

Developing a Delphi Validated Instrument for Assessing Digital Forensics Readiness Based on COBIT 2019

Tri Rochmadi^{1,2}, Abdul Fadli³, Imam Riadi⁴

¹Department of Informatics Universitas Ahmad Dahlan, Indonesia

²Department of Information System, Universitas Alma Ata, Indonesia

³Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia

⁴Department of Information System, Universitas Ahmad Dahlan, Indonesia

Article Info

Article history:

Received Jun 30, 2025

Revised Oct 23, 2025

Accepted Nov 18, 2025

Keywords:

Digital Forensic Readiness

COBIT 2019

Delphi Method

IT Governance

ABSTRACT

The increasing complexity of cyber threats has reinforced the need for robust digital forensic readiness in higher education institutions. However, existing frameworks often lack integration between forensic capabilities and IT governance practices. **Objective:** This study aims to develop and validate a new instrument to assess digital forensic readiness based on the COBIT 2019 framework. **Methods:** A three-round Delphi process was conducted with seven digital forensics and IT governance experts to develop and validate a new instrument comprising forty proposed indicators across six domains. **Results:** The instrument achieved full context, with I-CVI values increasing from 0.60 to 0.99 and IQR values reaching ≤ 1.00 across all items. **Implications:** The validated instrument integrates governance and forensic principles, providing a standardized tool for institutional self-assessment and policy development, while contributing methodologically through the use of a structured Delphi validation process.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Tri Rochmadi,

Department of Informatics,

Universitas Ahmad Dahlan,

Jl. Ringroad Selatan, Kragilan, Tamanan, Banguntapan, Bantul, Daerah Istimewa Yogyakarta 55191

Email: 2437083008@webmail.uad.ac.id

1. INTRODUCTION

Digital transformation has brought fundamental changes in various aspects of life [1], [2], [3], [4], including in the business sector [5], government [6], health [7] and public services [8], [9]. The development of information and communication technology (ICT) has created great opportunities for organizations to improve operational efficiency and effectiveness [10], [11]. But on the other hand, digitalization also presents new challenges, especially in terms of cybersecurity [12], [13], [14]. The increased use of digital devices and the internet has led to a significant surge in cyber threats [15], including spamming, hacking, data theft, ransomware attacks, as well as other cybercrimes [7], [16].

Digital forensics is becoming an increasingly important field in helping organizations identify, analyze, and address cyber incidents [17], [18]. Digital forensics is a discipline that focuses on the collection, analysis, and interpretation of digital evidence can be found in various devices, such as computers, cell phones, servers, and the Internet of Things (IoT) [19], [20], [21] to support cybercrime investigations and ensure that the evidence obtained is admissible in legal proceedings or internal organizational investigations [20]. The existence of digital forensics not only helps in criminal investigations, but also data recovery [22], [23], security audits [24], [25], and information technology risk mitigation [26], [2]. The main goal of digital forensics is to ensure

that the data collected can be used as valid evidence in legal proceedings and internal organizational investigations [27], [28], [29].

The increase in cybercrime cases has forced organizations [30], both in the public and private sectors, to strengthen their ability to handle cyber incidents [31]. However, organizational readiness in implementing digital forensics remains a challenge. Many organizations do not have adequate policies, procedures, and infrastructure to effectively deal with cyber incidents [32]. Therefore, it is important for organizations to have a digital forensics readiness standard that can be used to measure the extent to which they are able to respond to and manage cyber incidents systematically. Digital forensic readiness is a crucial element in an organization's cybersecurity strategy [6], [25]. This readiness covers various aspects, including digital investigation policies and procedures, people resource competence in handling digital evidence, and the availability of infrastructure that supports the digital forensics process. However, to date, there is no comprehensive standard to measure an organization's readiness to effectively implement digital forensics.

Several standards, such as ISO/IEC 27037, which focuses on the identification, collection, and acquisition of digital evidence [33], and NIST 800-86, which provides guidelines for incident handling and evidence analysis [27], offer valuable technical guidance in digital forensics. However, these frameworks do not explicitly address how to assess or enhance organizational readiness from a managerial and governance perspective. The lack of standardized digital forensic readiness models makes it difficult for organizations to evaluate their preparedness for cyber incidents, identify procedural weaknesses, or implement corrective actions systematically. As a result, there is a critical need for a comprehensive readiness model that integrates not only technical guidance but also governance structures, policy frameworks, procedural clarity, and people resource competencies to support effective digital forensic investigations.

COBIT 2019 is an IT governance framework developed by ISACA and recognized globally for its flexibility in adapting to organizational needs, including digital forensics readiness. This framework consists of several important domains such as EDM (Evaluate, Direct, Monitor), APO (Align, Plan, Organize), BAI (Build, Acquire, Implement), DSS (Deliver, Service, Support), and MEA (Monitor, Evaluate, Assess), which collectively support information security risk management and regulatory compliance. However, despite its effectiveness in IT governance, the use of COBIT 2019 in the context of digital forensics remains limited, and there is no specific digital forensics readiness assessment model that refers to the principles and domains of COBIT 2019.

Previous DFR frameworks, such as ISO/IEC 27037 and NIST SP 800-86, primarily focus on the procedural and technical aspects of evidence handling, while Elyas [34] provides a conceptual foundation for readiness assessment. However, these frameworks do not integrate IT governance mechanisms or provide standardized assessment indicators. Therefore, this study advances prior works by developing a Delphi-validated instrument that operationalizes Digital Forensics Readiness (DFR) through COBIT 2019's governance domains, offering a measurable and governance-aligned approach.

Based on these issues, this study aims to develop a COBIT 2019 based digital forensics readiness assessment instrument that is not only theoretically valid but also practically relevant, especially for higher education institutions. The instrument was developed through three rounds of the Delphi method involving seven experts in the fields of digital forensics and IT governance. This model is expected to bridge the gap between theory and practice and contribute to strategic cybersecurity planning and national policies such as the Electronic-Based Government System, known as SPBE and the development of digital audit standards by the National Cyber and Encryption Agency, known as BSSN. Thus, this model represents a strategic step in strengthening organizational investigative readiness and cybersecurity resilience in the digital age.

2. LITERATURE REVIEW

2.1. Digital Forensics Framework and Standards

Several frameworks and standards have been developed to support the practice of digital forensics, including: ISO/IEC 27037, International standard governing the identification, collection, and acquisition of digital evidence [35]. NIST 800-86, Guidelines issued by NIST regarding the investigation and analysis of digital evidence in organizations [27]. ACPO Good Practice Guide for Digital Evidence, Standards developed by the Association of Chief Police Officers (ACPO) to ensure the validity of digital evidence in legal proceedings [36]. Although existing frameworks like NIST SP 800-86 and ISO 27037 provide procedural and technical guidance on incident response and evidence handling, they lack emphasis on assessing institutional readiness and do not integrate governance principles [23], [21] such as those found in the COBIT 2019 framework. These standards are not designed as comprehensive assessment tools and often overlook the organizational complexity involved in digital forensics, where success depends not only on technical capabilities but also on cross-functional coordination, formal governance policies, and strategic risk management.

Compared with existing frameworks, this study differs in focus and scope. ISO/IEC 27037 and NIST SP 800-86 offer technical guidance for handling and analysis but lack governance integration and readiness measurement. Elyas [34] provides theoretical readiness dimensions but without validated indicators or governance linkage. In contrast, our COBIT 2019 based instrument translates these conceptual elements into quantifiable governance-aligned metrics validated through expert consensus, bridging the gap between technical frameworks and strategic IT governance.

2.2. COBIT 2019 and Digital Forensics Readiness

COBIT, developed by ISACA, is a globally recognized IT governance framework designed to help organizations manage risk, improve efficiency, and ensure regulatory compliance [37], [38]. In the context of digital forensics, COBIT 2019 offers a structured foundation for building a Digital Forensic Readiness (DFR) framework by aligning strategic governance principles with forensic capabilities. The EDM domain guides the development of policies and regulations for digital forensics, ensuring accountability and compliance. APO focuses on strategic planning to integrate forensic goals into IT governance, while BAI ensures the implementation of suitable forensic tools and systems. DSS supports the operational delivery of digital forensic services, and MEA enables continuous evaluation of forensic readiness and investigation effectiveness. Although COBIT 2019 is increasingly adopted, its application in digital forensics remains limited. Integrating DFR into COBIT's domains provides an opportunity to create a governance aligned, standardized assessment instrument an advancement not yet addressed by existing technical frameworks.

2.3. Delphi Method in Standar Development

The Delphi method is a research technique used to reach consensus among a group of experts through a series of iterations and surveys conducted anonymously [39], [40]. This method is very effective for developing new standards or frameworks because it involves independent expert opinions and is based on professional experience [41], [42].

The Delphi method consists of several main stages:

- Expert Panel Identification - Selecting experts with expertise in digital forensics and IT governance [41].
- Initial Questionnaire Development - Developed a list of COBIT 2019 based digital forensics readiness instruments.
- Iteration and Consensus - Conduct multiple rounds of surveys to gain consensus from the expert panel.
- Analysis of Results - Determine the agreed instrument and design the final instrument of the digital forensic readiness standard.

This method was chosen because it has several advantages, produces stronger consensus than traditional survey methods. The anonymity of the panelists prevents one individual from dominating the final decision. Iterative and flexible, allowing for continuous improvement of the developed instrument [39], [40].

2.4. Related Research

Various studies have been conducted to address the growing need for a DFR framework in organizations. Elyas [34] laid a conceptual foundation by proposing a theoretical framework based on expert perspectives, identifying key DFR factors such as strategy, policy, infrastructure, and stakeholder involvement. However, their model lacks a standardized assessment instrument and does not explicitly incorporate governance frameworks like COBIT. Azzam [11] focused on forensic readiness in Industrial Control Systems (ICS), emphasizing technical preparedness against covert attacks, but their approach remains heavily technology-centric and lacks governance-based evaluative tools. Similarly, Kebande [28] introduced a forensic intelligence repository to support evidence management, offering innovation in data handling, yet without aligning with IT governance or managerial standards. These studies, while significant in advancing technical understanding, reveal a gap in integrating DFR with organizational governance models.

Further studies reinforce this gap. Albugmi [24] highlights DFR elements like logging and encryption using a DSRM approach but notes the absence of integration with IT governance, particularly COBIT 2019. Odhiambo [9] show DFR's impact in reducing incident costs through previous frameworks addressing technological, legal, and organizational factors, but again, without a standardized, governance-aligned model. Nugroho [6] stress DFR's importance in e-Government services but acknowledge the lack of a COBIT based instrument, especially for public education. Nik Zulkipli [31] and Asante [17] also recognize the operational importance of SOPs, training, and BYOD risks, but their models remain unvalidated or detached from formal governance frameworks. Collectively, these studies highlight that most DFR research remains focused on technical readiness such as tools, infrastructure, and investigative processes while neglecting auditability, regulatory alignment, and strategic decision-making. As a result, current frameworks lack organizational scalability, consistency, and cross-sector applicability, reinforcing the need for a governance-integrated DFR model, particularly in regulated sectors like higher education and government.

Based on the reviewed literature, existing frameworks such as ISO/IEC 27037 and NIST SP 800-86 primarily emphasize technical and procedural aspects of digital forensics but do not provide a standardized method to assess organizational readiness from a governance perspective. Similarly, prior studies (e.g., Elyas, 2015 [34]; Kebande, 2021 [28]; Azzam, 2023 [11]) focus on sectoral or technical components, lacking a validated, governance integrated readiness model.

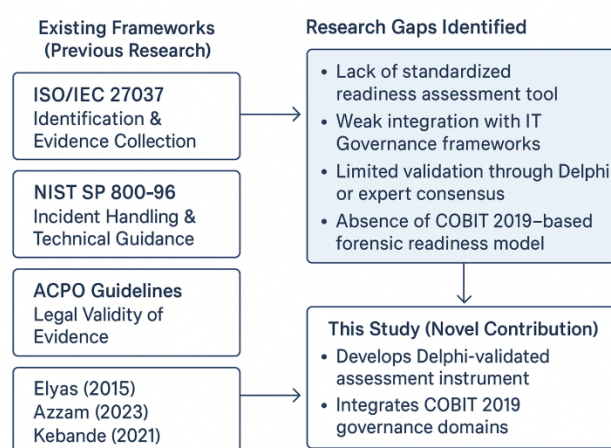


Figure 1. Conceptual Diagram of Research Gaps in Digital Forensic Readiness Studies

Figure 1 illustrates the conceptual summary of these research gaps and the positioning of this study, which aims to develop a Delphi-validated digital forensic readiness assessment instrument grounded in the COBIT 2019 framework.

3. RESEARCH METHOD

This study uses a qualitative and quantitative approach with the Delphi method to develop a digital forensic readiness assessment standard based on COBIT 2019 involving 7 experts, and can obtain credible results [40], [43], [44]. This approach was chosen because the Delphi method allows researchers to obtain consensus from experts consisting of 4 academics and 3 practitioners through a series of iterations so that the instruments developed have conceptual and practical validity.

This research approach focuses on the development of standardized instruments by way of:

- Identify digital forensic readiness instruments based on literature studies and the COBIT 2019 framework.
- Validating the instrument through the Delphi method by involving experts in the field of digital forensics and IT governance.
- Develop the final instrument based on the results of expert consensus.

With this approach, the research can produce a comprehensive framework, based on strong theory, and can be implemented in organizations to measure and improve digital forensic readiness.

3.1. Criteria and Expert Selection

In this research, the selected experts must fulfill several selection criteria, namely:

- Have ≥ 5 years of experience in digital forensics or IT governance.
- Have been involved in policy development, auditing, or implementation of digital forensics within the organization.
- Coming from various sectors, such as academics, digital forensics communities, and practitioners in the field of digital forensics or cybersecurity.

Table 1. Experts in Delphi Method Panelists

Expert	Expertise	Experience	Sector	Institution	Profession
1	Information Security, Digital Forensics, Networking	25 years	Higher Education	Public	Academics
2	Digital Forensics, Computer Security, E-Government	23 years	Higher Education	Private	Academics
3	Digital Forensics, Digital Evidence, Computer Security	31 years	Higher Education	Private	Academics
4	Digital Forensics, Network and Security Engineering	30 years	Higher Education	Public	Academics
5	Cyber Security, Digital Forensics, Data Science	14 years	Telco Service Provider	Public	Practitioner
6	Governance, Technology and Information Insurance	25 years	Information system audit consultant	Private	Practitioner
7	Cyber Security, Digital Literacy	7 years	Standardization/ certification	Private	Practitioner

The Delphi panel in this study consisted of seven purposively selected experts four academics and three practitioners, chosen for their proven experience in digital forensics and IT governance, as detailed in Table 1. The academics contributed conceptual depth and reinforced alignment with COBIT 2019 principles, while the practitioners brought real-world insights from government and industry related to forensic audits, cyber incident response, and IT policy development. Although the panel size was limited, it aligns with established Delphi standards, which consider panels of 5–10 experts sufficient for generating credible results when participants possess deep expertise and diverse perspectives [43], [44], [40]. The process involved multiple rounds with participant anonymity to prevent dominance bias, and used quantitative metrics such as I-CVI, S-CVI, and IQR to assess consensus. This methodological approach ensures that the resulting instrument is both theoretically grounded and practically applicable for assessing digital forensic readiness, particularly in higher education institutions.

3.2. Data Analysis

The data obtained from the Delphi method was analyzed using the following techniques:

- Descriptive statistics - To see the distribution of expert answers in each Delphi round.

- IQR (Interquartile Range) - Measures the level of agreement of panelists. Consensus is considered reached if $IQR \leq 1$.
 - Content validity index (I-CVI) - Used to assess expert agreement on each instrument.
 - Scale-level content validity index (S-CVI) is the ratio of the number of instruments or items rated 4 or 5 by all experts to the total number of items. The S-CVI is the average of the I-CVI.
- If in the first round the instrument has an $I-CVI \geq 0.78$ or an $IQR \leq 1$, it is revised before proceeding to the next round. An S-CVI of more than 0.90 indicates excellent content validity [45].

4. RESULTS AND DISCUSSION

4.1. Development of a Digital Forensics Readiness Standard Assessment Instrument

The instrument development is based on the basic theory of digital forensic readiness, related research, and the COBIT 2019 approach. A total of 40 initial indicators were derived through a structured literature coding process and expert brainstorming sessions. A total of 6 publications on DFR and 94 indicators, which were then extracted and mapped to COBIT domains. Duplicates were combined, resulting in 40 initial indicators representing six readiness domains. Related research from the Digital Forensics Readiness Framework (DFRF) to Secure Database Systems [24] has 10 indicators coded ALB01-ALB10. The study Towards Digital Forensic Readiness: A Framework for Financial Service Providers [9] has 14 indicators coded ODH01-ODH14. The study A Novel Digital Forensic Readiness (DFR) Framework for e-Government [6] has 33 indicators coded NUG01-NUG033. The study An Exploratory Study on Readiness Framework in IoT Forensics [31] has 13 indicators coded NIK01-NIK13. The Digital Forensic Readiness Framework Based on Honeypot and Honeynet for ByoD [17] study has 11 indicators and is coded ASA01-ASA11. The Digital forensic readiness: Expert perspectives on a theoretical framework [34] study has 13 indicators and is coded ELY01-ELY13. Several of these indicators, analyzed in depth, can then be grouped into 6 initial groups/domains, the mapping process is in Appendix 1.

Table 2. Proposed Mapping of Digital Forensics Readiness Instrument Using COBIT 2019

No	Component	COBIT 2019 Domain	Number of Instruments
1	Technology and Infrastructure	BAI04, BAI10, DSS01, DSS05, APO13, APO14	6
2	Policy, Regulation and Compliance	EDM01, APO01, APO09, APO10, MEA03, MEA04	6
3	People Competency and Security Awareness	APO07, APO08, BAI08, MEA01	4
4	Risk and Security Management	EDM03, APO12, APO11, DSS06, MEA02	5
5	Incident Management and Investigation	DSS02, DSS03, DSS04, APO03, APO04, BAI01, BAI02, BAI03, BAI05, BAI06, BAI07, BAI09, BAI11	13
6	Governance and Strategy	EDM02, EDM04, EDM05, APO02, APO05, APO06	6
Total Instrument			40

The mapping results are continued with the COBIT 2019 approach, resulting in the formulation of instrument mapping in Table 2, the mapping process in Appendix 2.

4.2. Instrument Validation through the Delphi Method

The validation process, summarized in Table 3, was conducted through three Delphi rounds involving seven experts from academia and professional practice in digital forensics and IT governance, aiming to establish content validity and expert consensus. Between each round, qualitative feedback was analyzed using thematic codes to identify patterns in expert comments (e.g., clarity, redundancy, relevance). Each coded theme informed the revision of a specific item, ensuring that changes were systematically informed by the expert's context, rather than ad hoc judgment. Consequently, there were some differences in the scores across components (domains) between rounds, due to shifts in indicators across components (domains) based on the analysis of expert feedback. In Round 1, of the 40 items evaluated, only 4 met the $I-CVI \geq 0.78$ and 9 had an $IQR \leq 1.00$, indicating limited initial agreement; revisions were made based on qualitative feedback. Round 2 showed marked improvement, with 36 items meeting the I-CVI threshold and 39 achieving $IQR \leq 1.00$, reflecting enhanced clarity and structural coherence. In Round 3, full

consensus was reached across all items, resulting in an overall S-CVI of 0.99 and all items satisfying the IQR criterion, demonstrating excellent content validity and expert agreement.

Table 3. Development of Delphi Round Validation

Validation Metric	Round 1	Round 2	Round 3
Total Number of Items Evaluated	40	40	40
Items with I-CVI ≥ 0.78	4	36	40
Items with IQR ≤ 1.00	9	39	40
Number of Domains Involved	6	6	6
Revisions Made	Rewording, Domain Shifting	Refinement, Clarification	Final Confirmation

Table 3 captures the progressive improvements in I-CVI and IQR across rounds, evidencing a rigorous and iterative refinement process. A summary of item-level changes, I-CVI development, and component and domain rearrangements throughout the Delphi rounds is presented in Appendix 3.

4.3. Final Assessment Instrument Standards

The content validation process in this study applied the Content Validity Index (CVI) method, which includes the Item-Level CVI (I-CVI) and Scale-Level CVI (S-CVI), following the recommendations of [45] who emphasized expert consensus in evaluating item relevance. I-CVI was calculated by dividing the number of experts rating an item as "relevant" or "highly relevant" by the total number of panelists, using a threshold of ≥ 0.78 to indicate sufficient content validity. The S-CVI, representing the overall content validity of each component, was derived by averaging the I-CVI values across items, with ≥ 0.90 considered excellent. As shown in Table 4, all six components in this study achieved an S-CVI of 0.99, exceeding the standard threshold and indicating that the items were consistently rated as relevant and representative by the expert panel. These results affirm that the instrument has strong content validity and is well-suited for further application in model development, policy formulation, or research.

Table 4. S-CVI Values

	First round	Second round	Third round
Total I-CVI	24.00	33.57	39.71
S-CVI	0.60	0.84	0.99

Thus, the validation and consensus process was comprehensively completed, and all remaining items could be considered ready to be used for conceptual model development, strategic policy framework development, and further research instrument development. This result reflects the substantial quality of the instrument items that have gone through an iterative process, based on expert judgment.

4.4. Discussion

The digital forensic readiness assessment instrument developed in this study goes beyond technical validation and represents a strategic effort to bridge the gap between operational forensic practices and institutional IT governance frameworks. By integrating COBIT 2019 principles, this research reframes digital forensic readiness as a strategic organizational capability rather than merely an operational function. Academically, the instrument reinforces digital forensics as a core component of IT governance, offering a rare synthesis between governance theory and forensic investigation domains. Practically, it provides higher education institutions with concrete tools to assess their investigative readiness, including components like Governance and Strategy and Incident and Investigation Management, which support planning, auditing, and performance evaluation. As detailed in Figure 2, the Delphi validation process showed progressive consensus improvement across three rounds, with items in the high consensus category ($\text{IQR} \leq 1.00$) rising from 22.5% in Round 1 to 100% by Round 3, demonstrating the method's effectiveness in refining the instrument through iterative feedback.

This study extends existing DFR frameworks by integrating governance principles from COBIT 2019, which are absent in ISO/IEC 27037, NIST SP 800-86, and Elyas [34]. While previous models emphasized technical or conceptual readiness, our approach incorporates

managerial accountability, policy integration, and performance monitoring within a validated instrument. The inclusion of Delphi validation ensures empirical rigor that has not been reported in earlier DFR studies, providing both theoretical and practical contributions.

This instrument holds strong regulatory relevance, especially in supporting SPBE as outlined in Presidential Regulation No. 132 of 2022, and the BSSN [46] digital security policies. The increasing cyber threats in the education sector such as ransomware, data breaches, and vulnerabilities in platforms like OJS and Moodle highlight the urgent need for a governance-aligned forensic readiness model. Yet, no existing standard explicitly connects digital forensic readiness with governance models like COBIT 2019. This research addresses that gap by producing a validated, structured, and adaptable tool aligned with national policy and institutional needs. As shown in Table 3 and Table 4, the instrument demonstrates high content validity ($S\text{-CVI} = 0.99$) and expert consensus, offering a robust foundation for forensic readiness assessment in the face of growing cybersecurity challenges.

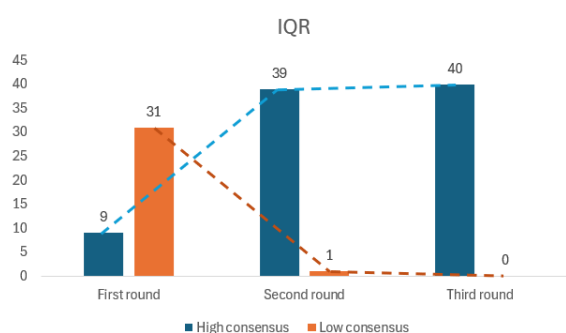


Figure 2. IQR Analysis Results

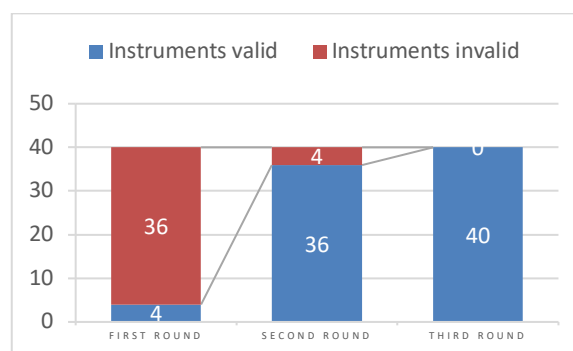


Figure 3. I-CVI Analysis Results

Content validity of the digital forensic readiness instrument was assessed using the I-CVI (Item-Content Validity Index) method, applying a threshold of $I\text{-CVI} \geq 0.78$ as recommended by Davis [45]. As shown in Figure 3, only 4 out of 40 items (10%) met this validity standard in the first round, indicating a lack of consensus among experts regarding item relevance. After revisions based on expert feedback, the second round saw a substantial improvement, with 36 items (90%) reaching valid I-CVI levels. The process culminated in the third round, where all 40 items (100%) achieved content validity, reflecting full expert consensus. This upward trend underscores the effectiveness of the iterative Delphi method in refining instrument clarity and aligning content with the COBIT 2019 framework. The final consensus validates the conceptual soundness of the instrument and confirms that structured expert feedback can significantly enhance content validity across evaluation rounds.

To evaluate the overall content validity of the instrument, the Scale-Content Validity Index (S-CVI) was used by averaging the I-CVI values of all items, as recommended by Davis [45]. As illustrated in Figure 4, the S-CVI showed a significant increase across the Delphi rounds from 0.60 in the first round, to 0.84 in the second, and finally reaching 0.99 in the third round. This upward trend indicates that iterative expert feedback and refinements significantly enhanced the relevance and clarity of the instrument. The initial S-CVI of 0.60 reflected limited agreement on item suitability, but by the third round, the S-CVI exceeded the accepted threshold of 0.90, signaling near-complete consensus on the instrument's content. These results confirm that the Delphi method effectively improved both the quality of individual items and the overall conceptual consistency of the instrument, affirming its high validity for use in COBIT 2019 based digital forensic readiness assessments.

The triangulation of the three validation metrics IQR (expert consensus), I-CVI (item-level content validity), and S-CVI (scale-level content validity) demonstrated a consistent improvement in the instrument's quality across all Delphi rounds. In the first round, only 4 items (10%) met the I-CVI threshold (≥ 0.78), 77.5% of items showed low consensus ($IQR > 1.00$), and the S-CVI was

just 0.60, reflecting weak agreement on the overall construct. However, by the second round, revisions based on expert feedback led to 36 items (90%) achieving content validity, 39 items (97.5%) reaching high consensus, and an increased S-CVI of 0.84. The third round finalized the process with 100% of items meeting both validity and consensus criteria, and an S-CVI of 0.99, indicating near-perfect agreement. As shown in Table 5, this trend affirms the Delphi method's effectiveness in refining both item quality and conceptual cohesion, resulting in a content-valid and consensus-aligned instrument for assessing digital forensic readiness.

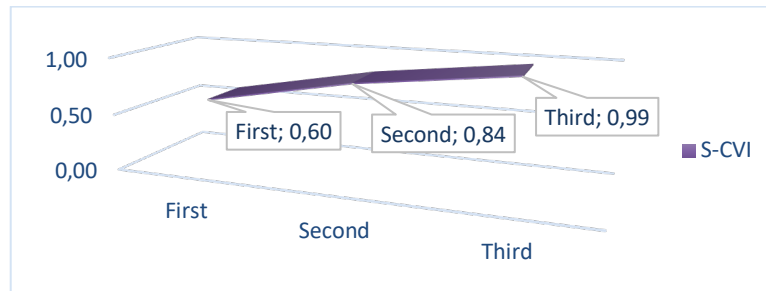


Figure 4. S-CVI Analysis Results

Beyond improvements in validity scores, the Delphi rounds also involved substantial structural refinement of the instrument's components, as shown in Table 2 and Table 5. Initially structured based on COBIT 2019 domains and prior research, the first-round evaluation revealed issues such as conceptual overlaps and ambiguous terminology. Based on expert input, items were reorganized to better reflect strategic-to-technical flow, and reclassified for logical consistency for example, items shifted from "People Competency and Security Awareness" to "Incident Management and Investigation," or from "Technology and Infrastructure" to "Governance and Strategy." These adjustments, validated by significant increases in I-CVI and reductions in IQR, continued into the third round. Further refinements included domain repositioning such as APO02 moving to "Policy, Regulation, and Compliance" and DSS04 to "Governance and Strategy," while "Technology and Infrastructure" remained unchanged. These structural changes, supported by improved validation metrics, confirmed the instrument's conceptual integrity and readiness for practical implementation.

Table 5. Comparison of First, Second, and Third Rounds

No	First Round		Second Round		Third Round	
	Component	COBIT 2019 Domain	Component	COBIT 2019 Domain	Component	COBIT 2019 Domain
1	Technology and Infrastructure	BAI04, BAI10, DSS01, DSS05, APO13, APO14 (6 item)	Governance and Strategy	EDM02, EDM04, EDM05, APO02, APO05, APO06 (6 item)	Governance and Strategy	EDM02, EDM04, EDM05, APO05, APO06, DSS04 (6 item)
2	Policy, Regulation, and Compliance	EDM01, APO01, APO09, APO10, MEA03, MEA04 (6 item)	Policy, Regulation, and Compliance	EDM01, APO01, APO09, APO10, APO11, APO13, MEA03, MEA04 (8 item)	Policy, Regulation, and Compliance	EDM01, APO01, APO02 APO09, APO10, APO11, APO13, MEA03, MEA04 (9 item)
3	People Competency and Security Awareness	APO07, APO08, BAI08, MEA01 (4 item)	People Competency and Security Awareness	APO07, APO08, BAI08, MEA01 (4 item)	People Competency and Security Awareness	APO07, BAI08, MEA01 (3 item)
4	Risk and Security Management	EDM03, APO12, APO11, DSS06, MEA02 (5 item)	Risk and Security Management	EDM03, APO12, DSS06, MEA02 (4 item)	Risk and Security Management	EDM03, APO12, DSS06, MEA02 (4 item)
5	Incident Management and Investigation	DSS02, DSS03, DSS04, APO03, APO04, BAI01, BAI02, BAI03, BAI05, BAI06, BAI07, BAI09, BAI11 (13 item)	Incident Management and Investigation	DSS02, DSS03, DSS04, APO03, APO04, BAI01, BAI02, BAI03, BAI05, BAI06, BAI07, BAI09, BAI11 (13 item)	Incident Management and Investigation	DSS02, DSS03, APO03, APO04, APO08, BAI01, BAI02, BAI03, BAI05, BAI06, BAI07, BAI09, BAI11

No	First Round		Second Round		Third Round	
	Component	COBIT 2019 Domain	Component	COBIT 2019 Domain	Component	COBIT 2019 Domain
6	Governance and Strategy	EDM02, EDM04, EDM05, APO02, APO05, APO06 (6 item)	Technology and Infrastructure	BAI04, BAI10, DSS01, DSS05, APO14 (5 item)	Technology and Infrastructure	(13 item) BAI04, BAI10, DSS01, DSS05, APO14 (5 item)
Total Instrument		40	Total Instrument		40	Total Instrument 40

The structural and positional changes made to the instrument were not superficial but rather consensus-driven revisions that enhanced both its theoretical soundness and practical applicability, affirming the value of an iterative and flexible Delphi approach in ensuring content relevance and precision. The final validated version of the instrument, as detailed in Appendix 4, emerged from a three-round Delphi process and comprises six core components that span strategic and operational aspects of information security governance. These components are not just technical indicators but form a conceptual framework that integrates COBIT 2019 governance principles with the investigative needs of modern institutions. Developed through expert feedback that emphasized both content relevance and structural coherence, the instrument provides a robust foundation for implementing a governance-aligned digital forensic readiness assessment in higher education and public sector contexts.

4.4.1. Summary of Instrument Components and Their Theoretical-Practical Significance

The digital forensic readiness instrument developed in this study consists of six core components: Governance and Strategy, Policy, Regulation, and Compliance, People Competency and Security Awareness, Risk and Security Management, Incident and Investigation Management, and Technology and Infrastructure, all aligned with the COBIT 2019 governance framework. These components were not only conceptually derived but also refined through expert consensus using the Delphi method, ensuring both theoretical rigor and practical relevance. Each component represents a strategic and operational domain essential for institutional forensic readiness. For instance, Governance and Strategy emphasizes leadership commitment and policy integration, while Policy, Regulation, and Compliance ensures legal and regulatory alignment [7]. People Competency and Security Awareness addresses human capital and culture, and Risk Management and Security highlights the proactive management of digital threats. Operational readiness is covered in Incident and Investigation Management, and technological capability is addressed in Technology and Infrastructure. The final structure of these components, validated and reorganized based on expert feedback, is detailed in Appendix 4.

4.4.2. Implications, Contributions, and Future Use of the Instrument

Practically, the instrument serves as a diagnostic tool for organizations especially in the public and higher education sectors to measure and improve their forensic readiness in alignment with SPBE policies and BSSN regulations. It can be used in internal audits, IT governance evaluations, training programs, and strategic cybersecurity planning (Presidential Regulation No. 132/2022; BSSN, 2024). Theoretically, this study expands the concept of forensic readiness beyond technical domains, embedding it into institutional governance ecosystems. It fills a gap in the literature by offering a standardized, governance-based assessment model, contrasting previous research that mostly focused on sectoral or technical perspectives [23], [28], [47], [48]. The instrument offers a conceptual foundation for further research on sector-specific or framework-based readiness models (e.g., ISO, NIST), and may serve as a reference in cross-institutional or international comparisons. Through systematic validation, structured component analysis, and policy alignment, this instrument offers a robust and adaptable framework for measuring digital forensic readiness in complex institutional environments.

5. LIMITATION

This study has several limitations that should be considered when interpreting its findings. The Delphi panel included only seven experts, which, although acceptable for exploratory studies [40], may limit the diversity of perspectives, especially in terms of sectoral and geographic representation, as most panelists shared similar national and institutional backgrounds. Additionally, the instrument was developed exclusively using the COBIT 2019 framework, which assumes a baseline familiarity with IT governance principles, potentially limiting its applicability in non-IT-centric organizations or small enterprises without formal governance structures. The validation process focused solely on content validity through expert consensus in the Delphi method, without employing statistical tests such as reliability analysis or factor analysis, making the validation conceptual rather than empirical. Moreover, the instrument was developed within the context of Indonesian higher education, shaped by sector-specific policies and priorities, so its generalizability to other sectors such as finance, private industry, or international institutions, requires careful adaptation.

6. CONCLUSION

This study successfully designed and validated a digital forensic readiness assessment instrument grounded in the principles and domains of COBIT 2019, using a three-round Delphi method with seven experts from academia and practice. The instrument comprises six key components, governance, policy, people, risk, incident management, and technology and marks a significant contribution by integrating IT governance into a domain previously dominated by technical perspectives. It provides a strategic and systematic tool for organizations, particularly higher education institutions, to evaluate and enhance their readiness for cyber incident response in a forensic, accountable manner, while also supporting regulatory compliance with frameworks like SPBE and BSSN guidelines. However, the instrument's current validation is conceptual, lacking statistical testing in real-world contexts, and its reliance on COBIT may limit applicability in non-IT sectors without formal governance structures. Additionally, the limited number and geographic scope of panelists pose constraints on generalizability. Future research should include field testing, quantitative validation (e.g., factor analysis, reliability testing), and model adaptation to alternative frameworks such as ISO/IEC 27037 or NIST SP 800-86 to broaden its applicability across institutional contexts.

APPENDIX

[Appendix 1](#)

[Appendix 2](#)

[Appendix 3](#)

[Appendix 4](#)

REFERENCES

- [1] A. Alenezi, R. K. Hussein, R. J. Walters, and G. B. Wills, "A Framework for Cloud Forensic Readiness in Organizations," in *Proceedings - 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2017*, Institute of Electrical and Electronics Engineers Inc., Jun. 2017, pp. 199–204. doi: 10.1109/MobileCloud.2017.12.
- [2] M. I. Ali and S. Kaur, "Next-Generation Digital Forensic Readiness BYoD Framework," *Security and Communication Networks*, vol. 2021, pp. 1–19, Mar. 2021, doi: 10.1155/2021/6664426.
- [3] C. Mpungu, C. George, and G. Mapp, "Developing a Novel Digital Forensics Readiness Framework for Wireless Medical Networks Using Specialised Logging," *Advanced Sciences and Technologies for Security Applications*, pp. 203–226, 2023, doi: 10.1007/978-3-031-20160-8_12.
- [4] B. Setiawan and M. A. Rizal, "Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 1396–1403. doi: 10.1016/j.procs.2024.03.138.

- [5] C. Mpungu, C. George, and G. Mapp, "Digital Forensics Readiness in Big Data Wireless Networks: A Novel Framework and Incident Response Script for Linux-Hadoop Environments," Jul. 23, 2024. doi: 10.20944/preprints202407.1803.v1.
- [6] H. A. Nugroho, O. C. Briliyant, and S. U. Sunaringtyas, "A Novel Digital Forensic Readiness (DFR) Framework for e-Government," in *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 184–189. doi: 10.1109/ICoCICs58778.2023.10276423.
- [7] M. Chernyshev, S. Zeadally, and Z. Baig, "Healthcare Data Breaches: Implications for Digital Forensic Readiness," *J Med Syst*, vol. 43, no. 7, pp. 1–12, Nov. 2018, doi: 10.1007/s10916-018-1123-2.
- [8] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Comput Secur*, vol. 106, Jul. 2021, doi: 10.1016/j.cose.2021.102267.
- [9] G. Odhiambo, R. Omollo, and P. Abuonji, "Towards Digital Forensic Readiness: A Framework for Financial Service Providers," *East African Journal of Information Technology*, vol. 7, no. 1, pp. 92–107, Apr. 2024, doi: 10.37284/eajit.7.1.1897.
- [10] T. Rochmadi and I. Y. Pasa, "Pengukuran Risiko dan Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi di BKD XYZ Berdasarkan ISO 27001 / SNI," *CyberSecurity dan Forensik Digital*, vol. 4, no. 1, pp. 38–43, May 2021, doi: 10.14421/csecurity.2021.4.1.2439.
- [11] M. Azzam, L. Pasquale, G. Provan, and B. Nuseibeh, "Forensic readiness of industrial control systems under stealthy attacks," *Comput Secur*, vol. 125, Feb. 2023, doi: 10.1016/j.cose.2022.103010.
- [12] N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. J. Pangalos, "Actionable threat intelligence for digital forensics readiness," *Information and Computer Security*, vol. 27, no. 2, pp. 273–291, May 2019, doi: 10.1108/ICS-09-2018-0110.
- [13] S. Oh and T. Shon, "Digital Forensics for Analyzing Cyber Threats in the XR Technology Ecosystem within Digital Twins," *Electronics (Switzerland)*, vol. 13, no. 13, Jul. 2024, doi: 10.3390/electronics13132653.
- [14] G. Angafor, I. Yevseyeva, and L. Maglaras, "MalAware: A tabletop exercise for malware security awareness education and incident response training," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 280–292, Jan. 2024, doi: 10.1016/j.iotcps.2024.02.003.
- [15] M. M. Al Mahdi and S. Baror, "Proof of Concept of a Digital Forensic Readiness Cybercrime Language as a Service," *Proceedings of the 19th International Conference on Cyber Warfare and Security*, 2024, doi: 10.34190/iccws.19.1.2059.
- [16] I. Riadi, S. Sunardi, and F. T. Fitri, "Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method," *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 6, no. 1, pp. 108–117, Feb. 2022, doi: 10.29407/intensif.v6i1.16830.
- [17] A. Asante and V. Amankona, "Digital Forensic Readiness Framework Based on Honeypot and HoneyNet for BYoD," *Journal of Digital Forensics, Security and Law*, vol. 16, no. 2, Sep. 2021, doi: 10.58940/1558-7223.1706.
- [18] M. B. Jimenez and D. Fernandez, "A Framework for SDN Forensic Readiness and Cybersecurity Incident Response," in *2022 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2022 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 112–116. doi: 10.1109/NFV-SDN56302.2022.9974648.
- [19] S. Khanji, O. Alfandi, L. Ahmad, L. Kakkengal, and M. Al-kfairy, "A systematic analysis on the readiness of Blockchain integration in IoT forensics," *Forensic Science*

- International: Digital Investigation*, vol. 42–43, Oct. 2022, doi: 10.1016/j.fsidi.2022.301472.
- [20] F. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, “A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field,” *Engineering, Technology and Applied Science Research*, vol. 13, no. 5, pp. 11608–11615, Oct. 2023, doi: 10.48084/etasr.6195.
- [21] M. H. Rais, M. Ahsan, and I. Ahmed, “FRoMEPP: Digital forensic readiness framework for material extrusion based 3D printing process,” *Forensic Science International: Digital Investigation*, vol. 44, Mar. 2023, doi: 10.1016/j.fsidi.2023.301510.
- [22] A. Yarramreddy, P. Gromkowski, and I. Baggili, “Forensic analysis of immersive virtual reality social applications: A primary account,” in *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*, Institute of Electrical and Electronics Engineers Inc., Aug. 2018, pp. 186–196. doi: 10.1109/SPW.2018.00034.
- [23] A. Al-Dhaqm, S. A. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, “Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field,” *IEEE Access*, vol. 8, pp. 145018–145032, 2020, doi: 10.1109/ACCESS.2020.3008696.
- [24] A. Albugmi, “Digital Forensics Readiness Framework (DFRF) to Secure Database Systems,” *Engineering, Technology and Applied Science Research*, vol. 14, no. 2, pp. 13732–13740, Apr. 2024, doi: 10.48084/etasr.7116.
- [25] A. Adel, A. Ahsan, and C. Davison, “ETHICore: Ethical Compliance and Oversight Framework for Digital Forensic Readiness,” *Information (Switzerland)*, vol. 15, no. 6, Jun. 2024, doi: 10.3390/info15060363.
- [26] A. A. Garba and A. Musa Bade, “A Recommended Digital Forensic Readiness Framework for Nigerian Banks,” *International Journal of Development Research*, vol. 9, no. 8, pp. 28920–28928, Aug. 2019.
- [27] ArKar Kyaw, Brian Cusack, and Raymond Lutui, “Digital Forensic Readiness In Wireless Medical Systems,” in *International Telecommunication Networks and Applications Conference (ITNAC)*, Auckland, New Zealand: [IEEE], Apr. 2020. doi: 10.1109/ITNAC46935.2019.9078005.
- [28] V. R. Kebande, N. M. Karie, K. R. Choo, and S. Alawadi, “Digital forensic readiness intelligence crime repository,” *Security and Privacy*, vol. 4, no. 3, May 2021, doi: 10.1002/spy2.151.
- [29] R. Thron, H. Dirnberger, S. Tjoa, and G. Quirchmayr, “Requirements and Challenges for Digital Forensic Readiness in Industrial Automation and Control Systems,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jan. 2022, pp. 232–238. doi: 10.1145/3524338.3524374.
- [30] W. Jiang, J. Legoria, K. J. Reichelt, and S. Walton, “Firm Use of Cybersecurity Risk Disclosures,” *Journal of Information Systems*, vol. 36, no. 1, pp. 151–180, Mar. 2022, doi: 10.2308/ISYS-2020-067.
- [31] N. H. Nik Zulkipli and G. B. Wills, “An Exploratory Study on Readiness Framework in IoT Forensics,” in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 966–973. doi: 10.1016/j.procs.2021.01.086.
- [32] T. Rochmadi, A. Fadlil, and I. Riadi, “Tinjauan Pustaka Sistematis: Tantangan dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital,” *CyberSecurity dan Forensik Digital*, vol. 7, no. 2, pp. 81–89, Dec. 2024, doi: 10.14421/csecurity.2024.7.2.4861.
- [33] A. Singh, R. A. Ikuesan, and H. Venter, “Secure Storage Model for Digital Forensic Readiness,” *IEEE Access*, vol. 10, pp. 19469–19480, 2022, doi: 10.1109/ACCESS.2022.3151403.
- [34] S. Friedl and G. Pernul, “IoT Forensics Readiness - influencing factors,” Jun. 01, 2024, *Elsevier Ltd*. doi: 10.1016/j.fsidi.2024.301768.
- [35] M. M. H. S. V. Sheunesu, R. K. Victor, A. I. Richard, and M. K. Nickson, “Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic

- Readiness Purposes,” *IEEE Xplore*, pp. 200–205, May 2020, doi: 10.1109/IIoT48696.2020.9089494.
- [36] ISACA, *COBIT 2019 Framework: Introduction and Methodology*. Schaumburg: ISACA, 2019.
- [37] S. L. Lambert, K. Agnew, T. N. A. Fezzey, and J. H. Batchelor, “Delineating Responsibilities for COBIT 2019 IT Control Activities Between Cloud Service Providers and Cloud Service Users,” *Journal of Emerging Technologies in Accounting*, pp. 1–19, May 2025, doi: 10.2308/JETA-2023-063.
- [38] E. Marlina, A. N. Hidayanto, and B. Purwandari, “Towards a model of research data management readiness in Indonesian context: An investigation of factors and indicators through the fuzzy delphi method,” *Libr Inf Sci Res*, vol. 44, no. 1, Jan. 2022, doi: 10.1016/j.lisr.2022.101141.
- [39] J. Landeta and A. Lertxundi, “Quality indicators for Delphi studies,” *Futures and Foresight Science*, vol. 6, no. 1, pp. 3–11, Oct. 2023, doi: 10.1002/ffo2.172.
- [40] S. Chhina, M. Chadhar, S. Firmin, and A. Tatnall, “The Role of Actors in Blockchain Adoption Decisions – An Innovation Translation Perspective,” *Australasian Journal of Information Systems*, vol. 27, pp. 1–26, Dec. 2023, doi: 10.3127/ajis.v27i0.4489.
- [41] D. R. Lombardi, M. Kim, J. C. Sipior, and M. A. Vasarhelyi, “The increased role of advanced technology and automation in audit: A delphi study,” *International Journal of Accounting Information Systems*, vol. 56, p. 1, Dec. 2025, doi: 10.1016/j.accinf.2025.100733.
- [42] M. Elyas, A. Ahmad, S. B. Maynard, and A. Lonie, “Digital forensic readiness: Expert perspectives on a theoretical framework,” *Comput Secur*, vol. 52, pp. 70–89, Jul. 2015, doi: 10.1016/j.cose.2015.04.003.
- [43] F. Hasson, S. Keeney, and H. McKenna, “Research guidelines for the Delphi survey technique,” *J Adv Nurs*, vol. 32, no. 4, pp. 1008–1015, Apr. 2020, doi: 10.1046/j.1365-2648.2000.t01-1-01567.x.
- [44] C. Okoli and S. D. Pawlowski, “The Delphi method as a research tool: An example, design considerations and applications,” *Information and Management*, vol. 42, no. 1, pp. 15–29, Mar. 2004, doi: 10.1016/j.im.2003.11.002.
- [45] L. L. Davis, “Instrument review: Getting the most from a panel of experts,” *Applied Nursing Research*, vol. 5, no. 4, pp. 194–197, 1992, doi: [https://doi.org/10.1016/S0897-1897\(05\)80008-4](https://doi.org/10.1016/S0897-1897(05)80008-4).
- [46] Id-SIRTII/CC – BSSN, “Lanskap Keamanan Siber Indonesia,” 2024. Accessed: Oct. 01, 2024. [Online]. Available: <https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanaan-Siber-Indonesia-2023.pdf>
- [47] S. J. Lee and G. B. Kim, “K-FFRaaS: A Generic Model for Financial Forensic Readiness as a Service in Korea,” *IEEE Access*, vol. 9, pp. 130094–130110, 2021, doi: 10.1109/ACCESS.2021.3114233.
- [48] F. I. Fagbola and H. Venter, “Smart Digital Forensic Readiness Model for Shadow IoT Devices,” *Applied Sciences (Switzerland)*, vol. 12, no. 2, Jan. 2022, doi: 10.3390/app12020730.