Available online at
https://jcrinn.com/
https://crinn.conferencehunter.com/

Journal of Computing Research and Innovation 11 (1) 2026

Journal of Computing Research and Innovation

Governance, Access Control, and Risk: A Conceptual Framework for Data Integrity in Malaysian Educational Systems

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.*

ARTICLE INFO

Article history:
Received 6 November 2025
Revised 1 January 2026
Accepted 23 February 2026
Online first
Published 1 March 2026

Keywords:
Access Control
Data Integrity
ICT Security Governance
Malaysian Educational Institutions
Risk Management

DOI:
10.24191/jcrinn.v11i1.620

ABSTRACT

This study proposes a standards-based framework that links governance, access control, and risk to data integrity in Malaysian education. Governance maturity strengthens access-control effects, while risk management acts independently on integrity. Constructs map to ISO/IEC 27001:2022, ISO 31073:2022, and NIST CSF 2.0 (Govern). We specify a small indicator set—MFA coverage, standing-privilege hours, orphan-account rate, hash-mismatch rate, and detect-to-correct time—and a prioritised roadmap for MOE. Validation will use pre-post or difference-in-differences pilots; moderation will be tested with SEM or multilevel models.

1. INTRODUCTION

Malaysia's education system is moving fast toward data-driven services for learning, assessment, finance, and governance. As platforms grow, the risk of unauthorised modification, inconsistent records, and weak audit trails also grows, which can harm trust and policy decisions. In practice, data integrity, accuracy, and protection from unauthorised change across the lifecycle depend on three linked pillars: governance, access control, and risk management. However, responsibilities are fragmented across agencies and vendors, access practices differ by application, and risk routines are not fully integrated into daily operations in schools and data centres. Sector studies also report uneven maturity in security culture and policy execution, which increases exposure (Medeiros, 2025; Al-Ibrahim et al., 2024).

We advance three claims. First, governance maturity moderates the effect of access control on integrity by improving ownership and enforcement. Second, risk-management maturity independently improves integrity through repeated identification and treatment of hazards. Third, joint improvement is super-

[2*] Corresponding author. *E-mail address*: yusuf_darus@uitm.edu.my
https://doi.org/10.24191/jcrinn.v11i1.620

additive: advancing governance, access, and risk together yields larger gains than any strand alone. We present a standards-anchored conceptual framework and testable propositions for Malaysian educational systems, using the MOE Data Center as the focal context.

2. LITERATURE REVIEW

Recent work in education cybersecurity shows that data integrity depends on how governance, access control, and risk processes are aligned across a complex ecosystem of ministries, data centres, schools, and vendors. International standards give the backbone for this alignment. ISO/IEC 27001:2022 treats security as a management system that links policy, accountability, and continuous improvement, with control choices driven by risk. In education, many integrity failures come not from one technical flaw but from weak governance links, unclear ownership, ad-hoc change management, and inconsistent audit trails. ISO/IEC 27001:2022, therefore, helps define roles, enforce document control, and track corrective actions that directly affect integrity.

NIST CSF 2.0 (2024) adds a formal Govern function and outcome profiles, making governance a first-class driver of risk reduction. Profiles let public education systems set a shared "target state" for integrity while tailoring goals to different entities (central data centre vs. schools). ISO 31073:2022 provides common risk vocabulary so ICT teams, leadership, and policy units share the same meaning for "incident," "likelihood," and "treatment," improving risk registers and audit narratives.

The threat landscape supports a governance-first stance. ENISA (2023) reports rising ransomware, data theft, and supply-chain compromise that often end in integrity drift through unauthorised changes. Education is a high-value target due to dispersed identities, legacy platforms, and limited resources, so integrity controls should be embedded "left of boom," not added after incidents.

At the institution level, Malaysian studies show uneven maturity and fragmented practice. Where risk treatment lags and identity governance is inconsistent, the chance of silent data alteration grows (Dioubate et al., 2023). Access control remains central: recent RBAC-based work shows that fine-grained roles and periodic reviews reduce unauthorised access and improve auditability (Saxena et al., 2023). These patterns transfer to ministry data hubs and school systems when paired with governance checkpoints such as quarterly recertification and orphan-account cleanup.

International standards provide a shared structure: ISO/IEC 27001:2022 aligns policy, roles, and continual improvement; NIST CSF 2.0 adds a formal Govern function and outcome profiles linking leadership aims to identity, change, and monitoring controls; ISO 31073:2022 standardises risk terms (likelihood, consequence, criteria). Together, they support traceability from policy to controls and integrity metrics in education settings.

3. METHOD

This study follows a standards-anchored conceptual design comprising three linked steps: standards mapping, expert consensus, and control prioritisation. First, we map governance, access control, and risk constructs to ISO/IEC 27001:2022, ISO 31073:2022 terminology, and NIST CSF 2.0's Govern function to ensure policy–to–controls traceability for education settings (ISO/IEC, 2022; ISO, 2022; NIST, 2024). Second, a modified Delphi engages 12–18 experts (MOE data-centre leads, school/HEI ICT heads, auditors, governance/risk officers) selected for ≥5 years' experience, active decision/oversight roles, and familiarity with ISO/IEC 27001:2022/CSF 2.0; conflicts of interest are excluded. Round 1 gathers qualitative critique; Round 2 rates relevance, clarity, and feasibility on a 4-point scale and computes Content Validity Index at item (I-CVI) and scale (S-CVI/Ave) levels with keep thresholds I-CVI ≥ 0.78 and S-CVI/Ave ≥ 0.90; sub-threshold items are revised or removed; Round 3 re-rates revised items with a stopping rule of stable medians and ≤10% change in S-CVI/Ave (Romero Jeldres et al., 2023). Third, Analytic Hierarchy Process

https://doi.org/10.24191/jcrinn.v11i1.620

(AHP) elicits pairwise comparisons on criteria—integrity impact, feasibility, cost, auditability—and on candidate controls (e.g., MFA, PAM, access recertification, checksum change-gates, immutable backups); weights are reported with Consistency Ratio target < 0.10 and sensitivity checks. Experts provide informed consent; responses are anonymised; only aggregated statistics are reported.

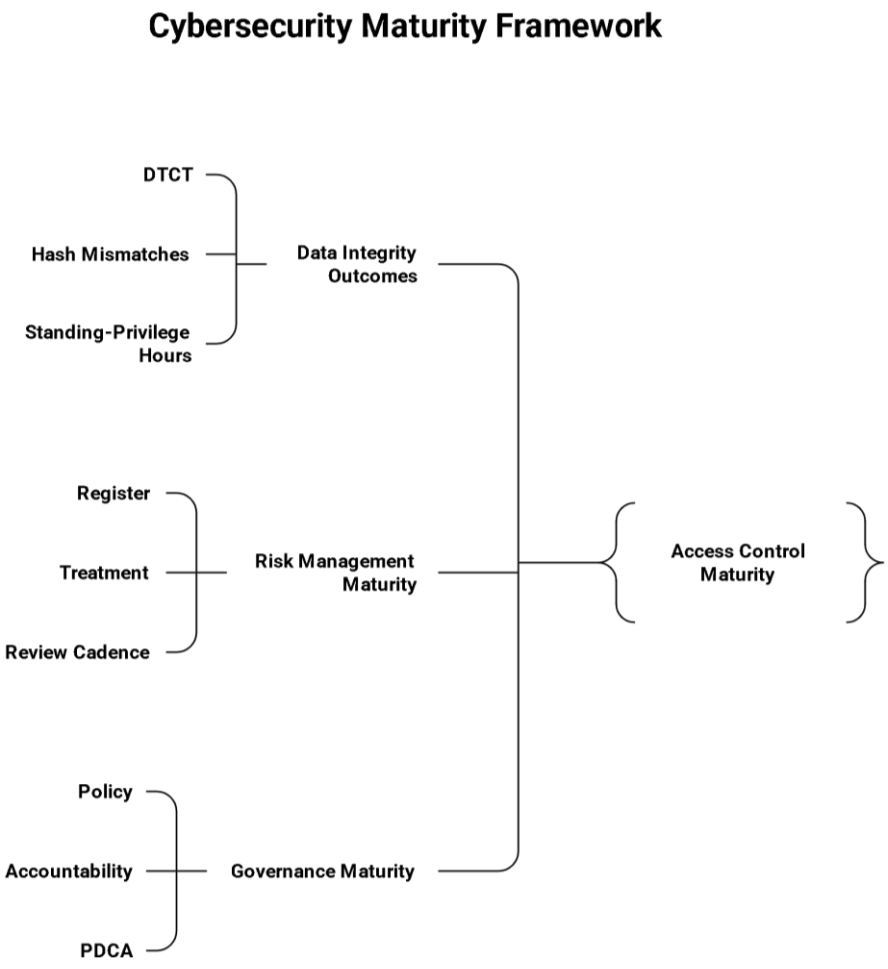

Fig. 1. Governance moderates the Access Control → Data Integrity path; Risk Management has an independent effect. Outcome KPIs include detect-to-correct time (DTCT), hash-mismatch rate, and standing-privilege hours. Solid arrows = direct effects; dashed arrows = moderation. Joint improvements in Governance and Risk are expected to produce super-additive gains.

Fig. 1 shows two direct paths to integrity (Access → Integrity; Risk → Integrity) and a governance moderation on the Access path. Governance improves ownership, review cadence, and enforcement, which strengthens control effects. Risk management acts independently through repeated identification and treatment of hazards. Integrity is observed through KPIs (DTCT, hash-mismatch rate, standing-privilege hours).

This study uses a design-oriented conceptual approach to build and justify a framework that links governance, access control, and risk to data integrity in Malaysian educational systems. The work proceeds in three stages: (1) standards-anchored construction, (2) expert validation via a modified Delphi with

https://doi.org/10.24191/jcrinn.v11i1.620

content validity analysis, and (3) prioritisation of controls using a multi-criteria method to guide adoption in MOE contexts. The choice of a standards-anchored pathway follows current guidance that security governance should be tied to recognised controls and shared risk terminology (ISO/IEC, 2022; ISO, 2022; NIST, 2024).

Stage 1: Framework construction (standards mapping and synthesis)

First, we map governance levers, access-control mechanisms, and risk routines to recognised sources: ISO/IEC 27001:2022 for information security management systems (policy, roles, continual improvement), NIST CSF 2.0 for outcomes and the Govern function, and ISO 31073:2022 for shared risk vocabulary that supports consistent decision-making across MOE units (ISO/IEC, 2022; ISO, 2022; NIST, 2024). The mapping produces a policy–process–technology–people matrix that identifies integrity-relevant practices (e.g., least-privilege enforcement, access recertification cadence, change-management checkpoints, integrity monitoring). These sources are current (2022–2024) and widely adopted, which supports external validity and future comparability in Malaysian settings.

Stage 2: Expert validation (modified Delphi + content validity)

Second, we conduct a modified Delphi with 12–18 experts (MOE data-centre leads, school ICT heads, auditors). Round 1 elicits critique on the draft constructs and indicators; Round 2 rates relevance, clarity, and feasibility on a 4-point scale; Round 3 seeks convergence on disagreements. The modified Delphi is appropriate for building consensus on complex, practice-linked artefacts and has recent methodological guidance for designing panels, rounds, and stopping rules (Hasson et al., 2025). To quantify agreement, we compute Content Validity Index (CVI) at item-level (I-CVI) and scale-level (S-CVI/Ave). Thresholds ≥ 0.78 for I-CVI and ≥ 0.90 for S-CVI/Ave are targeted to indicate strong content validity, following recent discussions and refinements of CVI practice (Romero Jeldres et al., 2023). Items failing thresholds are revised or removed, and free-text comments are thematically coded to inform redrafting before the next round.

Stage 3: Control prioritisation (multi-criteria decision analysis)

Because institutions face resource limits, we prioritise the framework's control bundle using the Analytic Hierarchy Process (AHP) with the Delphi experts. Pairwise comparisons estimate weights for criteria such as integrity impact, feasibility, cost, and auditability. Consistency ratios are checked (<0.10 target). Recent studies show AHP's utility for ranking cybersecurity controls and management guidelines in constrained environments (Moreira, 2025). The output is a ranked roadmap for MOE contexts (e.g., MFA coverage, privileged-access review cadence, change-control gates) that marries impact with feasibility.

From the constructed model and expert inputs, we formalise three propositions for future empirical testing: (P1) governance maturity moderates the effect of access control on integrity; (P2) risk-management maturity independently improves integrity; (P3) joint improvement produces super-additive gains. These propositions are grounded in standards logic, governance sets assurance rules, while access and risk operationalise those rules to reduce unauthorised modification and improve detect-to-correct times (ISO/IEC, 2022; NIST, 2024).

Method choices are documented via a protocol: inclusion criteria for standards and grey literature, expert-selection criteria (role, tenure, certification), Delphi round schedules, CVI computation worksheets, and AHP matrices. Using current global standards (ISO/IEC 27001:2022; NIST CSF 2.0) and shared risk vocabulary (ISO 31073:2022) supports reproducibility in other ministries or universities and enables alignment with audit expectations. All artefacts (construct dictionary, indicators, decision rules, and prioritised roadmap) are packaged for policy uptake and later empirical validation in pilot sites.

https://doi.org/10.24191/jcrinn.v11i1.620

Table 1. Prioritised control roadmap

Priority Rank (provisional)	Control	Integrity Impact	Feasibility	Final Weight (AHP)	Quarter to Start	Primary Owner	Dependencies	Notes
1	Multi Factor Authentication (MFA) enforced for all staff, vendors, and remote access	High	High	0.18	Q1	Identity Admin / ISMS Lead	IdP readiness; user directory hygiene	≥80% coverage in 1 quarter; track exceptions
2	Privileged Access Management (PAM) with just-in-time elevation and session recording	High	Medium	0.15	Q1	Identity Admin / SecOps	MFA baseline; admin account inventory	Reduce standing privileges; review recordings weekly
3	Quarterly access recertification for high-risk systems (student info, finance, HR)	High	Medium	0.12	Q2	System Owners / ISMS	Role catalogue; attestation workflow	Target orphan accounts ≤2%
4	Automated orphan-account detection and cleanup (joiner/mover/leaver)	High	High	0.1	Q1	Identity Admin	HRIS integration; directory sync	Daily detection, weekly cleanup SLA
5	Change-management gate with integrity checksums and mandatory peer review for production changes	High	Medium	0.09	Q2	Change Manager / DevOps	Version control; CI/CD hooks	Block deploys lacking checksum/ approval
6	Immutable backups (WORM) with quarterly restore tests and reconciliation to source records	High	Medium	0.08	Q2	Backup Admin / DBA	Storage support; runbook for restores	Track Mean Time to Restore (MTTR)
7	Database integrity controls: constraints, hashing of critical tables, and tamper-evident audit trails	High	Medium	0.07	Q3	DBA / App Owner	Schema review; app changes	Daily hash reconciliation on critical tables
8	Centralised logging with WORM storage and SIEM rules for integrity drift	Medium	Medium	0.06	Q2	SecOps	Syslog/agent rollout; parsers	Alert on unauthorised update patterns
9	Risk register with monthly review,	Medium	High	0.05	Q1	Risk Manager / ISMS	Shared taxonomy	≥90% risks with active

Priority Rank (provisional)	Control	Integrity Impact	Feasibility	Final Weight (AHP)	Quarter to Start	Primary Owner	Dependencies	Notes
	treatment tracking, and integrity-specific risk criteria						(ISO 31073); tooling	treatment plans
10	Incident-response tabletop focused on data tampering and recovery validation	Medium	High	0.04	Q3	IR Lead / App Owners	Runbooks; comms plan	Measure detect-to-correct time (DTCT)
11	Configuration baseline and drift detection (e.g., CIS benchmarks) on critical servers	Medium	Medium	0.03	Q3	Platform Team / SecOps	Baseline definition; agent rollout	Weekly drift reports to owners
12	Data classification and retention policy tied to integrity controls and purge routines	Medium	Medium	0.03	Q4	Records Officer / ISMS	Policy approval; DLP/archival	Reduce stale records exposure

Table 1 ranks controls by AHP weight (impact, feasibility, cost, auditability) and sets rollout quarter, owner, and dependencies. Notes list target thresholds (e.g., MFA ≥80% in Q1; orphan-accounts ≤2%) for monitoring; telemetry sources are defined for each KPI.

We will validate with pre-post or difference-in-differences pilots during PAM and checksum-gate rollouts; test moderation (governance × access-control → integrity) via SEM or multilevel models. Telemetry: IdP/IAM (MFA), PAM logs (standing-privilege hours), CI/CD & change-gate (blocked unsafe changes), DB integrity job (hash-mismatch), SIEM (tamper detection), backup (restore success), service desk (DTCT).

We mapped governance, access, and risk constructs to ISO/IEC 27001:2022, NIST CSF 2.0 (Govern), and ISO 31073:2022 to ensure traceability from policy to controls and metrics. A modified Delphi with 12–18 experts (≥5 years; MOE/schools/auditors; ISO/IEC 27001 and CSF familiarity) used Round-1 critique, Round-2 4-point ratings with CVI (keep thresholds I-CVI ≥ 0.78; S-CVI/Ave ≥ 0.90), and a Round-3 stability rule (≤10% S-CVI/Ave change). We then applied AHP to prioritise controls by integrity impact, feasibility, cost, and auditability, reporting local/global weights with CR < 0.10 and sensitivity checks. Only aggregated statistics are reported.

4. RESULTS AND DISCUSSION

Expert feedback clarified the framework: access control split into MFA, PAM (just-in-time + session recording), and quarterly recertification; KPI formulas were tightened (DTCT, orphan-account rate). Items with I-CVI < 0.78 were simplified; the instrument reached S-CVI/Ave ≥ 0.90. AHP moved orphan-account cleanup earlier and kept the checksum gate in wave one for hash-mismatch reduction. Each priority control maps to KPIs so change is visible: MFA lowers unauthorised-change incidents and DTCT; PAM cuts standing-privilege hours and improves detection; recertification + JML reduces orphan-accounts; a

checksum + peer-review gate lowers hash-mismatch, and boosts blocked unsafe changes; immutable backups increase restore success and further reduce DTCT and post-recovery variance.

Table 2. Integrity KPI mapping

Control (Priority)	Primary KPI(S) Expected To Move	Expected Direction	Short Mechanism (Why It Moves The KPI)
MFA for all users	Unauthorised-change incidents; DTCT	↓ incidents; ↓ DTCT	Blocks credential theft, so fewer silent edits and faster triage when alerts fire.
PAM (just-in-time + session recording)	Standing-privilege hours (KPI-2); DTCT (KPI-8); Tamper-detection rate (KPI-6)	↓ hours; ↓ DTCT; ↑ detection	Removes always-on admin rights and adds traceable sessions, improving detection and response.
Quarterly access recertification (IGA)	Access-recertification completion (KPI-4); Orphan-account rate (KPI-3)	↑ completion; ↓ orphan rate	Reviews "who should have what," reversing privilege creep and stale access.
Automated orphan-account cleanup (JML)	Orphan-account rate (KPI-3); Tamper-detection rate (KPI-6)	↓ orphan rate; ↑ detection quality	Eliminates stale identities often used for silent changes; cleaner identity set improves signal.
Checksum + peer-review change gate	Blocked unsafe change attempts (KPI-7); Hash-mismatch rate (KPI-5); Reconciliation variance (KPI-9)	↑ blocks; ↓ mismatches; ↓ variance	Stops deployments without integrity evidence; second-pair review catches risky edits.
Immutable backups (WORM) + restore tests	Restore success rate (KPI-10); DTCT (KPI-8); Reconciliation variance (KPI-9)	↑ success; ↓ DTCT; ↓ variance post-recovery	Guarantees clean rollback and proves recoverability

This study delivers three main outputs. First, it proposes a conceptual framework linking governance maturity, access-control maturity, and risk-management maturity to data-integrity outcomes. Governance is treated as a moderator that strengthens the access-control → integrity relationship, while risk management provides an independent path to integrity. The structure is anchored to ISO/IEC 27001:2022, ISO 31073:2022 terminology, and NIST CSF 2.0's Govern function, so policy intent can be translated into controls and measurable results (ISO/IEC, 2022; ISO, 2022; NIST, 2024). Second, the study offers a construct dictionary and indicator set for pilots, including MFA coverage, privileged-access hours, orphan-account rate, hash-mismatch rate, and detect-to-correct time (DTCT). Third, it proposes a prioritised control roadmap—MFA baseline, Privileged Access Management (PAM), quarterly access recertification, checksum-based change gate, and immutable backups, selected for high integrity impact and feasible rollout in MOE environments, consistent with current threat and control evidence (ENISA, 2023; Saxena et al., 2023).

Contribution to knowledge appears in three areas. Integration in many education cybersecurity studies treat governance, access control, and risk as separate tracks, policy teams write documents, ICT teams configure accounts, and auditors review risks later. This separation creates gaps in hand-offs (e.g., change requests without integrity checks, access reviews without owners). Our paper joins these strands into one integrity-centred pathway: governance sets ownership and cadence; access control enforces "who can do what, when, and how"; risk routines keep issues visible and treated. Operationalise the standards "policy-to-controls" bridge by mapping ISO/IEC 27001:2022 clauses and NIST CSF 2.0 Govern outcomes to concrete mechanisms (MFA coverage targets, PAM with just-in-time elevation, quarterly recertification, checksum gates, immutable backups) and to measurable integrity KPIs (DTCT, hash-mismatch rate, orphan-account rate). With this chain, leadership intent flows into daily controls and back into evidence for audits—closing the loop that many institutions miss (ISO/IEC, 2022; NIST, 2024). Mechanism by positing governance as a moderator and risk as an independent driver, the model provides a clear causal story that

https://doi.org/10.24191/jcrinn.v11i1.620

can be tested with maturity scales and integrity KPIs. In the education context, the indicators reflect sector realities—distributed identities, legacy systems, resource limits—and respond to maturity gaps reported in Malaysian HEIs and schools (Dioubate et al., 2023; Al-Ibrahim et al., 2024).

Strengths include standards-based design (external validity and audit alignment), testability via pre–post or quasi-experimental evaluations (e.g., checksum gate → lower hash mismatches; PAM → lower standing-privilege hours), and actionability through an ordered roadmap that answers the "what first?" question in public education ICT.

Weaknesses and limitations are typical of a conceptual study. There is no causal identification yet; effects depend on future pilots. Expert judgement can introduce selection/confirmation bias, even with structured consensus. The threat and tooling landscape changes quickly, so identities, SIEM rules, and controls need periodic re-weighting (ENISA, 2023). Measuring integrity is also difficult because many institutions lack instrumentation for reliable proxies (hash-mismatch rate, reconciliation variance, DTCT), and evidence linking training to durable behaviour remains mixed (Prümmer et al., 2024). Overall, the study provides a standards-based, measurable, and practical foundation for improving integrity in Malaysian education.

This is a conceptual study. There is no causal identification yet; findings depend on future pilots. Expert judgement may introduce selection and confirmation bias, although we used structured consensus, CVI thresholds (I-CVI ≥ 0.78; S-CVI/Ave ≥ 0.90), and AHP consistency (CR < 0.10) with sensitivity checks. Threats and tools change quickly, so control weights should be reviewed each quarter. Some institutions lack telemetry to measure integrity directly; we therefore specify KPIs and sources to support instrumentation and replication.

This framework supports policy and operations in practical ways. Indicators give the MOE Data Centre baselines and success targets during phased rollouts (e.g., MFA $\geq$80% in Q1; orphan accounts $\leq$2% after recertification). Audit alignment improves because ISMS non-conformities can map specific access and risk controls, consistent with ISO/IEC 27001:2022. For procurement and design, the roadmap lists selection criteria for identity, PAM, logging, and backup tools tied to integrity outcomes. On human factors, awareness programmes link to measurable behaviours (e.g., disciplined privileged-access requests), and work best when embedded in roles and feedback cycles (Al-Ibrahim et al., 2024; Prümmer et al., 2024). For sector profiling, NIST CSF 2.0 profiles allow a common "target state" while letting schools implement locally (NIST, 2024). Future research should validate maturity scales and moderation/independent effects (SEM/multilevel), run pre–post or DiD evaluations, and expand KPIs (lineage completeness, reconciliation reliability). Overall, this is a standards-based, testable, and pragmatic foundation for integrity in education.

5. CONCLUSIONS

This study proposes a standards-based conceptual framework that links governance, access control, and risk management to data integrity in Malaysian educational systems. Governance maturity is posited to moderate the effect of access controls on integrity, while risk processes exert an independent influence; advancing governance and risk together should yield super-additive benefits. By mapping constructs to ISO/IEC 27001:2022, ISO 31073:2022 risk terminology, and NIST CSF 2.0's Govern function, the framework translates policy intent into actionable mechanisms and measurable outcomes (ISO/IEC, 2022; ISO, 2022; NIST, 2024). It contributes a clear causal story, a compact indicator dictionary, e.g., MFA coverage, orphan-account rate, hash-mismatch rate, detect-to-correct time (DTCT) and a prioritised roadmap tailored to Ministry of Education (MOE) contexts.

Future work has three tracks. Empirical validation: run pre–post or difference-in-differences pilots as controls (e.g., PAM, checksum change-gates) are deployed; estimate the governance moderation using SEM or multilevel models. Metrics and instrumentation: strengthen integrity telemetry in schools and the MOE Data Center (lineage completeness, reconciliation variance, immutable backup restore success) and

align with CSF 2.0 profiles for sector benchmarking (NIST, 2024). Human factors and resilience: embed role-based training, tabletop exercises, and recovery drills; test for sustained behaviour change, where evidence remains uneven in education (Al-Ibrahim et al., 2024). Because the framework is anchored in universal standards, it is transferable to other data-intensive public institutions (e.g., hospital data hubs, university research/administrative centres). Because the framework rests on universal standards, it transfers to hospitals and universities with minor tailoring to domain models and regulations.

6. ACKNOWLEDGEMENTS/FUNDING

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. No specific funding was received for this work.

7. CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

8. AUTHORS' CONTRIBUTIONS

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

9. REFERENCES

Al-Ibrahim, H., Kamarudin, N. H., Abu Bakar, K. A., Shukur, Z. B., & Hasan, M. K. (2024). Cybersecurity awareness in schools: A systematic review of practices, challenges, and target audiences. *International Journal of Advanced Computer Science and Applications*, *15*(12), 469–480. https://doi.org/10.14569/IJACSA.2024.0151249

Dioubate, B. M., et al. (2023). The role of cybersecurity on the performance of higher education institutions in Malaysia. *Jurnal Pengurusan*, *67*, 31–41. https://doi.org/10.17576/pengurusan-2023-67-03

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape 2023 (July 2022–June 2023)*. Publications Office of the European Union. https://doi.org/10.2824/782573

Hasson, F., Keeney, S., & McKenna, H. (2025). Revisiting the Delphi technique-Research thinking and reporting standards: A discussion paper. *International Journal of Nursing Studies*, *168*, 105119. https://doi.org/10.1016/j.ijnurstu.2025.105119

International Organization for Standardization (ISO). (2022). *ISO 31073:2022—Risk management—Vocabulary*. https://www.iso.org/standard/79630.html

International Organization for Standardization/International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022—Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. https://www.iso.org/standard/82875.html

Medeiros, T., Araújo, A., Silva, J., & Silva, A. (2025). Data governance in education: Addressing challenges and unlocking opportunities for effective data management. In *Proceedings of the 27th International Conference on Enterprise Information Systems (ICEIS 2025): Vol 1* (pp. 367–374).

SciTePress. https://doi.org/10.5220/0013468300003929

Moreira, F. R., Canedo, E. D., Nunes, R. R., Serrano, A. L. M., Abbas, C. J. B., Pereira Júnior, M. L., & Lopes de Mendonça, F. L. (2025). Cybersecurity risk assessment through Analytic Hierarchy Process: Integrating multicriteria and sensitivity analysis. In *Proceedings of ICEIS 2025: Vol. 2* (pp. 117–128). SciTePress. https://doi.org/10.5220/0013197300003929

National Institute of Standards and Technology (NIST). (2024). *The NIST Cybersecurity Framework (CSF) 2.0. (NIST Cybersecurity White Paper 29)*. https://doi.org/10.6028/NIST.CSWP.29

Prümmer, J., van Steen, T., & van den Berg, B. (2024). Assessing the effect of cybersecurity training on end-users: A meta-analysis. *Computers & Security*, *150*, 104206. https://doi.org/10.1016/j.cose.2024.104206

Romero Jeldres, M., Díaz Costa, E., & Faouzi Nadim, T. (2023). A review of Lawshe's method for calculating content validity in the social sciences. *Frontiers in Education*, *8*, 1271335. https://doi.org/10.3389/feduc.2023.1271335

Saxena, U. R., & Alam, T. (2023). Provisioning trust-oriented role-based access control for maintaining data integrity in cloud. *International Journal of System Assurance Engineering and Management*, *14*(6), 2559–2578. https://doi.org/10.1007/s13198-023-02112-x

UNESCO. (2023). *Global Education Monitoring Report 2023: Technology in education—A tool on whose terms?* UNESCO. https://www.unesco.org/gem-report/en/publication/technology