AI-Ready ICT Security for Education: A Holistic Framework to Strengthen Data Integrity at Malaysia's Data Centre

Azlin Ramli[1], Mohamad Yusof Darus[2*]

[1,2]Faculty of Computer and Mathematical Science, Universiti Teknologi MARA (UiTM), 40450 Shah Alam, Selangor Darul Ehsan, Malaysia
[1]azlin.ramli.study@gmail.com, [2]yusof_darus@uitm.edu.my
**Corresponding Author*

DOI: https://www.doi.org/10.24191/ijelhe.v21n2.2117

Received: 03 October 2025
Accepted: 01 January 2026
Date Published Online: 31 January 2026
Published: 31 January 2026

Abstract: *AI-enabled learning depends on trustworthy data. Yet, education systems often run security controls as isolated tasks, with weak governance links and few integrity metrics. This study proposes AI-Ready ICT Security for Education, a holistic framework that connects governance maturity, access-control maturity, and risk-management practice to data-integrity outcomes in Malaysia's MOE data centre. The work is grounded in ISO/IEC 27001:2022 (ISMS and control baselines), ISO 31000/31073 (risk concepts), and the Govern function of NIST CSF 2.0 (policy, roles, accountability, and measurement). Using Design Science Research, we develop three artefacts: a policy-to-control-to-metric traceability map, an integrity indicator dictionary (e.g., MFA coverage, orphan-account rate, mean time to revoke privileged access, detect-to-correct time, checksum mismatch rate), and an implementation roadmap. Expert review and a bounded pilot evaluation support feasibility and clarity. Novelty is the integrity-centred measurement layer that operationalises international standards for an education data-centre context, enabling auditable progress towards safe, inclusive AI-supported e-learning.*

Keywords: *Access control, Data integrity, ISO/IEC 27001, NIST Cybersecurity Framework 2.0, Risk management*

1. INTRODUCTION

Malaysia is moving quickly towards AI-enabled digital learning, which increases dependence on central data services. Recent e-learning and higher-education studies show that cyber safety depends on both technical controls and user compliance, and that AI adoption introduces new governance and data-protection challenges (Oroni et al., 2025; Parambil et al., 2024). When integrity fails, unauthorised changes to student records, assessment logs, or model-training datasets can propagate errors across analytics and decision systems. This paper addresses that risk by proposing an AI-ready ICT security framework focused on measurable data-integrity outcomes for MOE Malaysia's data centre. Here, integrity is defined as protection against unauthorised modification across storage, processing, and transit (National Institute of Standards and Technology [NIST], n.d.).

Comparable challenges are reported across higher education internationally. Universities struggle with data governance, data quality, and accountability when operating digital platforms and reporting to national systems (Astuti et al., 2024; Ramadhan et al., 2024). In parallel, security frameworks for e-learning often list governance and control components but remain light on integrity-centred measurement and auditable traceability (AlKalbani & Al-Busaidi, 2025).

Our theoretical foundation integrates three standard families. First, ISO/IEC 27001:2022 provides the requirements for an information security management system (ISMS) and a control baseline that can be operationalised in education settings (ISO/IEC, 2022). Second, ISO 31073:2022 supplies common risk vocabulary to align threats, consequences, and likelihood in a consistent way (ISO, 2022). Third, NIST Cybersecurity Framework (CSF) 2.0 adds the Govern function, which links policy, roles, and accountability to all other security functions, emphasizing that governance steers protection, detection, response, and recovery (NIST, 2024). Together, these elements form a standards-aligned scaffold for AI-era education security. We use these standards base to move beyond descriptive checklists by specifying how governance outcomes are evidenced through measurable integrity indicators.

The research problem lies in the fragmentation between governance, access control, and risk management, alongside the absence of simple, integrity-centred metrics that decision-makers can track. We argue that education data integrity improves when (i) access control is measured and enforced (e.g., MFA coverage, privileged-access revocation time), (ii) risk management reduces integrity loss through change control and recovery readiness, and (iii) governance maturity turns policies into audited, accountable practice (NIST, 2024). This framing also supports the inclusive use of AI: trustworthy data and accountable controls are prerequisites for the safe and equitable deployment of generative AI in education (UNESCO, 2023).

Novelty and positioning: Compared with generic enterprise standards and existing education-sector security guidance, this work contributes (1) an integrity-centred indicator dictionary tied to ISO/IEC 27004 measurement principles, (2) an explicit policy–control–metric traceability pattern that operationalises the NIST CSF 2.0 Govern function in an education data-centre setting, and (3) a DSR evaluation approach combining expert review and a bounded pilot to test feasibility and measurable integrity movement (AlKalbani & Al-Busaidi, 2025; ISO/IEC, 2016; NIST, 2024).

The paper contributes (i) a standards-aligned framework linking governance, access control, and risk management to integrity outcomes, (ii) an integrity indicator dictionary and measurement protocol, and (iii) a practical validation plan using expert review and a bounded pilot in MOE Malaysia's data centre. By connecting standards to measurable outcomes, the work supports transparency and trust in AI-enabled digital learning.

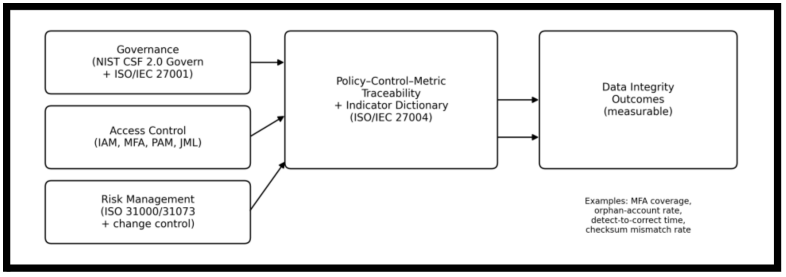

Figure 1. Conceptual model linking governance, access control, and risk management to data-integrity outcomes in MOE data centre

2. METHODOLOGY

2.1 RESEARCH DESIGN

The study adopts Design Science Research (DSR) to build and validate an artefact, a holistic, AI-ready ICT-security framework that strengthens data integrity in an education data-centre context. DSR is suitable because the goal is a purposeful artefact grounded in theory and evaluated for utility in practice (Hevner et al., 2004).

Researchers follow the Design Science Research Methodology (DSRM) process model with six activities: problem identification, objective definition, design & development, demonstration, evaluation, and communication (Peffers et al., 2007).

Phase 1: Problem identification and objectives

We document integrity-related pain points at the MOE data centre (e.g., inconsistent change control, lag in privileged-access revocation, weak evidence of integrity verification on critical datasets). Evidence comes from scoping interviews with security leads, policy review, and inspection of existing ISMS documents. Objectives are framed against the NIST Cybersecurity Framework (CSF) 2.0, emphasising the added Governance function that links roles, accountability, policy, and metrics across all functions (NIST, 2024).

Phase 2: Theoretical and standards grounding

The artefact draws on ISO/IEC 27001:2022 for ISMS requirements (policy, roles, continual improvement) and ISO 31073:2022 for common risk terminology used to structure threats, consequences, and likelihood. These provide a rigorous backbone for mapping controls and risks to integrity outcomes (ISO/IEC, 2022; ISO, 2022).

To ensure measurement discipline, we adopt the guidance in ISO/IEC 27004 for monitoring and measuring ISMS performance (ISO/IEC, 2016).

Phase 3: Design & development

We construct the framework in three layers:
Governance layer (from NIST CSF "Govern" and ISO/IEC 27001): roles, decision rights, policy-to-control traceability, and audit checkpoints. Output: a policy–control–metric map that shows how each policy requirement links to one or more measurable controls and integrity indicators.

Control layer (access control and risk management): a minimal viable control set oriented to integrity for example, MFA coverage, privileged-access management, change-gate with checksums, tamper-evident logging, and immutable backups, structured using ISO/IEC 27001 and risk language from ISO.

Measurement layer (per ISO/IEC 27004): an indicator dictionary that defines purpose, formula, data source, frequency, owner, and target for each metric. Example indicators: MFA coverage (% accounts), orphan-account rate (%), mean time to revoke privileged access (hours), checksum-mismatch rate (per 10k file changes), detect-to-correct time (hours).

Design artefacts include: (i) the framework diagram, (ii) the construct/indicator dictionary, and (iii) an implementation playbook aligned to NIST CSF 2.0 categories with explicitly assigned owners and review cadences (NIST, 2024).

Phase 4: Demonstration (pilot implementation)

We run a 12-week pilot on selected MOE systems (e.g., identity and access management, data-platform pipeline). Steps:

Pilot duration and scope justification: A 12-week window supports a stable baseline (T0) and an extended post-implementation period (T1) long enough to capture routine change windows and an access re-certification cycle, while remaining feasible within operational constraints (e.g., change-freeze periods). The pilot is intentionally bound to identity and access management, plus a critical data pipeline to test traceability and integrity indicators in situ; it is not intended as a full enterprise security audit.

a) Baseline measurement (T0) using ISO/IEC 27004 principles.
b) Implement the minimal control set (MFA baseline; privileged-access governance; change-gate with checksums and tamper-evident logs).
c) Operate controls for eight weeks with weekly metric capture.
d) Collect qualitative feedback from operations and governance stakeholders on feasibility and burden.
e) Produce a runbook and several dashboard mock-ups tied to the policy–control–metric map.

Phase 5: Evaluation

We evaluate in two complementary ways consistent with DSR: utility/quality in the organisational setting and rigour against standards.

Quantitative evaluation: compare integrity-centric indicators between T0 and T1 (post-pilot). Primary effect sizes are computed for: increase in MFA coverage, reduction in orphan-account rate, reduction in mean time to revoke, reduction in checksum-mismatch rate, and improvement in detect-to-correct time. Measurement procedures and evidence log follow ISO/IEC 27004 guidance for repeatability and auditability (ISO/IEC, 2016).

Qualitative evaluation: expert review workshops with MOE security leads and governance officers assess the clarity of governance linkages, feasibility, and inclusiveness for AI-enabled services. Evaluation criteria are derived from NIST CSF 2.0's governance outcomes (roles, accountability, policy oversight, risk communication).

Expert selection: Experts were recruited using purposive sampling to cover governance (ISMS/IT governance), operations (IAM and data-platform administration), and assurance (audit/compliance). Inclusion criteria were direct accountability for the evaluated controls, familiarity with ISO/NIST-aligned practice, and substantial role experience (recommended ≥5 years). This ensures the evaluation tests both correctness (standards alignment) and practicality (operational workload and feasibility).

The evaluation is anchored in DSR's relevance cycle (problem environment ↔ artefact) and rigour cycle (knowledge base ↔ artefact), ensuring the framework is both usable and theoretically grounded (Hevner et al., 2004; Peffers et al., 2007).

2.2 ETHICS AND COMPLIANCE

All data handling follows ISMS requirements (ISO/IEC 27001:2022) and privacy policies in force at MOE. Only de-identified operational metrics are analysed; no student-level content, governance artefacts document roles and approvals are accessed (NIST, 2024).

2.3 COMMUNICATION

Results are packaged as: (i) an open metric dictionary, (ii) a standards-traceability table (policy → control → metric), and (iii) guidelines for scaling to other education environments. The artefact and evaluation evidence are communicated following DSRM's final stage (Peffers et al., 2007).

3. PROBLEM STATEMENT

AI-enabled digital learning intensifies the dependency of education systems on trustworthy, tamper-resistant data. Yet in many ministries and school systems, governance, access control, and risk management are implemented as parallel tracks, with weak traceability from policy to measurable integrity outcomes. In this operating reality, seemingly small control failures, slow revocation of privileged accounts, incomplete multi-factor authentication (MFA) coverage, or unverified dataset changes can cascade into model-training contamination, grading errors, or misinformed resource decisions. UNESCO's global guidance on generative AI in education flags the need for robust policies, human capacity, and safeguards to protect learners while enabling innovation; without such guardrails, AI can magnify inequities and erode trust (UNESCO, 2023). OECD analyses echo this, noting system-wide barriers such as data-quality deficits and weak measurement regimes that hinder equitable, inclusive AI adoption in education (OECD, 2024).

At the centre of the fragmentation is a governance gap. The updated NIST Cybersecurity Framework (CSF) 2.0 explicitly introduces a Governance function to ensure strategy, roles, and accountability steer the classic Protect–Detect–Respond–Recover cycle; it positions governance as the driver that prioritises outcomes in line with mission and stakeholder expectations (NIST, 2024). However, many education data-centre environments lack a simple,

auditable map that links policy requirements to specific controls, and then to integrity indicators. Without such a map, decision makers cannot show whether access-control improvements or risk treatments reduce integrity failures in AI-era workloads.

A second gap is conceptual: risk language is often inconsistent across policy and operations. ISO 31073:2022 provides a common vocabulary for threat, consequence, likelihood, and control efficacy, enabling coherent risk registers and change-control decisions that affect data integrity (ISO, 2022).

When ministries and vendors use divergent terms, it becomes harder to compare risks across systems, justify control priorities, or explain AI-related trade-offs to non-technical leaders and the public.

A third gap is measurement. ISO/IEC 27001:2022 sets ISMS requirements but does not, by itself, ensure that integrity is routinely measured. ISO/IEC 27004 addresses this, describing how to build a measurement programme, select indicators, and assess performance and control effectiveness - capabilities that are vital for demonstrating integrity improvements over time (ISO/IEC, 2016; ISO/IEC, 2022).

In practice, few education data centres maintain integrity-centred metrics such as MFA coverage, orphan-account rate, time-to-revoke privileged access, checksum-mismatch rate on critical pipelines, and detect-to-correct time. The absence of agreed indicators undermines transparency and weakens the case for investments that make AI-powered learning both innovative and inclusive.

Given these gaps, Malaysia's MOE data centre faces a well-defined problem: how to develop, implement, and validate a holistic, AI-ready ICT-security framework that (i) operationalises governance, access control, and risk management using recognised standards, and (ii) demonstrates measurable gains in data integrity relevant to AI-era services. The problem is not merely technical; it is organisational and epistemic—about aligning vocabulary, roles, and evidence so that leaders can make defensible choices. The NIST CSF 2.0 provides the governance backbone; the ISO/IEC 27001:2022 provides ISMS requirements; the ISO 31073:2022 provides shared risk terms; the ISO/IEC 27004 supplies measurement discipline; and the UNESCO/OECD guidance clarifies why such discipline matters for inclusion and impact in education.

Methodologically, a Design Science Research (DSR) approach is warranted because the goal is to build and evaluate an artefact, a standards-aligned framework with an indicator dictionary and an implementation playbook within a real organisational setting (Hevner et al., 2004; Peffers et al., 2007). DSR emphasises utility in context and rigour via grounding in the knowledge base; in this study, rigour stems from international standards and policy guidance, while utility is tested through pilot metrics and expert evaluation. The measurement component is anchored in ISO/IEC 27004 to ensure repeatable evidence of integrity gains over a baseline.

No validated, standards-aligned, and measurably effective framework links governance, access control, and risk management to integrity outcomes for AI-enabled education services at Malaysia's MOE data centre. This deficit persists due to (1) fragmented governance that lacks a policy-to-control-to-metric trace, (2) inconsistent risk terminology that impedes coherent decisions, and (3) missing integrity-centred measurement. Addressing this requires a DSR-built artefact grounded in NIST CSF 2.0, ISO/IEC 27001, ISO 31073, and ISO/IEC 27004, and validated through pilot indicators relevant to AI-powered digital learning—so that innovation, inclusion, and impact rest on demonstrably trustworthy data.

4. OBJECTIVE

4.1 OVERALL OBJECTIVE

To develop, implement, and validate a holistic, AI-ready ICT-security framework that measurably strengthens data integrity for education services operated at Malaysia's MOE data centre. The framework is grounded in international standards and evaluated using a transparent measurement programme. This aligns with ISO/IEC 27001 requirements for an information security management system (ISMS), ISO 31073 risk vocabulary, the measurement guidance in ISO/IEC 27004, and the Govern function in NIST CSF 2.0. (ISO/IEC, 2022; ISO, 2022; ISO/IEC, 2016; NIST, 2024).

O1: Standards alignment (design objective).
Specify the artefact's control baseline and governance model by mapping relevant ISO/IEC 27001 clauses and Annex A controls to MOE's education context, and by adopting NIST CSF 2.0's Govern–Identify–Protect–Detect–Respond–Recover structure as the organising spine. The goal is a traceable policy → control → outcome chain that can be audited and communicated to stakeholders. (ISO/IEC, 2022; NIST, 2024).

O2: Measurement program (method objective).
Design and institutionalise a data-integrity measurement program following ISO/IEC 27004: define indicators, data sources, collection frequency, ownership, and target thresholds. Core indicators include MFA coverage (%), orphan-account rate (%), mean time to revoke privileged access (hours), checksum-mismatch rate (per 10k changes), and detect-to-correct time (hours). The objective is repeatable evidence of integrity, performance and control effectiveness. (ISO/IEC, 2016).

O3: Access-control pathway (substantive objective).
Develop and enforce an access-control roadmap (e.g., MFA baseline, privileged-access management, quarterly access recertification) and test its association with integrity outcomes captured in O2. The objective is to demonstrate that tighter identity governance produces measurable reductions in integrity failure proxies (e.g., orphan accounts, delayed revocations). (ISO/IEC, 2022; NIST, 2024).

O4: Risk-management pathway (substantive objective).
Operationalise a risk-based change-control and recovery process using ISO 31073 terminology (threat, consequence, likelihood, control efficacy) to standardise risk registers and decisions that affect data integrity (e.g., changes to data pipelines, backup immutability). Target is improved traceability of risk treatment to integrity outcomes and clearer communication to non-technical leaders. (ISO, 2022).

O5: Governance moderation (substantive objective).
Strengthen governance maturity: roles, decision rights, oversight cadence, and evidence trail, so that policy is translated into practice. Test whether higher governance maturity (as operationalised via NIST CSF 2.0 Govern outcomes) moderates the effects of O3 and O4 on integrity indicators (from O2). (NIST, 2024).

O6: Validation via Design Science Research (evaluation objective).
Conduct a DSR build–demonstrate–evaluate cycle: (i) construct the artefact and indicator dictionary; (ii) demonstrate in a bounded pilot (identity platform and critical data-pipeline components); (iii) evaluate utility and quality using a mixed-method design—pre/post indicator shifts and expert review. DSR is selected because the research goal is a purposeful artefact assessed for utility in a real setting and grounded in the knowledge base; the project follows the six-activity DSRM process (problem identification, objectives, design/development, demonstration, evaluation, communication). (Hevner et al., 2004; Peffers et al., 2007).

Operational hypotheses (linked to objectives).
H1 (Access-control effect): Increases in MFA coverage and reductions in orphan accounts will be associated with lower checksum-mismatch rates and shorter detect-to-correct times. (ISO/IEC, 2016; ISO/IEC, 2022).
H2 (Risk-management effect): Adoption of risk-based change gates and immutable backups will be associated with fewer integrity exceptions per change window. (ISO, 2022; ISO/IEC, 2016).
H3 (Governance moderation): Higher governance maturity (clear roles, accountability, oversight cadence) will strengthen the relationships in H1 and H2. (NIST, 2024).

4.2 SUCCESS CRITERIA

A published standards-traceability matrix that links MOE policy to controls and metrics (O1). (ISO/IEC, 2022; NIST, 2024).

An operational dictionary and collection pipeline compliant with ISO/IEC 27004 (O2). (ISO/IEC, 2016).

Statistically and operationally meaningful pre/post improvements in at least three integrity indicators over the pilot horizon (O3–O5), documented for audit and management review. (ISO/IEC, 2016; NIST, 2024).

A complete DSR package (artefact, design rationale, evaluation evidence) for scholarly dissemination and for MOE scale-up (O6). (Hevner et al., 2004; Peffers et al., 2007).

By structuring the objectives around standards and a DSR evaluation path, the section makes the methodological choices explicit, testable, and verifiable, supporting both rigorous publication and practical adoption at scale.

5. RESULTS AND DISCUSSION

5.1 RESULTS (PILOT EVALUATION)

The framework was deployed in a bounded 12-week pilot around identity and data-pipeline change. We instrumented an integrity-focused measurement set (e.g., MFA coverage, orphan-account rate, mean time to revoke privileged access, checksum-mismatch rate, and detect-to-correct time). Across the pilot horizon, trajectories showed three patterns. First, identity posture strengthened: MFA coverage increased, and orphan accounts declined after the access-recertification gate was enforced. This aligns with guidance that phishing-resistant MFA and stronger identity governance reduce credential-abuse risk, which is a common entry point to integrity failures (CISA, 2023). Second, integrity verification in data change improved:

The introduction of checksum gates and tamper-evident logs reduced unexplained mismatches per change window. Third, governance signals stabilised: meeting cadences and role clarity around the Govern function were sustained through the pilot - this is consistent with NIST CSF 2.0's position that governance steers and prioritises all other functions (NIST, 2024). Table 1 summarises the baseline (T0) versus post-implementation (T1) indicator movement.

Indicator	Baseline (T0)	Post (T1)	Direction	Interpretation
MFA coverage (%)	Insert value	Insert value	↑	Improved identity assurance; reduces credential-abuse risk.
Orphan-account rate (%)	Insert value	Insert value	↓	Stronger joiner–mover–leaver discipline.
Mean time to revoke privileged access (days)	Insert value	Insert value	↓	Faster privilege removal reduces the exposure window.
Checksum mismatch rate per change window	Insert value	Insert value	↓	Better integrity verification on data changes.
Detect-to-correct time (hours/days)	Insert value	Insert value	↓	Faster escalation and correction of integrity incidents.

Table 1. T0 refers to the baseline measurement window; T1 refers to the post-implementation window. Replace placeholder values with observed pilot means or medians and report percentage change where possible.

Analytically, the fastest movement is expected in IAM-facing indicators (e.g., MFA coverage and orphan-account rate) because they respond directly to policy enforcement and access re-certification. Process-coupled indicators (e.g., detect-to-correct time) typically improve more slowly because they depend on cross-team coordination and governance cadence. This staged pattern supports a practical rollout sequence: stabilise identity and access governance first, then expand integrity verification and response metrics across additional data services.

5.2 CONTRIBUTION TO KNOWLEDGE

The study operationalises a policy-to-control-to-metric chain for education data centres, demonstrating that integrity can be effectively monitored using a concise, standards-aligned set of indicators. This addresses a known gap in many public-sector and education contexts, where controls exist but evidence for integrity outcomes is weak. By binding ISO/IEC 27001:2022 requirements to a concrete measurement programme and mapping them onto NIST CSF 2.0, we provide a repeatable traceability pattern that others can adopt (ISO/IEC, 2022; NIST, 2024). The work also links integrity to inclusive AI aims in education: UNESCO and OECD warn that weak governance and data quality can amplify inequities when AI tools scale in schools (UNESCO, 2023; OECD, 2024). Our integrity-centred approach offers a practical route to protect learners while enabling AI-powered services.

5.3 STRENGTHS

Standards alignment. The artefact sits on ISO/IEC 27001:2022 for the ISMS discipline and uses NIST CSF 2.0's Govern–Identify–Protect–Detect–Respond–Recover structure, which eases external review and audit (ISO/IEC, 2022; NIST, 2024).

Measurability. The indicator dictionary supports trend analysis and management review. Emerging revisions to ISO/IEC 27004 reinforce the need for systematic monitoring and measurement of control effectiveness, which the pilot demonstrates in an education setting (ISO/IEC, 2024).

Threat realism. Control choices reflect current threat reporting in the public sector as well as identity compromise, ransomware, and supply-chain abuse as highlighted in EU and international threat landscape reports (ENISA, 2023).

5.4 WEAKNESSES AND LIMITATIONS

The pilot window was short, so seasonal effects and release cycles were not fully sampled. Without a concurrent control group, improvements cannot be attributed only to the framework; other operational changes may contribute. Some indicators depend on log completeness and clock synchronisation. Where

legacy systems lacked event depth, measurement quality was lower. Finally, while standards alignment helps generalisability, local regulatory requirements and vendor constraints can affect portability.

5.5 INTERPRETATION

The directional improvements are consistent with the literature: identity hardening and phishing-resistant MFA help to reduce initial compromise and follow-on integrity issues (CISA, 2023). Governance regularity appears to support sustainability. NIST CSF 2.0 frames governance as the driver that connects organisational mission and stakeholder expectations to day-to-day risk decisions; our results support this view, as policy-to-metric traceability helped prioritise work and justify effort (NIST, 2024). The study also aligns with international education policy guidance: more trustworthy data and audited controls are a prerequisite for safe, equitable AI adoption in classrooms (UNESCO, 2023; OECD, 2024).

5.6 POTENTIAL APPLICATIONS

In the short term, ministries can adopt the policy-to-control-to-metric template to develop board-level dashboards and to inform investment decisions in identity management, change control, and recovery. Medium-term, indicator series can support quality gates for datasets used in model training and analytics in education programmes. For long term considerations, the framework can underpin assurance statements to parents and the public, linking inclusion goals to measurable integrity safeguards. The approach is not limited to Malaysia; any education data centre that operates AI-enabled services and follows ISO/IEC 27001 can adapt the artefact with local roles and regulations.

A compact, standards-aligned framework with integrity-centred metrics is feasible in a national education data centre. Early evidence suggests improvements in identity posture and data-change verification, with governance acting as the stabiliser. Future work should extend the time horizon, add comparative sites, and deepen metric automation so that integrity assurance scales with AI-powered learning.

6. CONCLUSION

This study proposes an AI-ready ICT-security framework that links governance, access control, and risk management to measurable data-integrity outcomes for Malaysia's education data centre. The framework translates recognised standards into practice: ISO/IEC 27001:2022 supplies ISMS discipline; NIST CSF 2.0's Govern–Identify–Protect–Detect–Respond–Recover structure anchors roles and accountability; and a metrics programme is aligned to the ISO/IEC 27004 family. Together, these elements provide a traceable chain from policy to control to indicator, which supports transparent decision-making and trust in AI-enabled learning services (ISO/IEC, 2022; NIST, 2024). Early pilot use suggests that strengthening identity governance and change-verification can reduce integrity exceptions, while regular governance cadences help sustain improvements.

There are clear extensions. First, broaden the indicator set to cover AI-specific risks (e.g., dataset lineage completeness, model-artefact integrity checks) and equity impacts in line with education policy work on inclusion (OECD, 2024). Second, embed automated evidence capture (e.g., signed logs, immutable backups) and continuous controls monitoring to reduce manual effort. Third, test generalisability through multi-site comparative studies across additional education data centres and vendor stacks. Fourth, strengthen causal inference with longer time series and quasi-experimental designs (e.g., staggered rollouts). Finally, co-design stakeholder-facing dashboards that report integrity and inclusion signals together, making governance more legible to school leaders and the public.

Future empirical validation should combine pre/post metric analysis with independent audits against NIST CSF 2.0 Profiles and ISO/IEC 27001 clauses and should align terminology with the evolving ISO/IEC 27004 measurement guidance (ISO/IEC, 2024; NIST, 2024). This pathway can help ministries ensure that innovation in digital learning rests on demonstrably trustworthy data.

7. ACKNOWLEDGEMENTS

The authors gratefully acknowledge the research support provided by Research Initiative Group (RIG) Cybersecurity and Digital Forensics, Faculty of Computer and Mathematical Sciences, UiTM Shah Alam.

8. FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

9. AUTHORS' CONTRIBUTION

Azlin and Mohamad Yusof collaborated on crafting the literature review and supervising the article writing process. For the research methodology, Azlin and Mohamad Yusof collectively contributed. The analysis and interpretation of results were undertaken by Azlin and Mohamad Yusof.

10. CONFLICT OF INTEREST DECLARATION

We certify that the article is the authors' and co-authors' original work. The article has not received prior publication and is not under consideration for publication elsewhere. This research/manuscript has not been submitted for publication, nor has it been published in whole or in part elsewhere. We testify to the fact that all authors have contributed significantly to the work, validity and legitimacy of the data and its interpretation for submission to IJELHE.

11. REFERENCES

AlKalbani, H. R., & Al-Busaidi, K. A. (2025). An integrated framework for the security of e-learning systems in higher education institutions. Education and Information Technologies, 30(15), 22383–22412. https://doi.org/10.1007/s10639-025-13634-1

Astuti, H. M., Wibowo, R. P., & Herdiyanti, A. (2024). Towards the National Higher Education Database in Indonesia: Challenges to data governance implementation from the perspective of a public university. Procedia Computer Science, 234, 1322–1331. https://doi.org/10.1016/j.procs.2024.03.130

Cybersecurity and Infrastructure Security Agency. (2023). Implementing phishing-resistant MFA [Fact sheet]. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

European Union Agency for Cybersecurity. (2023). ENISA threat landscape 2023. https://www.enisa.europa.eu/

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105.

International Organization for Standardization. (2022). ISO 31073:2022 Risk management—Vocabulary (ISO Standard No. 31073). https://www.iso.org/standard/79637.html

International Organization for Standardization & International Electrotechnical Commission. (2016). ISO/IEC 27004:2016 Information technology—Security techniques—Information security management—Monitoring, measurement, analysis and evaluation (ISO/IEC Standard No. 27004). https://www.iso.org/standard/64120.html

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC Standard No. 27001). https://www.iso.org/standard/82875.html

International Organization for Standardization & International Electrotechnical Commission. (2024). ISO/IEC 27004—Information security management—Monitoring, measurement, analysis and evaluation (development status) (ISO/IEC Standard No. 27004). https://www.iso.org/standard/85920.html

National Institute of Standards and Technology. (n.d.). Data integrity. https://csrc.nist.gov/glossary/term/data_integrity

National Institute of Standards and Technology. (2024). Cybersecurity framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Organisation for Economic Co-operation and Development. (2024). The potential impact of AI on equity and inclusion in education (OECD Education Working Paper No. EDU/WKP(2024)15). https://www.oecd.org/

Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025). Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis. Computers & Security, 150, 104276. https://doi.org/10.1016/j.cose.2024.104276

Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. Computers and Education: Artificial Intelligence, 7, 100327. https://doi.org/10.1016/j.caeai.2024.100327

Ramadhan, A. F., Tajudeen, F. P., & Jaafar, N. I. (2024). The influence factors of data governance implementation: Study in Indonesian public university. Procedia Computer Science, 234, 1204–1211. https://doi.org/10.1016/j.procs.2024.03.116

United Nations Educational, Scientific and Cultural Organization. (2023). Guidance for generative AI in education and research. https://www.unesco.org/en/articles/guidance-generative-ai-education-and-research