IJECBE (2025), **3**, **4**, 770–785
Received (28 November 2025) / Revised (27 December 2025)
Accepted (30 December 2025) / Published (30 December 2025)
https://doi.org/10.62146/ijecbe.v3i4.201
https://ijecbe.ui.ac.id
ISSN 3026-5258

International Journal of Electrical, Computer and Biomedical Engineering

RESEARCH ARTICLE

KRAFF: An Integrated Digital Forensics and Cyber Incident Response Framework Based on International Standards (NIST, ISO/IEC, and ITIL 4) as a Practical and Measurable Adoption Guide

Andi Faridz Fakhriza* and Kalamullah Ramli

Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia
*Corresponding author. Email: andi.faridz@ui.ac.id

Abstract

Digital forensics and cyber incident response represent crucial capabilities for IT-based organizations to manage cyber incidents effectively. However, organizations often face a fundamental constraint characterized by digital forensic processes that are ad hoc, unstructured, and detached from incident management. This situation compromises the integrity of digital evidence, prolongs service recovery times, and stems from the absence of a practical framework capable of integrating forensic procedures into incident management. This paper presents a comprehensive and integrated framework for digital forensics and cyber incident response, named KRAFF, specifically designed to address these deficiencies. The framework is designed through a multi-standard synthesis that aligns technical guidelines from NIST and the ISO/IEC 27000 series with established service management principles from ITIL 4. A distinct feature of KRAFF is the strategic placement of pre-investigation acquisition prior to containment, effectively bridging the operational gap between digital evidence integrity and rapid service recovery. Structurally, the proposed framework comprises four main phases, supported by 19 detailed activities, 16 defined roles and responsibilities, 18 requisite report artifacts, and 18 key performance metrics. Validation was conducted using the expert judgement method, involving a panel of nine senior practitioners and academics with an average of 10 years of experience in cybersecurity governance and operations. A quantitative assessment using the Free-Marginal Multirater Kappa yielded a value of 0.9316, indicating "almost perfect agreement" regarding the framework's relevance and applicability. Consequently, KRAFF is positioned for widespread adoption within enterprise-scale organizations, serving as a practical guide

for establishing mature, measurable, and integrated capabilities in digital forensics and cyber incident response. By providing a structured roadmap for process standardization and performance measurement, this framework enables management to transition from reactive responses to a proactive posture, effectively elevating the organization's cyber defense maturity.

Keywords: Digital Forensics, Cyber Incident Response, NIST, ISO/IEC 27000 Series, ITIL 4, Expert Judgement, Free-Marginal Multirater Kappa

1. Introduction

Digital transformation has become a driving force in the operations of modern organizations. This intensifying reliance on information technology infrastructure, data, and networks presents significant opportunities for innovation while increasing exposure to cyber threats. Cybersecurity incidents, such as malware infections, ransomware attacks, and data breaches, have evolved from hypothetical threats to daily operational challenges that can cause significant financial losses, reputational damage, and service disruptions. Globally, the average cost of a data breach incident is estimated at USD 4.44 million in 2025 [1]. Meanwhile, the global cost of cybercrime is projected to reach USD 10.5 trillion by 2025 [2].

These high losses indicate a critical gap between the speed of threat evolution and organizational response capabilities. The root of the problem lies not only in the number of attacks but also in the complexity and inefficiency of internal processes for handling these incidents. Furthermore, while the cost of a data breach indicates that AI and automation significantly reduce breach lifecycles, reliance on technology alone is insufficient without robust process governance. The emergence of Shadow AI, unauthorized use of generative AI by employees, introduces opaque data leakage vectors that traditional incident response plans fail to address. To mitigate this, organizations need a framework that integrates forensic rigor with operational agility.

To address these challenges, organizations rely on two primary converging disciplines, including incident response and digital forensics [3]. Historically, these two disciplines have different priorities. Incident Response focuses on operational speed and recovery. Driven by business needs, the primary goal is availability, such as restoring normal service as quickly as possible to minimize impact and loss [4]. In contrast, Digital Forensics focuses on precision investigative methodologies. Its primary goal is integrity, such as ensuring that digital evidence remains unchanged so that it is legally admissible and accountable for in-depth analysis [5].

This fundamental conflict of priorities between the "need for rapid recovery" and the "need for evidence integrity" creates a critical operational gap. Failure to respond effectively has immediate consequences. Hasty incident response actions, such as shutting down servers or restoring systems from backups, carry a high risk of damaging or destroying volatile digital evidence (such as data in RAM) [6]. As a result, forensic investigations often fail to fully identify attack vectors and root causes. When root causes are not addressed, underlying vulnerabilities remain, ultimately leading to similar incidents in the future.

While various international standards and best practices exist, such as frameworks from NIST, ISO/IEC, and ITIL 4, a review of the literature indicates that their implementation in organizations still reveals significant gaps. Several studies have shown that many proposed frameworks are conceptual in nature and lack practical guidance [7] [8] [9] [10]. However, harmonizing existing standards presents a challenge due to inherent conflicts: ISO/IEC 27043 prioritizes evidence integrity (freezing the scene), whereas ITIL 4 and NIST SP 800-61r3 prioritize service availability (restoring the service). Implementing these standards in silos often leads to operational friction, where rapid restoration efforts inadvertently destroy legally admissible evidence. Furthermore, research often focuses on emerging technology domains, such as the Internet of Things (IoT) [11] [12] and cryptocurrency [13], making them less universally applicable to general enterprise IT environments.

This research aims to address this gap by designing a structured, adaptive, and integrated digital forensics process framework. Its contribution is a thorough synthesis of cybersecurity standards, such as NIST and ISO/IEC 27000 series, with IT service management practices, such as ITIL 4. This synthesis is essential to ensure that digital forensics processes not only meet technical requirements but are also seamlessly integrated into the service lifecycle and organizational governance, in accordance with service management practices. Thus, the proposed framework will fundamentally elevate an organization's incident response capabilities from merely reactive and ad-hoc to a mature, scalable, and sustainable program.

2. Literature Review

In the domain of digital forensics and cyber incident response, there are several standards and best practices formulated by various organizations. These organizations have the authority to publish globally recognized references. This section will discuss some of the standards commonly used as references in the application of digital forensics and cyber incident response.

2.1 NIST Framework

NIST is a non-regulatory agency under the United States Department of Commerce that develops standards and guidelines to advance technology and measurement. In the field of information security, NIST's contributions are significant and widely adopted globally. Several NIST publications that serve as pillars in the information security discipline, particularly related to digital forensics and incident response, include NIST CSF 2.0 [14], NIST SP 800-61 [15], and NIST SP 800-86 [16].

The primary focus of NIST CSF 2.0 is to provide a high-level framework that helps organizations of all sizes, sectors, and maturity levels manage cybersecurity risks. Its primary contribution is to present a cybersecurity taxonomy that is widely understood by various stakeholders, from technical to executive levels. This framework serves as a common language for communicating cybersecurity posture and serves as a foundation for an organization's risk management strategy. The core components of CSF 2.0 are organized into six core functions such as Govern, Identify, Protect, Detect, Respond, and Recover.

The primary focus of NIST SP 800-61 is on integrating incident response recommendations and considerations into overall cybersecurity risk management activities. This publication, which officially replaces the previous version, now serves as the Community Profile for NIST CSF 2.0. Its primary contribution lies in reforming the incident response model, transforming it from an isolated cycle to an integrated and continuous process aligned with the six functions of CSF 2.0. The model divides activities into three main levels: Preparation, encompassing the Govern, Identify, and Protect functions; Incident Response, which is the core of incident handling and encompasses the Detect, Respond, and Recover functions; and Lessons Learned, encompassing the Improvement of the Identify function.

The primary focus of NIST SP 800-86 is to provide practical guidance on the integration and implementation of forensic techniques in the incident response process. Its primary contribution is its role as a how-to guide for practitioners, covering methodologies, procedures, and technical considerations for a variety of digital data sources. This standard outlines a methodical and structured forensic process consisting of four basic phases: collection, examination, analysis, and reporting. These processes are designed to transform raw digital data into legally and organizationally accountable evidence.

2.2 ISO/IEC 27000 Series

ISO/IEC is an international non-governmental organization that develops and publishes standards for various industry sectors. In the context of information security, the ISO/IEC 27000 series of standards is the most relevant reference. This series provides a framework for an Information Security Management System (ISMS), including standards specifically relevant to digital forensics and cyber incident response. These standards include ISO/IEC 27001 [17], ISO/IEC 27035 [18] [19], ISO/IEC 27037 [20], ISO/IEC 27042 [21], and ISO/IEC 27043 [22].

ISO/IEC 27001 focuses on the requirements for establishing, implementing, maintaining, and continually improving an ISMS. This standard is used by organizations to obtain ISMS certification, with a primary focus on a risk-management-based approach. This standard is intended for all types of organizations, regardless of their type, size, or nature, and is used by both internal and external parties to assess compliance with information security requirements. Fundamentally, this standard serves as a framework that requires organizations to have a mature Digital Forensics and Incident Response (DFIR) capability. The link to DFIR can be outlined through guidance for several key controls, such as A.5.24 Information security incident management planning and preparation, A.5.25 Assessment and decision on information security events, A.5.26 Response to information security incidents, A.5.27 Learning from information security incidents, and A.5.28 Collection of evidence.

ISO/IEC 27035 and ISO/IEC 27037 are two international standards in the ISO/IEC 27000 series that focus on information security, specifically security incidents. ISO/IEC 27035, also known as Information Security Incident Management, provides guide lines and processes for effectively managing and responding to information security incidents within an organization. The primary objective of this standard is to ensure organizations are able to plan and prepare for incident responses; detect, report, and

assess information security incidents; respond to and resolve these incidents; and learn from past incidents to improve future defenses. ISO/IEC 27037, on the other hand, specifically provides guidance on proper procedures for the identification, collection, acquisition, and preservation of digital evidence, which is particularly relevant in the field of digital forensics. The primary scope of this standard includes identifying devices or systems that could potentially hold evidence; forensic data collection while ensuring it has not been altered or damaged; and preserving evidence in an unaltered state for a specified period, including the Chain of Custody.

ISO/IEC 27042 and ISO/IEC 27043 are standards that continue the digital forensics workflow begun in ISO 27037. ISO/IEC 27042's primary focus is on the analysis phase of the digital forensics process. While ISO/IEC 27037 focuses on how to securely retrieve evidence, ISO/IEC 27042 focuses on how to validly analyze that evidence in a laboratory. This standard covers activities such as recovering deleted data, reconstructing the timeline of events, validating forensic software, and properly documenting analysis findings. ISO/IEC 27043 provides a harmonized framework and process model for the overall incident investigation. Its focus is on providing a high-level overview of the entire investigation process, from pre-incident preparation to investigation closure.

2.3 ITIL 4

ITIL 4 is the latest version of ITIL (Information Technology Infrastructure Library), a framework that provides best practice guidance for IT Service Management (ITSM) and has been widely adopted worldwide for over 30 years. It is designed to equip organizations to meet the challenges of modern service management by integrating new ways of working, such as Lean, Agile, and DevOps, into proven ITSM practices [23]. The standard focuses on the Service Value System (SVS), which describes how the various components and activities of an organization work together to create value through IT-enabled services [24] [25] [26]. The five main components of the SVS include Guiding Principles, Governance, Service Value Chain (SVC), ITIL Practices, and Continual Improvement.

2.4 Previous Studies

Several studies have been conducted on the development of digital forensics and cyber incident response. A.R. Hakim et al. identified a fundamental challenge in current digital forensics investigations: the lack of a framework that specifically recognizes the unique characteristics of data breach incidents [7]. To address this issue, this paper proposes a new digital forensic investigation framework, the primary contribution of which is a phase-based data breach breakdown, consisting of four main phases (infiltration, propagation, aggregation, exfiltration), a 5WH analysis depth, and three evidence categorizations (host, network device, security device) visualized in a Chain of Artifacts (CoA).

S. Rudrakar et al. proposed an incident response and digital forensics management model specifically designed for Internet of Things (Ag-IoT)-based agricultural environments [11]. This model presents a structured workflow that encompasses the entire incident management lifecycle in four main phases: Pre-Incident, encompassing

technical and managerial aspects; Incident Response, which involves attack detection and stakeholder notification; post-incident, which combines Incident Response with Phase I Digital Forensics; and Phase II Digital Forensics, which serves as the in-depth investigation phase.

E. Munke and P. M. W. Musuva propose an innovative solution in the form of a Digital Forensics as a Service (DFaaS) implementation based on two industry best practice standards: ISO/IEC 27037 and NIST SP 800-101 [8]. The researchers implemented a DFaaS prototype using Python and open-source components. This prototype automates key steps in forensic procedures, such as imaging, hash calculation, and integrity verification, significantly reducing manual effort and accelerating the investigation process.

3. Proposed Framework

The design of this Digital Forensics and Cyber Incident Response Framework is based on a synthesis methodology of various globally recognized standards and practices. This framework synthesis process is designed to address the fundamental weaknesses of ad-hoc and isolated incident response, with the aim of transforming it into a mature, scalable, and comprehensive capability. This synthesis methodology does not adopt a single standard but rather combines and aligns the best elements of three pillars of global standards, namely NIST, ISO/IEC, and ITIL 4. The synthesis of NIST, ISO/IEC, and ITIL 4 was conducted using a comparative semantic mapping approach. Clauses from each standard were decomposed and mapped to a unified incident lifecycle. Conflicts were resolved by prioritizing 'Legal Defensibility' (ISO 27043) for evidence-handling activities and 'Service Restoration' (ITIL 4) for operational recovery steps. The result of this design is a systematic process model divided into four main phases, namely [PE] Preparation, [ID] Identification and Diagnosis, [IR] Investigation and Resolution, and [PP] Reporting and Continual Improvement, as shown in Figure 1.

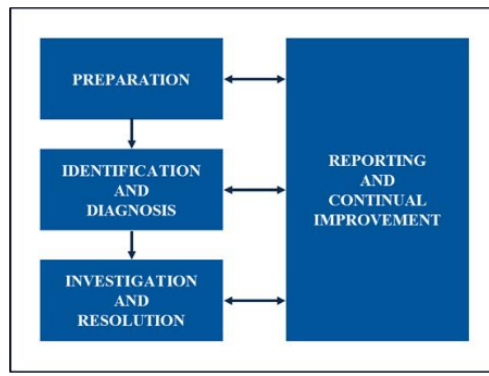

Figure 1. Digital Forensics and Cyber Incident Response Framework

The [PE] Preparation phase synthesizes the proactive functions of NIST CSF 2.0 (Govern, Identify, and Protect), the Plan and Prepare phase of ISO/IEC 27035, and

the Readiness principles of ISO/IEC 27043. The [ID] Identification and Diagnosis phase adopts the Detect function of NIST CSF 2.0 and combines two formal phases of ISO/IEC 27035, Detection and Reporting and Assessment and Decision, with the Initialization and Acquisition Process Classes of ISO/IEC 27043. This phase also detects for Shadow AI, the unauthorized use of AI tools like ChatGPT, Midjourney, or unapproved API integrations. Unlike traditional workflows, this activity anticipates threats like 'Shadow AI' data leaks, where volatile evidence in RAM must be captured before system shutdowns occur. The core [IR] Investigation and Resolution phase implements the Respond and Recover functions of NIST CSF 2.0 and the Responses phase of ISO/IEC 27035. The technical processes within it are synthesized from the NIST SP 800-86 guide, the Examination and Analysis phase, and the Investigative Process Classes from ISO/IEC 27043. Finally, the [PP] Reporting and Continual Improvement phase closes the cycle by synthesizing the Lessons Learned concepts from NIST SP 800-61 and Lessons Learned from ISO/IEC 27035, which are then operationally integrated with the Problem Management and Continual Improvement practices from ITIL 4.

During the synthesis process, conflicts between the availability-focused nature of ITIL 4 and the integrity-focused nature of ISO/IEC 27043 were resolved using a phased-prioritization approach. Specifically, the framework prioritizes forensic integrity in the early [ID] phase by mandating evidence acquisition prior to any aggressive containment or recovery actions dictated by standard Incident Management protocols. This ensures that the requirement for legal admissibility does not compromise the subsequent need for rapid service restoration.

3.1 Detailed Activities

Defining granular activity details is a crucial step in translating the four key phases into operational and implementable guidance. The goal is to provide a prescriptive and actionable workflow that addresses one of the framework's primary objectives, providing practical adoption guidance. The detailed activity definition is achieved through a synthesis methodology of globally recognized standards and practices, namely NIST, ISO/IEC, ITIL4, and other technical standards, into 19 specific activities summarized in Table 1.

The selection of the 19 activities was driven by a gap analysis of the synthesized standards. Activities were selected based on two primary criteria: their criticality in bridging the operational silos between security teams and IT operations, and their role in fulfilling 'Chain of Custody' requirements Redundant administrative steps were removed to streamline the workflow, while specific bridge activities, such as 'Pre-investigation Acquisition' [ID.05] and 'Service Validation' [IR.04], were explicitly retained to address the identified disconnect between restoration and preservation.

Table 1. Mapping Activities to Synthesized Standards

Activity Name	Synthesized Standards
[PE.01] Policy Determination	● NIST CSF 2.0 (Govern Function) ● ISO/IEC 27035 ● ITIL 4 (Information Security Management)
[PE.02] Asset Identification & Forensic Risk Assessment	● NIST CSF 2.0 (Identify Function) ● ISO/IEC 27043 (Readiness Principles) ● ITIL 4 (Risk Management, Service Configuration Management)
[PE.03] Implementation of Technology & Infrastructure Readiness	● NIST CSF 2.0 (Protect Function) ● NIST SP 800-86 (Device Validation Principles) ● ITIL 4 (Change Enablement)
[PE.04] Team Building & Competency Development	● ISO/IEC 27035 (Team Formation Guide) ● NIST CSF 2.0 (Protect Function) ● ITIL 4 (Workforce and Talent Management)
[PE.05] Incident Response Plan Design & Testing	● NIST CSF 2.0 (Subcategory ID.IM-P2) ● ISO/IEC 27035-1 (Incident Management Model) ● ITIL 4 (Service Continuity Management) ● SWGDE (Collection & Examination Procedure Guide)
[ID.01] Security Event Detection & Incident Reporting	● NIST CSF 2.0 (Continuous Monitoring Function) ● ISO/IEC 27043 (Initialization Process Classes) ● ISO/IEC 27035 (Detection and Reporting Phase) ● ITIL 4 (Monitoring and Event Management, Service Desk)
[ID.02] Incident Triage and Validation	● NIST CSF 2.0 (Domain Detect & Respond) ● ISO/IEC 27035 (Assessment and Decision Phase) ● ISO/IEC 27043 (Initial Response Process) ● ITIL 4 (Incident Management, Information Security Management)
[ID.03] Initial Investigation and Impact Analysis	● NIST CSF 2.0 (Impact Analysis & Estimation) ● ISO/IEC 27043 (Initialization & Acquisition Process Classes) ● ITIL 4 (Incident Management, Problem Management, Service Configuration Management)
[ID.04] Formal Escalation and Response Team Activation	● NIST SP 800-61 ● ITIL 4 (Incident Management, Relationship Management)
[ID.05] Acquisition and Preservation of Digital Evidence	● NIST CSF 2.0 (Integrity Guide) ● ISO/IEC 27043 (Acquisition Process Classes: Collection, Acquisition, Preservation) ● ITIL 4 (Service Configuration Management, Information Security Management) ● SWGDE (Implement Principle)
[IR.01] Digital Forensic Analysis	● NIST SP 800-86 (Examination & Analysis Phase) ● ISO/IEC 27043 (Investigative Process Classes) ● ITIL 4 (Problem Management) ● MITRE ATT&CK (TTP Grouping)
[IR.02] Incident Containment	● NIST CSF 2.0 (Respond Function) ● NIST SP 800-61 ● ISO/IEC 27035 (Response Phase)

	• ISO/IEC 27002 (Control A.5.26) • ITIL 4 (Change Enablement, Incident Management)
[IR.03] Eradication of Threats	• NIST SP 800-61 • ISO/IEC 27035 (Response Phase) • ITIL 4 (Incident Management, Information Security Management)
[IR.04] System Recovery and Validation	• NIST CSF 2.0 (Recover Function) • ISO/IEC 27035 (Response – Recovery Phase) • ITIL 4 (Service Validation and Testing, Service Continuity Management)
[IR.05] Incident Investigation & Resolution Documentation	• NIST SP 800-86 (Reporting Phase) • ISO/IEC 27043 (Concurrent Processes) • ISO/IEC 27035 (Input for Lessons Learned) • ITIL 4 (Knowledge Management)
[PP.01] Post-Cyber Incident Analysis	• NIST SP 800-61 (Lessons Learned Activity) • ISO/IEC 27035 (Lessons Learned Phase) • ISO/IEC 27002 (Control A.5.27) • ITIL 4 (Information Security Management, Continuous Improvement)
[PP.02] Root Cause Analysis	• ITIL 4 (Problem Management, Knowledge Management)
[PP.03] Continuous Improvement	• NIST CSF 2.0 (Function Improvement) • ISO/IEC 27035 (Follow-up on Lessons Learned) • ITIL 4 (Continuous Improvement)
[PP.04] Management Reporting and Metrics	• NIST CSF 2.0 (Governance Function) • ISO/IEC 27001 (Management Review Clause) • ITIL 4 (Governance, Continuous Improvement)

3.2 Defined Roles and Responsibilities

Defining roles and responsibilities is crucial to transforming this conceptual framework into an operational capability. Because digital forensics and cyber incident response are not the exclusive domain of a single team, but rather a complex, cross-functional effort, justifying role definitions is crucial. The goal is to eliminate ambiguity and establish clear accountability.

The methodology used is a RACI (Responsible, Accountable, Consulted, Informed) matrix, which maps 16 identified stakeholder roles to 19 specific sub-activities within the framework. This definition is granular to reflect operational realities. The Accountable role is clearly and singularly assigned to each process. The Responsible role, as the primary implementer, is assigned to technical teams. The Consulted role is allocated to units with specific expertise, such as the Risk Management Team for organizational risk alignment. The Informed role is reserved for executive leadership, who require strategic situational awareness. This comprehensive structure ensures that each activity has a clear owner and defined escalation and consultation paths.

It is important to note that the 16 proposed roles represent logical functions. In resource-constrained environments, one individual may assume multiple roles (e.g., Incident Handler and Evidence Custodian), provided that Segregation of Duties (SoD) is maintained. Furthermore, in the Preparation Phase [PE], the framework explicitly incorporates the Legal Counsel role within the RACI matrix. This inclusion addresses the critical need for advisory on data privacy regulations (e.g., GDPR, PDP Law) during the initial drafting of forensic policies.

3.3 Report or Document Artifacts

The development of these artifacts is a crucial step, transforming the conceptual framework into a guide that can be implemented and audited. Within this framework, each defined document serves as an output of an activity, which can also serve as input to subsequent activities. Formalizing these artifacts is essential to ensure a traceable and auditable workflow, eliminate ambiguity in handovers between teams, and establish concrete evidence of the implementation of each process.

For each of the 18 identified documents, the framework not only defines its name but also establishes its creation frequency (e.g., "Per Incident" or "Annually") and "Minimum Content". This "Minimum Content" specification serves as a clear definition of done for each activity and ensures the quality and completeness of the output.

3.4 Key Performance Metrics

Defining Key Metrics is an essential component of this framework, which is designed to meet several strategic and operational objectives. This is to measure effectiveness and performance and transform Digital Forensics and Cyber Incident Response capabilities from ad-hoc to mature and scalable programs. These metrics serve as the primary tool for communicating the performance, outcomes, and value of the Digital Forensics and Cyber Incident Response program to strategic leadership and stakeholders.

The development of these 18 key metrics is based on the four-phase process model structure of this framework. Each metric is explicitly mapped to its relevant phase to ensure holistic measurement across the incident lifecycle. To differentiate reporting audiences and measurement objectives, metrics are classified into two primary types: Strategic and Operational. Strategic metrics focus on measuring long-term impact and business value (e.g., "Cyber Risk Reduction"), while Operational metrics focus on day-to-day process efficiency (e.g., "Mean Time to Detection" or MTTD). Each metric is precisely defined by including a description, a specific measurement method (including the metric calculation formula), a measurement frequency (e.g., Per Incident), and an expected trend (Increasing or Decreasing).

4. Discussion

4.1 Analysis of the Proposed Framework

The design of the "Digital Forensics and Cyber Incident Response" framework aims to provide a process model that bridges the fundamental gap between two disciplines that often have conflicting priorities. A literature review confirms that Cyber Incident Response focuses on speed of service restoration (prioritizing Availability), while Digital Forensics focuses on precise investigative methodologies to maintain evidence integrity (prioritizing Integrity). This framework is designed for IT organizations that require a hybrid model that systematically integrates both needs.

In designing the framework, this research did not adopt a single standard but rather conducted a comprehensive multi-standard synthesis. NIST standards (CSF 2.0, SP 800-61, and SP 800-86) were synthesized to provide strategic architecture (six functions), a modern incident response lifecycle, and forensic technical guidance (Collection, Examination, Analysis, and Reporting). On the other hand, the ISO/IEC

27001 series standards (specifically ISO 27035 and ISO 27043) are integrated to provide a formal, auditable, and prescriptive management process structure, particularly for investigation and evidence handling flows.

A key innovation of this framework is its in-depth integration with ITIL 4, which explicitly maps Digital Forensics and Cyber Incident Response workflows with existing ITSM practices. This integration ensures that Digital Forensics and Cyber Incident Response capabilities are not isolated but directly connected to operational processes such as Incident Management, Problem Management, and Change Enablement. Additionally, technical guidance from SWGDE and MITRE ATT & CK was adopted to ensure that evidence acquisition procedures meet stringent legal integrity standards, strengthen analysis, and support advanced threat hunting.

The result of this research is a comprehensive framework consisting of four phases, 19 detailed activities, a mapping of 16 stakeholder roles (RACI Matrix), 18 report or document artifacts, and 18 key performance metrics (KPIs). This detailed list of activities, artifacts, and metrics is intended to meet the research objective of providing practical adoption guidance for IT organizations. The implementation recommendations from the activities in this framework can be adopted to build mature Digital Forensics and Cyber Incident Response capabilities.

4.2 Expert Judgement Validation

Framework validation serves as a verification and testing process to ensure that the proposed model is not only theoretically sound but also has relevance and applicability in the real world. Given the limitations of this study, which did not include direct implementation, the expert judgment method was chosen as the most effective and efficient validation approach. Expert judgment is a well-established qualitative technique for evaluating research artifacts, in this case, a framework, by leveraging the knowledge, experience, and intuition of experts in the field [27].

This expert judgment method involved nine experts selected through purposive sampling based on specific inclusion criteria: a minimum of 5 years of professional experience in cybersecurity or IT governance, possession of relevant professional certifications (e.g., CISSP, CISM, CHFI), and active roles in sectors requiring high compliance (government, banking, and telecommunications). The panel had an average of 10 years of experience, ensuring a balanced perspective between strategic governance and technical operations.

The experts were sent a questionnaire link within a period of less than one month and provided assessments, proposed improvements, suggestions, and input on the proposed framework. Then, the experts were asked to provide their assessments by selecting one of two responses: "agree" or "disagree" for each of the 26 areas of the framework assessment. This feedback was to ensure that the proposed framework met the aspects of Completeness (covering all essential matters), Clarity (easy to understand), Implementation (realistic to implement in the context of the organization in general), and Suitability (meeting international standards and best practices). As a result, the experts provided suggestions for improvements (4 items), suggestions and input (49 items) for analysis and follow-up improvements to the 26 assessment areas of this framework as shown in Table 2.

Table 2. Summary of Framework Validation Results

Validation Results	Total
"All experts have the same response." This shows that the nine experts had the same response, namely that they all agreed on the items being assessed.	22
"Eight experts have the same response." This indicates that eight experts provided the same response, agreeing with the item being assessed. Meanwhile, one expert provided a different response from the other nine, disagreeing with the item being assessed.	4

4.3 Free-Marginal Multirater Kappa Assessment

In this study, quantitative data analysis was conducted using the Free-Marginal Multirater Kappa approach to assess the content validity of the developed framework and the level of agreement of the experts. Free-Marginal Multirater Kappa is a measurement method that can be used to measure the level of agreement from several sources without knowledge of the distribution of categories at the start of the measurement [28]. This measurement is used to address the paradoxical Kappa value phenomenon, which is a high level of agreement but a low Kappa value. Free Marginal Multirater Kappa uses free marginals so it is not affected by changes in the distribution of validation results from experts and can be used for reliability studies. This study employed Randolph's Free-Marginal Multirater Kappa rather than Fleiss' Kappa. This choice was deliberate to avoid the 'prevalence paradox' common in agreement studies where the distribution of ratings is skewed toward the high end (e.g., most experts agreeing that an item is 'Relevant'). Randolph's metric provides a more robust measure of agreement when raters are not forced to assign a fixed number of cases to each category.

Based on the results of the expert validation, *the level of agreement* on the recommendations for implementing the framework will be measured by calculating the *Kappa value*. The validation process has a total of 26 items assessed (N=26) by 9 experts (n=9) and 2 types of ratings (k=2). Kappa value can be determined by calculating *the Proportion of Observed Agreement* (P_o) and the Proportion of Expected Agreement (P_e). The value P_o indicates the observed agreement value between experts based on the condition that the experts provide the same assessment, regardless of whether the existing agreement was made by chance or not. The value P_o can be calculated using the following formula.

$$P_o = \frac{1}{N \cdot n(n-1)} \left(\sum_{i=1}^{N} \sum_{j=1}^{k} n_{ij}^2 - N \cdot n \right) \tag{1}$$

Meanwhile, the value P_e is used to calculate the likelihood of agreement, where experts can freely provide their assessments. The value P_e can be calculated using the following formula.

$$P_e = \frac{1}{k} \tag{2}$$

Based on the calculations using the formula above, the values obtained are P_o is 0.9658 and P_e is 0.5. Both calculations can be used to measure *the level of agreement* between experts by calculating the *Kappa* value as follows.

$$(K) = \frac{P_o - P_e}{1 - P_e} \tag{3}$$

Based on the calculations that have been carried out using formula number (3), the results of *the level of agreement* of the experts are shown by the *Kappa value* (k) = 0.9316. Referring to the interpretation of Brennan and Prediger's research, this value is acceptable because it is above 0.7 [29]. Referring to the interpretation of Landis & Koch's research, this value is in the range of 0.81 to 1, thus falling into the almost perfect agreement category [30].

4.4 Comparison Evaluation with Previous Studies

The framework's added value is quantitatively demonstrated through the high level of expert consensus, yielding a Free-Marginal Multirater Kappa score of 0.9316. This 'Almost Perfect Agreement' indicates a strong expert validation that proposed framework offers significant process improvements over siloed approaches. Furthermore, the following is a feature comparison between the proposed framework and previous studies analyzed in the literature review. Based on Table 3, a further analysis was carried out on the evaluated frameworks using six key contribution aspects that have been identified. Generally, Table 3 highlights that KRAFF introduces critical integration points, such as early forensic triage, which are absent in standalone implementations of NIST or ISO standards. Role Definition measures the clarity of the framework in defining implementers. Metric Definition assesses the availability of quantitative metrics. ITSM Integration evaluates the degree of the framework's integration with IT service management processes. Domain Agnostic measures the universality of the framework's applicability (whether for general or highly specialized corporate IT). Reactive Process Focus reviews the depth of the framework's detail regarding reactive processes (such as triage, analysis, and response). Finally, Adoption Guidance assesses the nature of the guidance provided, i.e., whether it is practical and operational or merely conceptual.

Table 3. Comparison Evaluation with Previous Studies

Research Title	Role Definition	Definition of Metrics	ITSM Integration	Domain Agnostic	Reactive Process Focus	Adoption Guide
A Novel Digital Forensic Framework for Data Breach Investigation	No	No	No (Less Dynamic)	Yes	No	No (Conceptual)
Digital forensics and incident response management model for IoT based agriculture	No	No	No	No (IoT Specific)	Yes	No

Research Title	Role Definition	Definition of Metrics	ITSM Integration	Domain Agnostic	Reactive Process Focus	Adoption Guide
Digital Forensics as a Service Implementation – A Scalable Solution for Cyber Incident Response	No	No	No	Yes	Architect -tour Focus)	No
Holistic digital forensic readiness framework for IoT-enabled organizations	No	No	No	No (IoT Specific)	No (Focus on Readiness)	No
Illicit Cryptocurrency Investigation Digital Forensic Framework: Integrating Off-Chain and On-Chain Analysis for Two Types of Crime	No	No	No	No (Crypto Specific)	Yes (Specia lized)	No
K-FFRaaS – A Generic Model for Financial Forensic Readiness as a Service in Korea	No	No	No	No (Regulatio Specific)	No (Focus on Readiness)	No (Less Universal)
Next Generation Digital Forensic Investigation Model (NGDFIM) – Enhanced, Time Reducing, and Comprehensive Framework	No	No	No	Yes)	No (Sequen tial)	No (Concep tual)
Proposed Framework	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

5. Conclusion and Future Works

This research has successfully designed a comprehensive and systematic Digital Forensics and Cyber Incident Response framework. This framework directly addresses the primary problem statement: addressing the ad-hoc and isolated nature of forensic processes by formally integrating them into the incident management lifecycle.

This successful integration was achieved through a comprehensive multi-standard synthesis, which bridged the priority gap between the forensic discipline (prioritizing evidence integrity, aligned with ISO/IEC) and the incident response discipline (prioritizing service availability, aligned with NIST and ITIL 4). This study has met all specific objectives by producing a practical and measurable adoption guide for organizations. The main results of this study cover four detailed implementation components: A process model consisting of 4 phases and 19 activities; Definition of roles and responsibilities for 16 stakeholders through the RACI Matrix; A total of 18 standardized report or document artifacts equipped with "Minimum Content"; A total of 18 strategic and operational Key Performance Metrics (KPIs) to measure program effectiveness.

The proposed framework has been validated quantitatively and qualitatively through expert judgment. The results of the quantitative analysis using Free-Marginal Multirater Kappa obtained a κ value of 0.9316, indicating an almost perfect agreement level among nine experts. This confirms that the designed framework has met the aspects of completeness, clarity, implementation, and conformity with global standards.

While the proposed Key Performance Indicators (KPIs) have been validated for relevance and clarity by the expert panel with a high Kappa score, this study acknowledges the need for further empirical testing. Future research should focus on the longitudinal implementation of these metrics in diverse organizational environments to assess their practicality and to establish baselines for process efficiency. Additionally, research will explore the integration of the framework with Security Orchestration, Automation, and Response (SOAR) platforms, investigating how the framework's structured workflows can be translated into automated playbooks to further reduce Mean Time to Respond (MTTR).

References

[1] IBM. *Cost of a Data Breach Report*. 2025.

[2] SentinelOne. *Key Cyber Security Statistics for 2025*. Online. July 2025. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/.

[3] Fortinet. *What is DFIR?* Online. URL: https://www.fortinet.com/br/resources/cyberglossary/dfir (visited on 09/15/2025).

[4] Palo Alto Networks. *What is Digital Forensics and Incident Response (DFIR)?* Online. URL: https://www.paloaltonetworks.com/cyberpedia/digital-forensics-and-incident-response (visited on 09/15/2025).

[5] IBM. *What is Digital Forensics and Incident Response (DFIR)?* Online. URL: https://www.ibm.com/think/topics/dfir (visited on 09/15/2025).

[6] Brian Carrier. *File system forensic analysis*. Addison-Wesley Professional, 2005.

[7] Arif Rahman Hakim et al. "A novel digital forensic framework for data breach investigation". In: *IEEE Access* 11 (2023), pp. 42644–42659.

[8] E. Munke and P. M. W. Musuva. "Digital Forensics as a Service Implementation: A Scalable Solution for Cyber Incident Response". In: *IST-Africa 2024 Conference Proceedings*. 2024.

[9] S. J. Lee and G. B. Kim. "K-FFRaaS: A Generic Model for Financial Forensic Readiness as a Service in Korea". In: *IEEE Access* 9 (2021), pp. 130094–130110.

[10] A. A. Thakar, K. Kumar, and B. Patel. "Next Generation Digital Forensic Investigation Model (NGDFIM)". In: *Journal of Physics: Conference Series* 1767.1 (2021), p. 012054.

[11] S. Rudrakar, P. Rughani, and L. Sadineni. "Digital forensics and incident response management model for IoT based agriculture". In: *Scientific Reports* 15.1 (2025), p. 17797.

[12] V. R. Kebande et al. "Holistic digital forensic readiness framework for IoT-enabled organizations". In: *Forensic Science International: Reports* 2 (2020), p. 100117.

[13] O. Regina, K. Ramli, and A. H. Amarullah. "Illicit Cryptocurrency Investigation Digital Forensic Framework". In: *International Journal of Electrical, Computer, and Biomedical Engineering* 3.2 (2025), pp. 411–432.

[14] National Institute of Standards and Technology. *NIST Cybersecurity Framework Version 2.0*. USA, 2024.

[15] P. Cichonski et al. *NIST SP 800-61: Computer Security Incident Handling Guide*. USA, 2012.

[16] Incident Handling Guide. *Techniques into Incident Response*.

[17] International Organization for Standardization. *ISO/IEC 27001:2022 Information Security Management Systems*. 2022.

[18] International Organization for Standardization. *ISO/IEC 27035-1: Information Security Incident Management*. 2016.

[19] International Organization for Standardization. *ISO/IEC 27035-2: Guidelines to Plan and Prepare for Incident Response*. 2016.

[20] International Organization for Standardization. *ISO/IEC 27037: Guidelines for Digital Evidence*. 2012.

[21] International Organization for Standardization. *ISO/IEC 27042: Analysis and Interpretation of Digital Evidence*. 2015.

[22] International Organization for Standardization. *ISO/IEC 27043: Incident Investigation Principles*. 2015.

[23] AXELOS. *ITIL Foundation: ITIL 4 Edition*. London: The Stationery Office, 2019.

[24] AXELOS. *ITIL 4 Practice Guide: Incident Management*. London: AXELOS, 2020.

[25] AXELOS. *ITIL 4 Practice Guide: Information Security Management*. London: AXELOS, 2020.

[26] AXELOS. *ITIL 4 Practice Guide: Problem Management*. London: AXELOS, 2020.

[27] V. Braun and V. Clarke. "Using thematic analysis in psychology". In: *Qualitative Research in Psychology* 3.2 (2006), pp. 77–101.

[28] J. J. Randolph. "Free-Marginal Multirater Kappa". In: *Joensuu Learning and Instruction Symposium*. 2005.

[29] M. B. Miles, A. M. Huberman, and J. Saldana. *Qualitative Data Analysis: A Methods Sourcebook*. SAGE Publications, 2024.

[30] J. R. Landis and G. G. Koch. "An Application of Hierarchical Kappa-type Statistics". In: *Biometrics* 33.2 (1977), pp. 363–374.