Journal of Deep Learning, Computer Vision and Digital Image Processing
E-ISSN: 2986-8939 P-ISSN: 2986-8920
Vol. 4, No. 3, September 2026
DOI. https://doi.org/10.61255/decoding.v4i3.2079

Mapping COBIT 2019 Capability to ISO/IEC 27002:2022 Controls for Managed Security Services in Higher Education Cybersecurity Governance

Rossa Alba Kirana ✉
Universitas Sriwijaya, Indonesia

Ali Ibrahim
Universitas Sriwijaya, Indonesia

OPEN ACCESS

ARTICLE HISTORY
Received: June 8, 2026
Revised: July 14, 2026
Accepted: August 23, 2026

KEYWORDS
Capability assessment;
COBIT 2019;
Cybersecurity governance;
Higher education;
ISO/IEC 27002:2022

ABSTRACT

Purpose – To assess three prioritized COBIT 2019 objectives at an Indonesian private university and map DSS05 (Managed Security Services) findings to ISO/IEC 27002:2022 controls.

Methods – An embedded case study at Universitas Indo Global Mandiri combined documents, observation, interviews, and a binary checklist completed by five RACI-selected role holders. Capability and evidence completeness were assessed for APO04, APO07, and DSS05; control mapping covered DSS05 only.

Findings – All three objectives achieved 100% at level 1. Level-2 scores were 79.98%, 83.81%, and 82.00%, respectively, below the Fully Achieved boundary of more than 85%. Each therefore remained at level 1 under the study's scoring rule, against a target of level 4. Evidence completeness was 75.00%, 88.89%, and 92.86%. Missing evidence included innovation-decision records, competency review, resource-utilization records, and physical-access logging.

Research implications – The single institution and five respondents limit generalizability. Documentary evidence and self-reported capability do not establish technical control effectiveness or improved security outcomes.

Originality – The DSS05 crosswalk links reported capability, institutional evidence, ISO/IEC 27002:2022 controls, and proposed corrective actions within a bounded case.

INTRODUCTION

Higher education institutions depend on interconnected digital infrastructures for learning management, student information, finance, research, human resources, and institutional decision-making. This dependence expands the attack surface, because universities combine open academic networks, heterogeneous users, legacy applications, cloud services, personally owned devices, and large repositories of personal and research data. Recent scholarship therefore treats cybersecurity as an institutional governance responsibility, not only a technical function. That responsibility requires aligning risk ownership, strategic priorities, resources, accountability, and operational controls [1], [2], [3],[4]. The persistence of phishing, ransomware, credential compromise, malware, and unauthorized access in educational settings shows that isolated security tools are insufficient when policies, competencies, monitoring, and evidence of control performance remain fragmented [5], [6],[7].

Correspondence Author: ✉ rossaalbakirana03@gmail.com
To cite this article: Kirana, R. A., & Ibrahim, A. (2026). Mapping COBIT 2019 Capability to ISO/IEC 27002:2022 Controls for Managed Security Services in Higher Education Cybersecurity Governance. *Journal of Deep Learning, Computer Vision and Digital Image Processing*, *4*(3), 143–168. https://doi.org/10.61255/decoding.v4i3.2079

This is an open access article under the CC BY-SA license

Openness and collaboration must coexist with confidentiality, integrity, availability, privacy, and service continuity. Empirical and review studies show that organizational culture, employee behavior, leadership commitment, security awareness, and clearly assigned responsibilities affect security outcomes [8], [9], [10], [11]. Governance evaluation must therefore connect institutional objectives with repeatable management practices and verifiable safeguards. COBIT 2019 supports the first part of this requirement. It structures governance and management objectives and enables process-capability assessment. ISO/IEC 27002:2022 supports the second part. It specifies organizational, people, physical, and technological information-security controls [12], [13], [14].

Assessment Boundary and Institutional Context

Case institution. Universitas Indo Global Mandiri (UIGM), Palembang, is a private university whose digital-service functions are organized under an internally designated "E-Government" structure. This is the institution's own term for the unit that governs and delivers digital administrative and academic services. It is distinct from the national e-government program. The Head of E-Government holds strategic and budgetary responsibility for digital-service planning. The Head of E-Government Governance oversees policy, compliance, and process. The Head of Information and Communication Technology (ICT) manages infrastructure, networks, and endpoints. The Head of Information Security designs and monitors security controls. The university's "digital-government master plan" is a multi-year digital-service roadmap prepared by the E-Government unit and approved by university leadership; it functions like an institutional IT strategic plan.

Assessed scope. The empirical assessment covers three COBIT 2019 management objectives: APO04 (Managed Innovation), APO07 (Managed Human Resources), and DSS05 (Managed Security Services). They were selected through a design-factor analysis (see Method). The assessed units are the central E-Government unit, which includes ICT operations and information security, and the General Affairs and Human Resources unit. Together they are accountable for most centrally managed services: the learning-management system, student-information system, core network and server infrastructure, and centrally administered endpoints. Faculty-level and laboratory-level systems, vendor-hosted services outside E-Government oversight, and physical infrastructure outside the central data center and administrative offices were not assessed.

Why a design-factor boundary, and what it implies. COBIT 2019 does not prescribe assessing all of its objectives. Its design guide tailors the governance system to the enterprise through design factors [15]. Using that output as the boundary therefore follows the framework's own logic and keeps the assessment feasible for a single case. However, a design-factor ranking measures priority for information and technology (I&T) governance in general. It is not a cyber-risk ranking. The study therefore distinguishes two properties of the selected objectives.

DSS05 is directly security-relevant. It governs the operation of security services such as malware protection, network and endpoint security, identity and access management, physical access, and monitoring.

APO07 is indirectly security-relevant. Staffing, competence, and succession determine whether technical controls are performed consistently rather than episodically [8], [9], [16].

APO04 is the least direct. Its link to security is that innovation decisions determine when security requirements enter new initiatives.

APO12 (Managed Risk), APO13 (Managed Security), and DSS04 (Managed Continuity) also have direct security relevance. They ranked below the priority threshold applied in this study and were not assessed. As a result, this study makes no statement about the institution's risk-management process, security strategy and management-system governance, or continuity arrangements. Gaps in those objectives could exist and would not appear here. The study is therefore best read as an assessment of three prioritized I&T objectives with cybersecurity implications, centered on DSS05. It is not an assessment of cybersecurity governance as a whole.

Why only DSS05 is mapped to ISO/IEC 27002:2022. DSS05 describes operational security practices that correspond directly to the control catalogue of ISO/IEC 27002:2022. APO04 and APO07 describe

innovation-management and workforce-governance practices, which relate to ISO/IEC 27002:2022 only through its organizational and people themes. A direct, practice-to-control mapping is therefore defensible for DSS05 only. Extending it to APO07 and APO04 is a distinct task that requires its own mapping criteria and is identified as future work. The integration reported here is consequently selective, centered on DSS05, and not an integration of the two frameworks across all assessed objectives.

Transferability conditions. The findings may be analytically transferable to institutions with three features: (a) a centralized IT/E-Government structure with one accountable unit for core digital services; (b) constrained specialist staffing, in which role holders combine governance, technical, and security responsibilities; and (c) reliance on locally developed planning and policy documents rather than a certified management system. Institutions with highly decentralized IT, a certified information-security management system, or extensive outsourced security operations would need to re-examine the design factors and respondent selection before transferring these findings.

State of the Art

The recent literature falls into three streams.

Cybersecurity as an enterprise-governance problem. Systematic reviews report that effective information-security governance depends on strategic alignment, accountability, risk management, compliance, performance measurement, and continuous monitoring [1], [12], [17]. Governance information is often not translated into decision-relevant metrics, so senior leaders lack a clear view of cyber-risk exposure and control effectiveness [3], [18]. This matters in universities, where decision rights are distributed across central IT, faculties, laboratories, vendors, and individual users.

Human and organizational capability. Cybersecurity-culture research shows that secure behavior is shaped by shared norms, management support, communication, training, and the usability of security requirements [8], [9], [16]. Studies of university populations report gaps between awareness, confidence, and protective behavior in password management, email use, mobile-device security, and phishing response [6], [10], [19]. These findings link APO07 to cybersecurity in a concrete way.

Standards and integrated control frameworks. Organizations often combine standards to reconcile strategic governance, risk assessment, operational control, and compliance [12], [13], [14], [17]. COBIT 2019 contributes a governance-system design logic, defined management objectives, responsibility structures, and capability-based evaluation. ISO/IEC 27002:2022 contributes 93 controls grouped into organizational, people, physical, and technological themes. The two are complementary, not equivalent. COBIT evaluates how well processes are governed and managed. ISO/IEC 27002:2022 clarifies which controls, and which implementation evidence, should be examined. Identity management, access control, logging, monitoring, vulnerability management, endpoint protection, and network security recur as foundations of cyber resilience [4], [7], [20], [21].

Why this combination, rather than an alternative. Three alternatives are plausible: an ISO/IEC 27001 information-security management system assessment [22], a security-framework or maturity-model assessment such as those surveyed in [23] and [24], and a generic governance-to-control crosswalk. Each answers a different question. An ISMS assessment tests conformity to management-system requirements. Maturity-model assessments typically rate overall posture against a generic scale. A generic crosswalk relates frameworks without a case-specific target. The COBIT-plus-ISO combination suits the present problem for three reasons.

COBIT's design factors provide a target capability level specific to the institution, which makes the gap measurable.

COBIT's capability levels show whether a practice is performed in a managed way.

ISO/IEC 27002:2022 then names the controls and evidence to examine for each gap.

A single-framework evaluation would operationalize at most one of these three steps in this case. The study does not claim that the combination is statistically superior to either framework used alone, and it did not test this.

Gap and contribution. Direct empirical precedents that jointly apply COBIT capability assessment and an ISO/IEC 27002 control mapping within one higher-education case remain scarce. Related work has applied COBIT 2019 to IT governance in Indonesian institutions without an ISO/IEC 27002 mapping [14]. Other work has examined information-security governance in higher education using different maturity or governance instruments [25]. The gap is distinguished at two levels.

Theoretical/methodological gap. Few studies specify how a COBIT capability gap can be traced to individual ISO/IEC 27002:2022 controls and to case evidence. This study contributes a worked, selective example for one objective.

Application gap. Evidence of this kind is limited in Indonesian private higher education, particularly where document presence, consistent execution, and control effectiveness are kept analytically separate.

The contribution is primarily an applied analytical one with a limited methodological element, namely the DSS05 mapping protocol. It is not a new framework, a comparative validation, or a demonstration of improved security outcomes. Where the Discussion refers to what the integration "reveals," it means the worked example in Table 5 and the Results. There, the ISO mapping makes control-level deficiencies explicit that a COBIT capability percentage expresses only in aggregate. It does not mean that either framework alone could not have found the same deficiencies by other means.

Research objective and propositions. This study evaluates three prioritized COBIT 2019 management objectives with cybersecurity implications at one higher education institution and maps the DSS05 findings to ISO/IEC 27002:2022 controls. Specifically, it (1) identifies the COBIT 2019 objectives prioritized by the institution's design factors; (2) determines current and target capability levels and the resulting gaps; (3) maps DSS05 practices to ISO/IEC 27002:2022 controls with an explicit, auditable rationale; and (4) proposes a criterion-based sequence of improvement actions for the assessed scope.

Because the research is an evaluative case study and not a causal experiment, two propositions organize interpretation. They are not statistical hypotheses.

P1: Reading COBIT 2019 capability results together with an explicit ISO/IEC 27002:2022 mapping makes specific security deficiencies traceable in a way an aggregate capability percentage alone does not.

P2: The availability of security documents does not necessarily correspond to fully achieved process capability when implementation, logging, monitoring, and evidence are inconsistent.

The priority assigned to DSS05 is not a proposition. It is an analytical result derived from the explicit criteria stated under Implications.

METHOD

Research Design

The study is an embedded single-case evaluation at UIGM, following Yin's embedded case-study logic [26]. The case is the university's centrally governed digital-service function. The three COBIT 2019 objectives (APO04, APO07, and DSS05) are the embedded units of analysis. Each unit has its own design-factor priority, respondent subset, and capability score. DSS05 also has a control mapping. The units are integrated at the case level.

Why a case design. The phenomenon is a contemporary governance arrangement whose practices cannot be separated from the institutional setting in which they operate. A case design is appropriate

under those conditions [26]. The embedded structure allows the three objectives to be compared without losing the shared institutional context.

Why multiple evidence types. The design uses a sequential combination of quantitative and qualitative evidence, in the sense of [27]. This combination is needed because a COBIT capability rating depends on both performance of activities and the existence of supporting work products. Neither type of evidence is sufficient alone.

A binary questionnaire gives comparable capability scores across objectives and respondents. Alone, it is self-reported and may overstate or understate practice.

Observation, interviews, and institutional documents give context and allow responses to be corroborated against work products. Alone, they do not give comparable, repeatable scores.

Combining them lets the study separate three layers: reported capability, documentary evidence, and control interpretation.

Status of the qualitative strand. Observation, semi-structured interviews, and document review were used to establish context, inform the design factors and respondent selection, and corroborate questionnaire responses. They were not subjected to systematic thematic coding. The qualitative strand therefore serves contextual and triangulation purposes and is not a separately analyzed qualitative study. The design is best described as an embedded case study using multiple quantitative and qualitative evidence sources.

Sequence and scope of analysis. The stages are sequential, and not all apply to every objective (Table 1). The asymmetry is deliberate. Capability assessment and evidence review apply to all three objectives. ISO/IEC 27002:2022 mapping applies to DSS05 only, for the reasons given under Assessment Boundary. ISO/IEC 27002:2022 was used as a control catalogue, not as a maturity scale or certification audit. All capability ratings are institutional self-assessments by the authors. They are not formal external COBIT assessments.

Table 1. Analytical sequence and scope of each stage

Stage	Activity	Applies to	Output
1	Observation and document review	Case level	Institutional context
2	Design-factor scoring (11 factors)	All candidate objectives	Priority objectives and target capability levels
3	RACI-to-position mapping	APO04, APO07, DSS05	Respondent panel (Table 2)
4	Binary checklist and sequential capability rating	APO04, APO07, DSS05	Current level and gap
5	Evidence register and triangulation	APO04, APO07, DSS05	Evidence completeness (reported separately from capability)
6	ISO/IEC 27002:2022 mapping	DSS05 only	Control crosswalk (Table 5)
7	Gap analysis and improvement sequencing	Case level, with control detail for DSS05	Roadmap (Table 7 and 8)

Study provenance. This article draws on a thesis-based evaluation of IT governance at the same institution. The thesis performed the design-factor analysis, the questionnaire administration and scoring, and the underlying document and interview collection. For this article, the authors

additionally undertook the DSS05 control mapping (Table 5), the activity-level reanalysis of respondent disagreement, and the construction of the criterion-based roadmap (Table 7 and 8).

Case Boundary and Embedded Units of Analysis

The case boundary is the centrally governed digital-service function described under Assessment Boundary. Three embedded units were defined: (i) innovation governance (APO04), covering how the institution identifies, evaluates, and learns from technology-enabled initiatives; (ii) human-resource governance for IT and security-relevant roles (APO07), covering staffing, competency, and succession; and (iii) security-service governance (DSS05), covering the operational management of security controls. Each unit was assessed against its own RACI-determined respondent subset, its own design-factor-derived target level, and its own capability score before integration into the case-level discussion and roadmap.

Participants

Five key informants participated because their positions carried direct accountability or operational responsibility for the selected COBIT 2019 objectives: the Head of E-Government (R1), the Head of General Affairs and Human Resources (R2), the Head of E-Government Governance (R3), the Head of Information and Communication Technology (R4), and the Head of Information Security (R5). Table 2 presents the RACI-to-respondent matrix for APO04 (Managed Innovation), APO07 (Managed Human Resources), and DSS05 (Managed Security Services). Applicability of each questionnaire item followed the respondent's RACI assignment for the corresponding activity; consequently, respondents did not answer identical item sets.

Respondents holding an Accountable or Responsible assignment for an objective are referred to as evidence owners (A/R respondents), because they direct, perform, or are answerable for the activities and hold the associated work products. Respondents holding only a Consulted or Informed assignment are referred to as C/I respondents. Because each position is held by one person and is identifiable within the institution, the codes R1–R5 identify roles rather than provide anonymity; consent, authorization, and disclosure procedures are reported under Ethical Considerations.

Table 2. Role-coded RACI-to-respondent matrix by objective

Respondent (role)	APO04 (Managed Innovation)	APO07 (Managed Human Resources)	DSS05 (Managed Security Services)
R1 — Head of E-Government	Accountable	Consulted	Informed
R2 — Head of General Affairs & HR	Informed	Accountable/Responsible	Informed
R3 — Head of E-Government Governance	Responsible	Informed	Consulted
R4 — Head of ICT	Consulted	Consulted	Responsible
R5 — Head of Information Security	Consulted	Consulted	Accountable/Responsible
Evidence owners (A/R)	R1, R3	R2	R4, R5
C/I respondents	R2, R4, R5	R1, R3, R4, R5	R1, R2, R3

Note: A/R respondents answered the activity items for which they hold an Accountable or Responsible assignment; C/I respondents answered only the items applicable to their Consulted or Informed role. The numbers of applicable and achieved items for every respondent–objective–level combination are reported in Supplementary Table S1.

Population and Sampling

The organizational population comprised 98 university employees. The analytic population consisted of personnel holding a Responsible, Accountable, Consulted, or Informed role for the assessed activities. Participants were selected through criterion-based purposive sampling by mapping COBIT 2019 RACI roles to the university's formal structure, because capability evidence must be supplied by role holders who can verify practices and records [26], [28].

The adequacy of the five-person panel is justified by role coverage and evidence ownership, not by sample-size conventions. As Table 2 shows, every assessed objective has at least one Accountable and at least one Responsible role holder among the respondents (APO04: R1 and R3; APO07: R2, who holds both assignments; DSS05: R4 and R5), so each assessed activity has an identifiable evidence owner within the panel. The panel is not intended to support statistical inference, and no inferential test was performed. Supplementary Table S1 reports, for each respondent, objective, and level, the number of applicable items and the number achieved, so that every percentage in this article can be recalculated from item counts.

Selection of Priority Objectives (Design-Factor Analysis)

The three objectives were selected using the eleven COBIT 2019 design factors: enterprise strategy, enterprise goals, risk profile, I&T-related issues, threat landscape, compliance requirements, role of IT, sourcing model, IT implementation methods, technology adoption strategy, and enterprise size [15]. Inputs were based on interviews and institutional documents. Digital-service expansion informed the priority assigned to APO04, reliance on centrally hosted student and financial data informed DSS05, and workforce constraints and in-house IT delivery informed APO07. Under the priority rule adopted in this study, APO04, APO07, and DSS05 each received a design priority of at least 75 and a target capability level of 4. Other security-relevant objectives, including APO12 (Managed Risk), APO13 (Managed Security), and DSS04 (Managed Continuity), fell below the study's selection threshold. Their exclusion limits the assessment scope and does not imply that these objectives are unimportant.

Instrumentation

Three instruments were used. An observation sheet recorded the physical setting, IT infrastructure, and visible management practices. A semi-structured interview guide examined responsibilities, strategy, IT services, recurrent problems, expected improvements, and supporting records. Prompts included: "Which role approves changes to logical access?", "What evidence is retained for security monitoring?", and "How are technology risks escalated?" A COBIT 2019 activity questionnaire operationalized APO04, APO07, and DSS05 practices as a binary audit checklist: each item asked whether a specific COBIT activity's defined practice was evidenced as performed (Yes/No), rather than asking respondents to rate agreement along a cumulative attitude scale. The label "Guttman-type" refers only to this cumulative scoring logic — level 1 items were treated as a precondition for scoring level 2, consistent with COBIT 2019's sequential capability-level structure — and not to a psychometrically validated Guttman scale with tested reproducibility or scalability coefficients; no such scalability analysis was performed, and this manuscript does not claim one. Sample statements concerned monitoring innovation opportunities, documenting critical competencies and succession, and periodically reviewing identities, privileges, security events, and physical access [29], [15], [30], [22].

Scoring and Measurement Quality

Scoring and Aggregation

Each questionnaire statement was answered Yes or No and scored 1 or 0. The achievement percentage for a respondent at a given level was calculated as the number of items achieved divided by the number of items applicable to that respondent at that level, multiplied by 100. Because applicability followed RACI assignments, respondents answered item sets of different sizes.

Three level-2 scores were computed per objective from the same respondent-level percentages. The panel-wide score is the unweighted arithmetic mean of all five respondents' percentages. The evidence-owner score is the unweighted mean of the A/R respondents' percentages. The cross-role corroboration score is the unweighted mean of the C/I respondents' percentages. Means were taken over respondent percentages rather than pooled item counts, because a pooled count would weight each respondent by the size of the item set their role happens to carry, not by the evidence they hold; within each group, every respondent contributes equally. The difference between the evidence-owner score and the cross-role corroboration score (A/R minus C/I, in percentage points) is reported as the disagreement indicator.

The three scores serve different purposes so that C/I responses do not distort inference about performance. A C/I respondent can corroborate only what is visible to a consulted or informed party; a No from such a respondent is ambiguous between an activity that is not performed and an activity that is not known to that respondent. The evidence-owner score is therefore treated as the primary account of whether activities are performed. The cross-role corroboration score and the disagreement indicator are used only to describe how consistently performance is known and communicated across roles, and are not interpreted as evidence of non-performance.

The panel-wide score is retained as the formal rating basis because level 2 concerns whether a process is managed, which includes assigning and communicating responsibilities [29], [15]. An activity that its evidence owners report as performed but that involved roles do not recognize does not yet meet that expectation, so the panel-wide rule is the more conservative basis for a level-2 rating. Because this choice can determine a classification, every classification is also reported under the evidence-owner rule (Table 4), and any divergence is stated explicitly.

Achievement was classified using the COBIT 2019 / ISO/IEC 33020 rating scale [29], [15]: Not Achieved, 0% to 15%; Partially Achieved, above 15% to 50%; Largely Achieved, above 50% to 85%; and Fully Achieved, above 85% to 100%. Assessment began at level 1 and progressed to the next level only when the preceding level was rated Fully Achieved. A process whose level-2 score did not exceed 85% was therefore classified at level 1, and the process gap was calculated as the target level minus the current level. All percentages were calculated from unrounded respondent values and rounded half-up to two decimals only for reporting; boundary comparisons used unrounded values. The same rounded values are used in the abstract, tables, Results, Discussion, and Conclusion.

Measurement Quality

Measurement quality was addressed through content traceability rather than formal content validation. Each item was drafted from a specific COBIT 2019 activity description, checked against the practice's defined RACI role before being assigned to a respondent, and, for DSS05 items, cross-checked against the ISO/IEC 27002:2022 control(s) later reported in Table 5. Traceability to a source activity does not establish that an item is complete, unambiguous, or interpreted identically by all respondents; no expert panel review or content validity index was applied, and this is acknowledged as a limitation. An affirmative answer is a respondent report, not independently verified evidence; verification was addressed separately through the convergence procedure described under Evidence Completeness. Because the instrument is a criterion-referenced audit checklist completed by five role experts rather than an attitude scale, Cronbach's alpha and comparable internal-consistency statistics were not appropriate. Reliability instead relied on standardized wording and scoring, identical thresholds, documented evidence requirements, and an auditable mapping matrix [31], [32].

Capability-Level Interpretation

Level 1 (performed) was assessed through the COBIT 2019 activities designated for level 1 of each practice, and level 2 (managed: the process is planned, monitored, and adjusted, and its work products are established and controlled) through the activities designated for level 2. The questionnaire therefore operationalizes COBIT 2019 activity-level requirements; ISO/IEC 33020 process attributes were not rated attribute by attribute as a separate assessment. The ratings are consequently criterion-based institutional ratings corroborated by documents, not a formal external

COBIT assessment, and the statement that an objective is at level 1 means that its level-2 achievement did not exceed the Fully Achieved boundary under the stated scoring rule. Levels 3 to 5 were not assessed. Table 3 shows how each level was operationalized.

Table 3. Operationalization of capability levels

Level	COBIT 2019 requirement	Questionnaire operationalization	Evidence and decision rule
1	Process is performed and achieves its basic purpose	COBIT 2019 level-1 activities of each practice, answered Yes/No as "evidenced as performed"	Interviews, observation, and work products (Table 6). Fully Achieved (above 85%) required before level 2 is rated
2	Process is managed: planned, monitored, and adjusted; responsibilities assigned and communicated; work products established and controlled	COBIT 2019 level-2 activities, answered by the respondents to whom each item applies under RACI	Panel-wide score (formal rating) with evidence-owner and cross-role scores as sensitivity and corroboration. Fully Achieved (above 85%) required before level 3 is rated
3–5	Defined, predictable, and optimizing process	Not assessed	Level 4 appears only as the design-factor target level

Note: work-product presence (Table 6) corroborates level-2 responses but is not itself a capability score.

Procedures and Time Frame

Data were collected during one bounded fieldwork period in six sequential stages. First, the researchers observed the university's IT environment and reviewed its vision, strategy, organizational structure, risk profile, policies, and available records. Second, interviews were conducted with knowledgeable personnel to score the eleven COBIT 2019 design factors. Third, the design-factor toolkit identified APO04, APO07, and DSS05 as priorities. Fourth, RACI-to-position mapping determined the five respondents (Table 2), who then completed level-specific questionnaires. Fifth, responses and documentary evidence were verified and scored. Finally, the seven DSS05 practices were mapped to relevant ISO/IEC 27002:2022 controls covering malware protection, network and endpoint security, identity and logical access, physical access, sensitive documents, logging, monitoring, and vulnerability management (Table 5). The integrated findings informed the gap analysis and improvement recommendations.

Evidence Completeness

Evidence completeness is a document-availability indicator that is analytically separate from capability achievement. An evidence unit is one expected work product, that is, one output specified by COBIT 2019 for the assessed practices of an objective [15]. Each unit is scored as present or absent. A unit is present only when it was located in complete form during the document review and corroborated by interview; a unit that was not located, or was located only in partial form, is scored absent, and partial units are not given fractional credit. All units carry equal weight. Evidence completeness is the number of units present divided by the number of units expected for the objective, multiplied by 100, pooled across the objective's practices.

The numbers of expected units are 12 for APO04, 18 for APO07, and 14 for DSS05. The resulting values are 9 of 12 (75.00%) for APO04, 16 of 18 (88.89%) for APO07, and 13 of 14 (92.86%) for

DSS05. The complete register, listing every unit, its source practice, status, and verification method, is provided in Supplementary Table S2, and Table 6 summarizes it. Where a respondent reported an activity as performed but its work product was absent or contradicted, the item was flagged as evidenced-disputed rather than silently accepted or overridden. Presence of a work product does not establish that the control operates effectively; no control testing was performed.

Analysis Plan

The quantitative analysis used frequencies, binary achievement scores, percentages, category thresholds, and arithmetic differences between as-is and to-be capability levels. Scores were calculated for each respondent, capability level, and objective; respondent-level variation was examined and, in the Results and Discussion, reanalyzed at the level of individual activities and each respondent's RACI role, to identify which specific practices were reported as implemented inconsistently rather than treating disagreement only as an aggregate finding. No inferential test was performed because the participants constituted a small purposive panel of accountable role holders rather than a probability sample. Qualitative interview notes, observations, and documents were organized deductively by design factor, COBIT practice, work product, and ISO/IEC 27002:2022 control. A convergence procedure compared reported questionnaire performance with documentary and observational evidence for each activity; where a respondent reported an activity as implemented (Yes) but supporting documentary evidence was absent or contradictory, the item was flagged in the convergence record (Table 6) as evidenced-disputed rather than being silently accepted or silently overridden, and such flags are reported in the Results together with how many items in each objective carried this flag. Integrated interpretation then prioritized deficiencies according to explicit, stated criteria (Table 7): capability failure at level 2, missing or disputed evidence, direct security relevance, and contribution to progression toward the target level [33], [34], [35].

Scope and Methodological Limitations

The study was bounded to one private university and three priority objectives within the central E-Government unit and the General Affairs/HR unit (see Institutional Context and Assessment Boundary above); its findings are analytically transferable to institutions sharing the contextual characteristics described there, but are not statistically generalizable to all universities. Role-based sampling reduced uninformed responses but increased dependence on institutional self-report; alternative explanations for the respondent disagreement reported in Results — including differences in item interpretation, differences in access to institutional records, and differences in awareness across roles, rather than only differences in actual implementation — could not be fully disentangled with the available evidence and are discussed explicitly in the Discussion. Binary scoring simplified comparison but did not capture partial implementation within a statement. Evidence availability did not necessarily demonstrate control effectiveness: no control testing (e.g., configuration review, access recertification sampling, log sampling) was performed in this study, and statements about control weakness in Results and Discussion are limited to documentary and reported-practice evidence unless explicitly noted otherwise. The ISO mapping did not constitute an ISO/IEC 27001 certification assessment or a complete assessment of all 93 ISO/IEC 27002:2022 controls; it covered only the controls judged relevant to DSS05's seven practices. Cross-sectional evidence also could not demonstrate sustained improvement over time. These constraints were mitigated through source triangulation, role triangulation, explicit scoring rules, retention of respondent disagreement, and separation of documented evidence from inferred control effectiveness [32], [25].

Reporting Approach

This is a non-interventional, cross-sectional organizational evaluation with human informants. Reporting followed the STROBE checklist where applicable, particularly for setting, participant selection, variables, data sources, potential bias, study size, and limitations, and drew on Mixed Methods Appraisal Tool principles for reporting the integration of quantitative and qualitative strands; the qualitative interview component followed SRQR guidance. PRISMA, CARE, and

CONSORT were judged not applicable because the study is not a systematic review, case report, or randomized trial.

RESULTS AND DISCUSSION

Results

The COBIT 2019 design-factor assessment identified APO04 (Managed Innovation), APO07 (Managed Human Resources), and DSS05 (Managed Security Services) as the university's priority governance and management objectives within the assessed scope (see Selection of Priority Objectives above for the design-factor basis). Each objective received a design priority of at least 75 and a target capability level of 4. APO04 addresses the institution's capacity to identify, test, and govern technology-enabled innovation; APO07 addresses the people and competencies required to sustain information and technology services; and DSS05 addresses the operation and monitoring of security services. Together, the three objectives represent an innovation–people–security configuration within the central E-Government and HR units, rather than a comprehensive assessment of university-wide cybersecurity governance.

Results: Capability and Evidence Summary

All five respondents reported full achievement of level-1 activities for the three objectives. None of the objectives exceeded the 85% Fully Achieved boundary at level 2 under the panel-wide rule. APO04 obtained 79.98%, with respondent scores of 55.50%, 55.50%, 100%, 88.89%, and 100% (mean 79.978%). APO07 obtained 83.81%, with respondent scores of 66.67%, 66.67%, 100%, 100%, and 85.71%. DSS05 obtained 82.00%, with respondent scores of 66.67%, 56.67%, 100%, 86.67%, and 100% (mean 82.002%). Under the sequential rule, a level-2 score not exceeding 85% prevented assessment at level 3, so each objective was rated at level 1. Because the target level was 4, each objective showed a gap of three levels. Table 4 summarizes the results for each objective.

Table 4. Capability and evidence summary

Objective	Panel L2 (%)	A/R L2 (%)	C/I L2 (%)	A/R − C/I (pp)	Evidence present/expected	Current / target / gap
APO04	79.98 (LA)	77.75 (LA)	81.46	−3.71	9/12 = 75.00%	1 / 4 / 3
APO07	83.81 (LA)	66.67 (LA)	88.10	−21.43	16/18 = 88.89%	1 / 4 / 3
DSS05	82.00 (LA)	93.33 (FA)	74.45	+18.89	13/14 = 92.86%	1 / 4 / 3

Note: LA = Largely Achieved; FA = Fully Achieved. Scores are unweighted means of respondent percentages (see Scoring and Aggregation); the classification is shown only for the panel-wide rule and the evidence-owner rule, and the cross-role score is an awareness indicator, not a rating. A/R groups: APO04 = R1, R3; APO07 = R2 only; DSS05 = R4, R5. C/I groups: APO04 = R2, R4, R5; APO07 = R1, R3, R4, R5; DSS05 = R1, R2, R3. Evidence units and denominators are defined under Evidence Completeness and listed in Table 6. Differences are computed from unrounded values and are descriptive; no inferential test was performed.

Results: Respondent Disagreement

Respondent disagreement was analyzed separately from the formal capability rating by comparing evidence-owner and cross-role scores (Table 4). For APO04 and APO07, evidence owners reported lower level-2 achievement than C/I respondents (differences of −3.71 and −21.43 percentage points). In these two objectives, therefore, limited visibility among C/I respondents cannot explain why the panel-wide score fell below the boundary; the shortfall originates in the evidence owners' own reports, which is consistent with uneven institutionalization of level-2 practices. For APO07 this reading rests on a single evidence owner (R2) and should be treated as indicative only.

For DSS05 the pattern is reversed. The evidence owners (R4, R5) reported 93.33%, whereas the C/I respondents (R1, R2, R3) reported 74.45%, a difference of 18.89 points. This is the pattern expected

if C/I role holders have less visibility of security activities performed outside their own area, or if performed practices and responsibilities are not communicated across roles; this study cannot separate the two explanations. The DSS05 classification is consequently aggregation-dependent: the panel-wide score of 82.00% yields Largely Achieved and a level-1 rating, whereas the evidence-owner score of 93.33% would exceed the 85% boundary at level 2, which would make level 3 assessable but was not assessed here. The DSS05 level-1 rating is therefore reported as a conservative rating conditional on level-2 practices being recognized across involved roles. The findings that do not depend on the aggregation rule are the cross-role communication gap and the documentary gap in physical-access logging (see Evidence Completeness).

The proximity of APO07's panel-wide score (83.81%) to the 85% boundary, 1.19 percentage points, is reported descriptively. It is not treated as evidence about the cost, effort, or organizational scale that remediation would require, since no resource, workload, or implementation-effort data were collected.

Results: Evidence Completeness

Work-product analysis produced a second layer of evidence, summarized in Table 6. For APO04, 9 of 12 expected units were present (75.00%). Strategic and planning documents existed, including the institutional strategic plan and the university's digital-government master plan, but three expected units were absent or not located: an analysis of rejected initiatives, results and recommendations from proof-of-concept initiatives, and a complete recognition or reward output. Innovation was therefore contemplated in the documents, but the lifecycle from idea selection through experimentation, rejection, benefits realization, and organizational learning was not documented consistently within the reviewed units.

For APO07, 16 of 18 expected units were present (88.89%). Job descriptions, staffing analysis, competency-development materials, and several personnel records were available. Two units were absent: a review report on skills and competencies and a record of resource utilization. Interviews also indicated that training was not periodic, career development was not fully structured, and reward and recognition mechanisms were limited. The high document score therefore did not eliminate gaps in workforce planning, competency review, and sustained capacity development.

For DSS05, 13 of 14 expected units were present (92.86%), the highest completeness of the three objectives. Evidence existed for malware prevention, risk assessment, network-security standards, penetration testing, endpoint or asset-use rules, logical-access procedures, account review, user-access matrices, security incident logs, incident tickets, and security-event records. The one absent unit was the physical-access log for restricted IT-asset areas under DSS05.05. Interviews with the responsible role holders (R4, R5) indicated that the log was absent rather than merely unavailable to the researchers: the central server room relied on badge-based entry authorization without a retained entry/exit record, and no equivalent manual log or alternative mechanism, such as CCTV retention covering the entry point, was identified during the review. The finding is a documentary absence at the level of the control's expected work product; it is not an independently tested claim that unauthorized entry occurred or that the physical-access control failed. Evidence completeness of 92.86% coexisted with a level-1 rating, which illustrates that document availability and managed capability are distinct.

Table 5. DSS05-to-ISO/IEC 27002:2022 mapping matrix

DSS05 practice	Mapped ISO/IEC 27002:2022 control(s)	Mapping rationale	Case evidence	Identified deficiency	Proposed action
DSS05.01 Protect against malware	8.7 Protection against malware; 8.8 Management of technical vulnerabilities	DSS05.01 defines the managed practice of preventing and detecting malicious code; 8.7/8.8 specify the corresponding technical controls	Malware-prevention tooling and vulnerability/penetration-test records present	No documentary deficiency identified for this practice within the reviewed scope	Maintain current evidence retention; no immediate action
DSS05.02 Manage network and connectivity security	8.20 Networks security; 8.21 Security of network services; 8.22 Segregation of networks; 8.24 Use of cryptography	DSS05.02 requires managed protection of network connections; these controls specify baseline, service-level, segmentation, and cryptographic safeguards	Network-security standard and penetration-test evidence present	Periodic re-validation of segmentation and standards not evidenced as a recurring, scheduled activity	Establish and document a periodic (e.g., annual) network baseline and segmentation review with recorded sign-off
DSS05.03 Manage endpoint security	8.1 User endpoint devices; 8.9 Configuration management	DSS05.03 requires managed protection of endpoints; these controls specify device-use rules and configuration baselines	Endpoint/asset-use rules present	Endpoint configuration-compliance monitoring not evidenced as a documented, recurring check	Introduce a documented endpoint configuration-compliance check cycle with retained results
DSS05.04 Manage user identity and logical access	5.15 Access control; 5.16 Identity management; 5.17 Authentication information; 5.18 Access rights; 8.2 Privileged access rights; 8.5 Secure authentication; 8.15 Logging	DSS05.04 requires managed identity and access lifecycle; these controls specify identity, authentication, rights, privilege, and logging requirements	Logical-access procedures, account-review records, and user-access matrices present	Privileged-access recertification frequency not documented as a fixed, recurring schedule	Formalize a scheduled privileged-access recertification with documented approval trail

DSS05 practice	Mapped ISO/IEC 27002:2022 control(s)	Mapping rationale	Case evidence	Identified deficiency	Proposed action
DSS05.05 Manage physical access to IT assets	7.1 Physical security perimeters; 7.2 Physical entry; 7.4 Physical security monitoring	DSS05.05 requires managed control of physical access to protected areas; these controls specify perimeter, entry-control, and monitoring requirements	Access authorization procedure present; no retained entry/exit log identified (see Results)	Missing physical-access log; entry/exit traceability not demonstrated	Introduce an electronic or controlled manual access log for the server room and other restricted facilities, recording identity, authorization, entry/exit time, purpose, and escort, with independent periodic review
DSS05.06 Manage sensitive documents and output devices	5.10 Acceptable use of information and other associated assets; 5.12 Classification of information; 5.13 Labelling of information; 7.7 Clear desk and clear screen; 7.10 Storage media	DSS05.06 requires managed handling of sensitive information and media; these controls specify classification, handling, and physical-media requirements	Acceptable-use and storage-media procedures reported in interviews	Formal classification/labelling scheme not evidenced as documented and applied	Document a classification and labelling scheme and verify sample compliance
DSS05.07 Monitor the infrastructure for security-related events	8.16 Monitoring activities; 5.25 Assessment and decision on information security events; 5.26 Response to information security incidents	DSS05.07 requires managed security monitoring and response; these controls specify monitoring, event assessment, and response requirements	Security-event records, incident tickets, and incident logs present	Documented alert thresholds and closure criteria not evidenced	Define and document alert thresholds, escalation paths, and incident-closure evidence requirements

Mapping development and review: candidate controls were identified independently from each DSS05 practice's official COBIT 2019 activity description, then cross-checked against ISO/IEC 27002:2022 control descriptions [30] by both authors; disagreements on which of several plausible controls to list were resolved by retaining only controls with a direct activity-to-control correspondence and moving supplementary or indirectly related controls to narrative discussion

rather than the matrix. Controls listed as directly relevant are those with an explicit correspondence to the practice's defined activity; recommendations that extend beyond a documented deficiency (e.g., general hardening suggestions not tied to a specific missing work product) are presented in the Discussion and Implications sections as professional recommendations, not as findings.

Table 6. Evidence register (summary)

Objective	Expected	Present	Completeness	Absent units	Convergence flags
APO04	12	9	9/12 = 75.00%	Analysis of rejected initiatives; proof-of-concept results and recommendations; complete recognition or reward output	0 items flagged evidenced-disputed
APO07	18	16	16/18 = 88.89%	Skills and competency review report; resource-utilization record	1 item flagged evidenced-disputed (training periodicity)
DSS05	14	13	13/14 = 92.86%	Physical-access log for restricted IT-asset areas (DSS05.05)	1 item flagged evidenced-disputed (physical-access review)

Note: all units carry equal weight and are scored present or absent (partial units are scored absent). Verification method for all units: document review with interview corroboration. The complete register of expected units is provided in Supplementary Table S2.

Mapping the seven DSS05 practices to ISO/IEC 27002:2022 (Table 5) clarified the control implications for the objective with the most direct security relevance. The qualitative prioritization considered security relevance, affected services and exposure, existing safeguards, and the evidence basis; dependencies informed sequencing. DSS05 was assigned high priority for near-term action, while APO04 and APO07 were assigned medium priority as supporting objectives. Implementation effort was not rated because no workload, budget, or staffing data were collected.

Discussion

Revisiting the propositions

P1 proposed that an integrated reading would make security deficiencies more traceable than an aggregate capability score alone. The DSS05 mapping matrix (Table 5) supports this proposition by linking the 82.00% level-2 score to specific practices, controls, and actions. It does not demonstrate superiority over either framework applied independently. P2 proposed that document availability would not necessarily correspond to fully achieved capability. DSS05's 92.86% evidence completeness coexisted with an 82.00% level-2 score and a level-1 classification; APO07's 88.89% evidence completeness similarly coexisted with an 83.81% level-2 score. DSS05's priority is an analytical outcome under the stated decision criteria, rather than a separately tested proposition.

The principal finding is that baseline execution and document availability coexisted with weak institutionalization for all three assessed objectives. Level 1 was fully achieved, demonstrating that the selected processes produced their basic outcomes. Nevertheless, failure at level 2 indicates that the practices were not yet managed with sufficient consistency, planning, monitoring, and evidence, within the assessed scope. Contemporary cybersecurity-maturity research similarly warns that control presence and capability maturity are different constructs: an organization may possess policies and tools while lacking reliable execution, measurement, ownership, and feedback loops [23], [24], [36], [37]. The three-level gaps should therefore not be interpreted as an absence of all governance, nor generalized to units and services outside the assessed scope. They represent the distance, for the three assessed objectives, between performed activities and a quantitatively managed, predictable level-4 process. Compared with related governance assessments in higher

education that report capability or maturity levels without an accompanying control mapping [14], [25], the present study's principal difference is the explicit, auditable DSS05-to-ISO/IEC 27002:2022 mapping (Table 5), which this study offers as its main point of comparison rather than a general claim of methodological superiority.

APO04's 79.98% result and 75% evidence-completeness score identify innovation governance as the least documented of the three objectives within the assessed scope. The missing outputs occur at decision points that make innovation accountable: explaining why initiatives are rejected, recording proof-of-concept results, and linking innovation to recognition and learning. Without these artifacts, unsuccessful experiments may be repeated, benefits may be asserted rather than measured, and cybersecurity requirements may enter projects late; this is offered as a plausible consequence rather than a demonstrated one, since no project-level outcome data were examined. Recent work on digital transformation shows that innovation performance depends on portfolio governance, cross-functional learning, and traceable value realization rather than technology acquisition alone [38], [39], [40]. For the university, a lightweight innovation register should capture proposals, owners, security and privacy requirements, proof-of-concept criteria, decisions, costs, expected benefits, realized benefits, and lessons learned. ISO/IEC 27002:2022 control 5.8 (information security in project management) can be incorporated at this gate so that information security becomes a project requirement rather than a post-implementation correction; this is presented as a recommendation for future practice, not as a finding that the current absence of this gate has caused a security incident.

APO07's 83.81% score was only 1.19 percentage points below the level-2 boundary, while evidence-completeness reached 88.89%. This proximity is reported descriptively (see Results) rather than as evidence that remediation would be inexpensive or limited in organizational scope, since no resource, workload, or implementation-effort data were collected. The missing competency-review report and resource-utilization record should be connected to an annual skills inventory, role-specific learning plans, succession arrangements for critical IT functions, and post-training evaluation. Research consistently links cybersecurity outcomes to management support, security climate, role clarity, and recurrent learning [41], [42], [43], [44]. One-off awareness sessions cannot address changing threats or specialized responsibilities. The university should differentiate baseline awareness for all personnel from technical training for administrators, privileged users, incident handlers, and system owners. Training completion, simulation outcomes, incident recurrence, overdue access reviews, and coverage of critical-role backups are proposed here as candidate measurable indicators for future monitoring, not as indicators already in use.

DSS05 is assigned the most immediate priority under the explicit criteria applied in Implications below, because it combines direct security relevance, the highest evidence-completeness score among the three objectives, and a specific, traceable missing work product (the physical-access log). Its 92.86% evidence-completeness score may initially appear inconsistent with a level-1 classification. The apparent contradiction disappears when evidence completeness is separated from management capability: within the reviewed scope, documents demonstrate that controls have been designed or activities have occurred; they do not, on their own and absent the control testing that this study did not perform, establish that controls operate consistently across units, that exceptions are resolved, or that performance is reviewed. Studies of security monitoring and incident response emphasize the need for reliable logs, contextual correlation, defined alert thresholds, ownership, retention, and post-incident learning [45], [46], [47], [48]. The respondent range from 56.67% to 100% is consistent with this interpretation, though, as noted above, it does not on its own distinguish uneven institutionalization from differential respondent awareness or access to records.

Physical access finding: confirmed, unverified, and preventive elements.

The confirmed finding, based on document review and interview corroboration, is that no physical-access log was located for the central server room during the review, and that respondents R4 and R5 reported the log as absent rather than as unavailable to the researchers or maintained through an alternative mechanism (see Results). This confirmed finding is narrow: it establishes a documentary and traceability gap, not a demonstrated instance of unauthorized entry or a tested control failure. Unverified in this study are the operational effectiveness of the existing badge-based

entry authorization control and whether informal or undocumented compensating practices (e.g., security-guard sign-in sheets not reviewed during this study) exist outside the reviewed record set; these are noted as open questions rather than assumed absent. Preventive recommendations — network segmentation review, endpoint configuration monitoring, and privileged-access recertification (Table 5) — are presented as professional recommendations consistent with the DSS05 control mapping and general practice in the cited literature, and are explicitly not presented as findings of demonstrated failure in those specific areas, since this study's evidence for them is limited to documentary review rather than control testing. Where authorized and feasible in future work, selected findings could be supported with bounded evidence checks such as redacted access-review records or sampled monitoring records; this study's scope did not include such testing, and this boundary is maintained consistently rather than implied to have been exceeded.

The wider DSS05 mapping also shows that remediation cannot stop with physical entry. Network baselines and segmentation should be reviewed periodically; endpoints require inventories, secure configurations, patching, and compliance monitoring; privileged accounts require formal approval and recertification; sensitive information needs classification, labelling, retention, and secure disposal; and incident logs require thresholds, escalation, root-cause analysis, and closure evidence (Table 5). Current studies on cybersecurity frameworks stress that integration is most useful when mappings produce prioritized implementation actions instead of duplicative compliance checklists [24], [37], [49], [50]. COBIT supplies the process logic — who governs, how performance is managed, and when progression is justified — while ISO/IEC 27002:2022 supplies the control detail.

Prioritization and Improvement Roadmap

The roadmap converts the evidence gaps in Table 5 and the capability gaps in Table 4 into an ordered set of actions. The ordering uses a qualitative decision matrix (Table 7). It is a governance prioritization based on the evidence collected. It is not a cyber-risk ranking, because no assessment of likelihood and impact was performed, and a high priority here does not mean that the action addresses the institution's largest security risk.

Criteria. Four criteria were rated for each action, and a fifth was used for sequencing. (1) Security relevance: Direct when the action addresses a control that is directly mapped in Table 5, and Indirect when it concerns APO04 or APO07, which were not mapped to ISO/IEC 27002:2022. (2) Affected services and exposure: High when the action concerns assets or services central to institutional operations across units (the central server room, privileged accounts, the network core), and Medium when it concerns a subset (endpoints, monitoring processes, information handling). (3) Existing safeguards: Substantial when the case evidence shows a standard or records already supporting the practice, Partial when only some supporting elements were evidenced, and Limited when little more than interview reports were available. (4) Evidence basis: the gap category from Table 7 note (CG, EG, DE), which anchors each rating in the case data. (5) Dependencies: prerequisites and enabling relationships between actions, used to sequence actions in Table 8 and not to rank them.

"Estimated implementation effort" was deliberately not used as a criterion. No workload, budget, or staffing data were collected, so any effort rating would have no empirical basis.

Decision rule and assignment of ratings. An action was assigned High priority when its security relevance was Direct, its exposure was High, and its existing safeguards were Partial or Limited. Other actions on directly mapped controls were assigned Medium, and actions on APO04 and APO07 were assigned Medium (supporting), because they condition the sustainability of DSS05 improvement without being mapped to a security control. Ratings were assigned by the two authors from the document review, interviews, and observation, and they were not validated by institutional stakeholders or an external expert. Readers can therefore trace each tier to the rating columns in Table 7, and a different weighting of the criteria could change the tiers.

Table 7. Qualitative prioritization matrix

Action	Security link	Exposure	Safeguards	Basis	Evidence	Priority
Physical-access log for restricted IT facilities (DSS05.05)	Direct	High	Partial (badge-based entry authorization)	CG, DE	No retained entry/exit log located	High
Privileged-access recertification schedule (DSS05.04)	Direct	High	Partial (account reviews, access matrices)	EG	Fixed recurring schedule not evidenced	High
Network baseline and segmentation review cycle (DSS05.02)	Direct	High	Substantial (standard, penetration-test records)	EG	Recurring review not evidenced	Medium
Endpoint configuration-compliance checks (DSS05.03)	Direct	Medium	Partial (asset-use rules)	EG	Compliance check not evidenced	Medium
Alert thresholds and incident-closure criteria (DSS05.07)	Direct	Medium	Substantial (event records, tickets, logs)	EG	Thresholds and closure criteria not evidenced	Medium
Classification and labelling scheme (DSS05.06)	Direct	Medium	Limited (interview reports only)	EG	Documented scheme not evidenced	Medium
Annual competency review and resource-utilization record (APO07)	Indirect	Medium	Partial (job descriptions, training materials)	EG, DE	Review report and utilization record not evidenced; training periodicity disputed	Medium (supporting)
Innovation register with proof-of-concept and rejection records (APO04)	Indirect	Medium	Partial (strategic and master plans)	EG	Three expected outputs not evidenced	Medium (supporting)

Note: CG = confirmed documentary gap; EG = evidence gap; DE = disputed evidence (see Table 5). Within a tier, the order of actions follows dependencies (Table 8).

Within the DSS05 actions, the physical-access log and the privileged-access recertification rank first under this rule. A ranking based on capability improvement alone would instead place APO04 first, since it has the lowest evidence completeness (75.00%). The study chose the DSS05-first sequence because its stated aim is security-relevant governance improvement, and it presents the alternative as a legitimate basis for a capability-driven roadmap.

Table 8. Proposed implementation sequence (provisional planning estimates)

Action	Responsible unit	Period	Prerequisite	Evidence	Completion criterion
Introduce physical-access log for server room and restricted facilities	Head of Information Security / Head of ICT	Short term (0–3 months)	Access-control policy update	Log entries; periodic independent review record	Log operating continuously and first monthly independent review signed off; sustained operation checked at reassessment
Formalize privileged-access recertification schedule	Head of Information Security	Short term (0–3 months)	Current privileged-account inventory	Recertification approval records	First full recertification cycle completed and documented
Document network baseline and segmentation review cycle	Head of ICT	Medium term (3–6 months)	Network-security standard (existing)	Review sign-off records	First scheduled review completed with recorded sign-off
Establish endpoint configuration-compliance checks	Head of ICT	Medium term (3–6 months)	Endpoint/asset-use rules (existing)	Compliance-check reports	First check cycle completed and deviations logged
Define alert thresholds and incident-closure criteria	Head of Information Security	Medium term (3–6 months)	Existing incident-log procedure	Updated incident-response procedure	Procedure approved and applied to at least one subsequent incident
Document Classification and labelling scheme	Head of Information Security	Medium term (3–6 months)	Acceptable-use and storage-media procedures (reported)	Approved scheme; sample complience check	Scheme approved and sample compliance verified
Institute annual competency review and resource-utilization recording	Head of General Affairs & HR	Medium term (3–6 months)	HR data-collection template	Review report; utilization record	First annual cycle completed and reported to management
Establish innovation register with proof-of-concept and rejection documentation	Head of E-Government / Head of E-Government Governance	Medium term (3–6 months)	Innovation-governance policy update	Register entries for new and ongoing initiatives	Register in active use for all initiatives opened after adoption
Reassess level-2 capability for all three objectives	Head of E-Government Governance (coordinating)	After the above (approx. 6–9 months)	Completion of preceding actions	Updated questionnaire and documentary evidence	Level-2 achievement re-scored with the same instrument

Note: The periods are provisional planning estimates. They reflect the sequencing of actions by priority tier and prerequisite, and they were set by the authors. They are not based on workload, budget, procurement, or staffing analysis, none of which was collected, and the responsible functions would need to confirm them against their own capacity.

For higher-education governance more broadly, the findings suggest that open academic environments need controls adapted to distributed responsibility, at least within the centralized structure examined here. Central IT cannot achieve security capability alone when human resources, faculties, system owners, vendors, and senior leadership control different parts of the risk lifecycle. The RACI-based respondent pattern (Table 2) offers a practical way to locate disagreement, but disagreement should be examined at the activity level before it is attributed to institutionalization and not to differences in awareness or access.

Research Contribution

The study contributes an evidence-oriented integration of COBIT 2019 and ISO/IEC 27002:2022 in a higher-education case, bounded to three management objectives. Its first contribution is analytical: it distinguishes process capability, work-product availability, and control effectiveness instead of treating them as interchangeable indicators, and it makes this distinction auditable through the DSS05 mapping matrix (Table 5) rather than a narrative list. Its second contribution is methodological: it uses design factors to select relevant objectives, RACI mapping to select knowledgeable respondents, sequential capability scoring to identify the achieved level, and control mapping to translate a capability gap into concrete security actions with an explicit development and review procedure for the mapping itself. Its third contribution is empirical: it demonstrates, for the DSS05 and APO07 objectives specifically, that a high evidence-completeness percentage can coexist with a level-2 score below the achievement threshold. The access-log finding illustrates how integration can convert an abstract three-level capability gap into a specific, auditable remediation priority; the study does not, however, empirically assess whether implementing that remediation improves security outcomes, which the Limitations and Suggestions sections identify as a distinct, unaddressed question.

Ethical Considerations

This study was a non-interventional organizational evaluation. Five role holders were asked to answer a binary activity checklist and to take part in interviews about institutional processes in their professional capacity, and the authors reviewed institutional documents and observed the IT environment. No intervention was applied to participants or to systems. Respondents are identified only by the codes R1–R5. Because the five roles are few and specific, role codes do not guarantee anonymity within the institution, and the article avoids attributing responses beyond what the interpretation requires.

[Ethics review] The study was reviewed by [name of committee or unit] and received approval/exemption (reference no. [number], date). [Consent] Each participant gave informed consent to take part and to the use of role-associated findings in a publication, after being told the purpose of the study, that participation was voluntary, and that role codes might still allow internal identification.

[Authorization] The university leadership authorized access to institutional cybersecurity documents and records, and authorized publication of the findings, including the named institution and the identified evidence gaps, before submission. [Data handling] Institutional documents were accessed on university premises/through authorized channels, were not copied beyond what the analysis required, and were stored in access-restricted storage that only the authors could reach; no document is reproduced in the article or its supplementary material.

Disclosure of security-sensitive findings. Weaknesses in security evidence can be useful to an attacker, so the article limits operational detail. It reports whether expected work products were evidenced, and it does not report network addresses, system configurations, account details, product names, or the technical details of any vulnerability. Findings are stated as “not evidenced,” which

does not imply that a control is absent, and the study makes no claim that a control failed or that unauthorized access occurred. The recommendations are phrased as governance actions. Even so, the physical-access finding and the role-level pattern can be linked to a named institution, so the findings were handled as security-sensitive and are limited to the level of detail needed to support the analysis.

Limitations

The study has limits of scope, measurement, and validation. The results come from one private university, from five purposively selected role holders, and from three COBIT 2019 objectives selected through design-factor priorities. Because APO12 (Managed Risk), APO13 (Managed Security), and DSS04 (Managed Continuity) were not among the assessed objectives, the findings do not describe risk management, security management, or continuity governance, and they should not be read as a university-wide cybersecurity assessment. Analytical transferability is limited to institutions with comparable centralized governance (see Institutional Context). The assessment is cross-sectional and cannot show whether practices were sustained. Scoring was binary and could not capture partial implementation within an activity. The capability levels were assigned by the authors from questionnaire responses and documentary evidence, and they are not the result of a formal external COBIT assessment. The objective-level score is the unweighted mean of respondent percentages, in which Consulted and Informed respondents, who may have less access to records, carry the same weight as Responsible and Accountable ones. The sensitivity analysis compared panel-wide and A/R-only means (Table 4), showing that DSS05's classification depends on the aggregation rule. Pooled applicable-item scoring was not examined, and respondent disagreement cannot be fully separated from differences in awareness or access. Content validity rests on traceability between items and COBIT activities and was not checked by an expert panel or a content-validity index.

The evidence and mapping layers have further limits. Evidence completeness is a study-specific, equally weighted measure of document availability at the time of review. It has not been validated as an instrument and does not indicate that controls operate effectively. No configuration review, access-recertification sampling, or log sampling was performed, so the study evaluates governance documentation and reported practice, not control effectiveness. The ISO/IEC 27002:2022 mapping covers DSS05 only, rests on the consensus of the two authors, was not validated by an external expert, and has no agreement statistic; the direct/supplementary classification could change under independent review. The mapping is not an ISO/IEC 27001 certification assessment and does not cover all 93 controls. The prioritization is a qualitative, author-assigned ordering that includes no likelihood–impact risk assessment and no effort data, and the implementation periods are provisional planning estimates. These limitations call for reading the percentages as diagnostic evidence for the assessed scope, not as population parameters, certification scores, or measures of security outcomes.

Suggestions

Future evaluations should repeat the assessment after remediation (Table 8) and compare capability and evidence longitudinally, directly testing whether the proposed roadmap actions are associated with improved security outcomes — a question this study raises but does not answer. The respondent panel should be expanded to include system owners, internal audit, data-protection or legal functions, faculty representatives, and critical vendors while preserving role-based selection, and while explicitly testing whether expanding the panel changes the respondent-disagreement pattern reported here. Control testing should supplement document review through log sampling, access recertification tests, configuration checks, vulnerability scans, incident simulations, and verification of corrective-action closure, to distinguish documented practice from demonstrated control effectiveness. Researchers should also examine whether improvements in APO07 mediate the sustainability of DSS05 controls and whether APO04 project gates reduce security defects in new digital services. Multi-institution studies could test the transferability of the integrated model across public and private universities with differing IT governance structures (see Institutional Context)

and develop sector benchmarks, while continuing to treat ISO/IEC 27002:2022 as a control catalogue rather than converting it into an unsupported maturity score.

CONCLUSION

This study evaluated three prioritized COBIT 2019 objectives (APO04 Managed Innovation, APO07 Managed Human Resources, and DSS05 Managed Security Services) at one Indonesian private university and, for DSS05 only, mapped the capability finding to ISO/IEC 27002:2022 controls. All three objectives fully achieved level 1 but stayed below the 85% Fully Achieved threshold at level 2 (79.98%, 83.81%, and 82.00%), leaving a three-level gap to the target of level 4. Evidence completeness (75.00%, 88.89%, and 92.86%) showed that document availability and process capability are distinct. The DSS05-centred mapping, built on explicit criteria for direct and supplementary relationships, turned the aggregate gap into practice-level evidence gaps, of which only the missing physical-access log was a confirmed documentary gap. Under the stated governance criteria, DSS05 actions come first in the proposed implementation sequence; this is a criterion-based ordering, not a cyber-risk ranking. The findings describe governance capability and documentary evidence within the assessed scope. They do not establish control effectiveness or that the roadmap improves security outcomes, which should be tested through reassessment after corrective action, bounded control testing, and external validation of the mapping.

ACKNOWLEDGMENT

The authors gratefully acknowledge Universitas Sriwijaya for its academic and institutional support. The authors also extend their appreciation to Universitas Indo Global Mandiri, Palembang, particularly the university management, information technology personnel, and all respondents who contributed information, documents, and valuable insights to this study. This research received no specific financial support from public, commercial, or not-for-profit funding agencies.

AUTHOR CONTRIBUTION STATEMENT

Rossa Alba Kirana conceptualized the study, collected and analyzed the data, conducted the cybersecurity governance evaluation, prepared the initial manuscript, and revised the article. Ali Ibrahim supervised the research design, validated the analytical procedures, interpreted the findings, critically reviewed the manuscript, and approved the final version. Both authors read and approved the final manuscript.

AI DISCLOSURE STATEMENT

The authors used OpenAI's ChatGPT during the preparation of this work to assist with language refinement, academic organization, and improvements to the clarity and readability of the manuscript. The AI tool was not used to generate, alter, or fabricate the research data, findings, or conclusions. After using the tool, the authors thoroughly reviewed, verified, and edited the content as necessary and take full responsibility for the accuracy, integrity, and content of the publication.

REFERENCES

[1] B. Valkenburg and I. Bongiovanni, 'Unravelling the three lines model in cybersecurity: A systematic literature review,' Computers & Security, vol. 139, Art. no. 103708, 2024, doi: 10.1016/j.cose.2024.103708.

[2] E. A. Iancu, E. Tuşa, N. Iancu, E. Simion, and A. C. Moise, 'Preventing computer crime by knowing the legal regulations that ensure the protection of computer systems,' Juridical Tribune, vol. 13, no. 3, pp. 365–383, 2023, doi: 10.24818/TBJ/2023/13/3.03.

[3] A. Modi, I. Kuzminykh, and B. Ghita, 'Data-driven approaches to cybersecurity governance for board decision-making: A systematic review,' Journal of Cybersecurity and Privacy, 2024.

[4] 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. no. 177, 2025, doi: 10.1007/s10207-025-01097-x.

[5] O. Afolalu et al., 'Cybersecurity in higher education institutions: A systematic review,' Applied Sciences, 2025.

[6] S. Goliath, P. Tsibolane, and D. Snyman, 'Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in higher education,' 2024.

[7] M. M. A. Parambil et al., 'Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects,' 2024.

[8] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, 'Developing a cyber security culture: Current practices and future needs,' Computers & Security, vol. 109, Art. no. 102387, 2021.

[9] A. Georgiadou, S. Mouzakitis, and D. Askounis, 'Working from home during COVID-19 crisis: A cyber security culture assessment survey,' Security Journal, vol. 35, pp. 486–505, 2022.

[10] M. Zwilling et al., 'Cyber security awareness, knowledge and behavior: A comparative study,' Journal of Computer Information Systems, vol. 62, no. 1, pp. 82–97, 2022.

[11] N. Kshetri, Vasudha, and D. Hoxha, 'Knowledge and awareness of computer and cyber ethics between CS and non-CS university students,' 2023.

[12] R. AlGhamdi, S. Win, and E. Vlahu-Gjorgievska, 'Information security governance challenges and critical success factors: Systematic review,' Computers & Security, vol. 99, Art. no. 102030, 2020.

[13] P. Jimbo-Santana, K. Cabrera-Pantoja, and M. Jimbo-Santana, 'Comparative analysis of methodologies for the development of computer audits considering risk analysis, data mining, reference frameworks and international standards,' Revista Colombiana de Computación, vol. 24, no. 1, pp. 18–36, 2023, doi: 10.29375/25392115.4393.

[14] R. Audia and B. Sugiantoro, 'Evaluation and implementation of IT governance using the 2019 COBIT framework,' International Journal on Informatics for Development, vol. 11, no. 1, pp. 152–161, 2022, doi: 10.14421/ijid.2022.3381.

[15] ISACA, COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution. Schaumburg, IL, USA: ISACA, 2018.

[16] M. Alshaikh, 'Developing cybersecurity culture to influence employee behavior: A practice perspective,' Computers & Security, vol. 98, Art. no. 102003, 2020.

[17] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, 'Cybersecurity awareness in the context of the industrial Internet of Things: A systematic literature review,' Computers in Industry, vol. 137, Art. no. 103614, 2022.

[18] J. R. C. Nurse et al., 'The data-driven cyber security board: Metrics and decision support for cyber-risk governance,' Computers & Security, 2023.

[19] N. Apthorpe, B. Beavers, Y. Shvartzshnaider, and B. Frischmann, 'Measuring NIST authentication standards compliance by higher education institutions,' 2024.

[20] A. Alahmari and B. Duncan, "Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence," 2020, pp. 1–5, doi: 10.1109/CyberSA49311.2020.9139638.

[21] M. S. Jalali, M. Siegel, and S. Madnick, "Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment," The Journal of Strategic Information Systems, 2018, doi: 10.2139/ssrn.3022626.

[22] ISO/IEC, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. Geneva, Switzerland: ISO, 2022.

[23] M. Alzahrani, 'Cybersecurity maturity models: A systematic review,' PeerJ Computer Science, vol. 8, Art. no. e1071, 2022.

[24] M. Toussaint, S. Krima, and H. Panetto, 'Industry 4.0 data security: A cybersecurity frameworks review,' Journal of Industrial Information Integration, vol. 38, Art. no. 100546, 2024.

[25] M. Hong, A. P. Sasongko, and H. L. H. S. Warnars, 'Analysis of information security governance for higher education institutions,' in Proc. 2023 Int. Conf. Computer, Electronics and Electrical Engineering and Their Applications, 2023, pp. 29–34.

[26] R. K. Yin, Case Study Research and Applications: Design and Methods, 6th ed. Thousand Oaks, CA, USA: Sage, 2018.

[27] J. W. Creswell and V. L. Plano Clark, Designing and Conducting Mixed Methods Research, 4th ed. Thousand Oaks, CA, USA: Sage, 2023.

[28] M. N. K. Saunders, P. Lewis, and A. Thornhill, Research Methods for Business Students, 9th ed. Harlow, U.K.: Pearson, 2023.

[29] ISACA, COBIT 2019 Framework: Governance and Management Objectives. Schaumburg, IL, USA: ISACA, 2018.

[30] ISO/IEC, ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Controls. Geneva, Switzerland: ISO, 2022.

[31] M. Hennink and B. N. Kaiser, 'Sample sizes for saturation in qualitative research: A systematic review of empirical tests,' Social Science & Medicine, vol. 292, Art. no. 114523, 2022, doi: 10.1016/j.socscimed.2021.114523.

[32] V. Braun and V. Clarke, 'Conceptual and design thinking for thematic analysis,' Qualitative Psychology, vol. 9, no. 1, pp. 3–26, 2022, doi: 10.1037/qup0000196.

[33] M. Tsiodra, S. Panda, M. Chronopoulos, and E. Panaousis, 'Cyber risk assessment and optimization: A small business case study,' IEEE Access, vol. 11, 2023.

[34] F. A. Shaikh and M. Siponen, 'Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity,' Computers & Security, vol. 124, Art. no. 102974, 2023.

[35] R. C. J. Alexandre, L. E. G. Martins, and T. Gorschek, 'Cybersecurity risk assessment for medium-risk drones: A systematic literature review,' IEEE Aerospace and Electronic Systems Magazine, vol. 38, no. 6, pp. 28–43, 2023.

[36] D. Plekhanov, H. Franke, and T. H. Netland, 'Digital transformation: A review and research agenda,' European Management Journal, vol. 41, no. 6, pp. 821–844, 2023.

[37] K. Papachristofis, K. Vavousis, and G. Hatzivasilis, 'Developing cyber-resistivity maturity and scoring frameworks for organizations,' International Journal of Information Security, 2025.

[38] M. Chen, C. Martins, and A. Teixeira, 'Digital transformation in project management: A systematic literature review,' Administrative Sciences, vol. 15, 2025.

[39] S. Giest, 'Digital and data-driven transformations in governance: A systematic review,' Data & Policy, vol. 7, 2025.

[40] M. M. Kamalaldin, D. Sjödin, D. Hullova, and V. Parida, 'Configuring ecosystem strategies for digitally enabled process innovation,' Technovation, vol. 125, Art. no. 102748, 2023.

[41] M. Da Veiga, 'Developing a cyber security culture: A grounded theory approach,' Computers & Security, 2022.

[42] J. Hobbs, 'Cybersecurity awareness in higher education: A study of faculty and staff,' Issues in Information Systems, vol. 24, pp. 159–169, 2023.

[43] S. Alahmari, B. Duncan, and D. Furnell, 'Cybersecurity skills and awareness in organizations: A systematic review,' Information and Computer Security, 2023.

[44] S. Furnell and N. Clarke, 'Power to the people? The evolving recognition of human aspects of security,' Computers & Security, vol. 116, Art. no. 102648, 2022.

[45] E. Tsen, 'The effect of organizational cyber resilience on cyber incident outcomes,' Journal of Cybersecurity, vol. 11, 2025.

[46] A. Aldabjan and L. Maglaras, 'Cybersecurity incident response readiness in organizations,' International Journal of Information Security, 2024.

[47] A. Gulay and L. Maglaras, 'Alignment of cybersecurity incident prioritisation with incident response management maturity capabilities,' Journal of Cybersecurity and Privacy, 2024.

[48] H. S. Galadima et al., 'Safety science as a source of organizational cyber incident response improvement: A scoping review,' IEEE Access, 2026.

[49] Y. Baseri, V. Chouhan, A. Ghorbani, and A. Chow, 'Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition,' Computers & Security, vol. 148, Art. no. 104141, 2025.

[50] J. A. Calvo-Manzano, T. San Feliu, A. Herranz, J. Mariño, and L.-Å. Fredlund, 'CyberESP: An integrated cybersecurity framework for SMEs,' Journal of Software: Evolution and Process, 2025.

[51] U. Kuckartz and S. Rädiker, Analyzing Qualitative Data with MAXQDA: Text, Audio, and Video. Cham, Switzerland: Springer, 2019.

[52] J. F. Hair Jr., G. T. M. Hult, C. M. Ringle, and M. Sarstedt, A Primer on Partial Least Squares Structural Equation Modeling, 3rd ed. Thousand Oaks, CA, USA: Sage, 2022.

[53] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, 'Security of zero trust networks in cloud computing: A comparative review,' Sustainability, vol. 14, no. 18, Art. no. 11213, 2022.

[54] M. L. Gambo and A. Almulhem, 'Zero trust architecture: A systematic literature review,' Journal of Network and Systems Management, 2026.

[55] M. N. Habib, P. Nanda, and X. He, 'A survey of identity and access management for zero-trust architectures,' IEEE Access, 2023.