Ingénierie des Systèmes d'Information
Vol. 31, No. 7, July, 2026, pp. 2301-2313
Journal homepage: http://iieta.org/journals/isi

Developing a Governance-Oriented Digital Forensic Readiness Framework for Higher Education Institutions: An Empirical Study Based on COBIT 2019

Tri Rochmadi[1,2*], Abdul Fadlil[1], Imam Riadi[1]

[1] Doctoral Program in Informatics, Universitas Ahmad Dahlan, Yogyakarta 55191, Indonesia
[2] Department of Information Systems, Universitas Alma Ata, Yogyakarta 55183, Indonesia

Corresponding Author Email: 2437083008@webmail.uad.ac.id

https://doi.org/10.18280/isi.310714

Received: 17 February 2026
Revised: 22 May 2026
Accepted: 30 June 2026
Available online: 31 July 2026

Keywords:
Digital Forensic Readiness, higher education institutions, information technology governance, COBIT 2019, cybersecurity governance, design science research

ABSTRACT

Digital Forensic Readiness (DFR) has become an important capability for higher education institutions, where decentralized information systems and diverse stakeholders create challenges for evidence preservation, incident response, and accountability. However, existing DFR frameworks are often technology-oriented or sector-neutral and provide limited guidance for integrating forensic readiness with institutional governance processes. This study proposes the Educational Digital Forensic Readiness Framework (EduDFR), a governance-oriented framework that integrates DFR principles with COBIT 2019 governance and management objectives for higher education institutions. An adapted Design Science Research approach was employed using empirical evidence collected from semi-structured interviews and questionnaires involving 18 information technology (IT) personnel from six accredited private universities in Yogyakarta, Indonesia. Thematic analysis identified six core components: Governance and Strategy; Policy, Regulation, and Compliance; People Competency and Security Awareness; Risk and Security Management; Incident Management and Investigation; and Technology and Infrastructure. The proposed framework was evaluated by seven experts using a four-point relevance scale and Aiken's V analysis. Results showed that all 40 framework items achieved acceptable content validity, with 30 items classified as highly valid and 10 items classified as valid, with coefficients ranging from 0.76 to 1.00. The findings demonstrate expert agreement on the framework structure rather than operational effectiveness. EduDFR offers a governance-aligned approach for organizing Digital Forensic Readiness responsibilities in universities and provides a foundation for future implementation and longitudinal evaluation.

1. INTRODUCTION

Higher education institutions increasingly depend on interconnected information systems for academic services, research, finance, human resources, and institutional administration. This dependence expands the attack surface and increases the consequences of ransomware, data leakage, account compromise, and unauthorized access [1-4]. Digital Forensic Readiness (DFR) is therefore essential not only to support post-incident investigation but also to ensure that potentially relevant evidence is identified, recorded, preserved, and governed before an incident occurs [5-9].

Conventional security controls such as firewalls, access controls, and intrusion detection systems (IDS) remain essential [10-12]. However, they do not automatically ensure that evidence is complete, legally defensible, and available when an investigation is initiated [9, 13-16]. A university may successfully contain an incident yet still lose volatile data, retain incomplete logs, or fail to preserve chain-of-custody information. DFR addresses this gap by linking preventive security, incident response, evidence management, and organizational accountability [17-20].

Implementing DFR in higher education is challenging because universities combine decentralized decision-making, academic autonomy, heterogeneous systems, external service providers, and large student and staff populations [21]. The empirical institutions in this research also reported uneven availability of trained personnel, formal procedures, centralized logging, and forensic tools. These characteristics indicate that a higher education DFR framework must address governance, policy, human capability, risk, incident processes, and infrastructure as an integrated information systems management problem rather than as a stand-alone technical function.

Existing DFR research has produced technical frameworks for databases, cloud computing, the Internet of Things (IoT), software-defined networks, and specialized infrastructures; governance-oriented frameworks for public organizations; and maturity models for assessing organizational capability [8, 9, 17, 19, 22-25]. These contributions are valuable, but they generally do not combine higher-education-specific empirical conditions with an explicit COBIT 2019 mapping, role-differentiated assessment indicators, and an implementation sequence that connects strategic decisions to evidence-preserving operations.

To address these gaps, this research develops the

Educational Digital Forensic Readiness Framework (EduDFR). EduDFR is not presented as a wholly new theory of digital forensics or information technology (IT) governance. Its novelty lies in the sector-specific configuration and operationalization of established DFR principles through COBIT 2019 governance and management objectives, empirical themes from six Indonesian universities, and 40 role-specific indicators for IT leaders, managers, and technical staff. The framework organizes six validated components into four implementation pillars: Strategic Forensic Governance, Policy and Human Foundation, Operational Control, and Technology and Infrastructure, supported by a forensic risk register and continuous improvement.

From an information systems perspective, EduDFR supports university IT managers by clarifying decision rights, policy ownership, resource allocation, vendor obligations, risk prioritization, service continuity, incident escalation, and performance monitoring. The research aims to (1) explain the conceptual distinction between EduDFR and previous DFR frameworks, (2) describe the integration of DFR factors with COBIT 2019 objectives, (3) validate the content and structure of the framework through expert assessment, and (4) provide an implementation-oriented interpretation without claiming real-world effectiveness that has not yet been empirically demonstrated.

2. LITERATURE REVIEW

2.1 Digital Forensic Readiness

DFR extends digital forensics from a reactive investigation activity into a proactive organizational capability [9, 26-29]. It is commonly defined as the ability to maximize the potential use of digital evidence while minimizing investigation cost and operational disruption [9, 26, 27]. This capability requires organizations to identify potential sources of evidence, establish lawful collection and retention practices, assign responsibilities, and maintain procedures before an incident occurs [22, 28, 29].

Contemporary DFR is socio-technical. Reliable tools and logs are necessary, but their evidential value depends on governance, policy, competent personnel, risk controls, documented incident procedures, and coordination across organizational units [22, 25, 26, 30]. Consequently, DFR contributes to information systems resilience, regulatory accountability, and service continuity by ensuring that security events can be reconstructed and evaluated using evidence whose integrity and provenance are maintained [23, 31].

Cyber incidents can generate financial, operational, reputational, and legal consequences [9, 23, 30-35]. Organizations without DFR may be subject to an attack but remain unable to determine what occurred, which assets were affected, whether personal data were exposed, or whether the collected evidence is admissible. Readiness, therefore, complements preventive cybersecurity by preparing the organization to preserve facts, support internal and external investigations, and learn from incidents through post-incident review [36, 37].

Higher education institutions require this broader interpretation because they manage academic, administrative, research, financial, and personal data through heterogeneous systems and distributed stakeholders. Their culture of openness, decentralized ownership, high user autonomy, and dependence on cloud or third-party services complicate evidence ownership, logging consistency, escalation, and privacy compliance [38].

Research on cybersecurity in higher education has primarily emphasized preventive controls, security policy, awareness, and institutional risk [1-4, 10, 11]. These areas are relevant to DFR, but they do not, by themselves, establish procedures for evidence identification, preservation, chain of custody, investigation coordination, or post-incident learning [39, 40]. The resulting gap supports the need for a contextual framework that connects forensic requirements with university information systems governance.

Accordingly, the present research treats DFR as an information systems governance capability: strategic direction defines the expected forensic outcomes; management processes translate these outcomes into policies, competencies, controls, and services; and operational technologies generate and protect the evidence required for investigation. This position provides the conceptual basis for integrating DFR with COBIT 2019.

2.2 Comparative analysis of existing Digital Forensic Readiness frameworks

Previous DFR research can be grouped into three broad categories. First, technical frameworks focus on evidence-producing environments such as databases, the IoT, software-defined networks, wireless medical networks, and other specialized infrastructures [5, 7, 8, 19, 20, 22, 24, 25, 41]. These studies strengthen logging, acquisition, filtering, preservation, and forensic-by-design mechanisms, but their applicability is often constrained by specific technologies or operational environments.

Second, governance-oriented frameworks extend DFR toward policy, compliance, ethical oversight, risk, and institutional accountability [23, 24, 42]. They demonstrate that readiness cannot be sustained by technical controls alone [23, 29]. However, frameworks developed for e-government, industry, or regulated organizational contexts do not directly address academic autonomy, decentralized information ownership, diverse university stakeholders, and resource constraints in higher education [43].

Third, maturity models provide structured levels for assessing organizational DFR capability [9, 17]. Their principal contribution is measurement and improvement planning. However, they are generally sector-neutral and do not prescribe a higher-education-specific integration among COBIT 2019 objectives, role-based assessment items, and practical incident workflows. The comparison in Table 1 shows that EduDFR builds on these contributions while addressing a different combination of context, governance integration, empirical grounding, and validation.

The comparison does not imply that previous frameworks are unsuitable in all university settings. Rather, it identifies limitations when they are transferred without adaptation. Technical frameworks can inform logging and evidence preservation; governance frameworks can inform accountability and compliance; and maturity models can inform assessment. EduDFR integrates these strengths into a sector-specific structure in which Strategic Governance, Policy and People, Operational Control, and Infrastructure are linked through explicit dependencies.

EduDFR is therefore an original framework at the level of

configuration, operationalization, and sectoral application, rather than a replacement for the underlying DFR and COBIT theories. Its distinctive value lies in translating validated COBIT 2019 objectives and university field evidence into 40 role-specific indicators and a four-pillar implementation architecture. This distinction clarifies both the contribution and the boundary of the proposed framework.

Table 1. Comparison of Educational Digital Forensic Readiness Framework (EduDFR) with selected technical, governance, and maturity-oriented Digital Forensic Readiness (DFR) frameworks

Framework / Research	Category	Objective and Core Components	Application Area	Validation or Evidence Base	Principal Limitation / Distinction
Bankole et al. [9]	Maturity model	Extends DFR readiness and maturity assessment to support improvement planning.	General organizational context	Model development and maturity-oriented evaluation.	Emphasizes measurement; higher education governance, role-based indicators, and incident workflow remain outside its main scope.
Englbrecht et al. [17]	Maturity model	Assesses organizational and infrastructure capability levels for DFR.	Cross-sector organizations	Literature-derived capability maturity model.	Provides a structured assessment but is sector-neutral and does not operationalize COBIT 2019 for university roles.
Kebande et al. [22]	Technical/holistic	Integrates organizational, legal, and technical readiness for IoT-enabled organizations.	IoT-enabled organizations	Conceptual synthesis of forensic readiness requirements.	Sector-specific to IoT and does not provide a higher education governance structure or a role-specific instrument.
Adel et al. [23]	Governance/ethics	Introduces ethical compliance and oversight principles for DFR.	General organizational context	Conceptual governance and compliance analysis.	Ethics-centered scope without an end-to-end higher education implementation structure.
Nugroho et al. [24]	Governance	Develops policy-oriented DFR governance for e-government using a plan, do, check, act (PDCA) structure.	Local government/e-government	Interviews, observation, document review, triangulation, and expert judgment.	Government-specific regulatory and organizational context; not designed for academic autonomy or university information systems.
Mpungu et al. [25]	Technical	Uses specialized logging and layered evidence management for wireless medical networks.	Wireless medical networks	Architecture assessed against forensic readiness and logging requirements.	Technology and network-specific; governance, university decision rights, and broad implementation dependencies are not central.
EduDFR (this study)	Sector-specific governance and operational framework	Integrates six components, 40 role-specific indicators, four implementation pillars, a forensic risk register, and continuous improvement through explicit COBIT 2019 objectives.	Higher education institutions	Empirical evidence from six Indonesian private universities and content validation by seven independent experts using Aiken's V.	Content validity is established; practical effectiveness, cross-country transferability, and long-term outcomes require further testing.

3. METHODOLOGY

3.1 Research design and framework development

This research adopted an adapted design science research process to develop and validate a contextual DFR artifact for higher education institutions. The process follows the framework development logic applied by Albugmi [8]: problem and requirement identification, artifact construction, expert evaluation, and refinement. The artifact in this research is the EduDFR, which combines theoretical DFR requirements, COBIT 2019 governance and management objectives, empirical university evidence, and expert assessment.

As shown in Figure 1, the research comprised four stages:

1. Problem identification and empirical data collection;
2. Framework construction through DFR, COBIT 2019 integration;
3. Content validation using Aiken's V expert assessment; and
4. Framework refinement and finalization.

The staged process supports traceability from the identified problem to the final framework. It also separates artifact development from validation: the empirical data and prior

Delphi research informed the framework content, whereas Aiken's V panel evaluated the relevance and feasibility of the resulting structure.

3.2 Data collection

Empirical data were collected from six purposively selected private universities in the Special Region of Yogyakarta, Indonesia. The inclusion criteria were: (1) a private higher education institution with university status known locally in Indonesia as Perguruan Tinggi Swasta (PTS); (2) an established IT management unit; (3) location in the Special Region of Yogyakarta; (4) university accreditation rated "Excellent" (Unggul); and (5) the university's willingness to participate. Selection was not based on the university's size, IT capability level, or system complexity. Geographic distribution across Yogyakarta City, Sleman Regency, and Bantul Regency was used to reduce concentration in a single locality.

Data were collected using two techniques: semi-structured interviews based on open-ended questions and evaluative questionnaires. The interviews explored existing incident-handling practices, policy conditions, personnel capabilities, risk controls, and technology support. The questionnaires provided structured evidence on the proposed readiness elements. No direct observation was used in this research. The instrument originated from DFR literature [5], COBIT 2019 design factors, and a previous three-round Delphi study [44].

The previous Delphi research involved a different panel from Aiken's V panel and produced 40 indicators after iterative refinement. The researcher conducted the coding and thematic grouping of the university responses. Interview responses were organized by university and role, coded for recurring readiness issues, and grouped into candidate themes. The grouping was then aligned with the structure of the Delphi-validated components, as reported by Rochmadi et al. [44]. Because a single researcher conducted coding, interpretive subjectivity is acknowledged as a methodological limitation.

3.3 Sampling and participants

The six universities provided contextual evidence for framework development rather than a statistically representative sample. Eighteen participants were involved: each university was represented by one IT unit leader or director, one manager or sub-division head, and one IT staff member. This role structure captured strategic, managerial, and operational perspectives. Table 2 presents the anonymized university profiles.

All universities were anonymized as PTS-1 to PTS-6. Although the universities were not selected to represent different organizational sizes, the participating IT units showed contextual variation in staffing levels, educational profiles, and dominant work experience. These differences support within-region contextual diversity, but they do not justify national or international generalization.

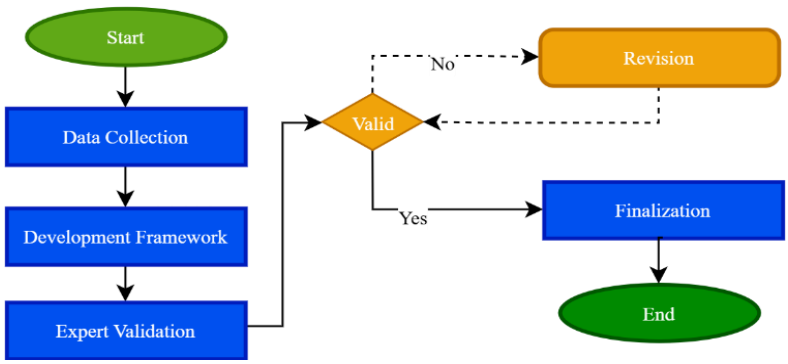

Figure 1. Research stages

Table 2. Anonymized profiles of the participating universities

Universities	Location	Number of Information Technology (IT) Personnel	Personnel Profile	Experience Pattern
PTS-1	Yogyakarta City	34	Leadership generally had higher formal education	IT unit leader or director > 5 years Manager or sub-division head > 5 years IT staff > 5 years
PTS-2	Sleman Regency	11	IT leader had higher formal education than several staff	IT unit leader or director > 5 years Manager or sub-division head > 5 years IT staff < 1 year
PTS-3	Sleman Regency	15	Leadership generally had higher formal education	IT unit leader or director > 5 years Manager or sub-division head > 5 years IT staff > 5 years
PTS-4	Sleman Regency	14	Comparable formal education across the IT unit	IT unit leader or director > 5 years Manager or sub-division head > 5 years IT staff > 5 years
PTS-5	Bantul Regency	6	IT leader had higher formal education than several staff	IT unit leader or director > 5 years Manager or sub-division head > 5 years IT staff 1 – 3 years
PTS-6	Bantul Regency	25	IT leader had higher formal education than several staff	IT unit leader or director > 5 years Manager or sub-division head > 5 years IT staff > 5 years

3.4 Aiken's V for framework validation

Content validation of EduDFR was conducted using Aiken's V, which quantifies expert agreement regarding item relevance [45-47]. The method was selected because the study evaluated the content and structure of a conceptual framework rather than testing causal relationships or implementation outcomes. The panel assessed whether each item was relevant and feasible for supporting DFR in higher education information systems.

The Aiken's V panel consisted of seven experts and was different from the seven-member Delphi panel used in the preceding instrument development research [44]. Experts rated each item using a four-point scale without a neutral midpoint, ranging from 1 (lowest relevance) to 4 (highest relevance), with intermediate scores indicating increasing relevance. The absence of a neutral category was intended to require a directional judgment [47].

Experts were selected using three criteria:

1. Demonstrated academic or professional expertise relevant to DFR;
2. At least five years of experience;
3. Direct involvement in information systems management, cybersecurity operations, digital investigations, or IT policy.

Seven experts met these criteria, comprising four academics and three practitioners with 8–25 years of experience. Their expertise covered digital forensics, incident response, cybersecurity, information security, network operations, cyber-physical systems, and IT governance, as detailed in Table 3.

Aiken's V was calculated for each of the 40 items. With seven raters and four response categories, the critical coefficient at the 0.05 significance level is 0.76. Items with V values from 0.76 to 0.86 were classified as Valid, whereas items with V values of 0.90 or higher were classified as Highly Valid. Items at or above the critical value were retained because they satisfied the prespecified content validity criterion [47, 48].

This procedure establishes content validity and expert agreement regarding the framework structure. It does not demonstrate that implementing EduDFR improves incident outcomes, evidence quality, or recovery performance in operational settings.

3.5 Data analysis

The analysis combined thematic synthesis and content validity assessment. First, the researcher coded the open-ended responses and grouped recurring issues into themes. Second, the themes were compared with the Delphi-validated 40-item instrument. Third, the proposed framework components were mapped to COBIT 2019 governance and management objectives. Finally, the framework was evaluated using Aiken's V.

Aiken's V was calculated using Eq. (1) [49]:

$$V = \frac{S}{n(c-1)} \tag{1}$$

where, r is the rating assigned by an expert, l_o is the lowest possible rating ($l_o = 1$), $S = r - l_o$, n is the number of experts, and c is the number of rating categories [50]. Aiken's V coefficient was calculated for each item to quantify expert agreement regarding item relevance. The statistical significance of the obtained coefficient was determined by comparing the calculated V value with the critical value of Aiken's V. In this research, the critical values were determined based on seven experts ($n = 7$), four rating categories ($c = 4$), and a significance level of $\alpha = 0.05$, as presented in Table 4. Items with V values that met or exceeded the corresponding critical value were considered statistically supported, while items with lower values were further reviewed using expert feedback and theoretical relevance before final retention in the EduDFR framework.

Aiken's V coefficient was interpreted based on the strength of expert agreement, where higher values indicate stronger content validity. The associated p-value was used to evaluate the statistical significance of the coefficient. For example, a V value of 0.86 with a p-value of 0.007 indicates statistically significant expert agreement. Items with lower coefficients were not automatically removed; instead, they were examined qualitatively based on expert feedback and their theoretical relevance to the EduDFR framework.

Table 3. Expert panel for Aiken's V validation

Expert	Expertise	Experience
Expert 1 Practitioner	Digital Forensics, Incident Response, Cybersecurity	15 years
Expert 2 Practitioner	Information Security, Digital Transformation	15 years
Expert 3 Practitioner	Network Operation Control	25 years
Expert 4 Academic	Information Security, Cyber-Physical System	9 years
Expert 5 Academic	Digital Forensics, Network Security	8 years
Expert 6 Academic	Digital Forensics	8 years
Expert 7 Academic	Digital Forensics	8 years

Table 4. Critical values for Aiken's V

Rater (n)	Rating Categories (c)											
	2		3		4		5		6		7	
	V	p	V	p	V	p	V	p	V	p	V	p
2							1.00	0.040	1.00	0.028	1.00	0.020
3							1.00	0.008	1.00	0.005	1.00	0.003
3			1.00	0.037	1.00	0.016	0.92	0.032	0.87	0.046	0.89	0.029
…												
6			0.92	0.010	0.89	0.007	0.88	0.005	0.83	.010	0.83	0.008
6	1.00	0.016	0.83	0.038	0.78	0.050	0.79	0.029	0.77	.036	0.75	0.041
7			0.93	0.004	0.86	0.007	0.82	0.010	0.83	.006	0.81	0.008
7	1.00	0.008	0.86	0.016	0.76	0.045	0.75	0.041	0.74	.038	0.74	0.036
8	1.00	0.004	0.88	0.007	0.83	0.007	0.81	0.008	0.80	.007	0.79	0.007
8	0.88	0.035	0.81	0.024	0.75	0.040	0.75	0.030	0.72	.039	0.71	0.047

4. RESULTS AND DISCUSSION

4.1 Framework development process

The framework development process began by synthesizing prior DFR research and identifying the need to integrate governance in higher education. The literature-derived indicators were mapped to COBIT 2019 design factors and refined through the previous three rounds of Delphi research [44]. The present research then used evidence from six universities to assess whether the validated domains reflected actual institutional conditions.

The Delphi process reported in Rochmadi et al. [44] produced a scale-level content validity index (S-CVI) of 0.99 across all 40 items after three rounds. These results support the conceptual coherence of the instrument used as an input to EduDFR. The current Aiken's V assessment was conducted by a separate panel and focused on the relevance and feasibility of the proposed framework structure.

The field data involved 18 respondents occupying strategic, managerial, and operational IT roles. Thematic analysis identified recurring differences between formal policy and operational practice. Universities varied in strategic direction, documentation, staff capability, incident handling, risk controls, and technology support. Table 5 summarizes the empirical themes, their university frequency, and the final COBIT 2019 objectives associated with each EduDFR component.

Table 5. Empirical basis and final COBIT 2019 mapping of the Educational Digital Forensic Readiness Framework (EduDFR) components

EduDFR Component	Empirical Theme and Illustrative Evidence	University Frequency	Final COBIT 2019 Objectives
Governance and Strategy	Strategic responses ranged from phased, evidence-aware planning to reactive action. Example: preparation, rapid containment without evidence destruction, and post-incident learning (PTS-5 leader).	Explicit strategic direction: 3/6; mainly reactive: 3/6	EDM02, EDM04, EDM05, APO05, APO06, DSS04
Policy, Regulation, and Compliance	Most universities lacked a written forensic standard operating procedure (SOP); some referred to ISO 27001, national guidance, or personal data regulation. Example: "No written policy/ procedure yet" (PTS-5 staff).	Formal written policy: 2/6; external standards referenced: 3/6; explicit personal data regulation awareness: 1/6	EDM01, APO01, APO02, APO09, APO10, APO11, APO13, MEA03, MEA04
People Competency and Security Awareness	All universities reported limited specialist capability and/or weak user awareness. Example: limited cybersecurity personnel constrained tracing and analysis (PTS-3 manager).	6/6	APO07, BAI08, MEA01
Risk and Security Management	Universities used controls such as vulnerability assessments, backups, firewalls, strong passwords, and two-factor authentication, but the maturity of these controls varied.	At least one preventive risk control: 6/6	EDM03, APO12, DSS06, MEA02
Incident Management and Investigation	Incident handling ranged from documented identification, containment, and recovery processes to ad hoc action without detailed records.	Structured/documented: 3/6; ad hoc or undocumented: 3/6	DSS02, DSS03, APO03, APO04, APO08, BAI01, BAI02, BAI03, BAI05, BAI06, BAI07, BAI09, BAI11
Technology and Infrastructure	Universities ranged from subscribed forensic tools and Wazuh-based monitoring to operating system utilities and inadequate security information and event management (SIEM) capability.	At least one technical security tool: 6/6; standardized forensic tooling: 2/6	BAI04, BAI10, DSS01, DSS05, APO14

4.2 Educational Digital Forensic Readiness Framework components and COBIT 2019 integration

EduDFR comprises six interrelated components derived from the convergence of DFR requirements, field themes, and the final COBIT 2019 mapping established through the Delphi process [44]. The integration adds governance value to traditional DFR by assigning decision, management, delivery, and monitoring responsibilities to specific COBIT objectives. It therefore changes DFR from a predominantly technical preparedness concept into an information systems governance capability that can be directed, resourced, monitored, and improved.

4.2.1 Governance and Strategy

Governance and Strategy establishes institutional direction, decision rights, resource commitment, business continuity priorities, and executive oversight for DFR. Its final COBIT 2019 mapping comprises EDM02, EDM04, EDM05, APO05, APO06, and DSS04. These objectives connect forensic readiness with value delivery, resource optimization, stakeholder transparency, portfolio and budget decisions, and continuity.

4.2.2 Policy, Regulation, and Compliance

Policy, Regulation, and Compliance translate strategic direction into documented rules, vendor obligations, personal device provisions, standards, and external compliance requirements. Its final mapping comprises EDM01, APO01, APO02, APO09, APO10, APO11, APO13, MEA03, and MEA04. The component ensures that evidence collection, retention, access, and disclosure are authorized, auditable, and aligned with institutional and legal requirements.

4.2.3 People Competency and Security Awareness

People Competency and Security Awareness defines forensic roles, training, knowledge management, coordination, simulation, and competency evaluation. Its final mapping comprises APO07, BAI08, and MEA01. The component recognizes that technology cannot preserve evidential value when personnel do not understand escalation, documentation, chain of custody, or the consequences of altering potential evidence.

4.2.4 Risk and Security Management

Risk and Security Management identifies threats to the availability, integrity, confidentiality, and admissibility of evidence. Its final mapping comprises EDM03, APO12, DSS06, and MEA02. A forensic risk register is introduced as the operational mechanism for recording evidence loss scenarios, affected assets, control owners, residual risk, and required treatment.

4.2.5 Incident Management and Investigation

Incident Management and Investigation govern detection, triage, containment, evidence preservation, analysis coordination, recovery, communication, and post-incident review. Its final mapping comprises DSS02, DSS03, APO03, APO04, APO08, BAI01, BAI02, BAI03, BAI05, BAI06, BAI07, BAI09, and BAI11. This component is forensic-driven because response actions must contain the incident without unnecessarily destroying logs, volatile data, or provenance.

4.2.6 Technology and Infrastructure

Technology and Infrastructure provide the technical foundation for centralized logging, time synchronization, security monitoring, configuration management, evidence storage, retention, backup, and forensic tools. Its final mapping comprises BAI04, BAI10, DSS01, DSS05, and APO14. The component supports the other five components but does not replace governance, policy, or competent personnel.

The six components are operationalized through 40 role-specific items: 12 for IT leaders or directors, 16 for managers or subdivision heads, and 12 for IT staff. This role differentiation links strategic accountability to managerial coordination and technical execution. Appendix A presents the complete item statements. The framework then consolidates the six components into four implementation pillars without eliminating their individual assessment functions.

4.3 Discussion

4.3.1 Content validation results

The proposed framework was evaluated by seven experts using Aiken's V. Tables 6 and 7 present the item-level ratings for the six components. The analysis assesses content validity and expert agreement; it should not be interpreted as evidence that EduDFR has already improved operational outcomes.

Table 6 presents 18 items across Governance and Strategy; Policy, Regulation, and Compliance; and People Competency and Security Awareness. Thirteen items (72.2%) were Highly Valid, and five items (27.8%) were Valid. The lowest coefficient was 0.76, which met the critical threshold for seven raters and four categories.

Table 7 presents the remaining 22 items across Risk and Security Management, Incident Management and Investigation, and Technology and Infrastructure. Seventeen items (77.3%) were Highly Valid, and five items (22.7%) were Valid. Across both tables, 30 of 40 items (75%) were Highly Valid, and 10 items (25%) were Valid.

Figure 2 summarizes the combined distribution of the 40 items. The coefficients ranged from 0.76 to 1.00. These results support retention of all items and indicate satisfactory expert agreement regarding the proposed framework's content and structure. They do not establish causal effectiveness, adoption success, or improved incident performance.

Based on the content validation results, EduDFR can be advanced to implementation testing. Figure 3 presents the proposed architecture. The arrows should be interpreted as governance and information dependencies rather than a rigid one-time sequence. Governance establishes direction; policy and human capability enable controlled operations; technology supports evidence generation and preservation; operational experience then feeds continuous improvement and updates the forensic risk register.

Table 6. Aiken's V results for Governance and Strategy; Policy, Regulation, and Compliance; and People Competency and Security Awareness

Domain/Component	Item	Expert Value							S							Total S	n(c-1)	V	Category
		1	2	3	4	5	6	7	1	2	3	4	5	6	7				
Governance and Strategy	D1	4	4	4	4	4	4	4	3	3	3	3	3	3	3	21	21	1.00	Highly Valid
	D2	3	4	4	4	4	4	2	2	3	3	3	3	3	1	18	21	0.86	Valid
	D3	4	3	4	4	3	4	4	3	2	3	3	2	3	3	19	21	0.90	Highly Valid
	D5	4	4	4	4	4	4	4	3	3	3	3	3	3	3	21	21	1.00	Highly Valid
	D4	4	2	4	4	3	3	4	3	1	3	3	2	2	3	17	21	0.81	Valid
	D6	4	4	4	4	3	3	4	3	3	3	3	2	2	3	19	21	0.90	Highly Valid
	D7	4	4	4	4	4	4	4	3	3	3	3	3	3	3	21	21	1.00	Highly Valid
	D8	4	4	4	4	4	4	4	3	3	3	3	3	3	3	21	21	1.00	Highly Valid
Policy, Regulation, and Compliance	D10	3	1	4	4	4	4	3	2	0	3	3	3	3	2	16	21	0.76	Valid
	D11	4	1	4	4	4	4	4	3	0	3	3	3	3	3	18	21	0.86	Valid
	M2	4	4	4	4	4	4	4	3	3	3	3	3	3	3	21	21	1.00	Highly Valid
	M3	4	4	4	4	4	4	4	3	3	3	3	3	3	3	21	21	1.00	Highly Valid
	D9	4	4	4	4	4	4	4	3	3	3	3	3	3	3	21	21	1.00	Highly Valid
People Competency and Security Awareness	M1	4	4	4	4	3	3	4	3	3	3	3	2	2	3	19	21	0.90	Highly Valid
	M4	3	4	4	4	3	3	4	2	3	3	3	2	2	3	18	21	0.86	Valid
	M5	4	4	4	4	4	3	4	3	3	3	3	3	2	3	20	21	0.95	Highly Valid
	M6	4	4	4	4	3	4	4	3	3	3	3	2	3	3	20	21	0.95	Highly Valid
	M7	4	4	4	4	3	3	4	3	3	3	3	2	2	3	19	21	0.90	Highly Valid

Table 7. Aiken's V results for Risk and Security Management, Incident Management and Investigation, and Technology and Infrastructure

Domain/ Component	Item	Expert Value							S							Total S	n(c-1)	*V*	Category
		1	2	3	4	5	6	7	1	2	3	4	5	6	7				
Risk and Security Management	M8	4	4	4	4	4	4	4	3	3	3	3	3	3	3	21	21	1.00	Highly Valid
	M9	3	4	4	4	4	4	3	2	3	3	3	3	3	2	19	21	0.90	Highly Valid
	M10	3	4	4	4	3	3	4	2	3	3	3	2	2	3	18	21	0.86	Valid
	M11	4	4	4	4	3	3	4	3	3	3	3	2	2	3	19	21	0.90	Highly Valid
	M12	4	4	4	4	3	4	4	3	3	3	3	2	3	3	20	21	0.95	Highly Valid
	S1	4	4	4	4	3	4	4	3	3	3	3	2	3	3	20	21	0.95	Highly Valid
	S5	3	4	4	4	3	4	3	2	3	3	3	2	3	2	18	21	0.86	Valid
Incident Management and Investigation	M14	4	4	4	4	3	4	4	3	3	3	3	2	3	3	20	21	0.95	Highly Valid
	D12	4	4	4	4	4	3	4	3	3	3	3	3	2	3	20	21	0.95	Highly Valid
	M15	4	4	4	4	4	3	4	3	3	3	3	3	2	3	20	21	0.95	Highly Valid
	S2	4	4	4	4	4	3	4	3	3	3	3	3	2	3	20	21	0.95	Highly Valid
	S3	4	4	4	4	4	3	4	3	3	3	3	3	2	3	20	21	0.95	Highly Valid
	S4	3	4	4	4	4	3	4	2	3	3	3	3	2	3	19	21	0.90	Highly Valid
	S6	3	4	4	4	4	3	3	2	3	3	3	3	2	2	18	21	0.86	Valid
	S7	3	4	4	4	4	3	3	2	3	3	3	3	2	2	18	21	0.86	Valid
Technology and Infrastructure	M13	4	4	4	4	3	3	4	3	3	3	3	2	2	3	19	21	0.90	Highly Valid
	M16	3	4	4	4	3	3	3	2	3	3	3	2	2	2	17	21	0.81	Valid
	S10	3	4	4	4	4	4	4	2	3	3	3	3	3	3	20	21	0.95	Highly Valid
	S8	4	4	4	4	4	3	4	3	3	3	3	3	2	3	20	21	0.95	Highly Valid
	S9	3	4	4	4	4	3	4	2	3	3	3	3	2	3	19	21	0.90	Highly Valid
	S12	4	4	4	4	3	3	4	3	3	3	3	2	2	3	19	21	0.90	Highly Valid
	S11	4	4	4	4	4	4	4	3	3	3	3	3	3	3	21	21	1.00	Highly Valid

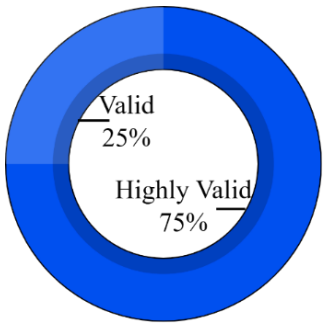

Figure 2. Combined distribution of Educational Digital Forensic Readiness Framework (EduDFR) item validity based on Aiken's V

4.3.2 Component dependencies and implementation sequence

Strategic Forensic Governance. Implementation begins with Strategic Forensic Governance because policy authority, budget, accountability, risk appetite, and continuity priorities must be established before technical or operational controls can be sustained. This pillar defines the institutional mandate and assigns ownership for readiness objectives.

Policy and Human Foundation. The Policy, Regulation, and Compliance component and the People Competency and Security Awareness component are implemented together because documented procedures require capable personnel, while trained personnel require clear authority and boundaries. Outputs include approved DFR policies, vendor and service level obligations, role descriptions, training programs, simulation exercises, and competency evaluation.

Operational Control. The Risk and Security Management and Incident Management and Investigation components form the Operational Control pillar. The forensic risk register identifies evidence loss and admissibility risks before an incident, while the incident lifecycle applies those controls during detection, containment, preservation, investigation, recovery, and review. Operational Control depends on governance authorization, policy, competent personnel, and reliable technology.

Technology and Infrastructure foundation. The Technology and Infrastructure component serves as a supporting foundation rather than an independent first step. Institutions may develop logging, time synchronization, retention, monitoring, and evidence storage in parallel with policy and capability development, but technical configurations should be traceable to approved risk and evidence requirements. Resource-limited universities can begin with centralized logs, synchronized time, protected backups, controlled evidence storage, and documented use of available tools before investing in advanced platforms.

Continuous improvement and the forensic risk register. Continuous improvement links the post-incident review back to Strategic Forensic Governance. Lessons from incidents, simulations, audits, and performance indicators are used to update policies, roles, controls, technology, and the forensic risk register. The register is therefore a cross-component mechanism within Operational Control, whereas continuous improvement is the feedback mechanism across all four pillars.

Figure 3 uses implementation-oriented labels for the same validated components: Strategic Forensic Governance corresponds to Governance and Strategy; Forensic-Oriented Risk Management corresponds to Risk and Security Management; and Forensic-Driven Incident Management corresponds to Incident Management and Investigation. Sistem Pemerintahan Berbasis Elektronik (SPBE) denotes the Indonesian electronic-based governance context and should be interpreted outside Indonesia as the applicable institutional digital governance system, whereas CSIRT denotes a Computer Security Incident Response Team.

4.3.3 Practical application scenario

An illustrative scenario was constructed from an open-ended response provided by PTS-5. The response described a sensitive data leakage incident that was addressed by closing an exposed port and restricting the associated access path.

Under EduDFR, Strategic Forensic Governance first authorizes escalation, assigns the incident owner, and determines continuity and reporting priorities. The Policy and Human Foundation activates the data breach procedure, defines access to evidence, checks vendor obligations, and assigns an incident lead and evidence custodian.

Operational Control records the exposed service in the forensic risk register, contains the incident without unnecessarily deleting logs or volatile data, preserves relevant records, documents the timeline and chain of custody, assesses the affected data, and coordinates recovery. Technology and Infrastructure supplies synchronized logs, network records, access histories, secure evidence storage, and integrity verification. The post-incident review then evaluates why the port was exposed and updates configuration standards, monitoring rules, training, policy, and the risk register. This scenario demonstrates how the components interact; it is not presented as an empirical test of implementation effectiveness. A summary of the EduDFR scenario is presented in Table 8.

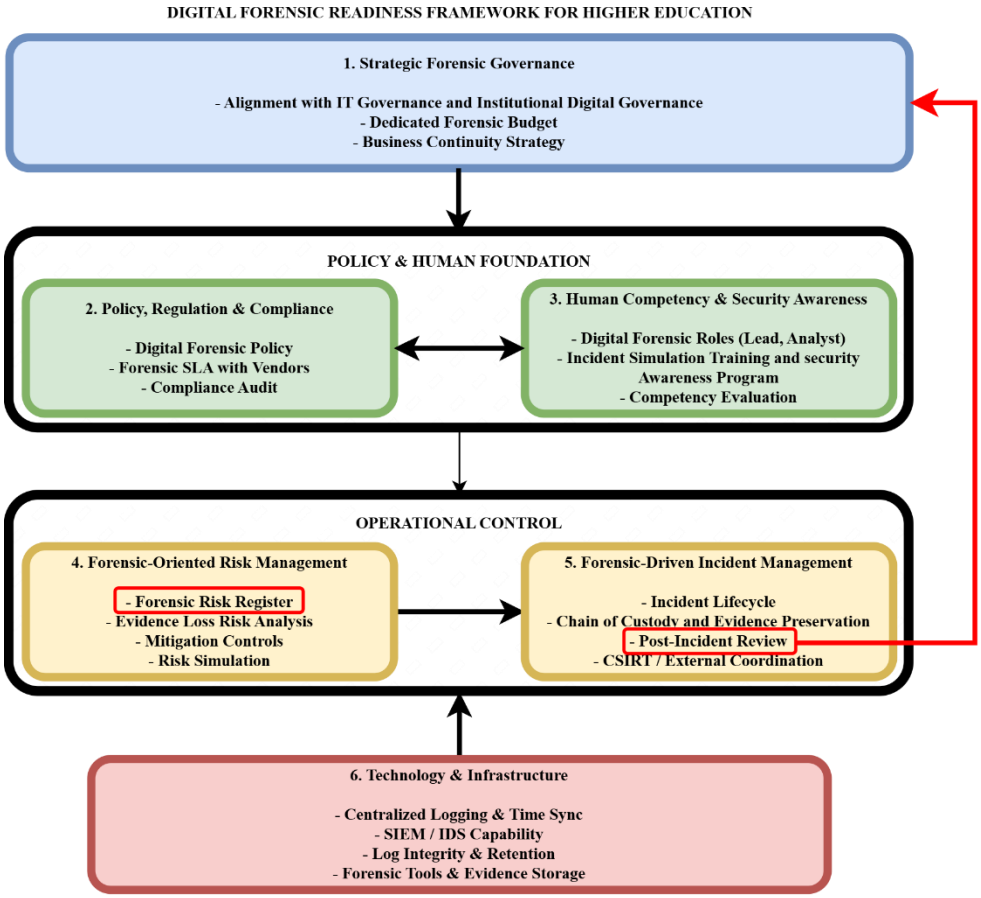

Figure 3. Conceptual architecture of the Educational Digital Forensic Readiness Framework (EduDFR)

Table 8. Educational Digital Forensic Readiness Framework (EduDFR) implementation sequence, dependencies, and indicative outcome measures

Implementation Stage	Primary EduDFR Elements	Key Dependency	Illustrative Outputs and Outcome Indicators
Establish direction	Governance and Strategy	Executive mandate and institutional risk appetite	Approved DFR charter; accountable owner; dedicated or identified budget; continuity objectives; reporting structure
Build policy and capability	Policy, Regulation, and Compliance; People Competency and Security Awareness	Governance approval and defined responsibilities	Approved policy and standard operating procedure coverage; vendor/ service level agreement (SLA) clauses; role assignment; training completion; simulation participation; competency evaluation
Establish operational controls	Risk and Security Management; Incident Management and Investigation	Policy, trained personnel, and evidence requirements	Forensic risk register coverage; documented incident lifecycle; chain of custody completeness; evidence preservation time; incident documentation rate
Configure supporting technology	Technology and Infrastructure	Approved risk, retention, and evidence requirements	Log source coverage; time synchronization compliance; retention compliance; protected evidence storage; monitoring availability; backup integrity
Review and improve	All components through continuous improvement	Incident, exercise, audit, and metric feedback	Post-incident actions closed; policy/ control updates; reduced evidence gaps; improved detection, containment, and preservation times

4.3.4 Evaluation of practical effectiveness

The present validation demonstrates expert agreement with the framework content, not practical effectiveness. Future implementation research should establish a baseline and reassess the university after a defined adoption period. Suitable indicators include policy and procedure coverage, percentage of critical systems producing synchronized and retained logs, time from detection to evidence preservation, completeness of chain-of-custody records, proportion of incidents with documented post-incident review, training and simulation completion, number of unresolved forensic risks, and closure of corrective actions. Comparative case studies and longitudinal measurements are required before claims of improved readiness or incident performance can be made.

4.4 Limitations and transferability

This research has four principal limitations. First, the empirical basis was limited to six private universities with Excellent accreditation in one Indonesian province; private universities with diverse resources and universities in other countries were not included. Second, the universities were not selected by size or IT capability, and the sample does not support statistical generalization. Third, a single researcher conducted the thematic coding, and both the Delphi and Aiken's V assessments depended on expert judgment. Fourth, the research did not include longitudinal implementation, control testing, incident simulation, or before-and-after performance measurement.

The six core components are expected to be broadly transferable because governance, policy, people, risk, incident management, and technology are common organizational requirements. Local adaptation is nevertheless required for national data protection law, evidence rules, institutional governance structures, terminology, staffing, vendor arrangements, and available infrastructure. Universities with limited resources can apply EduDFR incrementally by prioritizing governance ownership, minimum evidence preservation procedures, essential logging and time synchronization, staff awareness, and a basic forensic risk register before adopting advanced SIEM or specialized forensic platforms.

5. CONCLUSION

This research developed EduDFR as a higher-education-specific configuration of DFR and COBIT 2019 governance. The theoretical contribution is the positioning of DFR as an information systems governance capability that connects strategic direction, policy, people, risk, incident operations, and evidence-supporting infrastructure. The methodological contribution is the integration of field themes, a previously Delphi-validated 40-item instrument, explicit COBIT 2019 objective mapping, and content validation by a separate seven-expert panel using Aiken's V. The expert assessment demonstrated satisfactory content validity and agreement across the framework items, supporting the coherence of the proposed EduDFR structure. The practical contribution is a four-pillar implementation architecture supported by role-specific indicators, a forensic risk register, continuous improvement, implementation dependencies, and indicative outcome measures. EduDFR can provide structured guidance for university information systems managers on assigning responsibilities, prioritizing resources, defining vendor obligations, strengthening incident processes that preserve digital evidence, and planning technology controls. The findings do not demonstrate that EduDFR has already improved operational readiness. Future research should conduct implementation case studies in public and private universities, include universities from different countries and resource levels, apply independent coding or triangulation, and evaluate longitudinal changes using incident, evidence, governance, and service continuity indicators.

REFERENCES

[1] Lallie, H.S., Thompson, A., Titis, E., Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. Computers, 14(2): 49. https://doi.org/10.3390/computers14020049

[2] Haque, M.A., Ahmad, S., John, A., et al. (2023). Cybersecurity in universities: An evaluation model. SN Computer Science, 4(5): 569. https://doi.org/10.1007/s42979-023-01984-x

[3] Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: A systematic review. Annals of Telecommunications, 76(3): 255-270. https://doi.org/10.1007/s12243-020-00783-2

[4] Li, J., Xiao, W., Zhang, C. (2023). Data security crisis in universities: Identification of key factors affecting data breach incidents. Humanities and Social Sciences Communications, 10(1): 270. https://doi.org/10.1057/s41599-023-01757-0

[5] Rochmadi, T., Fadlil, A., Riadi, I. (2024). Tinjauan pustaka sistematis: Tantangan dan faktor-faktor pengembangan kesiapan forensik digital. Cyber Security dan Forensik Digital, 7(2): 81-89. https://doi.org/10.14421/csecurity.2024.7.2.4861

[6] Shoderu, G., Baror, S., Venter, H. (2024). A privacy-compliant process for digital forensics readiness. In International Conference on Cyber Warfare and Security, pp. 337-347.

[7] Alnajjar, I.A., Salameh, A.A., Almazaydeh, L., Al Tawil, A. (2026). Two-tier forensic readiness architecture for zero trust-enabled industry 4.0 applications. Information Security Journal: A Global Perspective, 35(3): 363-380. https://doi.org/10.1080/19393555.2025.2528065

[8] Albugmi, A. (2024). Digital forensics readiness framework (DFRF) to secure database systems. Engineering, Technology & Applied Science Research, 14(2): 13732-13740. https://doi.org/10.48084/etasr.7116

[9] Bankole, F., Taiwo, A., Claims, I. (2022). An extended digital forensic readiness and maturity model. Forensic Science International: Digital Investigation, 40: 301348. https://doi.org/10.1016/j.fsidi.2022.301348

[10] Cheng, E.C., Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. Information, 13(4): 192. https://doi.org/10.3390/info13040192

[11] Farid, G., Warraich, N.F., Iftikhar, S. (2025). Digital information security management policy in academic libraries: A systematic review (2010–2022). Journal of Information Science, 51(4): 1000-1014. https://doi.org/10.1177/01655515231160026

[12] Riadi, I., Herman, Siregar, N.H. (2022). Mobile forensic

analysis of signal messenger application on android using digital forensic research workshop (DFRWS) framework. Ingénierie des Systèmes d'Information, 27(6): 903-913. https://doi.org/10.18280/isi.270606

[13] Riadi, I., Sunardi, Aprilliansyah, D. (2023). Analysis of Anubis trojan attack on android banking application using mobile security labware. International Journal of Safety and Security Engineering, 13(1): 31-38. https://doi.org/10.18280/ijsse.130104

[14] Butt, U., Dauda, Y., Shaheer, B. (2023). Ransomware attack on the educational sector. In AI, Blockchain and Self-Sovereign Identity in Higher Education, pp. 279-313. https://doi.org/10.1007/978-3-031-33627-0_11

[15] Rizvi, I., Raj, S., Singh, V. (2025). Cybersecurity in the digital age. In Technology for Societal Transformation: Exploring the Intersection of Information Technology and Societal Development, pp. 131-148. https://doi.org/10.1007/978-981-96-1721-0_8

[16] Chae, Y. (2026). Forensics in healthcare cloud environments: Privacy-preserving evidence workflows. Forensic Science International: Reports, 14: 100498. https://doi.org/10.1016/j.fsir.2026.100498

[17] Englbrecht, L., Meier, S., Pernul, G. (2020). Towards a capability maturity model for digital forensic readiness. Wireless Networks, 26(7): 4895-4907. https://doi.org/10.1007/s11276-018-01920-5

[18] Mekala, S.H., Baig, Z., Anwar, A., Syed, N. (2024). Evaluation and analysis of a digital forensic readiness framework for the IIoT. In 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, USA, pp. 1-6. https://doi.org/10.1109/ISDFS60797.2024.10526471

[19] Jimenez, M.B., Fernandez, D. (2022). A framework for SDN forensic readiness and cybersecurity incident response. In 2022 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Phoenix, USA, pp. 112-116. https://doi.org/10.1109/NFV-SDN56302.2022.9974648

[20] Jiménez, M.B., Fernández, D., Rivadeneira, J.E., Flores-Moyano, R. (2024). A filtering model for evidence gathering in an SDN-oriented digital forensic and incident response context. IEEE Access, 12: 75792-75808. https://doi.org/10.1109/ACCESS.2024.3405588

[21] Fakhouri, H.N., AlSharaiah, M.A., Alkalaileh, M., Dweikat, F.F. (2024). Overview of challenges faced by digital forensic. In 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, pp. 1-8. https://doi.org/10.1109/ICCR61006.2024.10532850

[22] Kebande, V.R., Mudau, P.P., Ikuesan, R.A., Venter, H.S., Choo, K.K.R. (2020). Holistic digital forensic readiness framework for IoT-enabled organizations. Forensic Science International: Reports, 2: 100117. https://doi.org/10.1016/j.fsir.2020.100117

[23] Adel, A., Ahsan, A., Davison, C. (2024). ETHICore: Ethical compliance and oversight framework for digital forensic readiness. Information, 15(6): 363. https://doi.org/10.3390/info15060363

[24] Nugroho, H.A., Briliyant, O.C., Sunaringtyas, S.U. (2023). A novel digital forensic readiness (DFR) framework for e-government. In 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), Bogor, Indonesia, pp. 184-189. https://doi.org/10.1109/ICoCICs58778.2023.10276423

[25] Mpungu, C., George, C., Mapp, G. (2023). Developing a novel digital forensics readiness framework for wireless medical networks using specialised logging. In Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, UK, pp. 203-226. https://doi.org/10.1007/978-3-031-20160-8_12

[26] Pooe, A. (2024). Enhancing forensic readiness through an integrated approach to fraud risk management throughout the digital transformation lifecycle. In International Information Security Conference, Gqeberha, South Africa, pp. 124-133. https://doi.org/10.1007/978-3-032-09660-9_13

[27] Raza, S.A., Shaikh, M., Tahira, K. (2023). Cryptocurrency investigations in digital forensics: Contemporary challenges and methodological advances. Information Dynamics and Applications, 2(3): 126-134. https://doi.org/10.56578/ida020302

[28] Kebande, V.R., Karie, N.M., Ikuesan, R.A., Venter, H.S. (2020). Ontology-driven perspective of CFRaaS. Wiley Interdisciplinary Reviews: Forensic Science, 2(5): e1372. https://doi.org/10.1002/wfs2.1372

[29] Firmansyah, R.A., Prayudi, Y., Luthfi, A. (2025). Integrasi digital forensic readiness dan information security management system pada organisasi pemerintahan: Systematic literature review. Jurnal Mahasiswa Teknik Informatika, 9(2): 2852-2863. https://doi.org/10.36040/jati.v9i2.13126

[30] Vaseghipanah, M., Jabbehdari, S., Navidi, H. (2025). A game-theoretic approach for quantification of strategic behaviors in digital forensic readiness. Journal of Cybersecurity and Privacy, 5(4): 105. https://doi.org/10.3390/jcp5040105

[31] Kuku, O., Chrysikos, A., Salekzamankhani, S. (2025). Preparing IoT-enabled organisations for digital forensics: Model for readiness and resilience. International Journal of Information Security, 24(4): 170. https://doi.org/10.1007/s10207-025-01079-z

[32] Abrardi, L., Comino, S., Grassini, S. (2025). The economics of cyber risk: A survey of the literature. Journal of Industrial and Business Economics, 53: 573-607. https://doi.org/10.1007/s40812-025-00370-3

[33] Saveljeva, J., Uvarova, I., Peiseniece, L., et al. (2025). Cybersecurity for sustainability: A path for strategic resilience. In 2025 IEEE International Conference on Cyber Security and Resilience (CSR), Chania, Greece, pp. 745-752. https://doi.org/10.1109/CSR64739.2025.11129980

[34] Liu, C., Babar, M.A. (2026). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. Australian Journal of Management, 51(1): 62-92. https://doi.org/10.1177/03128962241293658

[35] Ngonyama, N., Mgxekwa, B., Sibanda, K. (2025). The impact of financial technology and cyber risk on non-bank financial intermediation. In Shadow Banking and Financial Risk in Emerging and Developing Markets: The Growth and Development of Non-Bank Financial Intermediation, pp. 275-306. https://doi.org/10.1007/978-3-031-86224-3_11

[36] Boumediene, S.L., Boumediene, S. (2025). Lessons learned from failed digital forensic investigations. Journal of Forensic Accounting Research, 10(1): 357-380. https://doi.org/10.2308/JFAR-2023-046

[37] Sibe, R.T., Kaunert, C. (2024). Digital evidence, digital forensics, and digital forensic readiness. In Cybercrime, Digital forensic Readiness, and Financial Crime Investigation in Nigeria, pp. 57-83. https://doi.org/10.1007/978-3-031-54089-9_3
[38] Kuku, O., Chrysikos, A., Salekzamankhani, S. (2024). Digital forensic readiness in IoT-enabled organisations: Forensic investigation analysis in real-time. In International Conference on Data Analytics & Management, London, UK, pp. 539-553. https://doi.org/10.1007/978-981-96-3355-5_41
[39] Nilendu, D. (2024). Enhancing forensic education: Exploring the importance and implementation of evidence-based education system. Egyptian Journal of Forensic Sciences, 14(1): 6. https://doi.org/10.1186/s41935-023-00375-w
[40] Alharasis, E.E., Haddad, H., Alhadab, M., Shehadeh, M., Hasan, E.F. (2025). Integrating forensic accounting in education and practices to detect and prevent fraud and misstatement: Case study of Jordanian public sector. Journal of Financial Reporting and Accounting, 23(1): 100-127. https://doi.org/10.1108/JFRA-04-2023-0177
[41] Katsini, C., Raptis, G.E., Alexakos, C., Serpanos, D. (2021). FoRePlan: Supporting digital forensics readiness planning for internet of vehicles. In Proceedings of the 25th Pan-Hellenic Conference on Informatics, Volos, Greece, pp. 369-374. https://doi.org/10.1145/3503823.3503891
[42] Hao, Z. (2025). Institutional autonomy in relation to academic freedom, the role of the government and the need for higher education as a federation. European Review, 33(S1): S70-S85. https://doi.org/10.1017/S1062798725000146
[43] Chugh, R., Turnbull, D., Cowling, M.A., Vanderburg, R., Vanderburg, M.A. (2023). Implementing educational technology in higher education institutions: A review of technologies, stakeholder perceptions, frameworks and metrics. Education and Information Technologies, 28(12): 16403-16429. https://doi.org/10.1007/s10639-023-11846-x
[44] Rochmadi, T., Fadlil, A., Riadi, I. (2025). Developing a Delphi validated instrument for assessing digital forensics readiness based on COBIT 2019. International Journal of Advances in Data and Information Systems, 6(3): 749-762. https://doi.org/10.59395/ijadis.v6i3.1453
[45] Suparman, A.R., Rohaeti, E., Wening, S. (2024). Development of computer-based chemical five-tier diagnostic test instruments: A generalized partial credit model. Journal on Efficiency and Responsibility in Education and Science, 17(1): 92-106. https://doi.org/10.7160/eriesj.2024.170108
[46] Utama, B., Tomoliyus, F., Widodo, H. (2021). Modification of reactive agility test measuring instrument for table tennis performance: Aikens validity and retest reliability test. Turkish Journal of Computer and Mathematics Education, 12(14): 3214-3220.
[47] Ismarau Tajuddin, N.I., Abas, U.H., Aziz, K.A., et al. (2025). Content validity assessment using Aiken'S V: Knowledge integration model for blockchain in higher learning institutions. International Journal of Advanced Computer Science & Applications, 16(6): 601-608. https://doi.org/10.14569/IJACSA.2025.0160659
[48] Castro Benavides, L.M., Tamayo Arias, J.A., Burgos, D., Martens, A. (2026). Measuring digital transformation in higher education institutions–content validity instrument. Applied Computing and Informatics, 22(1-2): 129-144. https://doi.org/10.1108/ACI-03-2022-0069
[49] Haryono, S., Sugiyanto, A.K., Suryana, R. (2022). Innovation for development of integrated digital-based jump power meter test for measuring limb muscle power in athletes: Aiken validity and inter-rater reliability. Journal of Hunan University Natural Sciences, 49(2). https://doi.org/10.55463/issn.1674-2974.49.2.17
[50] Aiken, L.R. (1985). Three coefficients for analyzing the reliability and validity of ratings. Educational and Psychological Measurement, 45(1): 131-142. https://doi.org/10.1177/0013164485451012

APPENDIX

The 40 items were assigned by respondent role: D1–D11 for IT leaders or directors, M1–M16 for managers or sub division heads, and S1–S12 for IT staff. Table A1 clarifies the meaning and component assignment of each item evaluated through Aiken's V.

Table A1. Educational Digital Forensic Readiness Framework (EduDFR) evaluation items

Code	Respondent Role	EduDFR Component	Evaluation Item
D1	IT leader/director	Governance and Strategy	Digital forensic readiness provides tangible benefits to the university, such as stronger IT security or more effective incident investigation.
D2	IT leader/director	Governance and Strategy	University resources, including people, technology, and policy, are optimized to support digital forensic readiness.
D3	IT leader/director	Governance and Strategy	University stakeholders actively participate in the policy, technical, or oversight aspects of digital forensic readiness management.
D4	IT leader/director	Governance and Strategy	The university maintains programs and initiatives that support digital forensic readiness, including technology investments, staff training, strengthening security policies, and IT integration.
D5	IT leader/director	Governance and Strategy	The university allocates a dedicated budget for software, staff training, or IT infrastructure that supports digital forensic readiness.
D6	IT leader/director	Governance and Strategy	The university maintains a business continuity strategy for cyber incidents or events requiring digital forensic investigation.
D7	IT leader/director	Policy, Regulation, and Compliance	The university has a documented governance framework that supports digital forensic readiness.
D8	IT leader/director	Policy, Regulation, and Compliance	University IT policies support digital forensic readiness, including incident investigation, risk mitigation, and the use of personal devices.

D9	IT leader/director	Policy, Regulation, and Compliance	Service level agreements with IT providers, including cloud, internet, and security providers, support forensic investigation and the collection and retention of digital evidence.
D10	IT leader/director	Policy, Regulation, and Compliance	The university's IT development policy is aligned with current cybersecurity threats and digital forensic requirements.
D11	IT leader/director	Policy, Regulation, and Compliance	The university has a documented personal device strategy that supports digital forensic readiness and is integrated with IT policy.
M1	Manager / sub-division head	Policy, Regulation, and Compliance	The university periodically evaluates external IT service providers for compliance with security standards and support for digital forensic readiness.
M2	Manager / sub-division head	Policy, Regulation, and Compliance	University digital forensic procedures follow applicable national or international standards.
M3	Manager / sub-division head	Policy, Regulation, and Compliance	The university has early incident detection procedures that support cyber incident prevention and digital forensic readiness.
M4	Manager / sub-division head	Policy, Regulation, and Compliance	The university periodically evaluates compliance with external regulations or policies relevant to digital forensics.
M5	Manager / sub-division head	People Competency and Security Awareness	The university has an organizational structure and defined responsibilities that support digital forensics and IT security.
M6	Manager / sub-division head	People Competency and Security Awareness	The university provides periodic digital forensic training to IT and security personnel.
M7	Manager / sub-division head	People Competency and Security Awareness	The university periodically evaluates training effectiveness and personnel readiness through internal quality assurance or forensic incident simulations.
M8	Manager / sub-division head	Risk and Security Management	The university identifies and manages IT security risks that affect digital forensic readiness, for example, through impact analysis or simulation.
M9	Manager / sub-division head	Risk and Security Management	University risk mitigation strategies include measures such as encryption, access control, or network segmentation that support digital forensic readiness.
M10	Manager / sub-division head	Risk and Security Management	The university has monitoring and evaluation mechanisms for business processes to ensure data protection that supports digital forensic readiness.
M11	Manager / sub-division head	Risk and Security Management	University internal controls, including internal quality assurance or simulation, support digital forensic readiness.
D12	IT leader/director	Incident Management and Investigation	Digital forensic projects or cases are managed effectively and receive leadership support.
M12	Manager / sub-division head	Incident Management and Investigation	The university identifies specific digital forensic requirements for its IT systems, including evidence recovery.
M13	Manager / sub-division head	Incident Management and Investigation	The university has a clear strategy or written policy for managing change while maintaining readiness for digital forensic investigation and involving the IT team.
M14	Manager / sub-division head	Incident Management and Investigation	University IT assets are managed effectively to support the collection and protection of digital evidence.
M15	Manager / sub-division head	Incident Management and Investigation	University project management supports digital forensic readiness through an appropriately designated team.
M16	Manager / sub-division head	Incident Management and Investigation	The university has communication and coordination mechanisms among internal and external teams, such as a CSIRT, for digital forensic readiness.
S1	IT staff	Incident Management and Investigation	The university has procedures for handling IT security incidents involving digital forensics, including response stages and documentation.
S2	IT staff	Incident Management and Investigation	University security investigation procedures are based on digital forensic principles.
S3	IT staff	Incident Management and Investigation	The university's IT architecture supports evidence tracing and investigation through activity logging or SIEM.
S4	IT staff	Incident Management and Investigation	The university uses innovative digital forensic technologies, such as artificial intelligence and big data, to improve the effectiveness of investigations.
S5	IT staff	Incident Management and Investigation	Technology solutions developed by the university are designed to support digital forensic investigation.
S6	IT staff	Incident Management and Investigation	Changes to university IT systems consider support for digital forensic investigation in accordance with established procedures.
S7	IT staff	Incident Management and Investigation	IT system transitions preserve digital forensic capability through testing or other evaluation mechanisms.
S8	IT staff	Technology and Infrastructure	University IT systems include automated capabilities such as logging, IDS, or SIEM to detect and flag suspicious activity relevant to digital forensic investigation.
S9	IT staff	Technology and Infrastructure	University IT configurations support integration with intrusion detection or other security systems in accordance with digital forensic requirements.
S10	IT staff	Technology and Infrastructure	University logging and monitoring mechanisms are centralized and standardized for digital investigation.
S11	IT staff	Technology and Infrastructure	University IT security services include threat detection capabilities that can initiate or support a digital forensic investigation.
S12	IT staff	Technology and Infrastructure	The university manages data through classification and encryption practices that support digital forensic investigation.