study reviews the integration of AI in cybersecurity, highlighting techniques like anomaly detection and predictive analytics along with practical implementation challenges.	The study informs organizations about AI adoption barriers and guides the development of more resilient, explainable cybersecurity systems.
Islam et al. (2024)	This study proposes an intrusion detection system for industrial Cyber-Physical Systems (CPS)	The research provides industrial organizations with an advanced, intelligent security solution
Chirra (2023)	It addresses the role and effectiveness of automated incident response processes in modern cybersecurity systems.	Automated incident response processes in modern cybersecurity systems have been evaluated through the analysis of automation techniques and system integration.

2. Meterials and Methods

This study adopts a multi-phase, expert-driven, and quantitatively enhanced methodology to perform a comparative analysis of four internationally recognized cybersecurity incident management frameworks and standards. The process was designed to ensure both academic rigor and practical applicability, especially in the context of rapidly evolving digital threat environments and sector-specific operational constraints.

2.1. Research Design and Phases

This section outlines the comprehensive research design and the phased methodology adopted throughout the study. It begins by detailing the identification and selection process of preliminary parameters through expert insight and literature synthesis. Following this, we describe the application of Likert scale surveys and calculation of additional descriptive statistics such as Standard Deviation, Coefficient of Variation (CV) and Z-Score normalization were incorporated into the methodology following the initial Likert-based analysis. After this phase, an AHP-based pairwise comparisons to derive weighted scores and reduce the parameters to a refined set of key criteria.

Subsequent phases include the comparative evaluation of cybersecurity incident management frameworks and standards using the CMMI maturity model and SWOT analysis. Each methodological step is carefully integrated to ensure analytical rigor, objectivity, and sectoral relevance.

The overall workflow adopted in this study is summarized in Figure 1, which illustrates the multi-phase methodology from the collection of preliminary parameters through to the final evaluation and recommendations.

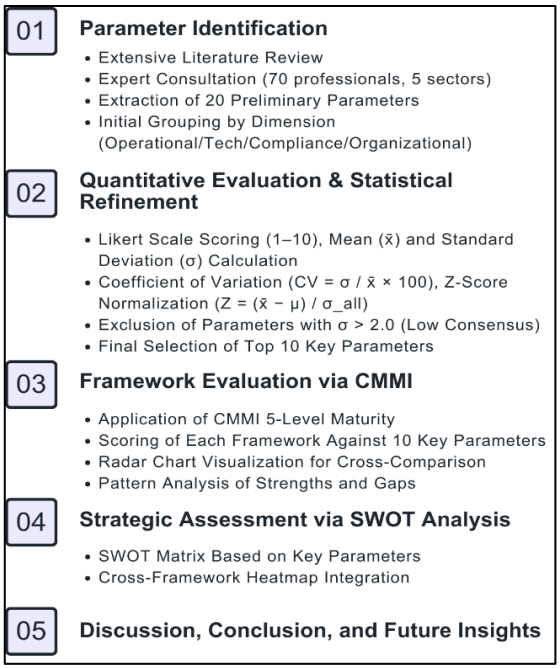

Figure 1. The methodology of "evaluation of incident management framework and standards" study.

2.1.1. Criteria identification and key parameter extraction

In the first phase, an initial set of 20 preliminary parameters were identified through an extensive review of existing standards, academic publications, and industry practices. These criteria included operational efficiency, regulatory compliance, scalability, automation, adaptability, and others deemed relevant for incident response maturity. To validate and prioritize these parameters:

- A Likert scale–based survey was conducted with 70 cybersecurity professionals from diverse domains (e.g., finance, transportation, manufacturing, health and defense).
- The mean scores and standard deviations were calculated to measure the centrality and variability of expert responses. Criteria with high variance ($\sigma > 2.0$) were excluded due to inconsistent expert consensus.
- In addition, to ensure statistical rigor and transparency in expert evaluations, specifically, the Coefficient of Variation (CV) and Z-score normalization were applied to assess the homogeneity, differentiation, and agreement intensity of expert responses. The CV quantifies relative dispersion independent of the parameter's mean, thus allowing for meaningful comparison among parameters with different scales or variances. The Z-score normalization situates each parameter's mean score within the overall distribution of all parameter means, thereby revealing how strongly each parameter deviates from the global average importance perception. These additions aim to strengthen interpretive granularity and provide a more transparent foundation for subsequent phases.

In parallel, the same experts were asked to conduct pairwise comparisons between grouped parameters using the AHP. Each group contained logically related parameters (e.g., operational performance, compliance, technology integration), and weights were derived using standard AHP calculations, including pairwise matrices, geometric means, and normalization procedures (e.g., Saaty, 2008; Bhole and Deshmukh, 2018).

To derive composite importance scores, Likert scores and AHP weights were normalized and integrated. The top 10 parameters were then selected as key evaluation parameters for comparison of frameworks and standards.

2.1.2. Framework evaluation and visualization

In the second phase, the frameworks and standards were evaluated against the 10 key parameters using two techniques: Firstly, the CMMI 5-level scoring system was adapted to quantify each framework's and standard's maturity across key parameters. The levels are stated in Table 2.

Table 2. CMMI Model Phase Definitions (Level 0-5)

Level	Name	Explanation
1	Initial	Characterized by uncertainty, lacks systematic structure, follows an ad-hoc pattern, operates without any form of documentation or measurable indicators.
2	Managed	Defined and implemented at a fundamental level, largely driven by individual effort, documentation remains weak and insufficient to ensure consistency or repeatability.
3	Defined	Well-documented and consistently executed in accordance with defined standards, underpinned by a mature and institutionalized organizational culture.
4	Quantitatively Managed	Guided by quantifiable metrics and key performance indicators (KPIs), ensuring traceability and enabling ongoing evaluation and continuous improvement.
5	Optimizing	Processes are subject to continuous improvement, enhanced through automation and AI-driven capabilities, and fully integrated with industry best practices to ensure efficiency, scalability, and strategic alignment.

Each framework and standard was scored based on its official documentation, best practice guides, and structured definitions. The evaluations were supported by a justification matrix that explained each score with direct references to the framework's and standard's sections and capabilities.

Additionally, the evaluation of each framework and standard based on CMMI (Team, 2006) scores was visualized using radar charts. In this study, we employed radar charts to provide a visual and multidimensional comparative analysis of each incident management framework and standard against the ten selected key parameters. Radar charts are particularly effective for presenting multi-criteria performance profiles. They allow readers to intuitively grasp the strengths, weaknesses, and gaps of each framework across several dimensions simultaneously. Their use supports pattern recognition and holistic interpretation, especially when dealing with non-linear and interrelated variables such as response time, automation levels, and compliance capacity. From a methodological standpoint, radar charts facilitate both internal evaluation (how well a single framework or standard aligns with the key parameters) and cross-framework and standard comparison without the cognitive overload often associated with complex tables or numerical matrices. Through this approach, we achieved a balanced blend of visual storytelling and analytical depth, enabling stakeholders to derive actionable insights with greater clarity and precision.

Rabii et al. (2020) have validated radar charts as suitable tools in multi-criteria decision-making (MCDM) and cybersecurity maturity assessments, enhancing the interpretability of technical assessments in risk, compliance, and performance benchmarking domains.

2.1.3. Strategic evaluation via SWOT analysis

In the final phase, each framework and standard was subjected to a structured SWOT analysis based solely on the 10 key parameters. This allowed the study to go beyond maturity scoring and examine the strategic positioning of each framework and standard, evaluated by parameters such as adaptability to AI, automation capabilities, compliance orientation, and future-readiness. Each SWOT cell was supported by citations from either framework or standard documentation or relevant academic and industry publications.

A cross-framework and standard SWOT heatmap was also proposed, integrating the evaluations to highlight sector-specific suitability, operational bottlenecks, and innovation gaps.

2.2. Tools and Ethical Considerations

All surveys were conducted by cybersecurity professionals through Google Forms, ensuring participant anonymity. Data analysis and scoring were performed using Excel and Python-based AHP calculators, while visualizations were built using Canva and Microsoft Excel Radar and Heatmap tools. Participation in the study was voluntary, and all expert input was anonymized and used solely for research purposes.

2.3. Scope and Limitations

This study evaluates frameworks and standards at the strategic and structural level, not their implementation maturity within specific organizations. As such, the results serve as guidance for selection, customization, or integration of frameworks and standards, rather than as audits of real-world deployments. Additionally, while the sample of 70 experts ensures reasonable confidence, broader demographic diversity and longitudinal validation would further improve the generalizability of the results.

3. Results

3.1. Definition of Key Parameters

The management of information security incidents is not merely a technical intervention but a multifaceted process requiring organizational decision-making, regulatory compliance, and effective communication. Therefore, Scarfone et al. (2008) describes that the success of a framework or standard depends not only on detection time but also on numerous parameters ranging from response speed and user experience to legal compliance and learning capacity. The literature highlights, through various academic studies (Saaty, 2008; Bhole and Deshmukh, 2018) that an effective Incident Management framework or standard (International Organization for Standardization, 2016) should encompass at least the dimensions of detection, response, reporting, learning, and communication. Additionally, Trifonov et al. (2019) suggest that the integration of automation and artificial intelligence has made real-time monitoring and response to modern threats nearly indispensable. However, considering that incident management is a multi-stage process with each stage interconnected, it is vital to incorporate objective, robust, and application-oriented criteria from users when evaluating incident management frameworks and standards. In this context, we believe that the opinions of cybersecurity professionals are critically important when defining the relative importance of criteria during the incident management process. So within this perspective, below, our methodology—based on academic foundations and expert opinions from cybersecurity professionals—used to select parameters for framework evaluation is explained step by step.

3.1.1. Determining of the preliminary parameters

In light of all these evaluations described; the "Identification of Key Parameters" phase of this study primarily involved a literature review related to Incident Management. Based on the examination of academic studies in this field, 20 preliminary parameters relevant to IMP are listed below and presented in Table 3. During the selection of these parameters, variables such as importance level, frequency of use, and overall performance during the IMP were not taken into consideration.

Table 3. 20 Preliminary Parameters chosen in the evaluation of IMP

No	Parameter
1	Detection Time
2	Response Time
3	Recovery Time
4	Adaptability
5	Scalability
6	False Positive Reduction
7	Compliance with Regulations
8	Reporting Capabilities
9	User Friendly Interface
10	Cost and Implementation Complexity
11	Traceability
12	Continuous Learning Capability
13	End-to-End Visibility
14	Training and Awareness Support
15	Human Intervention Requirement
16	Threat Intelligence Integration
17	Level of Automation
18	Emerging Tech Compatibility
19	SOAR Integration
20	Compatibility with AI

3.1.2. Ranking of Preliminary Parameters Using Likert Scale Scoring

In the subsequent phase, a prior evaluation of the 20 preliminary parameters was conducted using a Likert scale by 70 cybersecurity professionals holding roles in finance, defense, transportation, manufacturing, and health sectors in different organizations (21 of them were Chief Information Security Officers (CISO), 14 of them IT Security Managers, 11 of them Information Security Governance, 17 of them Risk & Compliance (GRC) Specialists and 7 of them Security Operations Center (SOC) Managers) each possessing over 10 years of substantial experience in information security management, service operations, and regulatory compliance. Each criterion was rated by these cybersecurity professionals in an impartial manner. The evaluation was conducted within a Likert scale provided by Donne et al. (2021) from 1 (least important) to 10 (most important) based on its performance within the IMP.

After scoring of the cybersecurity professionals, to ensure the highest stability to define the key parameters, the standard deviation values of the given scores were calculated by using equation 1 accordingly. During this calculation, low standard deviations indicated strong consensus among experts, whereas high standard deviations reflected significant disagreements.

$$\sigma = \sqrt{[\, \Sigma(x_i - \bar{x})^2 / (n - 1)\,]} \quad (1)$$

Where:
σ = Standard Deviation
Σ = Summation Symbol
x_i = The individual value (each participant's score)
$\bar{x}$ = The mean (average) of all scores
n = The number of observations (number of participants)
$(x_i - \bar{x})^2$ = The squared difference between each score and the mean value

To enhance further interpretive depth, two additional statistical indicators were computed for each parameter: The first one is Coefficient of Variation (CV) shown in equation 2, providing a normalized measure of dispersion, independent of the mean value, and is calculated as:

$$CV = \sigma / \mu \quad (2)$$

Where:
σ = standard deviation of expert scores
μ = mean Likert score of the parameter

Then, Z-score Normalization is calculated to evaluate the relative standing of each parameter's average score within the global distribution of all parameters, the Z-score was calculated and shown in equation 3 as follows:

$$Z = (\mu_i - \bar{\mu}) / \bar{\sigma} \quad (3)$$

Where:
μ_i = mean score of the parameter
$\bar{\mu}$ = mean of all parameter means
$\bar{\sigma}$ = standard deviation of all parameter means

Through the integration of mean, standard deviation, CV and Z-score analysis, this study achieved a multidimensional validation of parameter reliability. This approach enhanced both the robustness of expert-driven data and the transparency of the parameter selection process, ensuring that the retained criteria accurately represent the collective judgment of the expert group.

Then, data with low standard deviation (<2.0) because experts' opinions were consistent, while data with high standard deviation (>2.0) were excluded due to disagreements among experts. The combination of average Likert score, standard deviation, CV and Z-scores of the parameters rated by cybersecurity professionals are shown in Table 4.

Then, data with low standard deviation (<2.0) were included in the calculations because "experts' opinions were consistent," while data with high standard deviation (>2.0) were excluded due to "disagreements among experts". The combination of Average Likert Score of the parameters rated by cybersecurity professionals, standard deviation, CV and Z-scores are shown in Table 4.

This multi-metric approach ensures that the retained parameters are not only statistically stable but also reflect the collective and coherent judgment of cybersecurity professionals, thereby reinforcing the reliability and transparency of the parameter selection process used in this study.

Table 4. Data table including likert scores, standard deviation, CV and Z-score values

No	Parameter	LIK	SD	CV	Z
1	Detection Time	9.47	0.70	0.088	1.866
2	Traceability	8.97	1.15	0.151	1.225
3	Compliance with Regulations	8.96	0.99	0.131	1.097
4	Response Time	8.87	0.87	0.117	0.968
5	End-to-End Visibility	8.84	1.18	0.158	0.968
6	Recovery Time	8.67	1.53	0.212	0.584
7	Level of Automation	8.63	1.38	0.191	0.584
8	Reporting Capabilities	8.34	2.03*	0.243	0.313
9	User Friendly Interface	8.30	2.07*	0.253	0.056
10	SOAR Integration	8.28	2.13*	0.287	0.056
11	Adaptability	8.26	1.37	0.198	0.056
12	False Positive Reduction	8.21	1.38	0.200	-0.072
13	Threat Intelligence Integration	8.19	2.15*	0.314	-0.072
14	Emerging Tech Compatibility	7.92	1.51	0.224	-0.200
15	Scalability	7.72	1.59	0.246	-0.713
16	Human Intervention Requirement	7.67	1.50	0.234	-0.842
17	Training and Awareness Support	7.57	2.06*	0.277	-0.984
18	Cost and Implementation Complexity	7.28	1.61	0.260	-1.112
19	Continuous Learning Capability	7.26	1.45	0.240	-1.369
20	Compatibility with AI	6.33	2.39*	0.439	-2.409

LIK= average mean score (Likert Scale); SD= standard deviation; CV= coefficient of valuation score; Z= Z-Score normalization score.

* Eliminated parameters which have >2.0 standard deviation value.

3.1.3. Calculation of relative weights of preliminary parameters using the AHP technique

In the next phase - after the elimination of 6 parameters due to divergent decisions of the cybersecurity professionals – in order to ensure the conceptual coherence and enable domain-specific analysis in the "Future Insights" part. Thus, the remaining 14 candidate criteria were first categorized into three groups according to their roles in the incident management process: the first group contains operational performance and response procedures, the second group consists parameters of usability and regulatory compliance, and the third group includes parameters of technological integration and automation capability.

While the Likert scale scoring conducted in the previous phase provided a preliminary quantitative insight into expert preferences, the study would lack of comparative depth and short of balanced results. In order to provide an analytical and robust elimination regarding the parameters, we decided to apply the AHP method and the pairwise comparison technique as a second-layer evaluation to derive relative weights and prioritize criteria more robustly. AHP captures consistency in expert judgements and provides normalized weight vectors based on relative performance.

These categories were then scored by 70 cybersecurity professionals again (competencies of them already described in the Likert scale survey) using the AHP method and the pairwise comparison technique.

In this study, AHP method was applied to prioritize candidate criteria based on expert judgments.

$$n_{ij} = a_{ij} / \sum_k a_{kj} \quad (4)$$

Where:

a_{ij} = the original comparison value between criterion i and j

$\sum_k a_{kj}$ = is the sum of column j

n_{ij} = the normalized value of cell (i, j)

$$W_i = (1 / n) \times \sum_j n_{ij} \quad (5)$$

Where:

W_i = the standard weight for criterion i

n = the number of criteria

n_{ij} = the normalized score of criterion i over criterion j

First, pairwise comparisons were collected from cybersecurity professionals, and a comparison matrix was constructed. And then using equation 4 described above, each matrix was normalized by dividing individual elements by the sum of their respective columns *($n_{ij} = a_{ij} / \sum_k a_{kj}$)*.

After this, the average of each row was calculated to obtain the standard weight for each criterion by using equation 5 *($W_i = (1 / n) \times \sum_j n_{ij}$)*, representing its relative importance within its group.

Each pairwise comparison was quantified using vote ratios (e.g., 63/7 for Detection Time vs. Response Time), and a reciprocal matrix was constructed per group. All vote-based ratio values (e.g., 63/7) were directly normalized by column-wise division to construct a consistent reciprocal matrix, from which the priority vectors were derived. This approach aligns with AHP methodology principles while adapting to expert consensus data collected during the study, ensuring internal consistency and methodological rigor. From this, normalized priority vectors were calculated to determine AHP-based standard weights. These weights reflect the relative importance of each parameter within its group and enable structured prioritization based on expert consensus. Through this pairwise comparison method, the relative weight of each criterion was calculated. The grouping approach ensured better focus, reduced inconsistency, and preserved thematic coherence, as supported MCDM methodology literature. In addition, this approach enabled us to derive quantitative priorities from qualitative expert input and supported the identification of the most influential parameters for

incident management framework and standard evaluation. At the end of this phase, the resulting Pairwise Comparison Matrix and the AHP Weight Scores for the 14 preliminary parameters obtained are shown in Table 5.

Table 5. Pairwise comparison matrix and AHP weight scores of preliminary parameters

Group 1: Operational Performance And Response Processes								
No	Parameter	Detection Time	Response Time	Recovery Time	False Positive Reduction	Traceability	End-to-End Visibility	AHP STANDARD WEIGHTAGE
1	Detection Time	-	60/10	59/11	59/11	69/1	69/1	0,383
2	Response Time	10/60	-	42/28	59/11	57/13	61/9	0,207
3	Recovery Time	10/60	28/42	-	49/21	63/7	69/1	0,218
4	False Positive Reduction	11/59	12/58	21/49	-	20/50	43/27	0,063
5	Traceability	2/68	13/57	7/63	51/19	-	49/21	0,081
6	End-to-End Visibility	1/69	11/59	2/68	27/43	21/49	-	0,048

Group 2: Usability And Compliance Characteristics				
No	Parameter	Compliance with Regulations	Cost and Implementation Complexity	AHP STANDARD WEIGHTAGE
7	Compliance with Regulations	-	49/21	0,714
8	Cost and Implementation Complexity	21/49	-	0,286

Group 3: Technological Compliance And Automation Capability									
No	Parameter	Adaptability	Scalability	Continuous Learning Capability	Human Intervention Requirement	Level of Automation	Emerging Tech Compatibility	AHP STANDARD WEIGHTAGE
9	Adaptability	-	31/39	32/38	69/1	11/59	3/67	0,165
10	Scalability	39/31	-	27/43	60/10	7/63	21/49	0,072
11	Continuous Learning Capability	38/32	43/27	-	57/13	10/60	22/48	0,083
12	Human Intervention Requirement	1/69	10/60	13/57	-	20/50	9/61	0,032
13	Level of Automation	59/11	63/7	60/10	50/20	-	17/53	0,028
14	Emerging Tech Compatibility	67/3	49/21	48/22	61/9	53/17	-	0,366

3.1.4. Combination of techniques and identification of key criteria

To determine the most impactful criteria for evaluating incident management frameworks and standards, we applied MCDM approach that integrated results from Likert-scale scoring, standard deviation analysis, and AHP pairwise comparisons.

First, Likert-scale surveys (1–10 scale) were conducted with 70 cybersecurity professionals to capture perceived importance levels of 20 preliminary parameters. For each parameter, we calculated the mean Likert score to represent average perceived relevance. To assess the consistency of expert opinions, the standard deviation (σ) was calculated in order to get to a conclusion that a lower standard deviation indicated stronger consensus, while a higher one suggested divergence among respondents. And through this analysis, six preliminary parameters named "Threat Intelligence Action", "Reporting Capabilities", "User Friendly Interface", "Training and Awareness Support", "SOAR Integration" and "Compatibility with AI" were eliminated as they reflected divergence among cybersecurity professionals.

After this, an AHP pairwise comparison provided by Saaty (1987) was applied to the remaining 14 parameters. Experts compared pairs of parameters to express which one was more important and by what degree (as shown in Table 3, e.g., 59/11). From these binary judgements, normalized AHP weights were derived using geometric mean calculations and matrix normalization techniques.

To synthesize these data sources, a composite prioritization score was calculated for each criterion by using Equation 6 (Vaidya and Kumar, 2006; Ak and Gul, 2019).

- Normalized Likert mean score (reflecting perceived importance),
- Standard deviation (reflecting consensus reliability — lower values indicate agreement and increase the criterion's influence, whereas higher values reduce its impact due to expert inconsistency),
- Coefficient of Variation (CV) was incorporated into the equation. The CV term introduces a measure of relative dispersion, ensuring that parameters with consistent expert agreement (lower variability relative to their mean importance) are given proportionally higher weight.
- Z-score (Z_i) was additionally added to standardize each parameter's Likert mean across the dataset, highlighting parameters that significantly deviate (positively or negatively) from the overall population mean.
- AHP weight (reflecting relative priority in direct comparisons).
- The weighting coefficients applied in the composite Key Score model ($\alpha = 0.30$, $\beta = 0.30$, $\gamma = 0.15$, $\delta = 0.15$, $\varepsilon = 0.10$) were established following empirical balancing principles grounded in the multi-criteria decision-making (MCDM) literature. Specifically, the weights

assigned to the Likert-based expert evaluations (α = 0.30) and AHP-derived hierarchical priorities (β = 0.30) align with Saaty's (2008) and Bhole and Deshmukh (2018) recommendations, where subjective and objective components are designed to hold approximately equal influence (25–35%) in hybrid decision systems. The coefficients for statistical dispersion and reliability—standard deviation (γ = 0.15) and coefficient of variation (δ = 0.15)—follow the quantitative calibration approach of Moreira et al (2021), who emphasized that uncertainty-correcting metrics should collectively moderate roughly one-third of the model's total explanatory power to ensure analytical stability. Finally, the inclusion of the Z-score (ε = 0.10) as a normalization adjustment term is derived from Sahoo and Goswami (2023), suggesting that distributional corrections typically contribute a minor yet essential stabilizing effect (10–15%) in composite scoring models. This proportional configuration guarantees that no single dimension dominates the model while maintaining empirical robustness, interpretive transparency, and statistical balance across subjective and objective inputs.

$$K_i = 0.30 \cdot \bar{x}_i + 0.30 \cdot w_i - 0.15 \cdot \sigma_i + 0.15 \cdot (1/CV_i) + 0.10 \cdot Z_i \quad (6)$$

Where:

K_i = Key Score of parameter i

$\bar{x}_i$ = Likert mean score for parameter i

w_i = AHP-based standard weight for parameter i

σ_i = Standard deviation reflecting expert consensus

CV_i = Coefficient of Variation of parameter i (σ_i / $\bar{x}_i$)

Z_i = Z-score of parameter i, representing normalized deviation from the global mean

α, β, γ, δ, ε = Normalization coefficients used to balance the relative influence of each factor (set empirically or equally distributed if no specific dominance is assumed)

The selected coefficient ratios thus ensure a balanced interplay between expert judgment, analytical hierarchy structuring, and statistical reliability factors."

We can summarize this combination phase that:

• A higher Likert mean increases the Key Score (K_i),

• A higher standard deviation decreases the Key Score (K_i) and even results with elimination of the parameters that can be assumed reflecting lack of expert consensus,

• A lower CV score indicates higher homogeneity and stronger expert consensus relative to the mean.

• A higher Z-score denotes that the parameter's importance is above the global mean perception, while a negative Z-score indicates below-average perceived importance,

• A higher AHP weight increases the Key Score (K_i).

Each term contributes to a composite decision metric that blends subjective expert ratings, comparative importance, and statistical consistency.

At the end of this phase, the top 10 parameters in terms of Key Score (K_i) were selected as "Key Parameters" for use in subsequent evaluation stages; including the CMMI maturity scoring, SWOT analysis, and framework visualizations (e.g., radar charts and heatmaps).

This integrated scoring methodology ensured that selected criteria were not only validated by domain experts, but also statistically robust, thematically coherent, and highly impactful for cybersecurity incident management framework and standard analysis.

As shown in Table 6, parameters marked with an asterisk (*) were excluded due to a high standard deviation (>2.0), reflecting a lack of evaluative consistency among subject-matter experts. Table 6 presents the final key scores, highlighting the top 10 parameters with the highest composite values. In the next phase, it is aimed to enable an objective comparison of Incident Management Frameworks and Standards using these 10 systematically determined key parameters based on well-designed methodology and academic foundations.

Table 6. Incident management process criteria scoring

No	Parameter	LIK	SD	CV	Z	AHP	Key Score
1	Detection Time	9,47	0,70	0.088	1.866	0,383	4.040
2	Response Time	8,87	0,87	0.117	0.968	0,207	3.626
3	Compliance with Regulations	8,96	0,99	0.131	1.097	0,714	3.903
4	Traceability	8,97	1,15	0.151	1.225	0,081	3.477
5	End-to-End Visibility	8,84	1,18	0.158	0.968	0,048	3.391
6	Recovery Time	8,67	1,53	0.212	0.584	0,218	3.246
7	Adaptability	8,26	1,37	0.198	0.056	0,165	3.080
8	Level of Automation	8,63	1,38	0.191	0.584	0,028	3.053
9	False Positive Reduction	8,21	1,38	0.200	-0.07	0,063	3.013
10	Emerging Tech Compatibility	7,92	1,51	0.224	-0.20	0,366	2.966
11	Continuous Learning Capability	7,26	1,45	0.240	-1.37	0,083	2.768
12	Human Intervention Requirement	7,67	1,50	0.234	-0.84	0,032	2.689
13	Reporting Capabilities*	8,34	2,03*	0.243	0.313	0,268	3.120
14	Scalability	7,72	1,59	0.246	-0.71	0,072	2.671
15	Cost and Implementation Complexity	7,28	1,61	0.260	-1.11	0,286	2.617
16	User Friendly Interface*	8,30	2,07*	0.253	0.056	0,067	2.841
17	Training and Awareness Support*	7,57	2,06*	0.277	-0.98	0,069	2.683
18	SOAR Integration*	8,28	2,13*	0.287	0.056	0,14	2.914
19	Threat Intelligence Integration*	8,19	2,15*	0.314	-0.07	0,25	2.751
20	Compatibility with AI*	6,33	2,39*	0.439	-2.40	0,09	2.233

3.2. Comparative Analysis of Core Frameworks and Standards

The complexity and frequency of cybersecurity threats have significantly increased in recent years. Incident management stands as one of the most critical pillars of

modern cybersecurity architectures. In this context, Killcrece et al. (2003) states that organizations require a robust framework or standard to ensure preparedness for incidents, enable effective response, and integrate post-incident improvement processes into their institutional memory. In addition, Mızrak (2023) explains that considering the developments and lessons learned in this domain, it has become essential not only for organizations to implement relevant frameworks or standards in their security processes but also to assess their maturity levels.

3.2.1. Evaluation of incident management frameworks and standards through CMMI

In this phase of the study, we evaluate four fundamental frameworks widely employed in the IMP. This evaluation leverages CMMI, which provides a structured methodology (Caralli et al., 2010; Garae and Ko, 2017) to assess an organization's current maturity level and develop targeted improvement strategies. The assessment is grounded in the ten key parameters identified in the previous phase through academically rigorous methods, as summarized in Table 6. At this stage, each framework and standard will be analyzed according to the five-level structure of the CMMI model.

Caralli et al. (2010) explains that this structure enables the evaluation not only of the current maturity levels for each parameter but also of the attainable target states. In doing so, Eberhard (2023) describes that it facilitates situational assessment and provides decision-makers with a clear roadmap for process improvement. Accordingly, each of the ten key parameter was assessed for all four frameworks using the five-level CMMI structure presented in Table 2. The resulting data are presented in Figure 2 for ISO 27035, Figure 3 for NIST 800-61, Figure 4 for ITIL 4, and Figure 5 for PCI DSS and overall evaluation in Figure 6.

3.2.1.1. CMMI evaluation for ISO 27035

As shown in Figure 2; regarding ISO 27035 standard evaluation across 10 key incident management parameters using the CMMI maturity scale, presents a structured and procedurally strong approach, particularly excelling in foundational areas like Detection Time, Response Time, and Compliance with Regulations. The ISO 27035 standard underscores the critical role of continuous monitoring and analytical processes in the early detection of information security incidents. These mechanisms enable timely identification and effective reporting, thereby enhancing organizational responsiveness. (Clause 5.3 – Detection and reporting of information security events and incidents). Furthermore, the standard mandates a timely and effective response to security incidents, with comprehensive guidance provided on the planning and implementation of incident response activities (Clause 5.5 – Responses to information security incidents). And while the framework does not explicitly address legal and regulatory compliance, it emphasizes that legal notification requirements should be taken into account as part of the post-incident review process (Clause 5.6 – Post-incident activities).

The standard's structure additionally and explicitly addresses Traceability, Adaptability and Recovery Time (both Level 3), reflecting well-defined documentation practices and emphasis on post-incident review processes. For Traceability, the standard advocates for the collection and analysis of incident records as a means to ensure comprehensive documentation and end-to-end traceability of security incidents (Clause 5.6 – Post-incident activities). Furthermore, Adaptability is defined throughout the standard as it promotes a culture of continuous improvement, whereby organizations are expected to refine their processes and enhance resilience by incorporating lessons learned from past incidents (Clause 5.6 – Post-incident activities). And similarly for Recovery Time, the standard provides support for post-incident recovery and business continuity processes, thereby contributing to minimizing recovery time and enhancing organizational resilience (Clause 5.6 – Post-incident activities, Clause 6.2 – Relationship with business continuity management).

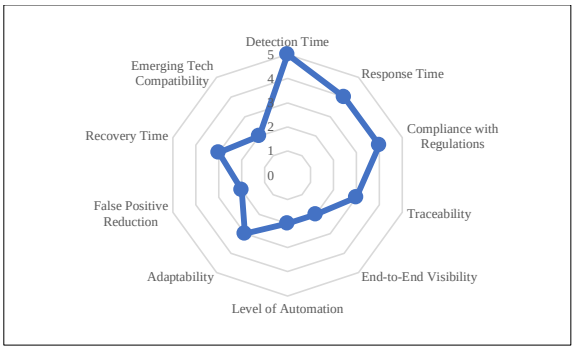

Figure 2. Radar chart for ISO 27035 CMMI evaluation scoring.

However, the ISO 27035 standard begins to show limitations in areas related to real-time performance and adaptive intelligence; such as Automation, End-to-End Visibility, False Positive Reduction and Emerging Tech Compatibility, all of which are scored at Level 2. For Automation parameter, although the standard does not place specific emphasis on the role of automation, it recognizes that automation may contribute to improving the efficiency and effectiveness of incident management activities (Clause 5.2 – Planning and preparation). And for End-to-End Visibility, while the standard promotes organization-wide adoption of IMP, it does not explicitly incorporate the concept of End-to-End Visibility within its scope (Clause 4.3 – Organizational responsibilities and preparedness). Regarding False Positive Reduction, it does not explicitly focus on reducing false positives, nevertheless it emphasizes the need to identify and manage false alarms as part of the incident assessment process (Clause 5.6 – Post-incident activities). And finally for Emerging Tech Compatibility, the standard does not specifically consider adaptation to emerging

technologies, but it underscores the necessity for IMP to be consistent with the organization's overarching information security strategy (Clause 4.2 – Alignment with information security and risk management). As sum, these lower scores highlight the need for external augmentation with modern technologies like SOAR, AI/ML analytics, or zero-trust architecture support, especially important in volatile threat environments.

In essence, ISO 27035 remains a strongly "structured-first" standard: it brings discipline, lifecycle continuity, and regulatory alignment to incident management. But to meet the expectations of modern enterprises especially in finance, defense, or critical infrastructure, organizations must supplement it with technological agility layers to fully support real-time operations, rapid containment, and autonomous response.

3.2.1.2. CMMI evaluation for NIST SP 800-61 Rev.2 (2012)

As shown in Figure 3 accordingly; NIST SP 800-61 Rev. 2 (2012) framework exhibits a clear orientation toward tactical agility and operational precision within the incident response lifecycle. The CMMI-based evaluation indicates top-tier maturity levels (Level 5 – Optimized) for both Detection Time and Response Time, which highlights NIST's effectiveness in defining clear detection protocols, structured containment stages, and expected incident durations. As for Detection Time, NIST SP 800-61 Rev.2 (2012) emphasizes rapid detection through continuous monitoring tools and centralized logging systems (Section 3.2: Detection and Analysis). And for Response Time, it defines precise incident handling timelines with stages and expected durations (Section 3.2, 3.4.4). These capabilities make it highly suitable for environments requiring fast, procedural, and accountable response execution, such as federal agencies, critical infrastructure sectors, and high-assurance networks.

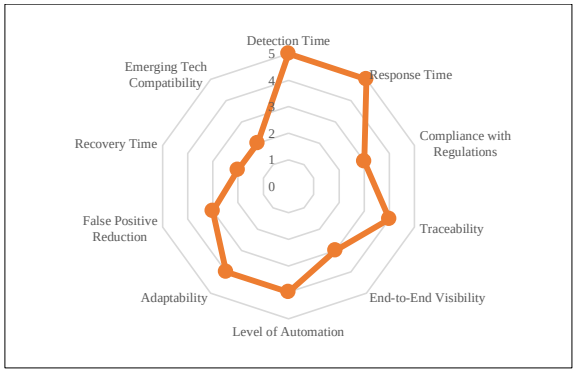

Figure 3. Radar chart for NIST SP 800-61 Rev.2 (2012) CMMI evaluation scoring.

The framework also demonstrates well-defined practices in Traceability, Adaptability, and Automation Support, all scoring at Level 4 (Quantitatively Managed). For Traceability, the framework requires detailed documentation and retention of incident-related data logs and actions (Section 3.2.5 — Incident Documentation). With regard to the Adaptability parameter, the framework contains regular updates and enabled lessons learned adaptive evolution of playbooks and procedures (Section 3.4.3 – Lessons Learned). Furthermore, for Automation, the framework encourages automation through SIEM and workflow tools but does not mandate AI-based orchestration (Section 2.3 – Coordination and Information Sharing, Section 3.2.3 – Sources of Precursors and Indicators). It is stated that these indicate a structured yet data-driven approach to documentation, response evolution, and partial automation.

However, notable limitations are present in Compliance with Regulations, Recovery Time, and Emerging Technology Compatibility, which receive Level 3. Pertaining to Compliance with Regulations, NIST SP 800-61 Rev.2 (2012) supports regulatory alignment, yet it does not explicitly enforce legal standards like GDPR or PCI DSS. For Recovery Time, the framework focuses more on containment and eradication than recovery planning. Recovery steps are referenced but not detailed (Section 3.3 – Containment, Eradication, and Recovery). And lastly for Emerging Tech Compatibility, the framework does not specifically reference IoT, edge, or AI but can be extended with complementary NIST documents. These findings emphasize that while NIST is exceptional in real-time detection and operational handling, it lacks prescriptive depth in governance, post-incident resilience, and next-gen system integrations such as AI or SOAR.

Overall, NIST SP 800-61 Rev.2 (2012) functions as an agile and actionable framework, excelling in tactical incident management but requiring strategic augmentation when deployed in regulated or technologically complex environments. It is best suited as a core incident response engine, ideally supplemented with governance-oriented frameworks and modern orchestration layers to ensure end-to-end resilience in contemporary threat landscapes.

3.2.1.3. CMMI evaluation for ITIL v4

As shown in Figure 4, the CMMI analysis of ITIL v4 illustrates its strengths in process maturity, especially in areas such as Response Time, Traceability, Adaptability, Automation, and Emerging Technology Compatibility, where it reaches Level 4 (Quantitatively Managed). For Response Time, Service Level Agreements (SLAs) and Incident Management processes are explicitly defined to measure and optimize response timelines. It is stated that regarding Traceability, all incidents are tracked from detection to closure using tools like CMDB and ITSM platforms. Moreover audit trails are maintained as part of Continual Service Improvement. Regarding Adaptability, the framework promotes adaptive service design and iterative learning through the Continual Improvement model. In the context of Automation, it explicitly encourages integration with AI and automation technologies, especially via "Digital and IT Strategy" guidance. In addition for Emerging Tech Compatibility, the framework includes "Guiding Principles" and

modular architecture enable seamless extension to cloud, AI, and edge technologies. These results reflect ITIL's core strength as a process-driven service management framework, designed to optimize workflows, enable traceability through ITSM tools (like CMDB and ticketing systems), and support modernization via integration with AI, automation, and digital transformation strategies (e.g., via the "Digital & IT Strategy" module).

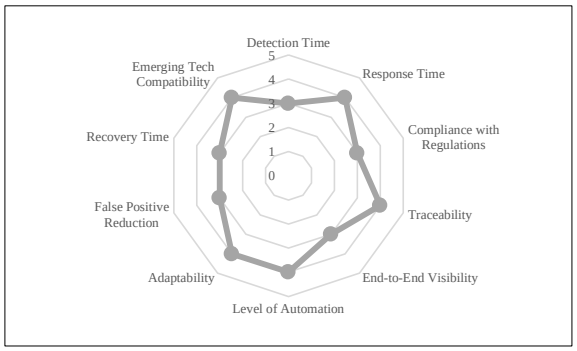

Figure 4. Radar chart for ITIL v4 CMMI evaluation scoring.

However, limitations arise in technical specificity and cybersecurity-centric implementation. Key parameters such as Detection Time, Compliance with Regulations, End-to-End Visibility, Recovery Time and False Positive Reduction remain at Level 3 (Defined) or lower and are indirectly addressed. Due to Detection Time, ITIL v4 emphasizes proactive monitoring through Event Management, but detection performance depends heavily on tool implementation rather than framework directives. With regard to Compliance with Regulations, ITIL itself is not a compliance framework but supports alignment with ISO 20000 and can be extended for compliance with GDPR, HIPAA, etc. Furthermore for End-to-End Visibility, it provides a service-centric view but lacks prescriptive guidance on visibility across complex hybrid infrastructures. It is stated in terms of Recovery Time that while recovery is supported within the Service Restoration flow, it is often reliant on other practices like Problem or Change Management.Lastly for False Positive Reduction parameter, ITIL allows tuning detection thresholds and escalation paths but lacks native methods to measure or model false positives. These scores suggest that while ITIL provides structure and cross-functional coordination, it relies heavily on external platforms (e.g., SIEM, SOAR) to fulfill operational cybersecurity demands. Moreover, regulatory alignment is possible but not embedded natively — requiring overlay with standards like ISO 20000 or GDPR-specific protocols.

In sum, ITIL v4 proves to be a strong foundational framework for orchestrating incident workflows and fostering continual improvement across IT teams. And upon comparison of other frameworks and standards, ITIL seems to be a "balanced framework" in terms of all 10 key parameters. Yet, for high-velocity, threat-focused environments, its role is best seen as a coordination layer — one that must be complemented by technical and regulatory-focused frameworks (e.g., NIST, ISO 27035) to form a full-spectrum incident response capability.

3.2.1.4. CMMI evaluation for PCI DSS

When we look at the data derived from Figure 5, CMMI-based assessment of PCI DSS reveals a standard with strong regulatory grounding but limited flexibility in several operational and technological dimensions. The standard scores high in compliance with regulations (Level 5 – Optimized) and maintains solid maturity in detection time, response time, and traceability (all rated Level 4 – Quantitatively Managed). For Compliance with Regulations, PCI DSS itself is a regulatory standard with strict compliance and auditability embedded in all controls. For Detection Time parameter, the standard mandates daily log review and anomaly detection, supporting fast incident detection (Requirement 10.6). For Response Time, it enforces a formalized incident response plan including clear responsibilities and escalation paths (Requirement 12.10). Moreover for Traceability, PCI DSS requires detailed log generation (Requirement 10) and retention for traceability and forensic investigations. These strengths stem from PCI DSS's explicit mandates in logging, incident planning, and auditability, particularly through Requirements 10 and 12.10, which enforce structured incident management practices and strict documentation protocols.

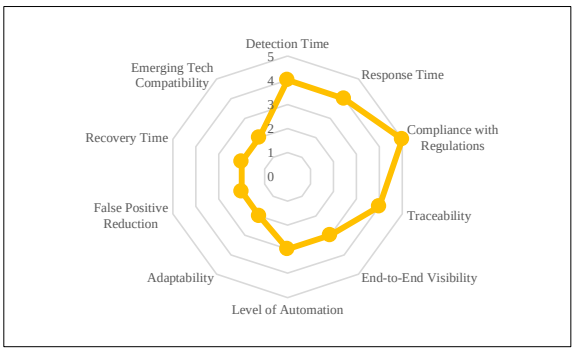

Figure 5. Radar chart for PCI-DSS CMMI evaluation scoring.

However, PCI DSS demonstrates notable constraints in adaptability, level of automation, and integration with emerging technologies, all of which are rated at Level 2. With regard to Adaptability, PCI DSS updates slowly over time and it is not highly adaptable to emerging threats without additional tools or frameworks. Furthermore for Automation, it encourages use of automated systems like SIEM but lacks prescriptive integration with modern SOAR/AI tooling. Lastly for Emerging Tech Capabilities, PCI DSS introduces some cloud compatibility, but overall support for edge, AI, or zero-trust systems remains limited. This suggests a lack of dynamic scalability and responsiveness in modern cyber threat environments. The standard's limited support for AI/ML-driven automation and SOAR tooling, as well as its slower update cycle compared to agile security standards,

reduces its alignment with cutting-edge incident management strategies. Furthermore, lower scores in false positive reduction, recovery time, and end-to-end visibility indicate that while PCI DSS is strong in containment and control, it lacks the procedural depth and cross-platform transparency required for comprehensive resilience.

In conclusion, PCI DSS offers robust compliance enforcement and well-documented incident procedures, but its lower maturity in automation, adaptability, and modern tech integration limits its viability as a standalone incident management standard in dynamic, multi-layered enterprise environments.

3.2.1.5. CMMI overall comparison of the frameworks

The radar chart shown in Figure 6 provides a comparative overview of the four incident management frameworks and standards based on 10 key parameters mapped through the CMMI capability maturity model. ISO 27035, while slightly more conservative in automation, stands out for its robustness in Detection Time, Recovery Time, and Traceability, reflecting its comprehensive procedural guidance and structured event classification approach. The chart also indicates that NIST 800-61 demonstrates the most consistent high-level maturity, especially excelling in Detection Time, Response Time, Automation Level, and Adaptability, showcasing its practical emphasis on operational readiness and structured coordination processes. ITIL v4 shows moderate and balanced maturity across most criteria but lags slightly in Detection Time and False Positive Reduction, which aligns with its service-oriented design lacking prescriptive technical detection measures. Conversely, PCI DSS, although achieving optimal levels in Regulatory Compliance and Traceability, reveals evident limitations in Adaptability, Automation, and Emerging Technology Compatibility. This reflects its narrower scope focused primarily on regulatory enforcement rather than adaptive incident response.

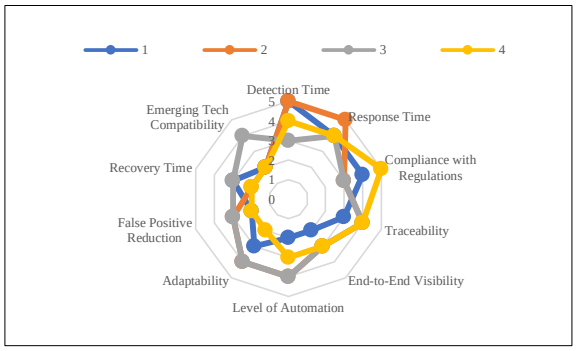

Figure 6. Overall evaluation of the frameworks and standards according to the CMMI model.

Overall, the radar chart underscores that while no framework or standard is universally superior, combining complementary strengths—such as ISO's structure, NIST's agility, ITIL's iterative processes and PCI DSS's compliance optimization—can create a more resilient and adaptive incident management strategy.

3.3. Evaluation of Frameworks and Standards Through Swot Analysis

Jayanthi (2017) states that the SWOT analysis in this phase is designed to systematically evaluate internal and external factors that influence an organization's cyber incident response capabilities. Furthermore, Humayun et al. (2020) explains that strengths identify the components within current processes and technological infrastructures that provide competitive advantage, while Weaknesses highlight critical gaps that require improvement, particularly in light of frameworks such as ISO 27035 and CMMI. Shaffi and Sidhick (2025) emphasized that opportunities reflect strategic areas for advancement such as adaptation to emerging technologies, improved regulatory compliance, and enhanced automation; whereas Cater-Steel (2007) articulates that threats encompass environmental risks such as external cyberattacks, insufficient resource allocation, and compliance challenges.

As a result, the ten key parameter identified in this study are used to assess each Incident Management framework and standard both in terms of internal competencies and external pressures. This strategic evaluation offers a holistic perspective to support robust and forward-looking decision-making processes.

The SWOT analysis of Incident Management frameworks and standards, initially established through the CMMI-based maturity assessment in earlier phases, is presented in this section.

3.3.1. SWOT analysis for ISO 27035

As we look into the SWOT analysis of ISO 27035; it reveals actually a standard rooted in global credibility and operational structure, particularly praised for its early detection enhancement and continuous improvement feedback loop.

For strengths, Thalmann et al. (2012) and Uutela (2025) state that the structured approach to incident classification and detection defined in ISO 27035 increases the potential for timely and proactive incident response. And also Agyebong and Onwubiko (2025) as well as Uutela (2025) expresses that by incorporating post-incident assessments and systematic updates, the standard contributes to the advancement of organizational information security maturity. In addition, also Agyebong and Onwubiko (2025) provided that the standard's globally accepted structure facilitates interoperability, traceability, and the development of a shared terminology among diverse systems and stakeholders.

However, some academic researchs (Bridges et al., 2023; Hatzivasilis et al., 2024) state that ISO 27035 shows technical weaknesses, due to its technology-independent design, the standard poses challenges in achieving effective integration with SOAR platforms and AI-driven security solutions. Furthermore Hatzivasilis (2024) as well as Gnasekaran et al. (2025) assert that due to the lack of technical specifications on incident correlation,

the standard offers limited guidance for minimizing false positives. In addition, according to Becker et al. (2009) the implementation of this standard may face constraints in small-scale organizations owing to the demands for significant resources and specialized expertise.

As for opportunities to stabilize and improve this standard, some academic researches (Zargar et al., 2013; Greiman, 2015) stated that the standard provides ease of auditability in adhering to legal frameworks and standards, including GDPR and NIS2 compliance requirements. Additionally; in the view of Casino et al. (2022) and Greiman (2015) integration with AI-powered threat intelligence systems can substantially enhance the speed and effectiveness of incident detection and response. And also as noted by Zargar et al. (2013) and Casino et al. (2022) the standard is designed to facilitate integration with other ISO standards (27001, 27005) as well as with contemporary technologies.

And finally according to the CMMI model integration, Scarfone et al. (2008) and AlHogail (2015) expressed that ISO 27035 processes might fall short in delivering the necessary proactive capabilities required to effectively counter advanced persistent threats (APTs). Moreover, Ying et al. (2015) outlined that the successful implementation of the standard is contingent upon factors including executive sponsorship, staff training, and organizational cultural awareness. Nevertheless, the standard presents a strong opportunity for organizations to layer modern tools on top of its structure, especially if combined with more dynamic frameworks or orchestration platforms.

3.3.2. SWOT analysis for NIST SP 800-61 Rev.2 (2012)

SWOT analysis for NIST SP 800-61 Rev. 2 (2012) highlights its distinctive strength in technical depth and tactical responsiveness.

For strengths of this framework, according to Dombora (2018) and Möller (2023) it offers detailed procedures for event detection, including network monitoring, indicators of compromise (IoCs), and log analysis frameworks. In addition, Zhong et al. (2019) and Möller (2023) states that it provides structured guidance on phases of incident handling, ensuring consistency and measurable outcomes. Also as noted by Yaseen (2022) it harmonizes well with standards like NIST SP 800-53, ISO 27001, and supports risk-based alignment strategies. This makes it particularly suitable for fast-paced operational environments such as SOCs, CERTs, and regulated sectors like energy or finance. Additionally, its strong alignment with U.S. federal cybersecurity programs (e.g., FISMA, FedRAMP) and interoperability with other NIST standards offers a robust baseline for organizations aiming for national compliance or maturity-based adoption.

Despite these advantages, based on the work of Abid et al. (2024) strategic limitations are evident such as NIST SP 800-61 Rev. 2 (2012) offers limited guidance on SOAR or AI-based automation; relies heavily on manual or tool-specific workflows. Moreover, Ali et al. (2025) claimed that it lacks detailed adaptations for cloud-native or hybrid multi-tenant environments. In addition to this, Abid et al. (2024) stated that some automation and orchestration recommendations lag behind industry evolutions in modern SOC architectures.

As for opportunities, in accordance with Chambers (2022) and Zhong et al. (2019), this framework can be extended with tools like MITRE ATT&CK or STIX/TAXII, and integrates well into enterprise SOC strategies. And with minor restructuring, the detection and triage phases can be enhanced by AI/ML models for behavior-based detection and anomaly scoring.

When it comes to talk about its shortcomings to be considered, Yaseen (2022) states that inconsistent adoption and interpretation across industries can lead to gaps in national-level cyber incident reporting standards. Furthermore without jurisdiction-specific alignment (e.g., GDPR, HIPAA), implementation might raise compliance concerns, especially in international organizations.

However, the framework remains a prime candidate for modular expansion: its clarity and modularity allow it to be integrated with AI-powered systems, regulatory overlays, and strategic coordination models to build a comprehensive cybersecurity incident response ecosystem.

3.3.3. SWOT analysis for ITIL v4

The SWOT analysis of ITIL v4 reveals a framework with strong foundations in service delivery optimization, cross-team collaboration, and continual improvement. Its modularity and scalability make it appealing to organizations aiming to integrate security within broader IT operations.

In the view of Aguiar et al. (2018) and Lopes et al. (2024); key strengths include that it emphasizes structured service value chains, aligning incident management with business continuity and service availability goals. And besides, Aguiar et al. (2018) and Freas et al. (2022) expresses that it especially focuses on iterative learning and systemic service feedback to strengthen response cycles and post-incident reviews. In addition, as noted by Narne (2023), the framework is modular and adaptable to any enterprise scale or industry; integrates easily with CMDB, ITSM platforms, and cloud-native systems.

However, according to some researches (Freas et al., 2022; Karanko, 2015) ITIL v4's primary weakness lies in its generalized nature. ITIL is a service framework, not a security-specific one; lacks deep cybersecurity threat intelligence, SIEM, or attack simulation integration guidance. And Narne (2023) highlights that while it supports AI and automation, detailed orchestration logic and tool selection remain vague or platform-dependent. Likewise, Lopes et al. (2024) added that full-scale ITIL deployments may overwhelm SMEs due to process complexity and overhead.

Despite these limitations, in the view of Narne (2023) ITIL v4 presents key opportunities: With growing AI-based incident routing and ticketing, ITIL v4 can

integrate with intelligent systems to automate triage and escalation effectively. Furthermore, ITIL's continual improvement loop and service lifecycle aligns well with ISO 20000 and ISO 27001-based compliance systems.

Talking about threats, Karanko (2015) claims that its implementation often depends on ITSM suites (like ServiceNow, BMC), which may restrict flexibility and increase vendor lock-in. Also too much focus on service delivery can create blind spots in rapidly evolving threat landscapes without dedicated cybersecurity intelligence integration.

As a sum; its interoperability with modern automation platforms, cloud-native toolchains, and enterprise-wide governance models allows it to serve as a unifying layer that bridges technical execution with business continuity. When appropriately combined with tactical frameworks, ITIL v4 offers valuable resilience through operational consistency, process harmonization, and continuous service improvement.

3.3.4. SWOT analysis for PCI DSS

The SWOT analysis of PCI DSS highlights its distinct strength as a regulation-centric standard, primarily designed to enforce compliance within organizations that process, transmit, or store payment card data.

As proposed by Williams and Adamson (2022) and Black Hat (2023), one of its most prominent strengths is that PCI DSS mandates detailed control mechanisms, log reviews, and incident response plans, ensuring strict compliance for financial institutions. Furthermore, according to Black Hat (2023) and Chippagiri and Ramesh (2025) section 10 mandates daily log review and centralized log retention, supporting forensic investigations and traceability. Gunnam and Kilaru (2021) states that another strength lies in its universally accepted in the payment ecosystem; as compliance is a legal and contractual necessity in many regions. PCI DSS also promotes cross-functional coordination during incidents by mandating predefined roles, communication plans, and escalation paths. Its globally accepted and auditor-friendly structure makes it especially powerful in compliance-heavy sectors such as finance, retail, and e-commerce.

Despite these regulatory advantages, PCI DSS presents several operational limitations. Karri and Jangam (2021) expresses that highly prescriptive structure makes it hard to integrate novel cybersecurity tools like adaptive AI or SOAR solutions. Moreover, according to Jangampeta and Khambam (2020) and Shabina et al. (2024), regarding this standard, emphasis is on detection and containment; lacks detailed guidance on organizational resilience and business continuity planning. And as noted by Chippagiri and Ramesh (2025) despite improvements in v4.0, PCI DSS has limitations in fully supporting edge computing, serverless systems, and modern identity fabric models. It is often considered prescriptive and rigid, leaving limited room for customization or scalability beyond payment environments. Furthermore, PCI DSS offers minimal technical guidance on automation, AI orchestration, or advanced threat analytics, meaning that organizations must rely heavily on external SOAR/SIEM platforms to meet dynamic incident response needs. Another notable weakness is its reactive stance because PCI DSS mandates the existence of an incident response plan but does not fully emphasize continuous learning, simulation, or post-incident adaptation as seen in standards like ISO 27035.

However, Karri and Jangam (2021) states that with proper mapping, PCI DSS controls can align with CSPM, CNAPP, and cloud-native compliance strategies. And also it can benefit from external CTI feeds and anomaly detection enhancements if layered on top of SIEM systems.

When it comes to threats assumed for this standard, some academic researches (Shabina et al, 2024; Chippagiri and Ramesh, 2025) highlights that as PCI DSS is an Audit-Driven, Not Security-Driven standard, organizations may treat compliance as checkbox exercise, ignoring real-time threat detection and proactive defense measures. Furthermore, increasing scope complexity by expanding the cardholder data environment (CDE) in hybrid/multi-cloud systems can complicate scoping, auditing, and tool interoperability.

To summarize, structure of PCI DSS offers clear integration opportunities with modern security controls, and its legal enforceability provides a strong baseline for layered security strategies, especially when embedded within a hybrid compliance framework.

3.3.5. Overall evaluation of SWOT analysis

In the overall comparison shown in Table 7, "F" denotes parameters that are Fully Addressed (parameter is robustly covered in framework or standard docs & real-world use) in the framework or standard, "P" indicates Partial Coverage (parameter addressed with limitations or needs enhancement), "W" signifies Weak or Minimal Support (parameter is addressed narrowly or through external tools), and "N" refers to parameters that are Not Supported (parameter is not addressed in scope or design of the framework) in scope or design.

As described and shown in Table 7, the final matrix, which consolidates the performance of four prominent incident management frameworks and standards across ten rigorously selected key parameters, provides a holistic visual synthesis of each framework's and standard's core strengths and limitations. NIST 800-61 emerges as the most balanced framework, exhibiting strong support in critical operational areas such as Detection Time, Response Time, Traceability, Adaptability, and End-to-End Visibility. Its consistently high alignment with modern incident response needs confirms NIST's maturity and extensibility, making it a reliable baseline for complex, threat-facing environments.

ISO 27035, while also demonstrating high operational maturity in foundational areas like Detection Time and Response Time, shows notable weaknesses in Automation Level and only moderate performance in

areas related to technological innovation and system integration, highlighting its more traditional and process-oriented structure.

ITIL v4, with its service management roots, performs strongly in Adaptability and User-Centric Design, yet its incident-specific capabilities are diluted due to the framework's broader IT operations focus. As such, its moderate to weak performance across traceability, recovery time, and technical automation suggests that ITIL may require augmentation to meet the responsiveness demands of security-focused environments.

Table 7. Comparison matrix regarding SWOT analysis of the frameworks and standards

Key Parameter	ISO 27035	NIST SP 800-61 Rev.2	ITIL v4	PCI DSS
Detection Time	F	F	P	F
Response Time	F	F	P	P
Compliance with Regulations	F	P	P	F
Traceability	P	F	P	F
End-to-End visibility	P	F	P	W
Automation Level	N	P	P	N
Adaptability	F	F	F	N
False Positive Reduction	P	P	P	F
Recovery Time	P	F	P	P
Emerging Tech Compatibility	P	F	F	N

PCI DSS, by contrast, demonstrates robustness in Compliance and Reporting but scores weakest overall in Adaptability, Automation, and New Technology Compatibility. Its rule-based, compliance-driven architecture makes it highly suitable for audit-heavy sectors like finance but ill-equipped for agile or AI-enhanced incident response needs.

Overall, Table 7 confirms that no single framework or standard fully addresses all dimensions of modern incident management, underscoring the value of adopting a hybrid, context-aware strategy. The matrix also reveals that forward-looking capabilities — particularly Automation, Technological Compatibility, and Adaptability — remain under-addressed in traditionally rigid frameworks. This visual tool offers immediate strategic value to decision-makers, guiding them toward framework selection or integration paths aligned with their sectoral priorities and security maturity levels.

4. Discussion

Conducting this study required not only rigorous methodological precision but also extensive field engagement. The initial and arguably most effort-intensive phase was identifying and reaching out to cybersecurity professionals with relevant experience in incident response frameworks. Gathering their participation for the Likert and AHP-based surveys demanded professional outreach, validation of respondent profiles, and clear articulation of research objectives. This step, while time-consuming, ensured that the dataset would be grounded in real-world experience across sectors such as finance, transportation, manufacturing, health and defense. Nguyen et al. (2024) also reflects a growing consensus in the academic community that human-in-the-loop expert elicitation is essential for modeling multi-criteria cybersecurity assessments.

The next phase involved defining a broad set of 20 preliminary parameters, derived from the intersection of existing literature, regulatory standards, and operational practices. This stage was particularly important for setting a comprehensive baseline before narrowing the scope. Parameters such as Detection Time, Traceability, Automation Level, and SOAR Integration emerged naturally from the overlap between modern threat environments and classical incident response life cycles, supporting the idea of Paul et al. (2021) that frameworks or standards must evolve to integrate both strategic governance and tactical technology.

However, during the analysis of Likert, CV, Z-scores and standard deviation values, six preliminary parameters with conceptually strong foundations were eliminated due to inconsistencies and low consensus among cybersecurity professionals. Specifically, "Threat Intelligence Action", "Reporting Capabilities", "User Friendly Interface", "Training and Awareness Support", "SOAR Integration" and "Compatibility with AI" although conceptually strong and aligned with modern cybersecurity trends, demonstrated standard deviation values exceeding 2.0, signaling low inter-rater consensus. This outcome highlights a critical tension in cybersecurity evaluation. While some features are forward-looking and theoretically essential, they are not yet uniformly valued or implemented across sectors. The decision to exclude them from the final evaluation aligns with best practices in MCDM methodologies (Damaševičius et al., 2019; Singh, 2025) where parameters lacking reliability are commonly downweighted or removed to preserve model stability and result clarity. However, it is worth noting that these excluded parameters may still hold strategic significance in future iterations of framework or standard modernization, particularly as automation and intelligence-led response become more mainstream. Additionally, Singh (2025) states that this finding underscores that not all technically significant parameters are viewed as universally important in operational settings. And finally, the exclusion of these parameters highlighted a known challenge in cybersecurity MCDM studies — the misalignment between theoretical importance and practitioner

prioritization.

After applying a combined weight scoring model (involving AHP pairwise comparisons, normalized Likert ratings, CV scores, Z-score normalization and standard deviation filters), the study finalized 10 key parameters. These included Detection Time, Response Time, Compliance with Regulations, and Compatibility with Emerging Technologies, among others. However, it is crucial to note that some non-selected parameters may still carry contextual significance — for example, Training Support or Cost of Implementation might be pivotal in small to mid-size enterprises or sectors with specific budgetary constraints. The methodology used here prioritized consensus-backed universality over contextual sensitivity.

Following the parameter definition, each of the four frameworks and standards were evaluated using a multilayered methodology including CMMI scoring, radar charts, SWOT analysis, and a final matrix. These tools offered distinct lenses of evaluation:

- CMMI highlighted maturity gaps in automation and learning across the frameworks.
- Radar charts offered criteria-specific strengths and weaknesses at a glance.
- SWOT analysis provided strategic insights into adaptability, integration potential, and sectoral constraints.
- The final matrix enabled a side-by-side comparison across the 10 core parameters, allowing decision-makers to identify framework suitability under specific organizational needs.

This multi-visual, multi-method approach provided by Damaševičius et al. (2019) aligns with recent literature on strategic cybersecurity assessments that call for layered evaluation models combining quantitative scoring with visual analytics.

Despite these strengths, the study also faced limitations. First, the participant sample — though composed of experienced professionals — was limited in size and not stratified by region or sector, potentially impacting generalizability. Second, while the Likert-AHP hybrid weighting ensured robustness, it did not include sensitivity analysis, which could have tested the model's resilience to minor scoring fluctuations. Finally, while frameworks and standards were assessed against unified criteria, their scope and intention differ: PCI DSS is regulation-first, ITIL v4 is service-first, NIST SP 800-61 Rev.2 (2012) is threat-focused — this asymmetry of design inevitably limits perfect comparability.

Overall, this study provides a high-confidence decision support structure that merges expert insight with advanced analytical stability. It emphasizes that cybersecurity incident management is not merely about compliance or documentation but about intelligent integration, adaptive planning, and human-informed prioritization in an ever-evolving threat landscape.

5. Conclusion

In conclusion, this study set out to establish a rigorous, expert-driven methodology for evaluating widely adopted cybersecurity incident management frameworks and standards using a structured and quantitative multi-criteria approach. Through the integration of Likert, CV score, Z-Score, AHP pairwise comparison, and standard deviation filtering, a set of 10 key evaluation parameters was distilled from an initial list of 20 preliminary parameters. These parameters reflect the core operational, compliance-related, and technological dimensions of incident management, and were applied consistently across four globally recognized frameworks and standards.

The application of a multi-layered evaluation architecture — including CMMI-based maturity scoring, radar charts and SWOT analyses — enabled a comprehensive cross-framework and standard comparison. While NIST 800-61 demonstrated balanced strengths in adaptability, visibility, and maturity, ISO 27035 scored consistently on foundational operational parameters but showed limited alignment with automation and emerging technology. ITIL v4 offered strong adaptability but showed gaps in traceability and integration, whereas PCI DSS excelled in compliance but lacked agility and technological innovation. These outcomes reinforce the necessity of aligning framework adoption decisions with organizational context, rather than adopting a one-size-fits-all approach.

Beyond its technical findings, the study contributes to both academia and industry by offering a scalable, replicable, and practitioner-informed evaluation model. Its methodological transparency makes it suitable for application across different sectors, particularly in finance, transportation, defense, manufacturing and health, where incident response capabilities must balance regulation, resilience, and innovation. The academic takeaway is clear: incident response must evolve into a data-informed, automation-compatible, and maturity-assessed discipline. Overall, the proposed methodology not only strengthens evaluation capability but also lays the groundwork for dynamic framework integration, hybrid architectures, and continuous adaptation—an essential evolution in the face of an ever-shifting cybersecurity threat landscape.

6. Future Work And Strategic Insights

The methodology and findings presented in this study lay a robust foundation for practical, data-informed, and adaptable applications across diverse organizations and sectors. With cybersecurity threats evolving in both complexity and velocity, the insights generated here can be immediately leveraged by CISOs, risk managers, and compliance leaders to make informed decisions about framework adoption, enhancement, and integration. The multi-phase evaluation process — beginning with expert-driven parameter selection, followed by AHP and Likert-

based prioritization, and concluded with CMMI and SWOT analyses — offers a scalable and modular blueprint for conducting incident management evaluations that are sensitive to both strategic goals and operational realities.

For future researchers, this study opens several avenues for expansion and refinement. One important direction is the inclusion of longitudinal or sector-specific studies, where the 10 key parameters may be tested in dynamic or high-frequency threat environments (e.g., SOCs, MDR services). For instance, sectors such as finance and e-commerce, which operate under stringent regulatory mandates, may favor the adoption of PCI DSS in conjunction with NIST SP 800-61 Rev. 2 (2012) to ensure both compliance and structured incident response, whereas critical infrastructure domains may derive greater value from ISO/IEC 27035 for its procedural depth and from ITIL v4 for its emphasis on cross-functional integration and service coordination. Additionally, a sensitivity analysis of AHP scores and Likert inputs could provide further insight into the robustness of parameter weighting across expert populations with differing roles or regional focuses. Future studies may also consider integrating Delphi techniques or machine learning–based parameter extraction to reduce expert bias and improve generalizability. The extension of this methodology to additional frameworks (e.g., COBIT, MITRE ATT&CK, NIST CSF) and even proprietary hybrid models could provide a richer comparative dataset.

One of the most critical and practical recommendations to emerge from this research is the creation of hybrid frameworks. No single existing framework fully addresses the needs of modern cyber risk — for instance, NIST SP 800-61 Rev. 2 (2012)'s operational robustness could be paired with ISO 27035's formal procedural clarity, while ITIL's service-centric orientation can complement the control-heavy precision of PCI DSS. Organizations, especially those in high-risk sectors, should consider designing their own hybrid response playbooks by aligning their maturity level (via CMMI) with the 10 key parameters highlighted in this research. These playbooks can then be tested and continuously improved via table-top exercises and red-team assessments.

Sector-specific implications are particularly vital. In the energy and manufacturing sectors, where OT (Operational Technology) systems coexist with IT infrastructure, incident frameworks and standards must ensure low-latency detection, traceability, and fault isolation, supported by automation. In the finance sector, regulatory compliance (e.g., PSD2, GDPR) must be tightly coupled with real-time anomaly detection and SOAR orchestration. In defense and aerospace, where zero-trust architectures and classified incident handling are paramount, the adoption of frameworks like NIST SP 800-61 Rev. 2 (2012) augmented with AI-driven threat intelligence fusion is essential. The future of sector-oriented incident response lies in tailoring a unified operational doctrine from modular frameworks, optimized for the environment in which it is deployed.

Looking even further ahead, innovation in incident management will likely come from intelligent, self-evolving systems capable of dynamically adapting to threat patterns and feedback loops. This includes AI-enhanced incident scoring, predictive behavioral baselining, and automated countermeasure recommendation engines. For instance, SOAR platforms such as Palo Alto Cortex XSOAR or Splunk Phantom can be integrated to automate containment workflows and orchestrate cross-platform playbooks, further improving response times.Moreover, the development of visual risk observability layers, integrated directly with cloud-native infrastructures and SOC dashboards, will redefine how incidents are understood and escalated. The concept of Framework-as-Code may soon emerge, where incident response logic is version-controlled, testable, and deployable just like software.

In conclusion, the road forward in incident management is both strategic and technological. This study provides a robust baseline to advance from static framework selection toward adaptive, integrated, and intelligent incident response ecosystems. Future work must embrace cross-disciplinary fusion — blending governance, automation, behavioral science, and AI — to craft the next generation of resilient cybersecurity operations. Those who invest in this path will not only respond to incidents more effectively but will lead the future of cyber defense innovation. Ultimately, the organizations that embrace this multi-layered, intelligence-driven approach will not only strengthen their security posture but will also shape the future landscape of adaptive, resilient cybersecurity operations.

Author Contributions

The percentages of the authors' contributions are presented below. All authors reviewed and approved the final version of the manuscript.

	H.C.A.	B.C.
C	50	50
D	50	50
S		100
DCP	80	20
DAI	50	50
L	50	50
W	60	40
CR	10	90
SR	50	50
PM	20	80

C=Concept, D= design, S= supervision, DCP= data collection and/or processing, DAI= data analysis and/or interpretation, L= literature search, W= writing, CR= critical review, SR= submission and revision, PM= project management.

Conflict of Interest

The authors declared that there is no conflict of interest.

Ethical Consideration

Ethics committee approval was not required for this study because of there was no study on animals or humans.

References

Abid, M., Nanda, P., & Mohanty, M. (2024). Incident Response Adaptive Metrics Framework. *17th International Conference on Security Information Networking (SIN)*, Sydney, Australia, 1–8.

Aguiar, J., Pereira, R., Vasconcelos, J. B., & Bianchi, I. (2018). An overlapless incident management maturity model for multi-framework assessment (ITIL, COBIT, CMMI-SVC). *Interdisciplinary Journal of Information, Knowledge, and Management, 13*, 137–163.

Agutter, C. (2020). *ITIL Foundation Essentials ITIL 4 Edition: The ultimate revision guide*. IT Governance Publishing Ltd.

Agyepong, E., & Onwubiko, C. (2025). An Exemplar Incident Response Plan for Security Operations Centre Analysts. In M. G. Jaatun et al. (Eds.), *Proceedings of the International Conference on Cybersecurity Situational Awareness, Social Media and Cyber Science Proceedings of Complex*. Springer, Singapore.

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology, 71*(8), 939–953.

Ak, M. F., & Gul, M. (2019). AHP–TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis. *Complex & Intelligent Systems, 5*(2), 113–126.

Alevizos, L. (2025). Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts. *International Journal of Information Technology, 17*, 767–781.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567–575.

Ali, G., Shah, S., & ElAffendi, M. (2025). Enhancing cybersecurity incident response: AI-driven optimization for strengthened advanced persistent threat detection. *Results in Engineering, 25*, 104078.

Almashaqbeh, I., & Almomani, A. (2023). AI4SOAR: A security intelligence tool for automated incident response. *IEEE Access, 11*, 52361–52372.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering, 1*, 213–222.

Bhole, G. P., & Deshmukh, T. (2018). Multi-criteria decision making (MCDM) methods and its applications. *International Journal of Research in Applied Sciences and Engineering Technology, 6*(5), 899–915.

Bin Ibrahim, I., Abdul, S., Khan, S. M., Sattar, S. A., & Safi, M. (2023). *AI for cyber security: Automated incident response systems*. (Kaynak türü ve yayıncı eksik olduğundan rapor/kitap olarak formatlanmıştır).

Black Hat. (2023). *Selected whitepapers and presentations from Black Hat USA 2023*. Black Hat Conference. https://blackhat.com/html/archives.html

Bridges, R. A., Liska, J. H., Khambam, S. K. R., Allen, M., & Sotomayor, P. (2023). Testing SOAR tools in use. *Computers & Security, 129*, 103201. https://doi.org/10.1016/j.cose.2023.103201

Caralli, J., Knight, M., Allen, J., & White, T. (2010). *CERT® Resilience Management Model: A maturity model for managing operational resilience* (pp. 8–21). Addison-Wesley Professional.

Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access, 10*, 25464–25493.

Cater-Steel, A. (2007). Integration of Service Management with CMMI® and SPICE. *Proceedings of the 5th Annual SEPG Australia Conference*.

Chambers, M. D. (2022). *Exploring the standards cybersecurity practitioners need to comply with multinational cybersecurity requirements* [Doktora tezi, Colorado Technical University].

Chippagiri, S., & Ramesh, A. (2025). PCI DSS: A Critical Analysis of Implementation, Effectiveness, and Legislative Impact in Payment Card Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11*(1), 1258–1266.

Chirra, D. R. (2023). Towards an AI-Driven Automated Cybersecurity Incident Response System. *International Journal of Advanced Engineering Technology and Innovation, 1*(1), 429–451.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61 Rev. 1). National Institute of Standards and Technology.

CMMI Product Team. (2006). *CMMI® for development, Version 1.2: Preface*. Software Engineering Institute, Carnegie-Mellon University.

Damaševičius, R., Toldinas, J., Venčkauskas, A., Grigaliūnas, Š., Morkevičius, N., & Jukavičius, V. (2019). Visual analytics for cyber security domain: State-of-the-art and challenges. In *Communications in Computer and Information Science: Information Software Technology* (Vol. 1078). Springer, Cham.

Dombora, S. (2018). Integrated incident management model for data privacy and information security. *Book of Proceedings*, 319.

Donne, K. E., Hughes, D. L., Williams, M. D., & Davies, G. H. (2021). The underlying complexities impacting accelerator decision making—a combined methodological analysis. *IEEE Transactions on Engineering Management, 70*(1), 312–327.

Dykstra, J., Met, J., Backert, N., Mattie, R., & Hough, D. (2022). Action Bias and the Two Most Dangerous Words in Cybersecurity Incident Response: An Argument for More Measured Incident Response. *IEEE Security & Privacy, 20*(3), 102–106.

Eberhard, K. (2023). The effects of visualization on judgment and decision-making: a systematic literature review. *Management Review Quarterly, 73*(1), 167–214.

Freas, R. L., Adair, H. F., & Hammad, E. (2022). An Engineering Process Framework for Cybersecurity Incident Response Assessment. *IEEE Conference on Dependable and Secure Computing (DSC)*, Edinburgh, United Kingdom, 1–8.

Garae, J., & Ko, R. K. (2017). Visualization and data provenance trends in decision support for cybersecurity. In *Data Analytics and Decision Support for Cybersecurity: Trends, methodologies and applications* (pp. 243–270). Springer International Publishing. (Editör bilgisi eksiktir).

Gnanasekaran, V., Fatima, U., & Glas, M. (2025). A Model-Based Framework for Developing Security-Safety Incident Response Plans. *International Journal of Information Security, 24*, 229.

Gnanasekaran, V., Neudert, R., Heegaard, P. E., & Pernul, G. (2025). A Role Taxonomy in Security-Safety Incident Response. In *Availability, Reliability, and Security: Lecture*

Notes in Computer Science (Vol. 15995). Springer, Cham.

Greiman, V. (2015). Cybersecurity and Global Governance. *Journal of Information Warfare, 14*(4), 1–14.

Grobauer, B., & Schreck, T. (2010). Towards incident handling in the cloud: challenges and approaches. *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop (CCSW '10)* (pp. 77–86). ACM.

Gunnam, V., & Kilaru, N. B. (2021). Securing PCI Data: Cloud Security Best Practices And Innovations. *Natural Volatiles & Essential Oils, 8*(4), 317–328. (Sayfa aralığı tahmini olarak eklenmiştir).

Hatzivasilis, G., Lakka, E., & Athanatos, M. (2024). Swarm-intelligence for the modern ICT ecosystems. *International Journal of Information Security, 23*, 2951–2975.

Humayun, M., Niazi, M., & Jhanjhi, N. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering, 45*, 3171–3189.

International Organization for Standardization. (2016). *ISO/IEC 27035-1:2016: Information technology—Security techniques—Information security incident management—Part 1: Principles and process*.

International Organization for Standardization. (2019). *ISO 22301:2019: Security and resilience—Business continuity management systems—Requirements*.

Islam, S., Javeed, D., Saeed, M. S., Kumar, P., Jolfaei, A., & Islam, A. N. (2024). Generative AI and cognitive computing-driven intrusion detection system in industrial CPS. *Cognitive Computation, 16*(5), 2611–2625.

Jangampeta, S., & Khambam, S. K. R. (2020). Impact of SIEM on compliance: Achieving security and adherence simultaneously. *Turkish Journal of Computer and Mathematics Education, 11*(01), 1080–1083.

Jäntti, M. (2009). Defining Requirements for an Incident Management System: A Case Study. *Proceedings of the 4th International Conference on Systems*, Gosier, France, 184–189.

Jayanthi, M. K. (2017). Strategic Planning for Information Security -DID Mechanism to befriend the Cyber Criminals to assure Cyber Freedom. *2nd International Conference on Anti-Cyber Crimes (ICACC)*, Abha, Saudi Arabia, 142–147.

Karanko, K. (2015). *Applying the information technology infrastructure library in a multi-vendor environment*. (Kaynak türü ve yayıncı eksik olduğundan rapor olarak formatlanmıştır).

Karri, N., & Jangam, S. K. (2021). Security and Compliance Monitoring. *International Journal of Emerging Trends in Computer Science and Information Technology, 2*(2), 73–82.

Killcrece, G., Kossakowski, K. P., Ruefle, R., & Zajicek, M. (2003). *Organizational models for computer security incident response teams (CSIRTs)* (SEI Hand book HB-001-15213). Software Engineering Institute, Carnegie-Mellon University.

Lopes, S., Leite, P., Carvalho, S., & Teixeira, P. (2024). Using ITIL as part of the NIST Cybersecurity Framework. *12th International Symposium on Digital Forensics and Security (ISDFS)*, San Antonio, TX, USA, 1–6.

Lourens, M., Dabral, A. P., Gangodkar, D., Rathour, N., Tida, C. N., & Chadha, A. (2022). Integration of AI with the Cybersecurity: A detailed Systematic review with the practical issues and challenges. *5th International Conference on Contemporary Computing and Informatics (IC3I)*, Uttar Pradesh, India, 1290–1295.

McLaughlin, K. (2023). Interweaving the strands of AI and SOAR onto the cybersecurity mesh: A deep dive into the cybersecurity mesh and its role in modern digital defense strategies. *EDPACS: The EDP Audit, Control, and Security Newsletter, 68*(5), 27–33.

Mızrak, F. (2023). Integrating Cybersecurity Risk Management Into Strategic Management: A Comprehensive Literature Review. *Research Journal of Business and Management, 10*(3), 98–108.

Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., de Sousa Júnior, R. T., & Nunes, R. R. (2021). Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology. *IEEE Access, 9*, 129605–129618.

Möller, D. P. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In *Guide to Cybersecurity and Digital Transformation: Trends, methods, technologies, applications, and best practices* (pp. 231–271). Springer, Cham.

Munteanu, V. I., Edmonds, A., Bohnert, T. M., & Fortis, T. F. (2014). Cloud Incident Management, Challenges, Research Directions, and Architectural Approach. *IEEE/ACM International Conference on Utility and Cloud Computing (UCC)*, London, UK, 786–791.

Narne, H. (2023). Revolutionizing IT Operations: AI-Driven Service Management for Efficiency and Scalability. *International Journal of Research and Analytical Reviews, 10*(3).

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems, 143*.

Nguyen, P. H., Nguyen, L. A. T., Pham, H. A. T., Nguyen, T. H. T., & Vu, T. G. (2024). Assessing cybersecurity risks and prioritizing top strategies In Vietnam's finance and banking system using strategic decision-making models-based neutrosophic sets and Z number. *Heliyon, 10*(19).

Onwubiko, C., & Ouazzane, K. (2022). SOTER: A Playbook for Cybersecurity Incident Management. *IEEE Transactions on Engineering Management, 69*(6), 3771–3791.

Paul, A., Shukla, N., Paul, S. K., & Trianni, A. (2021). Sustainable supply chain management and multi-criteria decision-making methods: A systematic review. *Sustainability, 13*(13), 7104.

Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R. G., & Bonders, M. (2025). Try to esCAPE from cybersecurity incidents! A technology-enhanced educational approach. *Technology, Knowledge and Learning, 30*(3), 1577–1606.

Rabii, A., Assoul, S., Ouazzani, T. K., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information and Computer Security, 28*(4), 627–644.

Reuben-Owoh, B., & Haig, E. (2025). A systematic review of voluntary cybersecurity standards and frameworks. *International Journal of Information Security, 24*(5), 206.

Saaty, R. W. (1987). The analytic hierarchy process—what it is and how it is used. *Mathematical Modelling, 9*(3-5), 161–176.

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences, 1*(1), 83–98.

Sahoo, S. K., & Goswami, S. S. (2023). A comprehensive review of multiple criteria decision-making (MCDM) methods: advancements, applications, and future directions. *Decision Making Advances, 1*(1), 25–48.

Scarfone, K. A., Grance, T., & Masone, K. (2008). *Computer security incident handling guide* (NIST Special Publication 800-61 Rev. 1). National Institute of Standards and Technology.

Shabina, A. R. F., Jahankhani, H., Siddiqi, Y., & Hassan, B. (2024). Ensuring Securing PII Data in the AWS Cloud: A Comprehensive Guide to PCI DSS Compliance. In *Cybersecurity and Artificial Intelligence: Advanced Science and Technology Security Applications*. Springer, Cham.

Shaffi, N. S. M., & Sidhick, N. J. N. (2025). Real-time incident

reporting and intelligence framework: Data architecture strategies for secure and compliant decision support. *World Journal of Advanced Research and Reviews, 26*(3), 110–118.

Singh, H. (2025). *The importance of cybersecurity frameworks and constant audits for identifying gaps, meeting regulatory and compliance standards*. (Kaynak ve yayıncı eksik olduğundan rapor olarak formatlanmıştır).

Thalmann, S., Bachlechner, D., Demetz, L., & Maier, R. (2012). Challenges in cross-organizational security management. *45th Hawaii IEEE International Conference on System Sciences* (pp. 5480–5489).

Trifonov, R., Manolov, S., Tsochev, G., & Pavlova, G. (2019). Automation of cyber security incident handling through artificial intelligence methods. *WSEAS Transactions on Computers, 18*(2), 274–280.

Uutela, K. (2025). *Cybersecurity standard-based model for IT/OT converged environments* [Doktora tezi, University of Turku].

Vaidya, O. S., & Kumar, S. (2006). Analytic hierarchy process: An overview of applications. *European Journal of Operational Research, 169*(1), 1–29.

Williams, B., & Adamson, J. (2022). *PCI compliance: Understand and implement effective PCI data security standard compliance*. CRC Press.

Yaseen, A. (2022). Accelerating the SOC: Achieve greater efficiency with AI-driven automation. *International Journal of Responsible Artificial Intelligence, 12*(1), 1–19.

Ying, H., Maglaras, L. A., Janicke, H., & Jones, K. (2015). An Industrial Control Systems incident response decision framework. *IEEE Conference on Communications and Network Security (CNS)*, Florence, Italy, 761–762.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046–2069.

Zhong, C., Yen, J., Liu, P., & Erbacher, R. F. (2019). Learning From Experts' Experience: Toward Automated Cyber Security Data Triage. *IEEE Systems Journal, 13*(1), 603–614.