SHM PUBLISHER
SURYA HIJAU MANFAAT

Journal of Information System Exploration and Research

https://joiser.shmpublisher.com

p-ISSN 2964-1160 | e-ISSN 2963-6361

Evaluation of the Implementation of Digital Forensic Readiness at the Managerial Level (a Study of Policy, Competencies, Risks, and Incidents)

Tri Rochmad[1,2*], Abdul Fadlil[3], Imam Riadi[4], Heni Inayatul Arifah[5], Dadang Heksaputra[6]
[1]*Department of Informatics Universitas Ahmad Dahlan, Indonesia*
[2,5,6]*Department of Information System, Universitas Alma Ata, Indonesia*
[3]*Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia*
[4]*Department of Information System,Universitas Ahmad Dahlan, Indonesia*

DOI: https://doi.org/10.52465/joiser.v4i2.06
Received 26 May 2026; Accepted 19 June 2026; Available online 21 June 2026

Article Info

Keywords:
Evaluation
Readiness
Managerial Level
COBIT 2019
Digital Forensic

Abstract

Indonesia's rapid digital transformation has improved efficiency, accuracy, performance, and accessibility across sectors, but has increased the complexity of cyberattacks. A 2023 BSSN report recorded more than 603 million cyberattacks, highlighting the need for stronger cybersecurity resilience. Digital Forensic Readiness (DFR) is essential to ensure organizations identify, preserve, and manage digital evidence during incidents. This study evaluates DFR in universities using the COBIT 2019 framework. A convergent mixed-methods design involved 10 IT managers or department heads from private universities in Yogyakarta. Questionnaire responses were converted into capability indices from 0 to 5 using weighted frequencies, while interview data were analyzed thematically and integrated with quantitative findings. The results show most processes at capability level 3, although capability varied across institutions and components. Interviews revealed several reported capabilities were based on operational practices not formalized through written policies, standardized procedures, competencies, or evidence-preservation mechanisms. These findings emphasize interpreting capability scores alongside qualitative evidence and conducting context-specific improvements.

1. Introduction

Large-scale digital transformation has been implemented in many countries, including Indonesia [1]. This digital transformation has had significant impacts, such as improved accuracy, efficiency,

* ***Corresponding Author:***

Tri Rochmadi,
Department of Informatics, Department of Information System,
Universitas Ahmad Dahlan, Universitas Alma Ata,
South Ringroad Road, Kragilan, Tamanan, Banguntapan District, Bantul Regency, Indonesia.
Email: trirochmadi@almaata.ac.id

performance, and accessibility across various sectors, ranging from finance, the economy [2], trade, security, transportation, agriculture, to education [3]. Consequences have emerged alongside these positive impacts, namely an increase in the number and complexity of cyberattacks [4], including phishing [5]. This phenomenon underscores the importance of optimal cybersecurity resilience to protect information systems from harmful impacts [6].

Digital forensics plays a crucial role in the collection of digital evidence [7]. Organizations need to have digital forensic readiness a state in which systems, policies, and personnel are pre-prepared to effectively collect and manage digital evidence in the event of an incident [8]. Albugmi's research on the Digital Forensic Readiness Framework (DFRF) to Secure Database Systems demonstrates that forensic readiness can protect database systems through structured digital evidence management policies that are ready for use when an incident occurs [9]. Meanwhile, research by Nugroho, Briliyant, and Sunaringtyas emphasizes the importance of policy components and human resource (HR) readiness in supporting digital forensic investigations in the public sector [10].

Zulkipli and Wills also highlight forensic readiness in the Internet of Things (IoT) environment, requiring strong policies and managerial competencies to ensure evidence is managed effectively [11]. Overall, all the above studies indicate that while many DFR models have been developed, they have not yet been widely adopted in practice within organizations [8]. This situation results in many organizations failing to handle cyber incidents effectively.

Digital forensics is no longer merely a technical domain but an integral part of business strategy and management [12]. Integrating digital forensics enables organizations not only to investigate cyber incidents but also to support regulatory compliance, strengthen organizational resilience, and ensure business continuity amid increasingly complex threats [13]. This makes digital forensics a proactive tool aligned with both cybersecurity strategies and organizational objectives. Therefore, continuous evaluation of digital forensics readiness is necessary to determine whether its implementation is truly effective.

Previous research by Rochmadi, Fadlil, and Riadi found that the use of the Control Objectives for Information and Related Technologies (COBIT) 2019 framework remains limited and is still rarely used to measure an organization's maturity level in implementing DFR [14]. The objective of this study is to identify and analyze the application of digital forensic readiness at the managerial level using COBIT 2019. The results of this study are expected to provide actionable insights for organizational managers, as well as highlight effective strategies for integrating digital forensics into business management and enhancing cybersecurity resilience.

2. Literature Review

To provide a deeper understanding of the concepts discussed, the following subsections present several relevant theories.

2.1. Digital forensic readiness

Digital forensic readiness is a proactive approach aimed at ensuring organizations can respond quickly and efficiently to cybersecurity incidents [15]. DFR provides organizations with a competitive advantage in addressing threats through information security risk management. On the other hand, this readiness also supports regulatory compliance, reputation protection, and the enhancement of overall system security [15]. In conclusion, DFR is no longer an option but a strategic necessity that must be implemented by organizations seeking to survive and thrive.

2.2. COBIT 2019 framework

COBIT 2019 is a best-practice framework that helps organizations manage technology and information more effectively and efficiently [16]. It has two focus areas: governance [17] and IT management [18]. COBIT covers 40 IT processes grouped into 5 domains [19], namely EDM [20], APO, BAI [21], DSS [22], and MEA [23]. The process capability level is used to measure the level of IT maturity within an enterprise [24]. The calculation formula is as follows for calculating the summary of respondents' answers:

$$RK = \frac{C}{\sum R} \times 100\% \quad (1)$$

where:

RK : Summary of questionnaire respondents' answers

C : Frequency of responses for each level from 0 to 5 for each process activity

$\sum R$: Total number of respondents

Calculating the capability level

$$AK = \frac{(RK \times L0)+(RK \times L1)+(RK \times L2)+(RK \times L3)+(RK \times L4)+(RK \times L5)}{100} \quad (2)$$

where:

AK : Capability value

RK : Summary of respondents' answers

L : Levels 0 through 5

Questionnaire responses were converted into decimal capability indices using six ordinal categories from level 0 to level 5. Calculation results are categorized based on capability levels [25].

1. Level 0 (0.00 – 0.99; Incomplete Process): The process does not yet exist or is not functioning properly.
2. Level 1 (1.00 – 1.99; Performed Process): The process has been implemented, but documentation is still minimal.
3. Level 2 (2.00 – 2.99; Managed Process): The process is documented and managed, but does not yet have established standards.
4. Level 3 (3.00 – 3.99; Established Process): The process has clear standards and is consistently implemented.
5. Level 4 (4.00 – 4.99; Predictable Process): The process is systematically monitored and measured.
6. Level 5 (5.00; Optimizing Process): The process is in a state of continuous improvement to enhance quality.

3. Method

This study employed a convergent mixed-methods design in which quantitative questionnaire data and qualitative interview data were collected from the same participants during the same research phase. The two datasets were analyzed independently and were then integrated during interpretation. The questionnaire provided standardized COBIT 2019 capability indices, whereas the interviews explained the organizational practices, constraints, and contextual conditions underlying those indices. The research flowchart is shown in Figure 1.

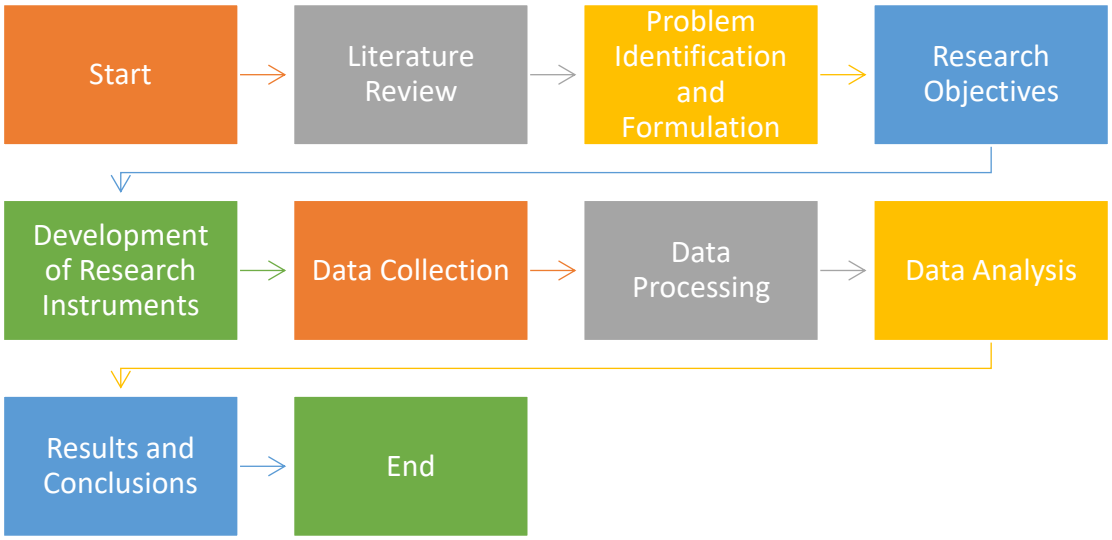

Figure 1. Stage of research

3.1. Data Collection

Data collection in this study employed three methods, categorized based on data sources: primary and secondary. Primary data was obtained directly from the field through interviews and questionnaires [26]. Secondary data, meanwhile, was obtained from literature reviews related to the research topic [27].

3.2. Data Analysis

Each questionnaire response was coded from 0 to 5 according to the capability anchor selected by the respondent. Frequencies were calculated for every component, converted into a weighted decimal capability index, and summarized at institution and regional levels. The expected level was set at 5; therefore, the capability gap was obtained by subtracting the current decimal index from 5.

Qualitative interview data were analyzed thematically through familiarization with the responses, initial coding, grouping related codes, reviewing the resulting themes, and selecting representative quotations. The analysis generated four themes: incident experience; written policies and procedures; technology, infrastructure, and security; and post-incident evaluation and learning.

Mixed-method integration was performed through a component-level side-by-side comparison. Interview themes and quotations were mapped to the four quantitative components policies, staff competence, risk and security management, and incident management. Qualitative evidence was not added numerically to the capability score; instead, it was used to confirm, explain, or challenge the interpretation of the questionnaire result. Convergent evidence strengthened the interpretation, whereas divergence was treated as an indication that a reported process might exist operationally but had not yet been consistently formalized, documented, or verified.

3.3. Research Instruments

A total of 16 manager-level instruments were adopted from the Delphi-validated study, "Developing a Delphi-Validated Instrument for Assessing Digital Forensics Readiness Based on COBIT 2019" [14]. The items were grouped into four components: (1) policies, regulations, and compliance; (2) staff competence and shared awareness; (3) risk and security management; and (4) incident management and investigation. Each activity statement used a six-point capability response from 0 to 5, following the anchors described in Section 2.2. The validated source instrument originally contained 40 instruments distributed across the IT director, IT manager, and IT staff levels; only the 16 items relevant to managers were used in this study.

3.4. Respondents

The respondents in this study were managers or department heads in the IT units of 10 private universities in the Special Region of Yogyakarta (DIY). They were divided by district/city: Sleman had 4 (R1, R2, R3, and R4), Bantul had 3 (R5, R6, R7), and the City had 3 (R8, R9, and R10).

4. Results and Discussion

This section presents and discusses the findings of the study. The following subsection outlines the thematic analysis derived from the data.

4.1. Thematic Analysis

The thematic analysis is organized into several key themes, as presented in the following subsections.

4.1.1. Theme: Incident Experiences

The results show that the types of incidents were dominated by attacks on websites, such as, "..Web defacement/gacor slots occurred several times" (R1, R3, R4, and R5). Other threats included, "..E-learning hacking" (R10). Attacks based on user manipulation and network service disruption, namely "..Phishing, Social Engineering, and DDoS Attacks" (R6). The prevalence of website attacks and user manipulation indicates that the organization's attack surface remains quite extensive and is not yet optimally protected, particularly regarding public applications and user awareness. Incident response patterns remain technical and reactive, with the primary focus on system recovery.

Generally, incident handling involves log analysis and system recovery through system reinstallation, access restriction, and backup. The following statements align with this: "...log analysis"

(R1, R5), "...reinstallation" (R3), "...check logs, check database, restore backup" (R7). This pattern indicates that universities prioritize recovery over incident preparedness, leading to the neglect of aspects related to the preservation and integrity of digital evidence. This situation increases the risk of losing critical digital evidence trails essential for forensic investigations and legal proceedings. Key challenges in incident handling include limited human resources (HR), weak regulations, limited technology, and the complexity of attacks. The following statements align with this: "...Lack of HR in the field of cybersecurity" (R1), "...HR readiness" (R2), "...Lack of forensic experts" (R6), "...Forensic tools" (R10), "...No regulations yet" (R3). "...Massive, coordinated attacks" (R8). This pattern indicates a structural gap in digital forensic readiness, where technological limitations not only impact the ability to respond to incidents but also hinder the development of sustainable security systems.

4.1.2. Theme: Written Policies and Procedures

The results indicate that the majority of universities do not yet have written policies or procedures. The following statements reflect this: "...Nothing has been put in writing" (R2, R3), as well as "...We have never formulated them in writing" (R4). "...No" (R7, R10). Only two universities have comprehensive and standardized written policies. The absence of these formal policies indicates that information security governance, particularly regarding digital forensics, has not yet become a strategic priority for universities. Without written policies, organizations lack standardized guidelines to reference in incident management, which may weaken organizational accountability. Meanwhile, team readiness varies significantly. Some universities stated they are operationally ready, while others are still at a minimal readiness level or are not yet ready. The following statements align with this: "...The team is ready at all times to receive incident notifications and is prepared to handle incidents according to their respective duties" (R1), "...Ready for on-call alerts" (R10). This indicates that the university's readiness is not yet supported by a measurable system and remains dependent on the readiness of individuals or teams. Universities tend to be better prepared to handle incidents and can be objectively measured, supported by concrete indicators such as those stated: "...The team has operational readiness, such as clear SOPs, availability of basic forensic tools, and routine training to handle incidents" (R6), "...Training and product security POCs" (R4). Some respondents provided answers reflecting that readiness is still a matter of subjective perception, such as "...Logically, we are ready" (R2), "...Spontaneous" (R3).

This results in readiness assessments being based more on assumptions than on measurable performance indicators. Meanwhile, three other respondents stated they were not yet ready. Of the ten respondents, two have established collaborations with external parties such as law enforcement or national authorities in the field of cybersecurity. On the other hand, the implementation of security standards has not yet become a common practice for the majority of universities; only three universities have adopted national or international security standards. The following statements align with this: "..SNI" (R8), "..ISO/IEC 27001" (R6), and "..ISO 270001" (R10). Technical security standards include "..Subscription to security firewall products" (R4) and "..Firewall usage standards" (R5). The low adoption of these standards indicates that organizations do not yet have a structured framework for managing information security. Meanwhile, others reported that no such standards exist. Overall, this situation indicates that digital forensics readiness is still in its early stages and requires strengthening in the areas of policy, standards, and collaboration.

The absence of written policies not only impacts operational aspects but also has significant strategic implications. Without formal policies, organizations lack a legal and procedural foundation for handling incidents, which can compromise the validity of digital evidence in legal proceedings. Additionally, this situation hinders process standardization, leading to inconsistent incident responses across units or individuals. From an IT governance perspective, the absence of policies indicates that digital forensics has not been integrated into the organization's risk management framework. This potentially increases exposure to cyber threats, as the organization lacks clear control mechanisms. These findings reinforce the argument that digital forensics readiness must begin at the policy level, not just the technical aspects. Thus, the development of written policies is a fundamental step in elevating the organization's capability to a higher level.

4.1.3. Theme: Technology, Infrastructure, and Security

The results show that a common pattern emerging is that most universities do not yet have forensic tools, while others rely on a combination of network security devices and basic log analysis tools. The following statements reflect this: "...None yet" (R3), "...None" (R7), and "... None yet, only open-source

applications" (R2), "..Text editor" (R5), "..Log analysis" (R10), "..Firewall devices" (R4, and R6). This indicates that the use of digital forensic technology is still in its early stages and has not yet become part of an integrated security infrastructure. Reliance on basic tools such as basic logs and text editors has the potential to hinder the evidence identification process if incidents are more complex and in-depth. Another respondent stated that they use an integrated security monitoring platform such as, "..Wazuh" (R1).

The limited use of forensic tools highlights a gap between operational needs and the organization's technological capabilities. Reliance on simple tools like text editors and basic logs indicates that the investigation process does not yet meet adequate forensic standards, particularly regarding the preservation of the integrity and chain of custody of digital evidence. Conceptually, this places the organization at high risk during further investigations, especially if the case proceeds to a legal context. Additionally, the low adoption of tools reflects a lack of investment and prioritization in the security domain. This reinforces the finding that digital forensic readiness cannot be separated from adequate technological infrastructure readiness.

4.1.4. Theme: Post-Incident Evaluation and Learning

The results indicate that incident handling is viewed as a strategic source of learning for enhancing both capacity and security awareness. The following statements align with this: "..The more frequently we experience incidents and strive to handle them, the more knowledge and skills we gain" (R1). "..We must truly safeguard the privacy of data" (R2), "..The importance of backups" (R5), and ".. "Forensic SOPs need to be updated periodically to ensure a more effective response" (R6), "...No system is safe & the importance of security awareness" (R8), "...We must always stay updated on information regarding security vulnerabilities" (R9), "...Tracking & tracing" (R10). The majority of universities have not utilized incidents as a means to improve policies, technology, or post-incident procedures, consistent with the statements, "..None yet" (R2, R3, R7), and "..No" (R10). This situation indicates that the organizational learning cycle is not functioning optimally, particularly during the evaluation stage and the integration of learning outcomes into formal policies and procedures. This situation risks the potential for the capacity derived from incident experiences to remain underutilized and may lead to the recurrence of the same incident patterns.

Meanwhile, other respondents noted changes in technological aspects. Relevant statements include, "Updating security devices" (R4), and "Strengthening website and server security (hardening)" (R8). Improvements to security operational procedures were also implemented, such as, "...Enhancing monitoring systems, tightening access controls, and adding evidence preservation measures" (R6). This indicates that some universities have begun moving toward adaptive learning, although this remains limited to technical and operational aspects.

4.2. Capability Level Analysis

The capability level analysis is further detailed by examining variations across regions, as presented in the following subsection.

4.2.1. Capability Level Analysis by Region

The results of the capability calculations for each component form the basis for determining the current capability level. Table 1 shows the capability levels by region.

Table 1. Capability levels by region

Region			
Components	Sleman	Bantul	Kota
Policies, Regulations, and Compliance	3.44	3.50	2.42
Staff Competence and Shared Awareness	3.25	3.44	2.11
Risk and Security Management	3.06	3.58	2.50
Incident Management and Investigation	3.50	3.33	2.27

Based on the Table 1, it is evident that the Sleman and Bantul regions have consistent scores; all four components are at capability level 3 with an "established process" status. Meanwhile, Kota is at capability level 2 for all components with a "managed process" status.

4.2.2. Analysis of Capability Levels by University

Capability levels by university are shown in Table 2.

Table 2. Capability levels by university

CODE	Components			
	Policies, Regulations, and Compliance	Staff Competence and Shared Awareness	Risk and Security Management	Incident Management and Investigation
R1	3.50	2.67	3.00	3.80
R2	4.00	4.33	4.25	4.00
R3	3.00	3.00	2.00	2.60
R4	3.25	3.00	3.00	3.60
R5	2.22	2.33	3.00	2.20
R6	4.00	5.00	4.00	4.20
R7	4.25	3.33	3.75	3.60
R8	4.25	4.00	4.00	3.80
R9	2.25	1.00	2.00	1.20
R10	2.25	1.33	1.50	1.80

Based on the table above, it is evident that the proficiency levels for each component among the 10 respondents vary. The highest score for the policy, regulations, and compliance component was achieved by two respondents (R7 and R8), who both scored 4.25. This was followed by the human competence and shared awareness component, which scored 5.00 under the “optimizing process” condition (R6). The risk and management security component also received a high score of 4.25. Finally, the incident management and investigation component had the highest score of 4.20 (R6).

4.2.3. Integration of Qualitative and Quantitative Findings

The two datasets were integrated by comparing each questionnaire-derived component score with the corresponding interview themes. This comparison revealed both convergence and divergence, thereby providing a more cautious interpretation of the decimal capability values.

Policies, regulations, and compliance. The quantitative results suggest that several universities operated at managed, established, or predictable capability levels. However, interview statements such as “nothing has been put in writing” and “we have never formulated them in writing” show that operational practices were not always supported by formal policies or standardized procedures. This divergence indicates that respondents may have rated the existence of routine practices, whereas COBIT level 3 also requires consistent institutionalization and documentation.

Staff competence and shared awareness. The wide quantitative range, from level 1 to level 5, is consistent with the qualitative evidence. Statements regarding limited cybersecurity personnel, the absence of forensic experts, and readiness based on spontaneous or individual action explain the lower scores. Conversely, references to routine training, operational readiness, and clear responsibilities support the higher scores. The qualitative findings therefore confirm that competence maturity differs substantially across universities.

Risk and security management. Higher capability results were generally supported by evidence of security standards, firewalls, Wazuh, monitoring, and periodic strengthening of systems. Lower results were associated with the absence of forensic tools or reliance on basic logs and text editors. The interviews complement the scores by showing that the presence of preventive security controls does not automatically ensure forensic evidence preservation, chain-of-custody procedures, or investigation readiness.

Incident management and investigation. Capability values around level 3 indicate that incident-handling processes exist in several universities. Nevertheless, the interviews show that responses remain predominantly reactive and recovery-oriented, including reinstallation, access restriction, log checking, and backup restoration. Limited attention to evidence integrity and preservation explains why an institution may report an established incident-response process while still having incomplete digital forensic readiness. Thus, the qualitative findings contextualize the scores and prevent capability values from being interpreted as direct proof of fully implemented forensic practices.

4.3. Gap Analysis

The gap analysis based on Level 5 expectations is grounded in the university's commitment to optimizing its management capabilities.

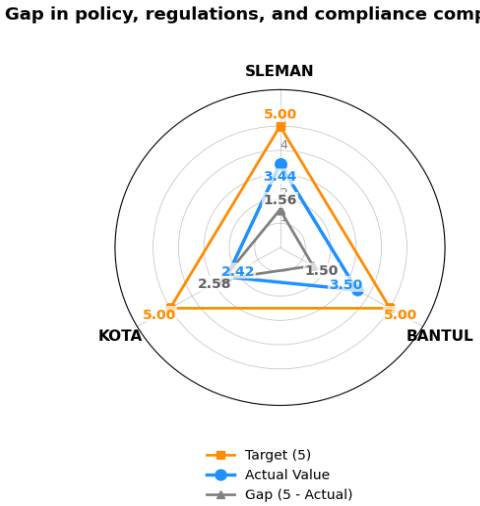

Figure 2. Gap in policy, regulations, and compliance components

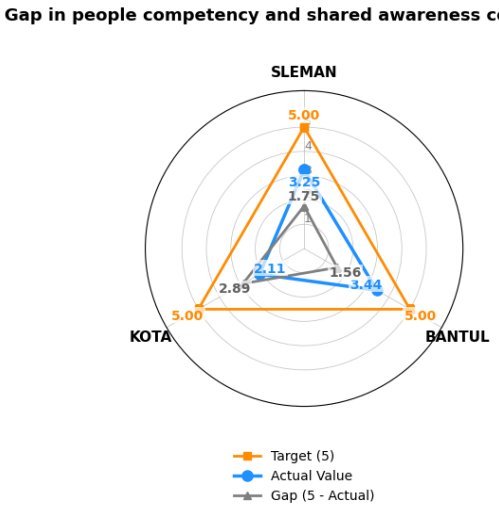

Figure 3. Gap in people competency and shared awareness components

As shown in Figure 2, Bantul has the smallest policy, regulation, and compliance gap at 1.50, followed by Sleman at 1.56, whereas Kota has the largest gap at 2.58. Figure 3 shows that Bantul has the smallest staff competence and shared awareness gap at 1.56, followed by Sleman at 1.75, while Kota has the largest gap at 2.89. Thus, Kota requires the greatest improvement priority for both components.

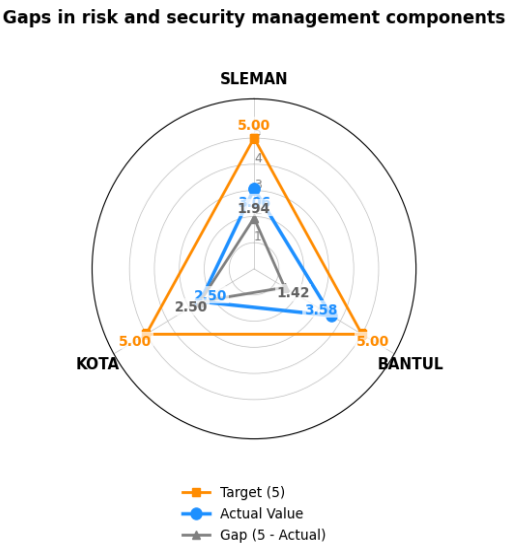

Figure 4. Gaps in risk and security management components

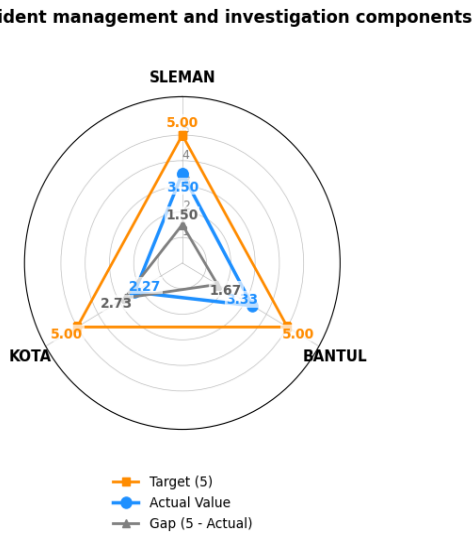

Figure 5. Gaps in incident management and investigation components

Based on Figure 4, Bantul has the smallest risk and security management gap at 1.42, followed by Sleman at 1.94, while Kota has the largest gap at 2.50. Figure 5 shows that Sleman has the smallest incident management and investigation gap at 1.50, followed by Bantul at 1.67, whereas Kota has the largest gap at 2.73.

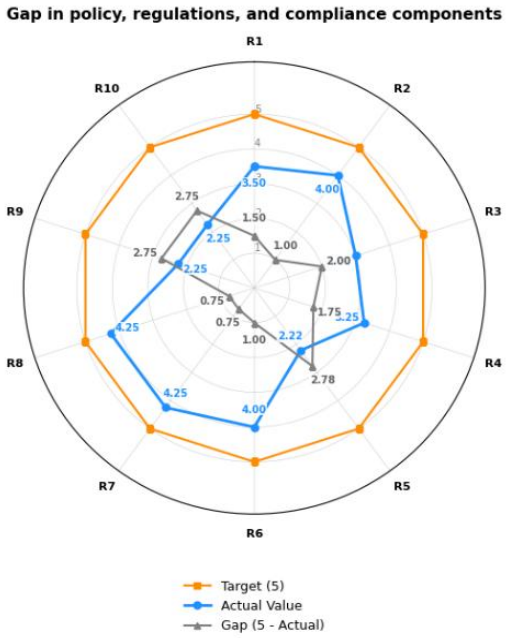

Figure 6. Gaps in policy, regulations, and compliance

Figure 7. Gaps in personnel competencies and shared awareness

As shown in Figure 6, R7 and R8 have the smallest policy, regulation, and compliance gaps at 0.75, followed by R2 and R6 at 1.00. R5 has the largest gap at 2.78, followed closely by R9 and R10 at 2.75. Figure 7 shows that R6 has reached level 5 in staff competence and shared awareness, producing a gap of 0.00, whereas R9 has the largest gap at 4.00, followed by R10 at 3.67.

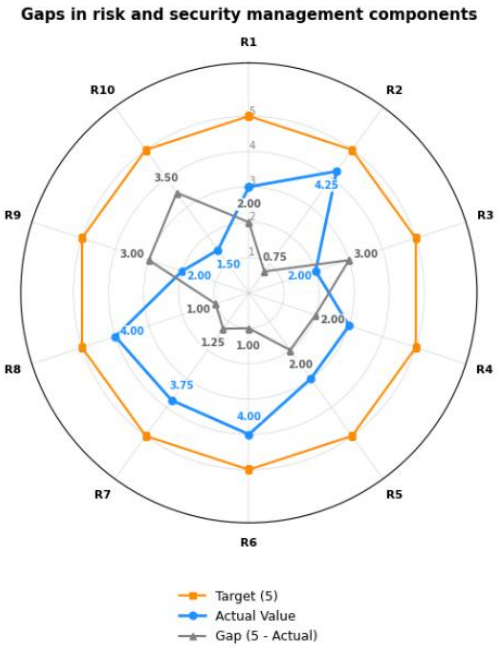

Figure 8. Gaps in risk and security management components

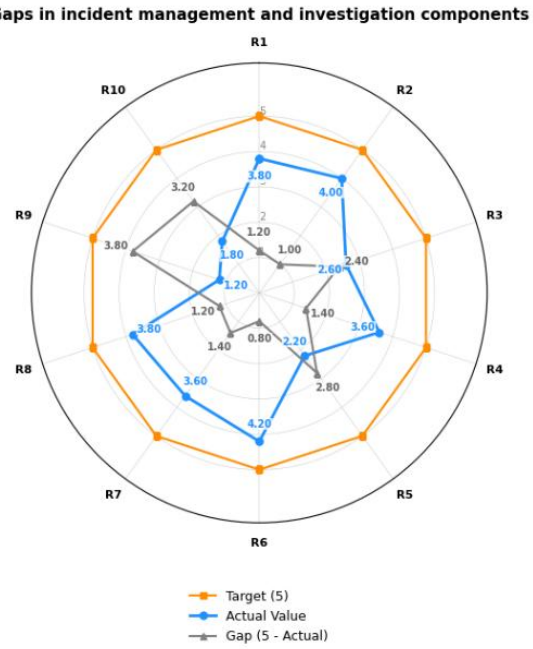

Figure 9. Gaps in incident management and investigation components

As shown in Figure 8, R2 has the smallest risk and security management gap at 0.75, followed by R6 and R8 at 1.00 and R7 at 1.25. R10 has the largest gap at 3.50. Figure 9 shows that R6 has the smallest incident management and investigation gap at 0.80, followed by R2 at 1.00, R1 and R8 at 1.20, and R4 and R7 at 1.40. R9 has the largest gap at 3.80.

4.4. Recommendation

Based on the research findings, there are significant differences in readiness levels across regions for all four components. A comparison of component capability levels by region is shown in Figure 10.

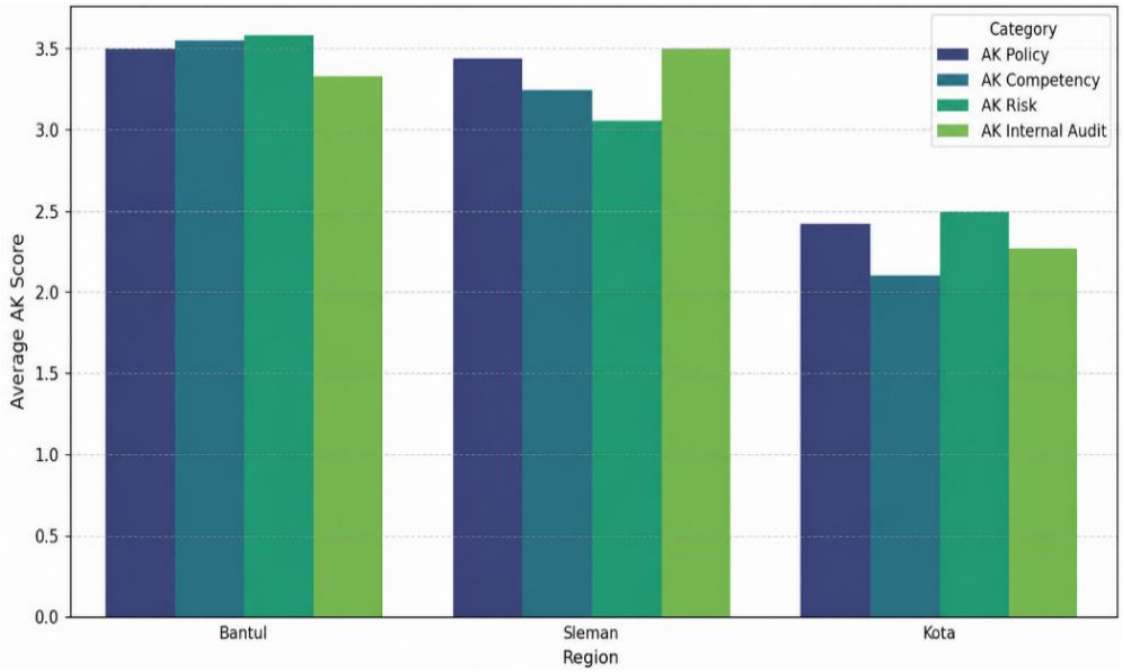

Figure 10. Comparison chart of component capability levels by region

Differences in capability levels across regions not only reflect numerical variations but also indicate structural disparities in IT governance and digital forensic readiness. The higher values observed in the Bantul region can be interpreted as the result of a combination of organizational factors, such as the level of managerial commitment, the presence of more formal SOPs, and the potential for more targeted allocation of IT resources. This finding is consistent with the literature stating that the success of Digital Forensic Readiness implementation is heavily influenced by management support and organizational policy readiness. Conversely, the low capability level in Yogyakarta City indicates that readiness has not yet become a strategic priority for the organization. This is likely related to resource constraints, both in terms of human resources and the IT budget. Additionally, the absence of written policies and low adoption of security standards indicate a weak governance structure. In the context of COBIT 2019, this condition reflects an organization still at the "managed process" stage, where processes are in place but not yet standardized and not systematically measured.

These differences may also be influenced by the size and complexity of the organization. Larger universities tend to have more mature IT structures, including clear role definitions and investments in security. Conversely, smaller organizations tend to rely on ad-hoc and reactive approaches. Therefore, the capability level reflects not only technical conditions but also the maturity of governance and organizational culture regarding information security.

The following are recommendations to support the achievement of the desired capability level, including, as shown in Tables 3, 4, 5, and 6:

Table 3. Recommendations for policy, regulatory, and compliance components by region

Policies, Regulations, and Compliance	
Code	Recommendations
R1	Formalize existing processes into written SOPs based on recognized standards (ISO/IEC 2001/SNI)
R2	The top priority is to develop and implement written policies and SOPs for digital forensic incidents
R3	Develop a foundational policy framework, including SOPs
R4	Convert training activities into formal, documented SOPs, and incorporate compliance evaluation mechanisms and internal audits
R5	Develop foundational security and digital forensics policies and procedures, and conduct training for human resource development
R6	Advance to the optimization phase by conducting periodic external audits to validate compliance
R7	Establish foundational policies and SOPs for digital forensic incidents; enhance capabilities through training and incident simulations
R8	Document technical practices into formal policies and SOPs integrated with SNI standards
R9	Build a solid foundation for policies, SOPs, and security team structures
R10	Align team readiness with written policies and SOPs based on ISO 27001

Table 4. Recommendations for Personnel Competencies and Awareness Standards

Personnel Competencies and Awareness Standards	
Code	Recommendations
R1	Conduct forensic training programs based on real-world cases
R2	Strengthen competencies through advanced technical training. Expand forensic tools (beyond basic open-source solutions)
R3	Build a culture of learning from incidents and train teams not only to reach the recovery stage but also to conduct forensic analysis
R4	Incorporate training on new technologies to stay current
R5	Form a dedicated security team and strengthen the team's competencies
R6	Develop an internal monitoring program for workforce development. Make incident learning a foundational knowledge base
R7	Increase the intensity and depth of training from basic operations to forensic investigation
R8	Advance to an advanced level with in-depth forensic training and develop a security awareness program based on real-world experience
R9	Establish an IT team structure and conduct entry-level cybersecurity training

Personnel Competencies and Awareness Standards	
Code	Recommendations
R10	Conduct post-incident evaluations for continuous learning

Table 5. Recommendations for Risk and Security Management Components

Risk and Security Management	
Code	Recommendations
R1	Conduct periodic risk assessments for early detection
R2	Optimize risk management through predictive risk analysis
R3	Establish a basic IT risk management framework and implement basic controls such as restricted access, backups, and logging
R4	Strengthen risk mitigation through a combination of technologies (firewalls, IDS/IPS) and real-time monitoring
R5	Build a centralized monitoring system/SIEM. Strengthen internal controls through audits and evaluation of SOPs
R6	Optimize monitoring with real-time log monitoring
R7	Develop a risk awareness program across all units
R8	Develop a more proactive risk mitigation strategy
R9	Improve staff understanding of risk management and establish a basic monitoring system
R10	Identify IT risks and establish simple monitoring

Table 6. Recommended components of incident management and investigation

Incident Management and Investigation	
Code	Recommendations
R1	Ensure that every system change is documented and has an audit trail.
R2	Strengthen security-focused project management and establish a dedicated forensic team for each IT project.
R3	Identify forensic needs by creating a forensic readiness plan.
R4	Enhance collaboration with external parties (CSIRT/law enforcement).
R5	Develop foundational policies for incident response and digital forensic investigations.
R6	Conducting periodic evaluations of incidents and enhancing coordination into cross-university collaboration.
R7	Clarify specific digital forensic needs (tools, SOPs, and personnel).
R8	Integrate asset management with a centralized monitoring system.
R9	Build a solid foundation for policies, team structure, and investigation procedures. Seek external guidance to establish an initial system.
R10	Strengthen project management through the involvement of the security team.

5. Conclusion

Based on the assessment of 10 private universities in the Special Region of Yogyakarta across four components, capability values varied substantially among institutions. The highest score was 5.00 in the staff competence and shared awareness component for R6, whereas the lowest score was 1.00 for R9 in the same component. Overall, many results were located around capability level 3, indicating that relevant processes existed but were not always fully standardized, documented, measured, or routinely evaluated. The mixed-method integration clarifies that the questionnaire scores represent perceived process capability, while the interviews reveal the quality of actual implementation. In particular, universities sometimes reported established operational processes even though written policies, specialist personnel, forensic tools, evidence-preservation procedures, and post-incident learning mechanisms remained limited. This partial divergence should be considered when interpreting decimal capability scores. R6, R2, and R8 demonstrated comparatively strong readiness, whereas R9 and R10 required priority improvement in competence, awareness, risk management, and incident investigation. Periodic reassessment and context-specific recommendations are necessary, and future

research should include documentary verification, multiple respondents per institution, and comparison with complementary forensic-readiness frameworks.

References

[1] Syaban, Abdul, et al. 'Analisis Peningkatan Literasi Digital Dan Jiwa Kewirausahaan Pelaku Umkm Provinsi Sulawesi Tenggara Melalui Optimalisasi Platform Umkm. Academy.,' *Community Dev. J. J. Pengabdi. Masy.*, vol. 5, no. 6, pp. 12366-12375., 2024.

[2] R. P. Sari and J. Veri, "Pengaruh Digitalisasi Terhadap Ekonomi Sirkular: Systematic Literature Review," *eCo-Buss*, vol. 8, no. 1, pp. 842–864, Aug. 2025, doi: 10.32877/eb.v8i1.2954.

[3] A. V. Oktareza, D., Noor, A., Saputra, E., & Yulianingrum, "Transformasi Digital 4.0: Inovasi yang Menggerakkan Perubahan Global.," *Cendekia J. Hukum, Sos. dan Hum.*, vol. 2, no. 3, pp. 661–672, 2024, doi: 10.5281/zenodo.12742216.

[4] and A. N. K. Isadora, N. Putri Aqila, H. Gustina, "'Analisis Modus Phising terhadap Whatsapp,'" *J. Akuntansi, Bisnis dan Ekon. Indones.*, vol. 3, no. 2, 2024, [Online]. Available: https://akuntansi.pnp.ac.id/jabei

[5] T. Rochmadi *et al.*, "Pengukuran Kesadaran Keamanan Informasi UMKM terhadap Phising pada Aplikasi Whatsapp," *J. Tata Kelola dan Kerangka Kerja Teknol. Inf.*, vol. 12, no. 1, pp. 10–16, Apr. 2026, doi: 10.34010/jtk3ti.v11i3.18935.

[6] Muhamad Febrian Aska, Deo Pratama Putra, and C. J. M. Sinambela, "Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital," *J. Inform. Inf. Secur.*, vol. 5, no. 2, pp. 187–200, Jan. 2025, doi: 10.31599/fzg80847.

[7] A. Yudhana, I. Riadi, and R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," *J. Inform. J. Pengemb. IT*, vol. 7, no. 1, pp. 43–48, Jan. 2022, doi: 10.30591/jpit.v7i1.3639.

[8] T. Rochmadi, A. Fadlil, and I. Riadi, "Tinjauan Pustaka Sistematis: Tantangan Dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital," *Cyber Secur. dan Forensik Digit.*, vol. 7, no. 2, pp. 81–89, Dec. 2024, doi: 10.14421/csecurity.2024.7.2.4861.

[9] A. Albugmi, "Digital Forensics Readiness Framework (DFRF) to Secure Database Systems," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 2, pp. 13732–13740, Apr. 2024, doi: 10.48084/etasr.7116.

[10] H. A. Nugroho, O. C. Briliyant, and S. U. Sunaringtyas, "A Novel Digital Forensic Readiness (DFR) Framework for e-Government," in *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, IEEE, Aug. 2023, pp. 184–189. doi: 10.1109/ICoCICs58778.2023.10276423.

[11] G. B. Zulkipli, N. H. N., & Wills, "An exploratory study on readiness framework in IoT forensics.," *Procedia Comput. Sci.*, vol. 179, pp. 966–973, 2021.

[12] E. Dheanda Absharina and T. Sutabri, "ANALISIS MODEL DIGITAL FORENSIC READINESS INDEX (DiFRI) UNTUK MENCEGAH CYBERCRIME," *Blantika Multidiscip. J.*, vol. 1, no. 2, pp. 71–78, Feb. 2023, doi: 10.57096/blantika.v1i2.12.

[13] G. Odhiambo, R. Omollo, and P. Abuonji, "Towards Digital Forensic Readiness: A Framework for Financial Service Providers," *East African J. Inf. Technol.*, vol. 7, no. 1, pp. 92–107, Apr. 2024, doi: 10.37284/eajit.7.1.1897.

[14] I. Rochmadi, T., Fadlil, A., & Riadi, "Developing a Delphi Validated Instrument for Assessing Digital Forensics Readiness Based on COBIT 2019.," *Int. J. Adv. Data Inf. Syst.*, vol. 1, no. 2, 2025.

[15] R. Agung Firmansyah, Y. Prayudi, and A. Luthfi, "INTEGRASI DIGITAL FORENSIC READINESS DAN INFORMATION SECURITY MANAGEMENT SYSTEM PADA ORGANISASI PEMERINTAHAN: SYSTEMATIC LITERATURE REVIEW," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 2, pp. 2852–2863, Mar. 2025, doi: 10.36040/jati.v9i2.13126.

[16] A. Prasetyo, T. Ridwan, and A. Voutama, "ANALISIS SENTIMEN TERHADAP APLIKASI GBWHATSAPP MENGGUNAKAN NAIVE BAYES CLASSIFIER DAN RANDOM FOREST CLASSIFIER," *JSiI (Jurnal Sist. Informasi)*, vol. 11, no. 1, pp. 1–9, Mar. 2024, doi: 10.30656/jsii.v11i1.6936.

[17] I. P. Y. Putri, R. F. I., Noviana, L. P. R., & Bawantara, "Penerapan Prinsip Tata Kelola Teknologi Informasi Pada Himpunan Mahasiswa Teknologi Informasi Uin Ar Raniry Banda Aceh," *J. Manaj. Dan Teknol. Informasi,* vol. 13, no. 2, pp. 95–103, 2023.

[18] D. Chalvari, K., & Gunawan, "Analisis Manajemen Tata Kelola Teknologi Informasi Satuan Kerja Di Instansi XYZ Dengan Kerangka Kerja Cobit 2019.," *J. Cahaya Mandalika*, pp. 26–36, 2020.

[19] S. Salimuddin, M. Ula, and N. Nurdin, "ANALISIS KINERJA TATA KELOLA TEKNOLOGI INFORMASI

MENGGUNAKAN FRAMEWORK COBIT 2019 PADA UNIVERSITAS JABAL GHAFUR," *J. Inform. dan Tek. Elektro Terap.*, vol. 13, no. 2, Apr. 2025, doi: 10.23960/jitet.v13i2.6130.

[20] A. Wattimury, G., & Faza, "COBIT 2019 implementation for enhancing IT governance in educational institutions.," *JISKA (Jurnal Inform. sunan kalijaga)*, vol. 8, no. 3, pp. 210–221, 2023.

[21] E. Sahara, Fachruddin, and J. Devitra, "Audit Tata Kelola Teknologi Informasi Universitas Nurdin Hamzah Menggunakan Framework COBIT 2019," *J. Ilm. Media Sisfo*, vol. 19, no. 2, pp. 279–290, Oct. 2025, doi: 10.33998/mediasisfo.2025.19.2.2489.

[22] J. Suroto, S., & Friadi, "Pengukuran Tingkat Capability IT Governance pada PT. Sarana Citranusa Kabil Menggunakan Framework Cobit 2019," *J. Ilmu Siber dan Teknol. Digit.*, vol. 1, no. 2, pp. 81–90, 2022.

[23] A. M. Mirza, Y. Wirani, and Y. G. Sucahyo, "Analysis of Information Technology Governance Implementation in Consulting Firms Using the COBIT Framework Approach: A Literature Review," *Sebatik*, vol. 29, no. 1, pp. 23–34, Jun. 2025, doi: 10.46984/sebatik.v29i1.2610.

[24] H. Herianto and W. Wasilah, "Asesment Capability Level dan Maturity Level Tata Kelola TI Pada Kantor Kementerian Agama Kabupaten Pesawaran Provinsi Lampung Menggunakan Framework COBIT 2019," *KONSTELASI Konvergensi Teknol. dan Sist. Inf.*, vol. 2, no. 2, May 2022, doi: 10.24002/konstelasi.v2i2.5553.

[25] M. A. Solikhah, "Pengukuran Capability Level pada Sistem Informasi Akademik di STAI Kuningan Menggunakan COBIT 2019.," *J. Tek. Indones.*, vol. 3, no. 2, pp. 72-81., 2024.

[26] M. Sulung, U., & Muspawi, "Memahami sumber data penelitian: Primer, sekunder, dan tersier.," *Edu Res.*, vol. 5, no. 3, pp. 110–116, 2024.

[27] R. A. Febrianto, A., & Siroj, "Studi literatur: Landasan dalam memilih metode penelitian yang tepat.," *J. Educ. Res. Dev. E-ISSN 3063-9158*, vol. 1, no. 2, pp. 259-263., 2024.