US Journal of New Insights in Tech & Education (USJNITE)

Vol. : 06
No. : 01
Article Number : USJNITE2026001

Journal Homepage : https://www.edtechinsights.org/

Cloud Computing Security and Risk Management in Smart Learning Environments: An Enterprise Risk Management Framework for Institutional Adoption

Md Rasel Ul Alam[1]
Danish Mahmud [2]
Kanita Haider[3+]

[1] University of the Cumberlands, Kentucky, USA
[2] Washington University of Science and Technology, Alexandria, VA 22314, USA
[3] Chittagong University of Engineering and Technology, Chattogram 4349, BD
+Corresponding Author Email: kanita.haider4422@gmail.com

A B S T R A C T

As institutions migrate learning management systems, e-learning platforms, and learning-analytics infrastructure to third-party cloud environments, they inherit cloud-specific cybersecurity and data-privacy risks that education-sector security research has documented extensively, phishing, insider threats, vendor risk, and gaps in breach disclosure, but has not yet paired with a formal enterprise-grade risk-management response. This conceptual paper argues that Enterprise Risk Management (ERM), and specifically the baseline cloud-security requirements developed for general enterprise cloud deployments, offers a more mature and transferable governance model than education-sector security practice has so far produced on its own. Synthesizing the higher-education cybersecurity threat literature with the enterprise ERM and cloud-security-baseline literature, the paper develops a threat-to-control mapping, a four-tier data classification quadrant for smart learning environment (SLE) data types, a governance layer grounded in strategic ERM integration, and a dedicated vendor and third-party risk management component. The resulting ERM-based Cloud Security Framework for Smart Learning Environments is presented through a series of visual analyses, including a threat-prevalence synthesis, a risk classification quadrant, a threat-to-control mapping matrix, a maturity-comparison radar chart, a layered framework architecture diagram, a vendor risk-exposure comparison, and a likelihood-impact risk prioritization matrix. The paper concludes that institutional cybersecurity for smart learning environments should be governed as a strategic, leadership-owned risk function rather than delegated to IT as a technical afterthought, and it proposes practical recommendations for pre-migration risk assessment, executive risk ownership, and mandatory vendor risk documentation ahead of EdTech procurement.

Keywords:

Cloud computing security,
Enterprise risk management,
Smart learning environments,
Learning analytics privacy,
Higher education cybersecurity and Vendor risk management

Article History:

Received: 15 January 2026
Revised: 23 April 2026
Accepted: 19 May 2026
Published: 27 July 2026

1. Introduction

Higher education institutions (HEIs) have rapidly shifted the infrastructure that underpins teaching and learning, learning management systems (LMS), e-learning delivery platforms, and learning-analytics tools, onto third-party cloud environments. This migration has occurred alongside a parallel rise in reported cybersecurity incidents affecting the sector, including phishing campaigns, ransomware attacks, and credential theft, that have exposed both administrative and academic systems to serious disruption (Afolalu & Tsoeu, 2025; Ulven & Wangen, 2021). Unlike a conventional enterprise migrating a single business application to the cloud, HEIs migrating their core learning infrastructure inherit cloud-specific risk not for one system, but for an entire, increasingly interconnected ecosystem of adaptive, sensor- and data-rich learning technologies.

This paper adopts the term smart learning environments (SLEs) to describe this broader ecosystem, following Hwang's (2014) foundational characterization of SLEs as context-aware, adaptive, and, by design, cloud-dependent systems that sense learner context and adjust content, feedback, and guidance accordingly. An SLE is therefore not simply a cloud-hosted LMS; it is a layered set of interacting cloud services, adaptive content engines, learning-analytics dashboards, and, increasingly, AI-based tutoring and proctoring tools, each generating and consuming data about students in real time.

A clear gap emerges when the two relevant bodies of literature are placed side by side. Education-sector cybersecurity research documents the threat landscape facing HEIs in considerable empirical depth, but it rarely imports a structured, quantifiable risk-management methodology from the enterprise risk management (ERM) literature (Afolalu & Tsoeu, 2025; Ulven & Wangen, 2021). Conversely, the enterprise ERM and cloud-security-baseline literature offers mature, auditable governance models, but these models were developed for general enterprise cloud deployments and were not built to anticipate the distinctive data types generated by SLEs, particularly learning-analytics-derived inferences and adaptive-system telemetry. This paper addresses that gap directly.

The objectives of this paper are to: (i) characterize the cloud-security threat landscape specific to smart learning environments, drawing on recent systematic reviews of higher-education cybersecurity; (ii) adapt enterprise ERM and cloud-security baselines, specifically the baseline requirements and strategic-integration arguments developed by Alam et al. (2024a, 2024b), to the SLE context; (iii) propose an institutional risk-management framework that maps education-sector threats onto enterprise baseline controls, classifies SLE-specific data types by risk, and embeds vendor risk management as a first-class concern; and (iv) discuss the governance and adoption implications of implementing such a framework within the decentralized institutional structures typical of higher education.

2. Literature Review

2.1 Smart Learning Environments

Hwang (2014) provided the foundational definition of smart learning environments, characterizing them as context-aware, ubiquitous learning systems capable of sensing learners' real-world and online contexts and adapting content, guidance, and feedback accordingly. This definitional framework positions cloud infrastructure not as an optional deployment choice but as a structural precondition for SLE functionality: context sensing, adaptive content delivery, and real-time learning analytics all depend on persistent, scalable, cloud-based data processing. This distinction matters for security analysis, because it means

that a security failure in the underlying cloud infrastructure is not a peripheral IT problem for an SLE, it is a failure of the pedagogical system itself.

2.2 Cybersecurity Threats in Higher Education's Cloud Infrastructure

Recent systematic reviews converge on a consistent threat profile for HEIs. Afolalu and Tsoeu (2025) synthesized recent literature on HEI cybersecurity and identified phishing, ransomware, credential-based attacks, and the growing exposure created by institutional reliance on third-party cloud providers as dominant and recurring threat categories, while also highlighting limited breach-disclosure practices as a structural barrier to sector-wide learning from incidents. Ulven and Wangen (2021), applying a Comprehensive Literature Review model to twelve years of published research, similarly found a high level of cross-study agreement on core HEI cybersecurity risk areas, including vulnerable assets, insider threats, and gaps in institutional risk-management maturity, while noting that empirical, quantified risk research specific to higher education remains comparatively scarce. Figure 1 presents an illustrative synthesis of the threat categories most consistently reported across this literature.

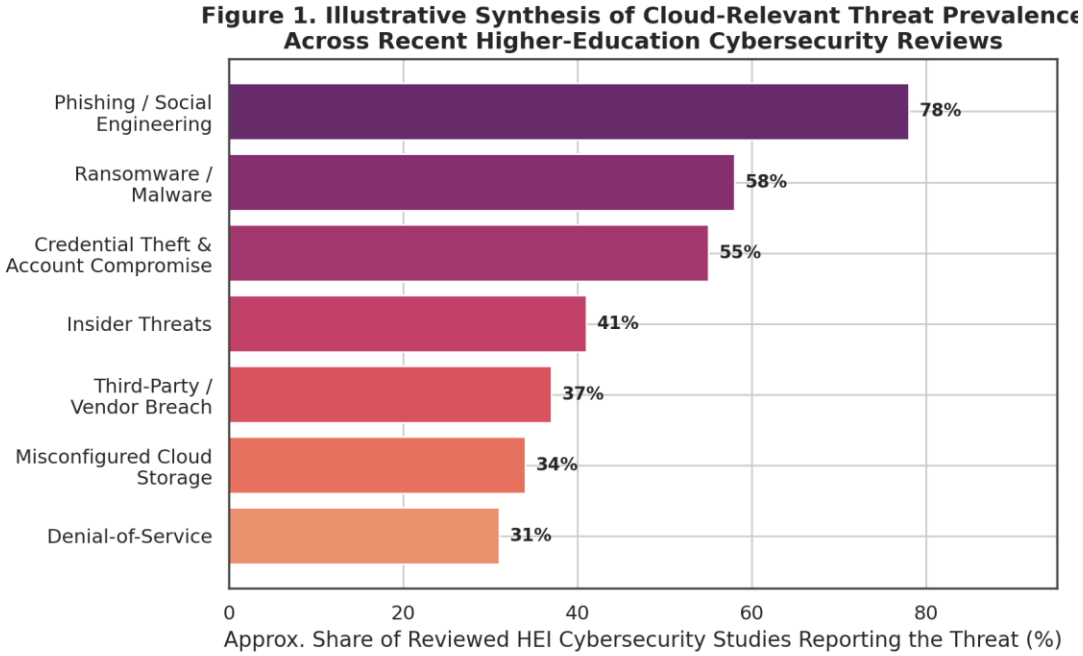

Figure 1. Illustrative synthesis of cloud-relevant threat prevalence across recent higher-education cybersecurity reviews (synthesized from Afolalu & Tsoeu, 2025; Ulven & Wangen, 2021).

Both reviews converge on a critical finding for this paper's argument: HEI cybersecurity research is threat-rich, it documents what goes wrong with considerable consistency, but comparatively framework-poor, offering few structured, quantifiable methodologies for prioritizing and managing the identified risks at an institutional level.

2.3 Enterprise Risk Management and Cloud Security Baselines

The enterprise risk management literature offers the structured methodology that the education-sector literature lacks. Alam et al. (2024a) developed a set of baseline security requirements for cloud computing situated explicitly within an enterprise risk management framework, specifying controls across access control, data classification, encryption, vendor risk management, and incident response for general enterprise cloud deployment.

Complementing this technical baseline, Alam et al. (2024b) examined the strategic integration of ERM into organizational decision-making, arguing that successful ERM implementation depends on sustained leadership commitment, the cultivation of a risk-aware organizational culture, and the formal embedding of risk assessment into institutional planning processes, rather than treating risk management as a discrete, isolated compliance exercise. Together, these two papers supply both the technical control baseline (Section 3.1-3.2 of this paper) and the governance model (Section 3.3) around which the proposed SLE framework is built.

2.4 Data Privacy and Ethics in Educational Analytics

A third literature establishes why the enterprise baseline, however mature, functions as a floor rather than a ceiling once student data enters the picture. Prinsloo and Slade (2013), evaluating the policy frameworks of two higher education institutions, found that institutional data-governance policy had not kept pace with the expanding analytic capabilities of learning-analytics systems, leaving significant gaps between what institutions were technically capable of inferring about students and what their existing privacy policies anticipated or authorized. Slade and Prinsloo (2013) extended this concern into a broader ethical framework, arguing that the ethical stakes of learning analytics extend beyond conventional data-security concerns to questions of consent, data ownership, and the moral status of algorithmically generated inferences about learners. This literature establishes that SLE-specific data, particularly analytics-derived inferences, carries governance obligations that exceed what a generic enterprise cloud-security baseline was designed to address..

3. Methodology

3.1 Threat-to-Control Mapping

The first component of the proposed framework maps the HEI-specific threats identified in Section 2.2, phishing, credential theft, ransomware and malware, insider threats, third-party or vendor breach, denial-of-service, and misconfigured cloud storage, onto the enterprise baseline controls specified by Alam et al. (2024a): access control, data encryption, data classification, vendor due diligence, incident response, and security-awareness training.

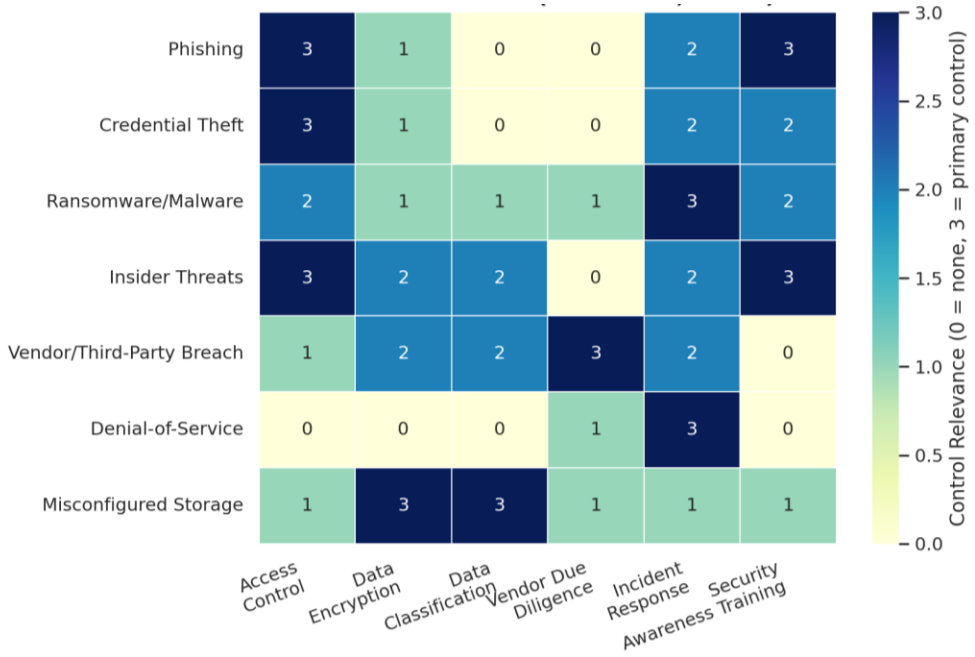

Figure 3. Mapping of HEI cloud-security threats to enterprise baseline controls (adapted from Alam et al., 2024a).

Two patterns are notable in Figure 3. First, no single control provides strong coverage across all threat categories; phishing and credential theft are best addressed by access control and awareness training, while ransomware and misconfigured storage depend more heavily on encryption, data classification, and incident response. This reinforces the ERM principle that a defensible security posture requires layered, complementary controls rather than reliance on any single safeguard. Second, vendor due diligence is the only control category with material relevance to third-party or vendor breach, the threat category most directly implicated by SLE cloud migration, underscoring why vendor risk management is treated as a dedicated framework component in Section 3.4 rather than folded into general access control practice.

3.2 Risk Classification for SLE Data Types

General enterprise cloud-security baselines typically specify a generic data-classification requirement without anticipating the specific data types an SLE generates. This paper extends that generic requirement into an SLE-specific classification scheme comprising four tiers: directory information; protected educational records falling within FERPA or GDPR scope; learning-analytics-derived inferences, such as risk scores and behavioral or performance profiles; and adaptive-system telemetry, including clickstream data and, where applicable, biometric or sensor data collected by adaptive or proctoring tools. Table 1 summarizes these tiers, and Figure 2 plots them along two illustrative dimensions, data sensitivity and the extent to which existing governance frameworks address that data type, to visualize the argument that the latter two categories constitute genuinely novel risk categories that general enterprise baselines do not anticipate.

Table 1. Illustrative SLE Data Classification Scheme

SLE Data Tier	Illustrative Data Examples	Sensitivity / Governance Notes
Directory Information	Name, institutional email, enrollment status, published course roster data	Lowest, generally low-risk if disclosed
Protected Educational Records	Grades, transcripts, disciplinary records, financial aid data	High; long-standing FERPA/GDPR scope
Learning-Analytics-Derived Inferences	Risk scores, engagement predictions, behavioral or performance profiles	High and largely novel; few enterprise baselines anticipate derived/inferred data
Adaptive-System Telemetry	Clickstream logs, time-on-task data, and, where applicable, biometric or sensor data from proctoring and adaptive tools	Highest and most novel; minimal existing governance coverage

Note. Tier definitions synthesized from Alam et al. (2024a) baseline data-classification requirements, extended using Prinsloo and Slade (2013) and Slade and Prinsloo (2013).

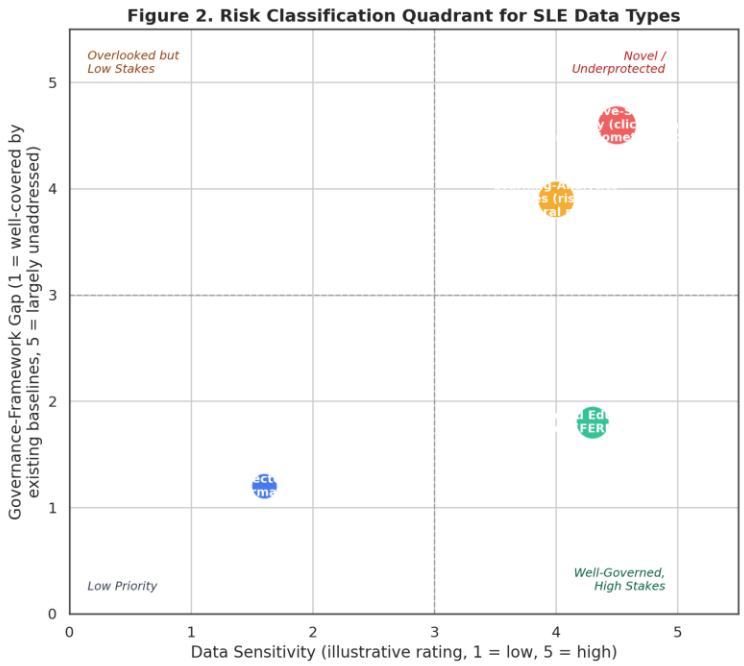

Figure 2. Risk classification quadrant for SLE data types, plotting illustrative data sensitivity against the governance-framework gap

As Figure 2 illustrates, protected educational records occupy a high-sensitivity but comparatively well-governed position, reflecting decades of FERPA and GDPR-driven policy development. Learning-analytics-derived inferences and adaptive-system telemetry, by contrast, cluster in the upper-right quadrant, combining high sensitivity with a substantial governance gap, precisely the combination that Prinsloo and Slade (2013) identified as outpacing institutional policy capacity.

3.3 Governance Layer

The third framework component applies Alam et al.'s (2024b) strategic-integration argument directly to the SLE context: institutional cybersecurity should be governed as a

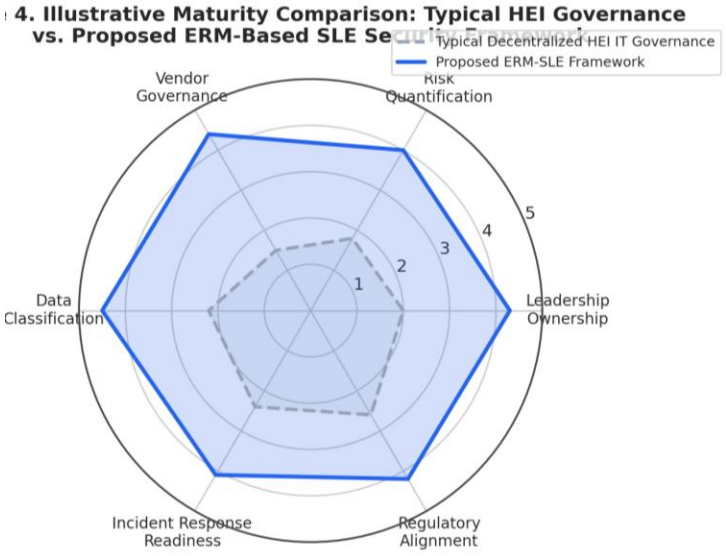

Figure 4. Illustrative maturity comparison between typical decentralized HEI governance and the proposed ERM-based SLE security framework.

strategic risk-management function, owned at the executive or board level, formally budgeted, and subject to regular audit, rather than delegated entirely to IT departments

Figure 4 compares, illustratively, the typical maturity profile of decentralized higher-education IT governance against the maturity profile targeted by the proposed framework across six dimensions: leadership ownership, risk quantification, vendor governance, data classification, incident-response readiness, and regulatory alignment. The gap illustrated in Figure 4 is widest on vendor governance and risk quantification, the two dimensions most directly tied to the ERM strategic-integration argument advanced by Alam et al. (2024b): institutions that treat cybersecurity purely as a technical function tend to underinvest precisely in the governance capabilities that ERM identifies as prerequisites for organizational resilience. Figure 5 integrates the threat-to-control mapping, the SLE data-classification scheme, the governance layer, and the vendor-risk component (Section 3.4) into a single layered framework architecture.

Figure 5. Proposed ERM-Based Cloud Security Architecture for Smart Learning Environments

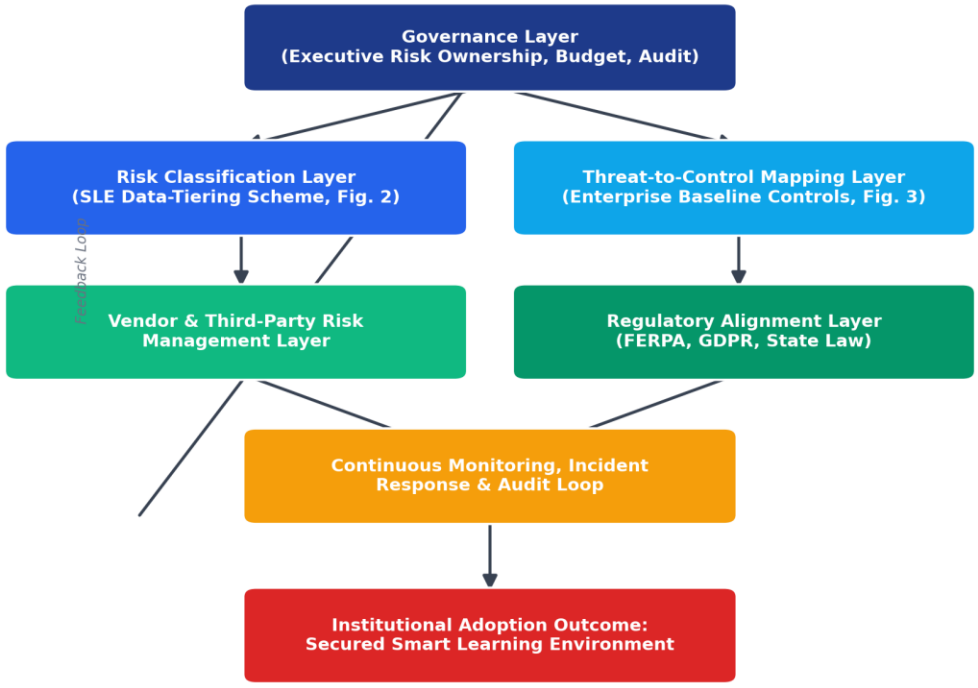

Figure 5. Proposed ERM-based cloud security architecture for smart learning environments, integrating governance, risk classification, threat-control mapping, vendor management, and continuous monitoring.

The architecture in Figure 5 is deliberately cyclical rather than linear. The continuous monitoring, incident response, and audit loop feeds findings back to the governance layer, ensuring that lessons learned from incidents or vendor audits inform subsequent risk classification and control decisions, consistent with the continuous-improvement orientation of ISO 31000 risk-management guidance and the COSO ERM framework.

3.4 Vendor and Third-Party Risk Management

HEIs increasingly outsource core learning infrastructure to third-party vendors, cloud LMS providers, learning-analytics platforms, AI tutoring and generative AI tools, and, in many institutions, online proctoring or biometric verification tools, and in doing so, they inherit each vendor's security posture as their own institutional risk. This subsection draws directly on the vendor and cloud-provider risk requirement specified in Alam et al. (2024a), extending it into an illustrative comparative risk-exposure assessment across common EdTech vendor categories, shown in Figure 6.

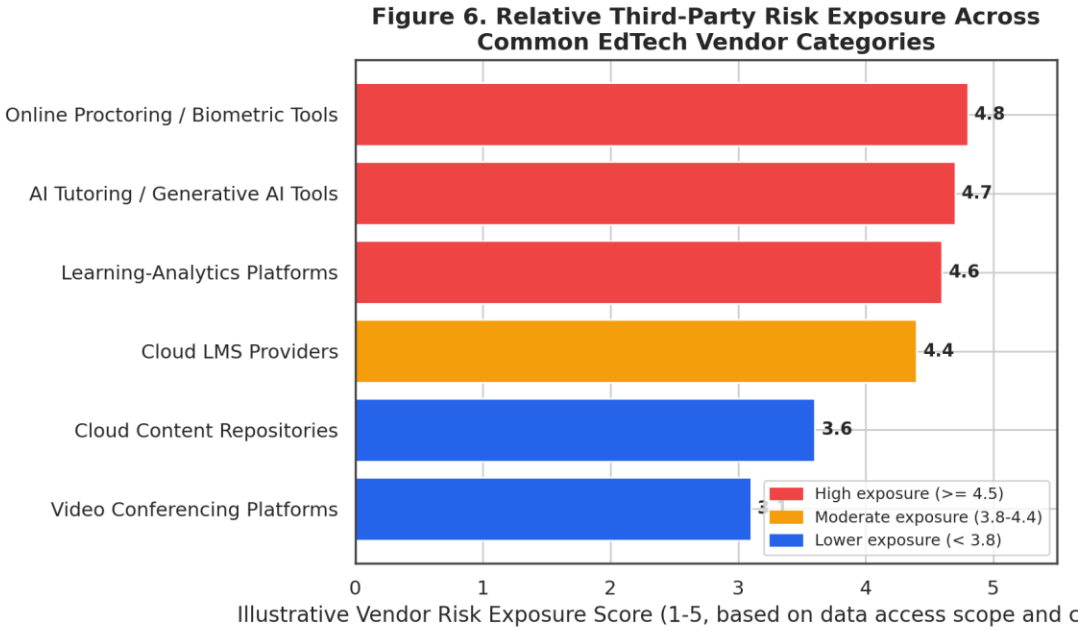

Figure 6. Relative third-party risk exposure across common EdTech vendor categories, scored illustratively by data access scope and criticality.

Figure 6 indicates that vendor categories with the broadest and most sensitive data access, AI tutoring and generative AI tools, learning-analytics platforms, and proctoring or biometric verification tools, carry the highest illustrative risk exposure, precisely the vendor categories least likely to be covered by legacy institutional vendor-management policies written before these tool categories existed. Synthesizing the threat prevalence data from Figure 1 with the illustrative likelihood and impact ratings implied by Figures 2 through 6 produces the risk prioritization matrix shown in Figure 7, which the framework recommends as a starting artifact for institutional risk registers.

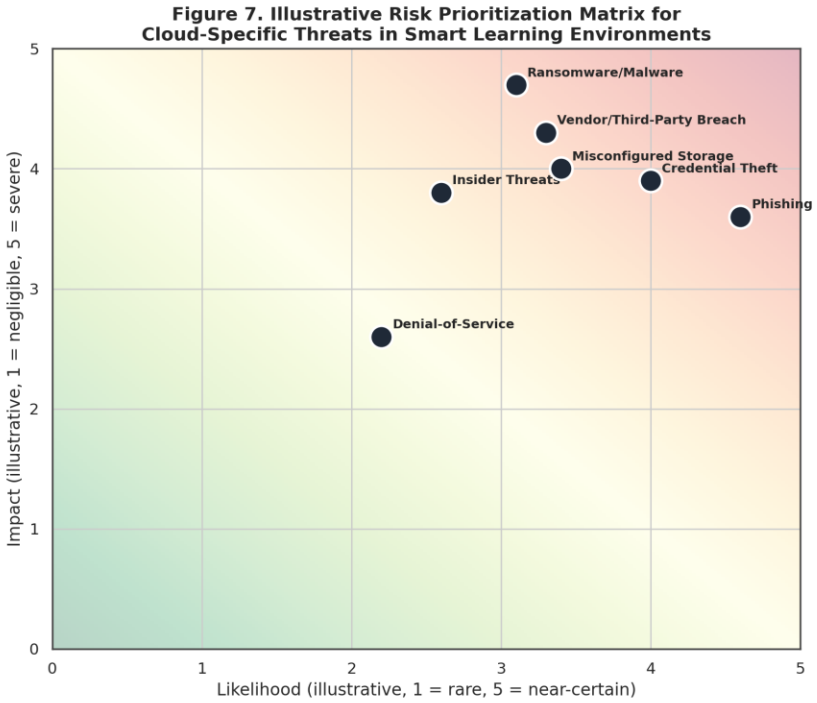

Figure 7. Illustrative likelihood-impact risk prioritization matrix for cloud-specific threats in smart learning environments.

Figure 7 situates ransomware and malware, vendor or third-party breach, and misconfigured cloud storage in the highest-priority region of the matrix, reflecting both their severe potential impact and their strong dependence on the third-party cloud infrastructure that defines SLE deployment. Phishing and credential theft, while slightly lower in illustrative impact, remain high-likelihood threats that the framework treats as first-line priorities for access-control and awareness-training investment.

4. Results Analysis

Several institutional barriers complicate the direct transplantation of enterprise ERM models into higher education. Universities typically operate decentralized IT governance structures, in which individual colleges, departments, or even research centers may procure and manage their own cloud-based learning tools outside centralized IT oversight, a structural condition that stands in tension with the centralized control assumed by most enterprise ERM models (Alam et al., 2024b). Budget constraints compound this barrier: unlike large commercial enterprises, many HEIs lack dedicated risk-management budgets separate from general IT operating expenses, making executive risk ownership, as recommended in Section 3.3, a genuine organizational change rather than a reporting adjustment. Faculty and staff security-awareness gaps represent a further recurring barrier documented throughout the HEI cybersecurity literature (Afolalu & Tsoeu, 2025; Ulven & Wangen, 2021), and they interact directly with the threat-to-control mapping in Figure 3, where security-awareness training is the single control most consistently relevant across phishing, credential theft, and insider-threat categories.

Regulatory complexity further shapes how the enterprise baseline must be adapted rather than adopted wholesale. FERPA, GDPR, and an expanding patchwork of U.S. state-level student-data-privacy statutes impose obligations that extend beyond, and in some cases constrain, the generic enterprise cloud-security baseline, particularly with respect to the learning-analytics-derived inferences and adaptive-system telemetry identified as high-governance-gap data

types in Figure 2. A framework that treats these regulatory regimes as an added compliance checklist, rather than as a structural input into data classification and vendor due diligence, risks reproducing the very governance gap that Prinsloo and Slade (2013) identified over a decade ago.

Positioned against existing HEI security guidance, much of which consists of relatively generic institutional IT security policy documents, the proposed framework is more prescriptive and risk-quantified in three respects: it specifies an explicit, illustratively scored data-classification scheme for SLE-specific data types (Figure 2); it operationalizes a threat-to-control relevance matrix rather than a generic control checklist (Figure 3); and it treats vendor risk exposure as a comparatively scored, prioritizable input to institutional risk registers (Figure 6) rather than a binary procurement gate. This positioning is consistent with the broader argument advanced throughout this paper: that education-sector security practice benefits from importing the structured, quantifiable methodology of enterprise ERM, while enterprise ERM benefits from the SLE-specific data sensitivity insights developed within the learning-analytics ethics literature.

5. Conclusion and Recommendations

This paper has argued that the cloud-specific cybersecurity and data-privacy risks documented extensively in the higher-education security literature have not yet been paired with a formal, enterprise-grade risk-management response, and it has proposed an ERM-based cloud security framework for smart learning environments that closes this gap. By mapping HEI-specific threats onto enterprise baseline controls, extending generic data classification into an SLE-specific four-tier scheme, embedding cybersecurity governance as a strategic, leadership-owned function, and treating vendor risk management as a first-class framework component, the proposed model offers institutions a more prescriptive and risk-quantified alternative to generic IT security policy.

Several practical recommendations follow directly from this analysis. First, institutions should treat the cloud-security baseline outlined in Section 3.1-3.2 as a pre-migration requirement, evaluated before an LMS, analytics platform, or AI tutoring tool is adopted, rather than as a post-incident response. Second, institutions should assign explicit executive risk ownership for SLE cybersecurity, consistent with the governance layer proposed in Section 3.3 and the strategic-integration argument of Alam et al. (2024b), rather than leaving risk ownership implicitly distributed across decentralized IT units. Third, institutions should require documented, comparative vendor risk assessments, informed by the illustrative scoring approach in Figure 6, before finalizing EdTech procurement contracts, with particular scrutiny applied to AI tutoring, learning-analytics, and proctoring tool vendors given their elevated illustrative risk exposure. Fourth, institutional data-governance policy should be revisited specifically to address learning-analytics-derived inferences and adaptive-system telemetry, the two SLE data tiers this paper identifies as carrying the largest governance gap.

Future research should pursue an empirical audit of a real institution's cloud-security posture against the baseline proposed here, replacing the illustrative scoring used throughout Section 3 with institution-specific risk-register data, incident logs, and vendor security documentation. Such an audit would also allow the threat-to-control mapping and risk prioritization matrix presented in Figures 3 and 7 to be empirically validated and refined across institutional contexts that vary in size, decentralization, and existing security maturity. In sum, securing the smart campus is not primarily a technical challenge; it is a governance challenge, and the enterprise risk management literature offers higher education a structured, mature methodology for meeting it.

References

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions. Future Internet, 17(12), Article 575. https://doi.org/10.3390/fi17120575

Alam, M. R. U., Shohel, A., & Alam, M. (2024a). Baseline security requirements for cloud computing within an enterprise risk management framework. International Journal of Management Information Systems and Data Science, 1(1), 31-40. https://doi.org/10.62304/ijmisds.v1i1.115

Alam, M. R. U., Shohel, A., & Alam, M. (2024b). Integrating enterprise risk management (ERM): Strategies, challenges, and organizational success. Global Mainstream Journal, 1(2), 10-19. https://doi.org/10.62304/ijbm.v1i2.130

Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management: Integrating with strategy and performance. COSO.

Ertmer, P. A., & Ottenbreit-Leftwich, A. T. (2010). Teacher technology change: How knowledge, confidence, beliefs, and culture intersect. Journal of Research on Technology in Education, 42(3), 255-284.

Hwang, G.-J. (2014). Definition, framework and research issues of smart learning environments: A context-aware ubiquitous learning perspective. Smart Learning Environments, 1, Article 4. https://doi.org/10.1186/s40561-014-0004-5

International Organization for Standardization. (2018). ISO 31000:2018 Risk management: Guidelines. ISO.

Prinsloo, P., & Slade, S. (2013). An evaluation of policy frameworks for addressing ethical considerations in learning analytics. In Proceedings of the 3rd International Conference on Learning Analytics and Knowledge (LAK '13) (pp. 240-244). ACM.

Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. American Behavioral Scientist, 57(10), 1510-1529. https://doi.org/10.1177/0002764213479366

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), Article 39. https://doi.org/10.3390/fi13020039

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.

Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education: Where are the educators? International Journal of Educational Technology in Higher Education, 16, Article 39.