Electronic Integrated Computer Algorithm Journal
Vol. 4, No. 1, October 2026, pp 18~32

ISSN: 3031-0350, DOI: 10.62123/enigma.v4i1.201

Traceable Privacy and Cybersecurity Compliance Control Baseline for Indonesian Academic Information Systems

Yudhi Nugroho Adi[1*], Nurwanto Ade Setiawan[1], Nendi Isharmawan[1], Muhammad Farrell Alaric Zada[1], Muharman Lubis[1]

[1] *Master's Program in Information Systems, School of Industrial Engineering, Telkom University, Jl. Telekomunikasi No. 1, Terusan Buahbatu, Bandung, 40257, West Java*, Indonesia.

DOI : 10.62123/enigma.v4i1.201

Received : June 21, 2026
Revised : July 07, 2026
Accepted : August 08, 2026

Keywords:
Information systems; Privacy governance; Cybersecurity compliance; IT governance; Audit readiness

ABSTRACT

Academic information systems process student identities, academic records, library transactions, authentication logs, learning analytics, and third-party service integrations. In Indonesia, privacy and cybersecurity compliance is difficult to operationalize because legal obligations are often separated from system risks, IT governance controls, ownership, and audit evidence. This study develops a traceable privacy and cybersecurity compliance control baseline for Indonesian academic information systems. The method applies structured literature-based conceptual synthesis and design science-inspired artifact development through source selection, concept coding, framework reconciliation, regulatory mapping, control mapping, and ex-ante conceptual evaluation. The evidence base consists of 55 academic, regulatory, framework, and design science sources. The results produce a five-layer governance model, framework reconciliation protocol, Indonesian regulatory mapping, privacy and cybersecurity risk-control-evidence matrices, an audit evidence schema, and an implementation roadmap. The contribution is an initial control-oriented governance baseline for aligning privacy obligations, cybersecurity safeguards, accountable ownership, and audit preparation. The model is conceptual and requires future expert validation and institutional case evaluation.

1. INTRODUCTION

Academic information systems have become core infrastructure for higher education institutions. Student information systems, learning management systems, digital library platforms, authentication services, financial administration modules, research repositories, academic analytics tools, and student service portals process personal data across interconnected organizational and technical boundaries. These systems support administrative efficiency and data-driven decision making, but they also increase privacy and cybersecurity exposure because academic data are collected, stored, integrated, monitored, and shared across internal units, cloud services, and external providers.

The Indonesian regulatory landscape has changed substantially through the enactment of personal data protection and electronic-system regulations. However, legal compliance is not automatically achieved by publishing a privacy notice, quoting statutory provisions, or assigning general responsibility to an information technology unit. Universities must be able to demonstrate what personal data are collected, where the data flow, who has access, which purposes are legitimate, how long data are retained, how vendors are governed, how incidents are handled, and what evidence can support compliance assurance. These questions are information-systems governance questions because they require system ownership, data lifecycle control, access management, monitoring, evidence retention, and auditability.

Academic institutions have specific governance constraints. Students often have limited practical choice to opt out of institutional platforms, learning analytics may generate behavioral traces, library and repository systems may reveal intellectual activity, and third-party learning or cloud services may create opaque data flows. Therefore, privacy and cybersecurity compliance in universities should not be treated only as a legal documentation issue. It should be operationalized as a control architecture that links regulatory obligations, academic data processes, cybersecurity safeguards, institutional roles, and verifiable evidence.

Existing research provides useful but fragmented foundations. Information privacy literature establishes privacy as an interdisciplinary information-systems concern involving individuals, organizations, technologies, and institutions [18][26]. Privacy ethics and contextual integrity explain why information flows must be appropriate to their institutional context [1][29]. Data protection compliance, privacy-by-design, requirements engineering, and data governance studies show that privacy obligations must be translated into system requirements and organizational capabilities [2][3][9][10][17][21][24][25][38]. Higher education studies further show that learning platforms, learning analytics, online proctoring, library systems, and academic information systems create privacy risks, third-party data flows, and governance weaknesses [5][6][19][22][23][31][32][33][34][37].

*Corresponding Author Email: yudhinugrohoadi@telkomuniversity.ac.id

Despite these foundations, a specific gap remains. Indonesian legal and regulatory studies often focus on normative interpretation; academic cybersecurity studies often focus on vulnerability assessment or selected COBIT domains; GDPR-readiness studies provide useful compliance logic but are mostly developed outside the Indonesian context; and generic frameworks such as NIST, ISO/IEC, and COBIT require local and sectoral translation. Existing studies rarely specify how regulatory obligations should be decomposed into implementable control objectives, responsible actors, and verifiable evidence artifacts within academic digital platforms. The unresolved gap is therefore not the absence of frameworks, but the absence of a contextual translation layer that connects Indonesian regulatory obligations to academic information-system risks, IT governance controls, accountable control owners, and audit-oriented evidence.

This study addresses the gap by developing a traceable privacy and cybersecurity compliance control model for academic information systems in Indonesia. The research question is: How can Indonesian privacy and electronic-system regulations be operationalized into IT governance controls, accountable ownership, risk-control-evidence matrices, and audit-oriented compliance evidence for academic information systems? The objective is to construct a governance artifact that translates ethical and regulatory obligations into system risks, control activities, accountable roles, and evidence artifacts that can support internal audit and continual improvement.

The study contributes to computing and informatics in three ways. Theoretically, it reframes privacy and cybersecurity compliance as information-systems governance capabilities rather than legal documentation. Methodologically, it proposes a regulation-risk-control-owner-evidence traceability logic for constructing a governance artifact from domestic obligations and recognized control frameworks. Practically, it offers an audit-readiness baseline for academic institutions to design data inventories, access matrices, API registers, vendor governance, incident response, privacy officer coordination, compliance dashboards, and internal audit preparation. The novelty of this study is not a new legal interpretation, but a traceable governance architecture that converts Indonesian privacy and electronic-system obligations into academic information-system risks, control objectives, accountable owners, and audit evidence artifacts.

2. LITERATURE REVIEW

2.1 Privacy, Digital Regulation, and Cyber Ethics as Information-Systems Concerns

Digital regulation provides the formal basis for rights, responsibilities, prohibited actions, and institutional obligations in digital environments. Cyber ethics complements legal compliance by evaluating whether digital practices respect autonomy, dignity, fairness, transparency, proportionality, accountability, security, and non-maleficence. In academic services, ethical issues emerge when students are required to use platforms that collect identity data, learning logs, behavioral traces, assessment data, library transactions, or authentication records without sufficient transparency or meaningful control.

The ethical dimension is important because a system can be legally documented but still problematic if it collects excessive data, hides third-party tracking, applies unclear consent mechanisms, or reuses data outside the original academic context. Contextual integrity argues that privacy depends on whether information flows are appropriate to the context in which data are collected and used [29]. Privacy taxonomy helps classify privacy harms related to collection, processing, dissemination, and invasion [1]. These foundations indicate that privacy controls should not only secure data but also regulate purposes, flows, roles, and accountability. However, these theories do not by themselves specify operational control ownership or audit evidence for academic digital platforms.

2.2 Data Privacy, Personal Data Protection, and Compliance Capabilities

Information privacy has long been recognized as an interdisciplinary information-systems issue involving individuals, organizations, technologies, and institutional arrangements [18][26]. Data protection compliance extends this issue by requiring organizations to define lawful processing, manage data subject rights, implement safeguards, and maintain accountability evidence. Recent literature shows that organizations need decision-support mechanisms, maturity models, data management capabilities, and requirements engineering to operationalize privacy regulations [2][9][10][24][25][38].

Privacy-by-design and security-by-design studies emphasize that privacy and security requirements should be embedded into the system development lifecycle instead of being added after deployment [3][30]. Data governance, privacy, and ethics are increasingly viewed as interconnected organizational capabilities [14][36]. For academic information systems, this means that personal data protection must be connected to data classification, access control, retention, logging, vendor management, incident handling, and evidence-based assurance. The remaining challenge is to connect these capabilities to concrete control records, responsible actors, and evidence artifacts that can be audited in university information systems.

2.3 Academic Digital Information Systems and Domain-Specific Risks

Academic information systems process sensitive and high-value data, including student identities, grades, attendance, disciplinary records, financial status, library borrowing histories, research activities, authentication logs, and learning analytics. Studies on higher education cybersecurity indicate that open academic networks, decentralized governance, diverse user communities, and resource constraints increase exposure to phishing, unauthorized access, ransomware, malware, application vulnerabilities, and third-party risks [11][12]. Technical assessments and COBIT-based audits of academic systems are useful but often focus on specific domains such as DSS controls, vulnerability testing, or user privacy awareness [4][5][6][7][8].

Higher education privacy studies show that learning management systems, third-party plugins, online proctoring platforms, learning analytics, and student success systems may introduce opaque data flows and unclear responsibility allocation [31][32][33].

Library and academic information environments require specific privacy maturity considerations because user data may include reading history, borrowing records, research activity, and learning-related traces [23]. These studies indicate the need for a domain-specific governance model that connects academic data flows with privacy rights, cybersecurity controls, vendor governance, and audit evidence. Nevertheless, they often stop at selected risks or platforms and do not provide an integrated privacy-cybersecurity control-evidence model

2.4 IT Governance, Cybersecurity Governance, and Audit Evidence

IT governance concerns the alignment of digital systems with organizational goals, risk appetite, accountability structures, performance expectations, and control mechanisms [35]. Cybersecurity governance transforms security from a technical function into an organizational capability that includes accountability, risk management, policy enforcement, monitoring, incident response, and continual improvement [20]. For academic institutions, these capabilities are necessary to coordinate system owners, data owners, security teams, legal or compliance units, privacy officers, vendors, and internal auditors.

The NIST Privacy Framework, NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, ISO/IEC 27701:2025, ISO/IEC 27005:2022, COBIT 2019, and OECD Privacy Guidelines provide structured references for identifying privacy risks, assessing information security risks, establishing controls, responding to incidents, governing information and technology, and demonstrating accountability [46][47][48][49][50][51][53]. Their value for Indonesian universities depends on an intermediate translation layer that connects generic control logic with local obligations, academic data flows, and audit evidence.

Audit evidence is important because compliance cannot be verified only through policy statements. Evidence may include data inventories, processing registers, access matrices, log review records, backup test results, incident tickets, data processing agreements, SLA reports, API inventories, privacy request logs, and management review records. In this study, audit readiness is treated as the capacity to show both control design and control operation. This interpretation aligns with the assurance logic embedded in IT governance and information security management frameworks [48][50][53].

2.5 Synthesis and Research Positioning

The reviewed literature suggests five important insights. First, privacy is not only a legal issue but also an information-systems issue involving data flows, system design, control implementation, and organizational accountability. Second, academic systems have distinctive risks because students often have limited choice, services are highly interconnected, and third-party platforms are increasingly used. Third, existing Indonesian studies tend to focus separately on legal interpretation, vulnerability assessment, privacy awareness, or COBIT-based audits, leaving a gap between compliance obligations and operational controls. Fourth, international privacy and cybersecurity frameworks provide reusable control logic but require local and sectoral operationalization. Fifth, audit readiness depends on evidence of control design and operation, not merely policy statements. Table 1 summarizes how these literatures inform the positioning of this study.

Table 1. Literature synthesis and research gap

Literature cluster	Main focus	Limitation	Implication for this study
Legal and regulatory studies	Personal data protection, digital regulation, electronic-system obligations	Often normative and focused on statutory interpretation	Translate regulation into academic system risks, control activities, owners, and evidence
Privacy and data protection compliance	GDPR compliance, privacy-by-design, maturity, requirements engineering	Mostly non-Indonesian and not specific to academic services	Adapt compliance logic to Indonesian academic information systems
Academic information systems	SIAKAD, LMS, learning analytics, online proctoring, library systems	Often focuses on technical security, platform use, or isolated privacy issues	Connect academic data flows with privacy rights, cybersecurity risks, and vendor governance
IT and cybersecurity governance	Control frameworks, information security governance, audit and incident response	Often not mapped to Indonesian PDP and electronic-system obligations	Develop regulatory-to-control and risk-control-evidence matrices
Data governance, privacy officer, and audit assurance literature	Data management capability, DPO/privacy officer roles, compliance profession, and evidence-based assurance	Limited integration with academic system assurance and control ownership	Add role accountability, evidence repository, and audit readiness layer

3. RESEARH METHODS

3.1 Research Design

This study applies structured literature-based conceptual synthesis and design science-inspired conceptual artifact development. It is not presented as a full systematic literature review because the objective is not to estimate the distribution of empirical findings, calculate publication trends, or provide an exhaustive review of all privacy and cybersecurity literature. It is also not claimed as a complete design science study because the artifact has not yet been demonstrated or empirically evaluated in

an institutional case. Instead, the study constructs a conceptual governance artifact that can later be demonstrated, validated, and operationalized in academic institutions.

The unit of analysis is the traceable relationship among regulatory obligations, academic information-system risks, IT governance controls, control ownership, and compliance evidence. The design science orientation structures the study through problem identification, objective definition, artifact design and development, and ex-ante conceptual evaluation [13][52]. Artifact demonstration, expert validation, Delphi evaluation, case study implementation, and empirical measurement are positioned as future research stages rather than as completed empirical evaluation. **Methodological Positioning: Structured Conceptual Synthesis and Design Science-Inspired Artifact Development:** The methodological position combines two complementary logics. Structured conceptual synthesis is used to extract and organize concepts, obligations, risks, controls, owners, and evidence artifacts from academic literature, Indonesian regulations, and governance frameworks. Design science-inspired artifact development is used to convert these synthesized elements into a coherent governance artifact consisting of layers, mappings, matrices, a traceability scenario, and an implementation roadmap. Accordingly, the study covers problem identification, objective definition, artifact design and development, and ex-ante conceptual evaluation. It does not claim artifact demonstration or empirical validation. Expert review, Delphi evaluation, institutional case implementation, and measurement of control effectiveness are explicitly positioned as future research stages.

3.2 Source Identification and Selection Protocol

The evidence base was assembled through purposive but transparent source identification. Source identification, reference screening, and final bibliographic checking were conducted in June 2026. The search was conducted across Scopus-indexed literature, Google Scholar, publisher databases, official Indonesian regulatory repositories, and international framework publications. The search did not aim to produce a statistically representative bibliometric corpus. Instead, it aimed to identify conceptual, regulatory, and control-oriented sources that could support the construction of a regulation-to-evidence governance artifact. Table 2 presents the search strategy and selection rules used to improve transparency and replicability.

Table 2. Source identification and selection protocol

Element	Description
Search sources	Scopus-indexed literature; Google Scholar; publisher databases; Indonesian regulatory repositories, especially peraturan.bpk.go.id and JDIH sources; official NIST, ISO/IEC, OECD, and ISACA framework publications
Search terms	privacy; data protection; personal data protection; cybersecurity governance; IT governance; academic information systems; higher education; GDPR readiness; COBIT audit; NIST Privacy Framework; NIST Cybersecurity Framework; ISO/IEC 27001; ISO/IEC 27701; ISO/IEC 27005; Indonesian PDP Law
Inclusion criteria	Sources were included when they supported at least one element of the regulation-risk-control-owner-evidence chain, explained academic-system privacy or cybersecurity risk, provided governance/control logic, or defined Indonesian regulatory obligations
Exclusion criteria	Sources were excluded when they were unrelated to information systems, lacked relevance to privacy or cybersecurity compliance, provided purely legal commentary without operational implications, or did not support artifact construction
Selection logic	Recent academic sources were prioritized for current privacy, cybersecurity, higher education, governance, and compliance debates. Foundational sources were retained only when they provided seminal concepts for privacy, contextual integrity, privacy-by-design, or design science
Adequacy check	The source base was considered adequate when every artifact layer was supported by at least one academic, regulatory, or framework source and when each proposed control or evidence type could be traced to a conceptual or framework rationale
Search period	Source identification, reference screening, and bibliographic checking were conducted in June 2026. The access date used for Indonesian regulatory web sources in the reference list is June 20, 2026.

3.3 Evidence Base and Source Role

The final evidence base consists of 55 references. Indonesian regulatory and education-sector documents were treated as sources of binding or sector-specific data governance obligations, while international governance frameworks were used to derive risk, control, and assurance logic. Academic literature was used to identify domain-specific risks, privacy and cybersecurity governance issues, data governance capabilities, and research positioning. Table 3 explains the role of each source group in constructing the framework.

Table 3. Source selection and role in framework construction

Source group	Count	Example references	Inclusion rationale	Role in framework
Academic and domain studies	33	[2]-[12], [14]-[17], [19]-[25], [27]-[28], [31]-[39]	Relevant to privacy compliance, academic systems, cybersecurity, governance, data governance, DPO roles, or control mapping	Inform risk scenarios, governance capabilities, role accountability, and research gap

Foundational privacy and ethics sources	5	[1], [18], [26], [29], [30]	Provide conceptual basis for information privacy, privacy harms, contextual integrity, and privacy-by-design	Inform ethical principles and privacy risk categories
Design science methodology	2	[13], [52]	Provide logic for artifact construction and future evaluation	Frame the study as design science-inspired artifact development
Indonesian regulatory documents	8	[40]-[45], [54], [55]	Define privacy, electronic-system, cybersecurity, and education-sector data governance obligations relevant to academic digital services	Provide domestic regulatory obligation layer and academic-data governance mapping inputs
International governance frameworks	7	[46]-[51], [53]	Provide recognized privacy, cybersecurity, risk management, IT governance, and assurance guidance	Inform controls, evidence, monitoring, and risk treatment logic

Framework Filtering and Reconciliation Protocol: The international frameworks were not merged mechanically. They were filtered and reconciled according to their functional role in the regulation-risk-control-owner-evidence chain. A framework concept was retained only when it clarified a privacy risk, cybersecurity lifecycle activity, information security control, privacy information management requirement, risk treatment logic, IT governance responsibility, or privacy principle that could be translated into an academic information-system control or evidence artifact.

Table 4. Framework filtering and reconciliation protocol

Framework or standard	Main extracted concept	Filtering criterion	Reconciliation rule	Output in the proposed model
NIST Privacy Framework 1.0	Privacy risk and privacy governance functions	Retained when the concept addressed privacy risk, data processing, governance, or accountability	Mapped to privacy risk and governance control functions	Privacy risk layer; privacy control and evidence logic
NIST Cybersecurity Framework 2.0	Identify, Protect, Detect, Respond, Recover lifecycle	Retained when the concept addressed cybersecurity lifecycle or resilience	Used to structure cybersecurity safeguards and response activities	Cybersecurity control baseline; incident response and monitoring logic
ISO/IEC 27001:2022	Information security management and security control structure	Retained when the concept supported security management, access control, logging, continuity, or incident handling	Translated into security controls and evidence artifacts	Access control, logging, backup, vulnerability management, incident evidence
ISO/IEC 27701:2025	Privacy information management and PII accountability	Retained when the concept addressed PII processing, accountability, rights, or processor governance	Used to strengthen privacy-specific ownership and evidence requirements	Processing register, rights workflow, privacy officer coordination, vendor evidence
ISO/IEC 27005:2022	Risk identification, analysis, and treatment logic	Retained when the concept supported risk prioritization and treatment	Used as the risk-management rationale for conceptual priority categories	Risk priority explanation and recalibration requirement
COBIT 2019	IT governance, management objectives, ownership, and accountability	Retained when the concept clarified governance responsibility, control ownership, or management review	Mapped to RACI, accountable roles, and governance review functions	Control owner/RACI logic; management review and audit preparation
OECD Privacy Guidelines	Privacy principles and ethical governance logic	Retained when the concept supported privacy principles and responsible data flows	Mapped to the ethical and privacy governance layer	Ethical principles layer and principle-to-control translation

3.4 Coding, Extraction, and Synthesis Procedure

The coding process used predefined analytical categories derived from the research question. Each source was examined for constructs that could support one or more framework layers. Regulatory documents were coded based on obligation type, affected data or process, and governance requirement. Scholarly and framework sources were coded based on conceptual contribution, domain context, risk relevance, control relevance, ownership implication, and assurance implication. To maintain traceability, each extracted concept was linked to a framework layer and to a potential evidence artifact.

The coding procedure was conducted as an interpretive conceptual synthesis rather than statistical content analysis. To reduce arbitrary selection, a concept was retained only when it could be linked to at least one of three anchors: an Indonesian regulatory obligation, an academic information-system risk, or a recognized privacy/cybersecurity/IT governance control logic. Ambiguous mappings were resolved by prioritizing control traceability and audit evidence rather than legal interpretation alone. Table 5 summarizes the coding scheme.

Table 5. Coding scheme for conceptual synthesis

Coding category	Definition	Extracted element	Linked framework layer	Example output
Ethical principle	Normative value guiding appropriate academic data processing	Autonomy, transparency, fairness, proportionality, accountability	Ethical principles	Consent transparency and proportional monitoring
Regulatory obligation	Legal or policy requirement affecting digital systems	Lawful processing, rights handling, electronic-system reliability, incident readiness	Regulatory obligation	Data inventory, request workflow, breach response
Academic system risk	Privacy or cyber failure scenario in academic services	Excessive collection, unauthorized access, vendor misuse, retention failure	Information-system risk	Third-party LMS/plugin processing risk
Governance control	Technical or organizational activity that treats a risk	RBAC, MFA, audit logging, DPA, PIA, backup test, retention schedule	IT governance control	Periodic access review and API token review
Control ownership	Accountable institutional role for control operation	System owner, ICT directorate, privacy officer, data owner, internal auditor	Control and assurance	RACI allocation for privacy request handling
Compliance evidence	Artifact that demonstrates control design or operation	Processing register, access matrix, SLA dashboard, incident ticket, audit report	Compliance assurance	Audit-oriented evidence package

3.5 Framework Construction and Traceability Logic

The framework was constructed through a regulation-to-evidence traceability logic. Each regulatory obligation was interpreted as a governance requirement. Each requirement was mapped to a plausible information-system risk in academic digital services. Each risk was linked to a control objective and to technical or organizational controls derived from privacy, cybersecurity, and IT governance frameworks. Each control was then assigned to accountable institutional roles and translated into evidence artifacts that can be reviewed by internal auditors, privacy officers, system owners, or management.

This logic supports audit-readiness preparation because it prevents privacy programs from becoming purely documentary. A privacy notice, for example, is not sufficient unless it is connected to a data inventory, processing purpose, consent or rights workflow, access-control configuration, vendor arrangement, log review, and evidence repository. Figure 1 illustrates the research process and traceability chain used to construct the artifact.

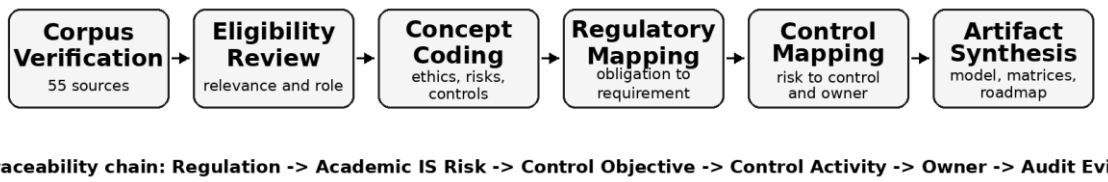


Figure 1. Research process and regulation-to-evidence traceability logic

3.6 Conceptual Evaluation and Risk Prioritization

The artifact was conceptually evaluated using five ex-ante criteria: relevance, completeness, coherence, traceability, and applicability. The evaluation is an ex-ante conceptual design justification, not external expert validation. Relevance examines whether each component addresses academic information-system privacy or cybersecurity compliance. Completeness checks whether ethics, regulation, risk, control, ownership, and assurance are represented. Coherence examines logical relationships among layers. Traceability checks whether obligations are linked to risks, controls, owners, and evidence. Applicability checks whether the model can guide institutional implementation.

Risk priority in the matrices is presented categorically rather than as an empirical score. Priority categories were assigned by considering the convergence of data sensitivity, third-party dependency, operational impact, compliance exposure, and detectability, following the risk-management logic of ISO/IEC 27005 rather than empirical institutional measurement [53]. A High priority indicates risks that involve sensitive academic data, strong third-party dependency, high operational impact,

legal/compliance exposure, or weak detectability. A Medium priority indicates risks that remain relevant to compliance but are more limited in scope, dependency, impact, or detectability. These categories are design priorities intended to support implementation planning and should be recalibrated during institutional deployment using actual architecture, data sensitivity, threat exposure, and institutional risk appetite.

Table 6. Conceptual evaluation criteria and ex-ante result

Criterion	Evaluation question	Expected indication in the artifact	Remaining limitation
Relevance	Does the component address academic information-system privacy or cybersecurity compliance?	Academic data, users, platforms, vendors, controls, or evidence are explicitly represented	Needs validation with real university systems
Completeness	Are ethics, regulation, risk, control, ownership, and assurance covered?	All five layers are present and connected	May need extension for sector-specific datasets such as biometrics or research data
Coherence	Are relationships among layers logically connected?	Regulations lead to risks; risks lead to controls; controls lead to evidence	Causal effectiveness is not empirically tested
Traceability	Can each obligation be followed to risk, control, owner, and evidence?	Mapping tables and matrices preserve end-to-end linkage	Detailed clause-level mapping should be refined by legal and audit experts
Applicability	Can institutions use the artifact as a starting point?	Roadmap, RACI, evidence examples, and control baseline are actionable	Feasibility depends on institutional maturity and resource capacity

4. RESULT AND DISCUSSIONS

4.1 Artifact 1: Five-Layer Privacy and Cybersecurity Compliance Control Model

The first artifact is a five-layer privacy and cybersecurity compliance control model. The Ethical Principles Layer defines the normative values of autonomy, transparency, fairness, accountability, proportionality, security, and non-maleficence. The Regulatory Obligation Layer translates Indonesian privacy and electronic-system requirements into obligations for controllers, processors, electronic-system operators, and institutional managers. The Information-System Risk Layer identifies privacy and cyber failure scenarios in academic platforms. The IT Governance Control Layer specifies technical and organizational controls. The Compliance Assurance Layer defines evidence, monitoring, audit, and continual improvement mechanisms.

The model contributes traceability by linking each ethical principle and legal obligation to an information-system risk, each risk to a control activity and control owner, and each control to compliance evidence. This structure is important for internal audit, regulatory readiness, and management accountability because it converts compliance from a policy statement into a reviewable system of controls. The artifact is not intended to replace NIST, ISO/IEC, COBIT, or Indonesian regulation; instead, it functions as a contextual translation layer that makes those references operational for academic information systems.

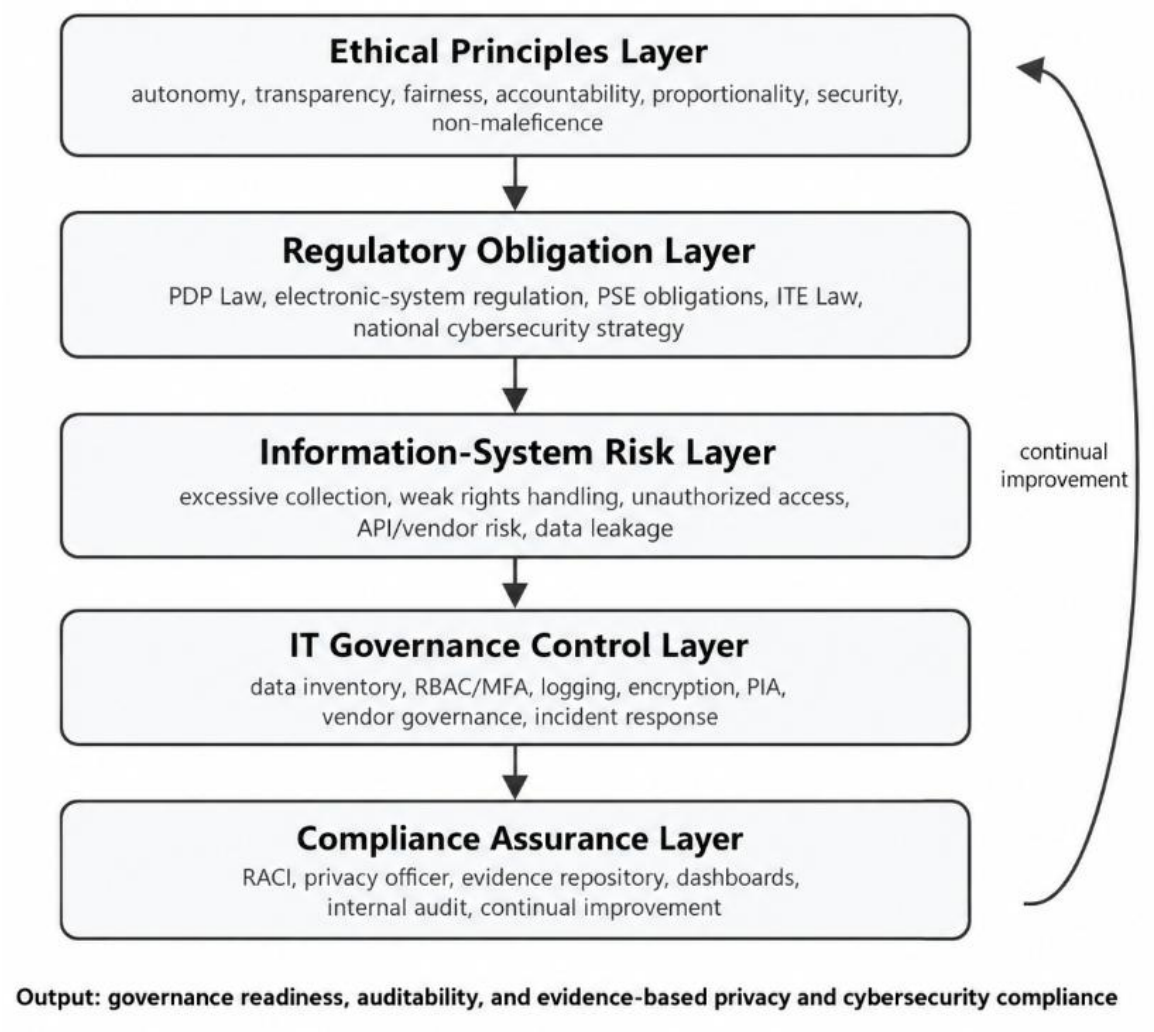


Figure 2. Five-layer privacy and cybersecurity compliance control model

4.2 Artifact 2: Regulatory-to-Risk and Control-Evidence Mapping

The second artifact translates Indonesian regulatory and education-sector governance sources into academic information-system risks and control-evidence structures. Each domestic source is treated as a governance requirement that must be operationalized through system ownership, data lifecycle controls, access management, vendor governance, incident response, academic-record stewardship, reporting integrity, and compliance evidence. The Indonesian Personal Data Protection Law provides the central basis for personal data protection, processing responsibilities, data subject rights, controller and processor obligations, transfer requirements, sanctions, and accountability mechanisms [40]. Government Regulation No. 71/2019 provides the electronic-system layer by requiring reliable, secure, and accountable electronic-system operation [41]. The ITE Law amendment, private Electronic System Operator regulations, and the national cybersecurity strategy add digital responsibility, platform governance, vendor oversight, and cyber crisis readiness dimensions [42] [43] [44] [45]. Education-sector data governance and higher education quality-assurance requirements add a domain-specific need for accurate student records, academic data lineage, reporting accountability, and PDDikti-related data stewardship [54] [55].

To improve auditability, the mapping is separated into two tables. Table 7 maps domestic obligations to affected academic data processes and risk scenarios. Table 8 then translates those risks into control objectives, control activities, accountable owners, evidence artifacts, and implementation priority. This separation prevents the model from merging controls and evidence, which would make it difficult for auditors or system owners to verify whether a control has been designed and operated.

Table 7. Indonesian regulatory mapping for academic information-system governance

Regulation	Regulatory obligation	Academic data/process affected	Main risk scenario	Priority
PDP Law No. 27/2022 [40]	Lawful processing, rights handling, controller/processor responsibility	Student identities, grades, attendance, library records, learning analytics, authentication logs	Unlawful processing, weak rights handling, unclear accountability	High

GR 71/2019 [41]	Reliable, secure, and accountable electronic-system operation	SIAKAD, LMS, digital library, repository, authentication service, financial module	Service disruption, weak logging, insecure operation, insufficient continuity	High
ITE Law amendment [42]	Electronic information, electronic transactions, and digital responsibility	User accounts, electronic records, digital academic communication	Misuse of electronic information, weak evidence preservation, abuse handling gaps	Medium
Private ESO regulations [43], [44]	Electronic-system operator governance and vendor/third-party obligations	Cloud services, LMS providers, payment gateways, analytics tools, library platforms	Unmanaged vendor, unclear processing location, weak contractual accountability	High
National cybersecurity strategy [45]	Cybersecurity coordination, cyber crisis readiness, and crisis response governance	Incident detection, escalation, breach response, service recovery, management reporting	Delayed response, fragmented escalation, crisis mismanagement	High
Education-sector data governance and higher education reporting context [54], [55]	Accurate higher-education data reporting, quality-assurance records, and student data management	PDDikti-related academic records, curriculum data, student status, learning outcomes, institutional quality data	Inaccurate student records, weak lineage, inconsistent reporting, poor retention, unclear data stewardship	Medium

Table 8. Control, ownership, and evidence mapping

Risk scenario	Control objective	Control activity	Evidence artifact	Control owner
Unlawful processing and unclear accountability	Ensure processing is lawful, limited, accountable, and reviewable	Data inventory; processing register; consent and rights workflow; privacy officer coordination	Data inventory; processing register; request logs; policy approval	Privacy officer; system owner; legal/compliance; data owner
Insecure or unreliable electronic-system operation	Maintain reliable and secure electronic services	System ownership; RBAC; audit logging; backup; monitoring; continuity plan	Access matrix; log review record; backup test; incident record; continuity procedure	ICT directorate; application owner; internal auditor
Misuse of electronic information and weak evidence preservation	Strengthen accountability for electronic interactions	Acceptable-use policy; authentication; evidence preservation; abuse reporting	User policy; authentication configuration; abuse ticket; evidence preservation log	System owner; legal/compliance; service desk
Unmanaged third-party processing	Control external processing and service obligations	Vendor due diligence; DPA; SLA; API permission boundary; audit rights	Vendor register; DPA; SLA; due diligence report; API inventory	Procurement; system owner; privacy officer; vendor manager
Delayed cyber incident response	Improve cyber resilience and coordinated response	Incident response plan; escalation matrix; cyber drill; crisis communication; RCA	Incident playbook; drill report; RCA; crisis communication record	Security team; ICT directorate; management; internal auditor

4.3 Artifacts 3 and 4: Privacy and Cybersecurity Risk-Control-Evidence Matrices

The third and fourth artifacts are privacy and cybersecurity risk-control-evidence matrices. The privacy matrix focuses on data lifecycle and rights-related risks, while the cybersecurity matrix focuses on access, application, infrastructure, incident, and integration risks. Both matrices include evidence artifacts because compliance cannot be verified only through control descriptions. No claim is made that the priority categories represent empirical audit results from a specific university; they are provided as a structured conceptual baseline for implementation planning and audit preparation.

The rationale for the highest conceptual priorities is domain-specific. Third-party LMS/plugin processing receives high priority because it involves external processing, API permissions, contract dependency, and unclear processing location. Unauthorized access, web/API vulnerabilities, ransomware, and insecure integrations receive high priority because they may simultaneously disrupt critical academic services, expose sensitive student records, and weaken the institution's ability to demonstrate compliance evidence.

Table 9. Privacy risk-control-evidence matrix

Privacy risk	Priority	Control owner	Key controls	Compliance evidence
Excessive student data collection	Medium	System owner; privacy officer; data owner	Field minimization; data classification; data justification review	Data inventory; data justification sheet; approved data dictionary
Weak consent and privacy notice	Medium	Privacy officer; system owner; service desk	Consent module; notice versioning; rights communication workflow	Notice history; consent log; request log; communication record
Third-party LMS/plugin processing	High	Procurement; system owner; privacy officer; vendor manager	Vendor due diligence; API restriction; DPA; SLA; PIA	Vendor register; DPA; SLA; due diligence report; PIA record
Unmanaged retention and deletion	Medium	Data owner; records manager; system owner	Retention schedule; deletion workflow; disposal approval	Retention policy; deletion log; disposal approval record
Learning analytics and monitoring misuse	Medium	Academic unit; ethics board; privacy officer; system owner	Analytics access control; purpose limitation; anonymization; ethics review	Analytics policy; access log; ethics approval; audit trail
Weak handling of data subject rights	Medium	Privacy officer; service desk; legal/compliance	Request tracking; identity verification; escalation; SLA monitoring	Request ticket; verification record; SLA dashboard; response evidence

Table 10. Cybersecurity risk-control-evidence matrix

Cybersecurity/ compliance risk	Priority	Control owner	Key controls	Compliance evidence
Unauthorized access to SIAKAD/LMS	High	ICT directorate; system owner; security team	RBAC; MFA; encryption; log monitoring; periodic access review	Access matrix; MFA report; log review record; access review approval
Credential compromise and phishing	High	Security team; user support; service desk	Awareness training; MFA; anomaly detection; phishing reporting workflow	Training record; alert log; incident ticket; reporting dashboard
Web application/API vulnerability	High	Application owner; security team; developer team	Secure coding review; vulnerability scanning; patch management; penetration testing	Scan report; patch log; code review record; penetration test report
Ransomware or destructive incident	High	Security team; ICT directorate; management	Backup testing; EDR/SIEM; incident response plan; recovery procedure	Backup test result; incident playbook; RCA; recovery evidence
Insecure API integration with third-party services	High	Application owner; security team; vendor manager	API inventory; token/key review; API security testing; integration agreement	API register; token rotation record; API test result; access log review
Weak monitoring and log governance	Medium	Security team; internal auditor; system owner	Logging policy; retention control; privileged access restriction; periodic review	Log policy; retention schedule; privileged access list; audit review record

Table 11. Audit evidence schema for academic information systems

Evidence object	Source system	Minimum fields	Control purpose	Responsible owner	Audit use
Data inventory	SIAKAD, LMS, library system, repository	data element, owner, purpose, category, retention, location	establish data visibility and minimization	system owner; data owner; privacy officer	verify scope of personal data processing
Data lineage record	database, integration layer, ETL/API documentation	source, destination, transfer purpose, vendor, timestamp, retention	trace academic data flows	system owner; application owner	test data-flow accountability

Access matrix	IAM, SIAKAD/LMS administration	user, role, privilege, approval, review date	control authorization and segregation of duties	ICT directorate; system owner	review least privilege and access approval
Authentication and log review record	SSO, LMS, SIAKAD, server logs	user ID, role, timestamp, action, IP/device, reviewer	detect unauthorized or suspicious activity	security team; internal auditor	support incident investigation and periodic control review
API register and token rotation record	API gateway, integration documentation	endpoint, token owner, permission, expiry, rotation date, vendor	control third-party access boundaries	application owner; vendor manager	verify API governance and key management
Vendor evidence file	procurement and vendor management system	DPA, SLA, due diligence result, audit rights, processing location	govern external processors	procurement; privacy officer; vendor manager	test vendor accountability and contractual controls
Rights request ticket	service desk/privacy workflow	request type, identity verification, status, SLA, response evidence	demonstrate data subject rights handling	privacy officer; service desk	verify timeliness and completeness of responses
Incident ticket and recovery evidence	SOC/helpdesk/incident management	incident type, severity, timeline, RCA, containment, recovery, communication	demonstrate breach and incident response readiness	security team; ICT directorate; management	test response, escalation, and recovery evidence
Compliance dashboard	GRC or reporting dashboard	control status, evidence status, unresolved risks, owner, review date	monitor continuous improvement	management; internal auditor; privacy officer	support management review and audit preparation

4.4 Traceability Walkthrough Scenario

To demonstrate how the artifact can be used, this section provides an illustrative third-party LMS/plugin processing scenario. The example is not an empirical case result; it is a design scenario showing how an obligation can be translated into a risk, then into controls, ownership, evidence, and audit questions. In this scenario, a university uses a learning platform or plugin that processes student identities, learning records, behavioral logs, or assessment data. The regulatory trigger is lawful processing and controller/processor responsibility under the PDP Law, combined with electronic-system reliability and vendor governance obligations. The main risk is that external processing, API permissions, processing location, and retention may be insufficiently documented. The corresponding controls include vendor due diligence, a data processing agreement, SLA, API permission boundary, privacy impact assessment, access review, and incident escalation clauses. The expected evidence includes a vendor register, DPA, SLA, API inventory, access log review, due diligence report, PIA record, and vendor incident communication record.

The walkthrough clarifies the added value of the model. Instead of treating compliance as a privacy notice or vendor contract alone, the traceability chain requires the institution to identify the processing purpose, define API boundaries, assign responsible owners, monitor vendor obligations, and retain evidence that can be reviewed. This strengthens the relationship between privacy governance, cybersecurity safeguards, and audit readiness.

4.5 Artifact 5: Implementation Roadmap

The fifth artifact converts the model into an implementation sequence. The roadmap does not replace institutional project planning, but it provides a practical order of activities for academic institutions that need to move from policy awareness to evidence-based control operation. Table 12 emphasizes data flow mapping, privacy and cybersecurity risk assessment, governance structure, technical controls, rights management, vendor governance, incident response, audit monitoring, and RACI/accountable role allocation.

Table 12. Implementation roadmap for academic information systems

Stage	Main activity	RACI/accountable roles	Expected evidence
1. Data inventory and flow mapping	Identify data elements, owners, systems, vendors, storage locations, and transfer paths	System owner; data owner; privacy officer	Data inventory; data-flow diagram; processing register
2. Privacy and cybersecurity risk assessment	Assess lawful basis, sensitivity, likelihood, impact, threat exposure, and vendor risk	Privacy officer; security team; internal auditor	Risk register; PIA; cybersecurity assessment

3. Policy and governance structure	Define privacy policy, RACI, system ownership, privacy officer role, and governance committee	Management; legal/compliance; ICT directorate	Policy documents; RACI matrix; appointment letter
4. Technical control implementation	Implement RBAC, MFA, encryption, logging, backup, vulnerability management, and retention controls	ICT directorate; security team; application owner	Control configuration; access matrix; scan report; backup test
5. Data subject rights management	Provide workflow for access, correction, deletion, objection, and consent withdrawal	Privacy officer; service desk; legal/compliance	Request log; SLA dashboard; response evidence
6. Third-party/vendor governance	Review LMS, cloud, authentication, payment, analytics, and library providers	Procurement; vendor manager; system owner	Vendor due diligence; DPA; SLA; audit rights
7. Incident response and breach notification	Establish detection, escalation, investigation, communication, containment, and recovery procedures	Security team; ICT directorate; management	Incident playbook; drill report; RCA; communication record
8. Audit, monitoring, and continuous improvement	Evaluate control effectiveness and update policies, risks, systems, and evidence repositories	Internal auditor; management; privacy officer	Internal audit report; compliance dashboard; management review

4.6 Comparative Discussion

The proposed model advances prior research in four ways. First, it reframes personal data protection as an information-systems governance capability. Legal-normative studies are useful for interpreting statutory duties, but they often stop before specifying system risks, control ownership, and evidence artifacts. In contrast, this model requires each duty to be represented by a risk scenario, a control objective, a control activity, an accountable owner, and reviewable evidence.

Second, the model expands beyond technical or COBIT-domain assessments of academic information systems. COBIT-based audits and vulnerability studies provide important insights into security controls and audit domains [4][5][7], but they do not fully address consent, data subject rights, privacy notices, data minimization, third-party processing, and privacy officer responsibility. Conversely, legal PDP and GDPR-readiness studies provide compliance logic [10][19][21][37][38], but they often lack system-level control details. The proposed framework connects both domains through end-to-end traceability.

Third, the model integrates privacy governance and cybersecurity governance. Unauthorized access, ransomware, third-party misuse, insecure APIs, unmanaged retention, and weak monitoring are not only security concerns; they also affect privacy rights, institutional trust, and legal accountability. The combined privacy and cybersecurity matrices therefore help institutions avoid fragmented compliance programs and align technical safeguards with personal data protection obligations.

Fourth, the model is adapted to academic information systems. Academic institutions operate complex ecosystems involving students, lecturers, administrative staff, libraries, repositories, learning analytics, proctoring services, cloud platforms, and external vendors. These characteristics create domain-specific governance needs that are not fully addressed by generic control frameworks. The model addresses this gap by connecting academic data flows, control ownership, vendor governance, evidence requirements, and continual improvement. The novelty is therefore not a new legal interpretation but a traceable governance architecture for converting regulation into control operation and audit evidence.

Across the compared frameworks, the distinctive element of the proposed model is its traceability coverage across regulation, risk, control objective, control activity, accountable owner, and evidence artifact. Existing frameworks provide strong principles, control domains, or risk-management logic, but they usually cover only part of this chain and require institutional translation before they can be audited in academic information systems.

The model also implies an implementation trade-off. Universities may seek comprehensive compliance coverage, but institutional feasibility depends on system maturity, distributed system ownership, available security capability, vendor cooperation, and evidence-management discipline. Therefore, audit readiness should not be interpreted as proof of control effectiveness; it is a staged capability that must be strengthened through monitoring, testing, and independent validatio

4.7 Contributions and Implications

The theoretical contribution is the integration of privacy ethics, digital regulation, personal data protection, cybersecurity governance, IT governance, and compliance assurance into one traceable information-systems governance model. This extends privacy governance literature by positioning accountability as a chain of system risks, controls, owners, and evidence rather than as a policy statement alone.

The methodological contribution is the regulation-risk-control-owner-evidence traceability logic for constructing a governance artifact from legal and ethical obligations. This logic can be reused in other regulated digital services where compliance obligations must be translated into information-system controls and assurance artifacts.

The practical contribution is a baseline for academic institutions to develop data inventories, access matrices, API registers, vendor due diligence, data processing agreements, incident playbooks, rights request workflows, compliance dashboards, and internal audit evidence. System owners can use the artifact to identify required controls; security teams can prioritize safeguards; privacy officers can coordinate rights and vendor governance; and auditors can test evidence.

The policy implication is that Indonesian personal data protection implementation in higher education requires institutional capacity, control maturity, and evidence-based assurance. Regulators and sectoral associations can adapt the model to develop

higher-education implementation guidelines, especially for universities transitioning from general electronic-system management toward accountable privacy and cybersecurity governance.

4.8 Limitations and Future Research

This study is conceptual and literature-based. It does not yet validate the model through interviews, surveys, focus groups, Delphi panels, expert judgment, or implementation in a university. The artifact has not been assessed against a deployed academic information system, and the proposed audit evidence schema represents a structured evidence design rather than evidence collected from an operational system. Risk priorities are conceptual and must be recalibrated in real institutions using actual architecture, data sensitivity, threat exposure, vendor dependency, control maturity, and institutional risk appetite. The regulatory and framework mapping is interpretive and should be refined through validation involving IT auditors, system owners, cybersecurity teams, legal experts, privacy officers, internal auditors, and vendor managers.

Future research should operationalize the design science evaluation phase through expert validation, Delphi evaluation, and institutional case studies. A practical evaluation scenario can test the model on subsystems such as digital library services, research repositories, academic database services, LMS platforms, or student service portals. Subsequent work should examine whether data inventories, access matrices, API registers, log-monitoring records, uptime metrics, incident tickets, vendor agreements, and privacy request workflows provide sufficient audit evidence. Future research should also develop a maturity assessment instrument and measure the relationship between privacy governance maturity, user trust, cybersecurity resilience, and compliance readiness

5. CONCLUSSION

This article developed a traceable privacy and cybersecurity compliance control baseline for Indonesian academic information systems. The model is based on a structured evidence base of 55 references covering academic literature, foundational privacy sources, Indonesian regulatory and education-sector documents, international governance frameworks, cybersecurity frameworks, and design science methodology. It integrates ethical principles, regulatory obligations, information-system risks, IT governance controls, control ownership, and compliance assurance into a five-layer framework.

The main contribution is the translation of Indonesian personal data protection, electronic-system, cybersecurity, and education-sector data governance obligations into implementable governance mechanisms: regulatory-to-risk mapping, control-evidence mapping, framework reconciliation, privacy and cybersecurity risk-control-evidence matrices, an audit evidence schema, and an implementation roadmap. The proposed model demonstrates how privacy and cybersecurity compliance can be treated as an information-systems governance capability rather than as legal documentation alone.

The proposed model should be viewed as a conceptual baseline for evidence-based privacy and cybersecurity governance in academic information systems. It supports audit-readiness preparation by linking regulatory obligations to risks, controls, owners, and evidence artifacts, but it does not prove operational effectiveness. Its practical applicability requires future expert review, Delphi evaluation, institutional case studies, and development into a maturity model or audit instrument for academic information systems.

REFERENCES

[1] D. J. Solove, “A taxonomy of privacy,” University of Pennsylvania Law Review, vol. 154, no. 3, pp. 477-564, 2006.

[2] N. Vieira Dantas, A. P. H. de Gusmão, and M. T. Gonzaga, “A multicriteria model to support decisions regarding data protection compliance,” Journal of Decision Systems, vol. 33, no. 4, pp. 744-760, 2024, doi: 10.1080/12460125.2023.2263683.

[3] C. Del-Real, E. De Busser, and B. van den Berg, “A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies,” International Review of Law, Computers & Technology, vol. 39, no. 3, pp. 374-405, 2025, doi: 10.1080/13600869.2025.2457227.

[4] Miftahurrizqi, I. S. Windiarti, and A. Prabowo, “Analisis keamanan sistem pada sistem informasi akademik menggunakan COBIT 5 framework pada sub domain DSS05,” Jurnal Sains Komputer dan Teknologi Informasi, vol. 3, no. 2, pp. 75-80, 2021, doi: 10.33084/jsakti.v3i2.2293.

[5] T. Ariyadi, T. L. Widodo, N. Apriyanti, and F. S. Kirana, “Analisis kerentanan keamanan sistem informasi akademik Universitas Bina Darma menggunakan OWASP,” Techno.COM, vol. 22, no. 2, pp. 418-429, 2023.

[6] Y. Hamdi, C. E. Gunawan, and I. S. Putra, “Analisis perilaku kesadaran privasi data pengguna sistem informasi akademik dengan pendekatan Technology Threat Avoidance Theory,” TIN: Terapan Informatika Nusantara, vol. 6, no. 1, pp. 24-33, 2025, doi: 10.47065/tin.v6i1.7590.

[7] A. S. Putra, E. R. Sambhodo, F. M. Aisfa, M. S. Nur, and M. A. Priyanta, “Audit menggunakan COBIT 5 domain DSS pada SIAKAD Universitas Merdeka Malang,” SATESI: Jurnal Sains Teknologi dan Sistem Informasi, vol. 5, no. 1, pp. 31-37, 2025, doi: 10.54259/satesi.v5i1.4044.

[8] T. I. Putra, N. Fibrianti, and M. R. Fakhrullah, “Basis of Data Protection Officer appointment: Comparative study of Indonesia and European Union regulation,” SASI, vol. 31, no. 1, pp. 1-15, 2025, doi: 10.47268/sasi.v31i1.2068.

[9] C. Labadie and C. Legner, “Building data management capabilities to address data protection regulations: Learnings from EU-GDPR,” Journal of Information Technology, vol. 38, no. 1, pp. 16-44, 2023, doi: 10.1177/02683962221141456.

[10] N. A. Zaguir, G. H. de Magalhães, and M. de M. Spinola, “Challenges and enablers for GDPR compliance: Systematic literature review and future research directions,” IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3406724.

[11] O. Afolalu and M. S. Tsoeu, “Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions,” Future Internet, vol. 17, no. 12, art. 575, 2025, doi: 10.3390/fi17120575.

[12] M. Salam, K. A. Abu Bakar, A. T. Abdul Ghani, and A. H. M. Aman, "Cybersecurity in higher education institutions digitalisation: Addressing threats and vulnerabilities," SAGE Open, Jan.-Mar. 2026, doi: 10.1177/21582440251413473.

[13] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," MIS Quarterly, vol. 28, no. 1, pp. 75-105, 2004, doi: 10.2307/25148625.

[14] K. D. Schubert and D. Barrett, "Data governance, privacy, and ethics," in Human Privacy in Virtual and Physical Worlds: Multidisciplinary Perspectives, M. C. Lacity and L. Coon, Eds. Cham: Springer Nature Switzerland, 2024, pp. 87-110, doi: 10.1007/978-3-031-51063-2_5.

[15] J. Wiwoho, U. K. Pati, and A. M. Pratama, "Enabling data portability and interoperability under Indonesia's data protection law," Masalah-Masalah Hukum, vol. 53, no. 3, pp. 271-282, 2024.

[16] F. Burmeister, C. Kurtz, and I. Schirmer, "Governing information privacy in data ecosystems with architectural thinking," Electronic Markets, vol. 35, art. 67, 2025, doi: 10.1007/s12525-025-00808-5.

[17] M. Rhahla, S. Allegue, and T. Abdellatif, "Guidelines for GDPR compliance in Big Data systems," Journal of Information Security and Applications, vol. 61, art. 102896, 2021.

[18] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," MIS Quarterly, vol. 35, no. 4, pp. 989-1015, 2011, doi: 10.2307/41409970.

[19] J. Fernandes, C. Machado, and L. Amaral, "Identifying critical success factors for the General Data Protection Regulation implementation in higher education institutions," Digital Policy, Regulation and Governance, vol. 24, no. 4, pp. 355-379, 2022, doi: 10.1108/DPRG-03-2021-0041.

[20] L. Magnusson, S. Iqbal, P. Elm, and F. Dalipi, "Information security governance in the public sector: Investigations, approaches, measures, and trends," International Journal of Information Security, vol. 24, art. 177, 2025, doi: 10.1007/s10207-025-01097-x.

[21] A. A. Nugraha and A. H. Nasyuha, "Integrating ISO 27001 and Indonesia's personal data protection law for data protection requirement model," Journal of Information Systems and Informatics, vol. 6, no. 2, 2024, doi: 10.51519/journalisi.v6i2.754.

[22] M. Yang, L. Tan, X. Chen, Y. Luo, Z. Xu, and X. Lan, "Laws and regulations tell how to classify your data: A case study on higher education," Information Processing & Management, vol. 60, art. 103240, 2023, doi: 10.1016/j.ipm.2022.103240.

[23] C. K. Bareh and T. Temjen, "Library privacy framework: Comparative review of data protection laws towards maturity model," Journal of Librarianship and Information Science, 2025, doi: 10.1177/09610006251372634.

[24] F. Knoke and I. Nwankwo, "Practitioner's Corner. Managing Data Protection Compliance through Maturity Models: A Primer," European Data Protection Law Review, vol. 8, no. 4, pp. 536-543, 2022, doi: 10.21552/edpl/2022/4/14.

[25] D. Torre, M. Alferez, G. Soltana, M. Sabetzadeh, and L. Briand, "Modeling data protection and privacy: Application and experience with GDPR," Software and Systems Modeling, vol. 20, no. 6, pp. 2071-2087, 2021, doi: 10.1007/s10270-021-00935-5.

[26] F. Bélanger and R. E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," MIS Quarterly, vol. 35, no. 4, pp. 1017-1041, 2011, doi: 10.2307/41409971.

[27] H. Ajiraga, "Peran dan tanggungjawab Data Protection Officer dalam pelaksanaan perlindungan data pribadi," Asas Wa Tandhim: Jurnal Hukum, Pendidikan & Sosial Keagamaan, vol. 5, no. 1, pp. 261-290, 2026.

[28] S. Yuniarti, "Petugas/Pejabat pelindungan data pribadi dalam ekosistem perlindungan data pribadi: Indonesia, Uni Eropa dan Singapura," Jurnal BECOSS, vol. 4, no. 2, pp. 111-120, 2022, doi: 10.21512/becossjournal.v4i2.8377.

[29] H. Nissenbaum, "Privacy as contextual integrity," Washington Law Review, vol. 79, no. 1, pp. 119-158, 2004.

[30] A. Cavoukian, Privacy by Design: The 7 Foundational Principles. Ontario, Canada: Information and Privacy Commissioner of Ontario, 2011.

[31] M. R. Sanfilippo, N. Apthorpe, K. Brehm, and Y. Shvartzshnaider, "Privacy governance not included: Analysis of third parties in learning management systems," Information and Learning Sciences, vol. 124, no. 9/10, pp. 326-349, 2023, doi: 10.1108/ILS-04-2023-0033.

[32] C. Mutimukwe, O. Viberg, C. McGrath, and T. Cerratto-Pargman, "Privacy in online proctoring systems in higher education: Stakeholders' perceptions, awareness and responsibility," Journal of Computing in Higher Education, vol. 38, pp. 732-761, 2026, doi: 10.1007/s12528-025-09461-5.

[33] M. Francis, M. B. M. Avoseh, K. Card, L. Newland, and K. Streff, "Student privacy and learning analytics: Investigating the application of privacy within a student success information system in higher education," Journal of Learning Analytics, vol. 10, no. 3, pp. 102-114, 2023, doi: 10.18608/jla.2023.7975.

[34] M. D. Birnhack and G. Mundlak, "The Brussels effect(s) and the rise of a privacy profession," International Data Privacy Law, vol. 15, no. 2, pp. 138-155, 2025, doi: 10.1093/idpl/ipaf005.

[35] H. M. Naguib, H. M. Kassem, and A. E.-H. M. Abou Naem, "The impact of IT governance and data governance on financial and non-financial performance," Future Business Journal, vol. 10, art. 15, 2024, doi: 10.1186/s43093-024-00300-0.

[36] H. Ketmaneechairat, M. Maliyaem, and P. Puttawattanakul, "Towards a management system framework for the integration of personal data protection and data governance: A case study of Thai laws and practices," International Journal of Technology, vol. 15, no. 1, pp. 219-229, 2024, doi: 10.14716/ijtech.v15i1.5885.

[37] J. Fernandes, C. F. Machado, and L. Amaral, "Towards a readiness model derived from critical success factors for the general data protection regulation implementation in higher education institutions," Strategic Management, vol. 28, no. 1, pp. 004-019, 2023, doi: 10.5937/StraMan2200033F.

[38] C. Negri-Ribalta, M. Lombard-Platet, and C. Salinesi, "Understanding the GDPR from a requirements engineering perspective: A systematic mapping study on regulatory data protection requirements," Requirements Engineering, vol. 29, pp. 523-549, 2024, doi: 10.1007/s00766-024-00423-4.

[39] J. G. Proudfoot, W. A. Cram, and S. Madnick, "Weathering the storm: Examining how organisations navigate the sea of cybersecurity regulations," European Journal of Information Systems, vol. 34, no. 3, pp. 436-459, 2025, doi: 10.1080/0960085X.2024.2345867.

[40] Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection, 2022.

[41] Republic of Indonesia, Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, 2019.

[42] Republic of Indonesia, Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, 2024.

[43] Ministry of Communication and Informatics of the Republic of Indonesia, Regulation No. 5 of 2020 on Private Electronic System Operators, 2020.

[44] Ministry of Communication and Informatics of the Republic of Indonesia, Regulation No. 10 of 2021 amending Regulation No. 5 of 2020 on Private Electronic System Operators, 2021.
[45] Republic of Indonesia, Presidential Regulation No. 47 of 2023 on National Cybersecurity Strategy and Cyber Crisis Management, 2023.
[46] NIST, NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0. Gaithersburg, MD: National Institute of Standards and Technology, 2020.
[47] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD, 2013.
[48] ISO/IEC, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements. Geneva: ISO, 2022.
[49] NIST, The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: National Institute of Standards and Technology, 2024.
[50] ISACA, COBIT 2019 Framework: Governance and Management Objectives. Schaumburg, IL, USA: ISACA, 2018.
[51] ISO/IEC, ISO/IEC 27701:2025 Information Security, Cybersecurity and Privacy Protection - Privacy Information Management Systems - Requirements and Guidance. Geneva, Switzerland: ISO, 2025.
[52] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," Journal of Management Information Systems, vol. 24, no. 3, pp. 45-77, 2007, doi: 10.2753/MIS0742-1222240302.
[53] ISO/IEC, ISO/IEC 27005:2022 Information Security, Cybersecurity and Privacy Protection - Guidance on Managing Information Security Risks. Geneva, Switzerland: ISO, 2022.
[54] Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia, Regulation No. 31 of 2022 on One Data for Education, Culture, Research, and Technology, 2022.
[55] Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia, Regulation No. 53 of 2023 on Quality Assurance of Higher Education, 2023.