International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

# DIGITAL INFRASTRUCTURE GOVERNANCE IN U.S. HIGHER EDUCATION: A PRACTITIONER FRAMEWORK FOR SYSTEM SELECTION

Fatema Akter *

Emporia State University, Emporia, Kansas 66801, United States.
* Corresponding Author

ORCID Details
Fatema Akter: https://orcid.org/0009-0004-1150-0243

International Journal of Science and Research Archive, 2026, 20(02), 289–297

Publication history: Received on 21 June 2026; revised on 12 August 2026; accepted on 14 August 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.20.2.1627



## ABSTRACT

U.S. colleges and universities increasingly depend on cloud platforms, identity services, integration layers, data repositories, and administrative applications to conduct admissions, registration, finance, human resources, advising, and student support. Yet technology selection is often organized as a procurement event even though the resulting decision redistributes institutional risk for a decade or more. This survey integrates information-systems research, higher-education studies, and current U.S. standards to identify recurring selection and governance failures and translate them into an auditable practitioner method. The analysis finds that weaknesses commonly arise from fragmented ownership, premature product comparison, opaque lifecycle costs, insufficient interoperability and exit planning, inconsistent vendor assurance, and failure to connect implementation with measurable benefit realization. In response, the article proposes the Digital Infrastructure Governance and Selection (DIGS) framework. DIGS combines seven decision domains with six stage gates spanning problem definition, mandatory assurance, comparative assessment, controlled piloting, contracting and implementation, and lifecycle review. It distinguishes noncompensatory requirements from weighted preferences, records evidence confidence, and treats portability, accessibility, privacy, cybersecurity, and operational resilience as governance obligations rather than optional features. The framework is a transparent decision aid rather than a statistically validated prediction model. Its contribution is a practical bridge between sociotechnical research and institutional artifacts including requirements, scorecards, risk registers, contracts, pilots, and post-implementation reviews.

**Keywords:** Administrative information systems; Digital infrastructure; Higher education; Information technology governance; Vendor risk; Interoperability

## 1 INTRODUCTION

Administrative information systems are no longer peripheral utilities in higher education. Student information systems, enterprise resource planning platforms, identity and access services, customer relationship management tools, integration platforms, analytics environments, and collaboration suites mediate routine institutional work. They

determine how students register, how employees are paid, how financial aid is processed, how leaders interpret performance, and how an institution continues operating during disruption. A selection decision therefore changes more than software. It changes workflows, data definitions, control boundaries, skill requirements, vendor dependencies, and the institution's capacity to adapt.

The literature on digital transformation consistently treats transformation as organizational change enabled by technology rather than simple digitization [1-4]. Research on enterprise systems in universities likewise shows that structural complexity, decentralized authority, and institutional culture can frustrate implementation even when a system is technically capable [5], [6]. These findings matter in the United States, where institutions range from small private colleges to multi-campus public systems and must reconcile mission, shared governance, regulation, accessibility, cybersecurity, and constrained budgets.

In practice, however, selection is often compressed into a sequence of product demonstrations, request-for-proposal scores, and contract negotiations. That sequence encourages three errors. First, solution features are compared before the institution has agreed on the problem, process boundaries, and desired outcomes. Second, criteria that should be mandatory—such as identity integration, data export, accessibility evidence, or incident-notification obligations—are averaged with attractive but nonessential features. Third, governance attention declines after the contract is signed, just as configuration, data conversion, adoption, and vendor dependence begin to create durable risk.

This article addresses the gap between broad governance principles and the concrete artifacts used by institutional decision makers. It asks: (1) Which recurring challenges shape the selection and governance of digital infrastructure and administrative systems in U.S. higher education? (2) Which requirements should operate as noncompensatory gates rather than weighted preferences? and (3) How can institutions make selection evidence auditable across the full technology lifecycle? The contribution is the Digital Infrastructure Governance and Selection (DIGS) framework, a practitioner-oriented synthesis that converts established research and standards into seven assessment domains and six decision gates.

The article is a structured integrative survey, not an empirical evaluation of a specific institution or vendor. It does not claim that DIGS has been statistically validated. Rather, it offers a transparent design proposition, consistent with design-oriented information-systems inquiry [22], that can be tested, adapted, and compared in future case research.

## 2 MATERIAL AND METHODS

The review combined peer-reviewed research on digital transformation, enterprise systems, information-systems success, technology governance, and higher-education implementation with authoritative U.S. guidance on cybersecurity, privacy, accessibility, and vendor assurance. Priority was given to sources that supplied one of four kinds of evidence: explanatory models, higher-education observations, control requirements, or operational tools. Seminal sources were retained where later work continued to rely on their constructs; current standards were used where requirements have changed.

The synthesis was organized around a decision lifecycle rather than around product categories. Evidence was coded conceptually against six questions: What institutional problem is being addressed? Who has decision rights? What architecture and data dependencies are created? Which risks cannot reasonably be traded away? What evidence reduces uncertainty before commitment? How will outcomes and obligations be monitored after implementation? Recurring issues were then consolidated into the seven DIGS domains.

This approach has limits. It is integrative rather than a PRISMA systematic review, does not estimate effect sizes, and does not rank products. The practitioner interpretation is most applicable to U.S. institutions selecting enterprise or shared administrative capabilities. Local law, collective bargaining, system-level policy, institutional classification, and technical maturity may change the appropriate thresholds and weights.

## 3 RESULTS

### 3.1 Institutional technology environment

#### 3.1.1 A Coupled Sociotechnical Stack

Digital infrastructure is best understood as a coupled stack. Network and cloud services support identity, integration, data, and applications; governance obligations cut across every layer. An administrative application can appear successful in a demonstration while still failing institutionally because its identity model conflicts with account-lifecycle

practices, its application programming interfaces are incomplete, its data definitions fragment reporting, or its support model exceeds local capacity.

This layered view discourages isolated product evaluation. A student-facing interface, for example, may depend on identity proofing, role assignment, application integration, authoritative records, notification services, and accessible content. The relevant unit of analysis is therefore the service ecosystem and its operating model, not the user interface alone.

### 3.2 Distributed Authority and Mission Diversity

Universities combine professional administration, academic governance, departmental autonomy, and centralized fiduciary responsibility. Decision rights are consequently distributed. Enterprise-system studies have long shown that standardized software can collide with local practices and meanings [5], while higher-education evidence identifies structural and cultural barriers to advanced information-system adoption [6]. Governance must therefore do more than approve a purchase. It must specify who owns outcomes, data, risk acceptance, architecture, process design, and post-launch performance.

The objective is not maximum centralization. Local variation can reflect legitimate differences in pedagogy, research, student populations, or regulatory obligations. The governance problem is to distinguish mission-relevant variation from accidental duplication and unmanaged risk. A useful decision record makes that distinction explicit.

### 3.3 Success Is Multidimensional

The DeLone and McLean information-systems success model distinguishes system quality, information quality, service quality, use, user satisfaction, and net benefits [7]. That distinction is valuable for administrative technology because deployment is not equivalent to benefit. A system may be available but produce unreliable data, impose workarounds, shift labor to departments, or reduce students' ability to complete a task. Evaluation should therefore include both technical service measures and outcome measures tied to the original problem.

## 4 RECURRING SELECTION AND GOVERNANCE CHALLENGES

### 4.1 Problem Framing and Requirements Integrity

Premature solution comparison is a foundational failure. When demonstrations begin before an institution maps the current service, exceptions, data flows, and desired outcomes, requirements tend to mirror vendor vocabulary. Attractive features then displace the business case. DIGS begins with a problem charter that states the affected population, baseline performance, process boundaries, nontechnology alternatives, intended benefits, constraints, and accountable owner.

Requirements also need provenance. Each requirement should identify its source—law, policy, architecture, user research, control framework, or strategic objective—and its verification method. This makes it possible to challenge a requirement without losing institutional memory and prevents a long list of unprioritized preferences from masquerading as a specification.

### 4.2 Interoperability, Data Semantics, and Exit

Integration is frequently treated as a count of available interfaces. The more important questions concern completeness, direction, latency, error handling, identity context, versioning, and the ownership of integration labor. Open standards, including sector specifications such as Learning Tools Interoperability [25], can reduce some friction, but nominal support does not guarantee semantic compatibility. Institutions must examine whether identifiers, effective dates, organizational structures, permissions, and historical records retain their meaning across systems.

Portability is equally important. Cloud services redistribute infrastructure responsibility but can deepen dependence on proprietary data models, configuration tools, and vendor-specific skills [8]. An exit plan should therefore be evaluated before entry. Required evidence includes export formats, metadata and audit-log availability, extraction frequency, assistance fees, deletion attestations, transition support, and the time needed to restore an operational service elsewhere.

### 4.3 Privacy, Cybersecurity, and Supply-Chain Risk

Administrative platforms process identity, education, employment, financial, and behavioral data. Their risk cannot be evaluated solely by confirming that a vendor has a certification. NIST Cybersecurity Framework 2.0 places Govern alongside Identify, Protect, Detect, Respond, and Recover and explicitly connects cybersecurity with enterprise risk and

supply chains [9]. NIST supply-chain guidance further recommends establishing an organizational capability and communicating requirements to suppliers [10], [11].

For higher education, HECVAT provides a sector-specific instrument covering cybersecurity, privacy, accessibility, and compliance [12]. A questionnaire, however, is evidence input rather than a decision. Responses should be reconciled with architecture diagrams, independent assessment reports, penetration-testing practices, subprocessor lists, incident history, contract language, recovery objectives, and the sensitivity of the proposed data use. NIST control catalogs and CISA's cross-sector goals can supply additional control and outcome references [23], [24]. Risk acceptance must be assigned to an accountable institutional role, not silently embedded in a procurement score.

Privacy assessment must also address purpose and proportionality. The NIST Privacy Framework connects privacy risk with organizational governance [13]. For institutions, this means documenting data categories, authority and purpose, access roles, retention, secondary uses, disclosures, automated decision support, and deletion. FERPA and the Gramm-Leach-Bliley Act may be relevant, but minimum legal compliance does not resolve every ethical or mission concern [14], [15].

### 4.4 Accessibility and Equitable Service

Accessibility cannot be postponed to implementation because remediation may require vendor engineering, workflow redesign, or a different product. WCAG 2.2 provides testable accessibility criteria [16], and the U.S. Department of Justice's 2024 rule establishes technical requirements for state and local government web content and mobile applications, affecting public institutions covered by Title II [17]. Procurement evidence should include an Accessibility Conformance Report based on the current Voluntary Product Accessibility Template, independent testing where risk warrants it, keyboard and assistive-technology demonstrations, a remediation roadmap, contractual commitments, and a process for reporting barriers. HECVAT's inclusion of accessibility questions supports integrated rather than siloed review [12], [18].

Equity is broader than conformance. Institutions should test critical tasks with users who have varied disabilities, language needs, devices, bandwidth, digital experience, and institutional roles. A system that technically conforms but makes a high-stakes task difficult on a phone or with assistive technology has not fully met the service objective.

### 4.5 Lifecycle Economics and Capacity

License price is a poor proxy for total cost. Relevant costs include implementation partners, integration, identity changes, data cleansing, testing, training, backfill, migration, storage, premium support, security monitoring, accessibility remediation, upgrades, contract escalation, and eventual exit. Benefits should likewise be stated as measurable changes rather than generic efficiency claims.

Capacity is part of feasibility. A configurable platform may be less suitable than a simpler alternative if the institution cannot sustain its required product ownership, release management, analytics, and support. Lifecycle evaluation should therefore pair financial estimates with staffing, skill, and governance commitments.

### 4.6 Adoption, Process Change, and Benefit Realization

Digital transformation research repeatedly emphasizes capabilities, leadership, and organizational change [1-4]. Implementation plans must identify process decisions, affected roles, training, communications, support escalation, and measures of adoption. A controlled pilot should test representative end-to-end tasks and exception cases, not merely collect impressions after a demonstration.

Benefit realization closes the loop. Baselines and target measures should be approved with the business case and reviewed after launch. A balanced set is preferable to a single financial measure [20]. Examples include processing time, error and rework rates, task completion, accessibility defects, integration failures, support volume, data-quality exceptions, recovery performance, and user trust. If benefits do not materialize, governance should trigger corrective action, scope change, renegotiation, or exit.

### 4.7 The DIGS framework

#### 4.7.1 Seven Decision Domains

DIGS organizes evidence into seven domains. The domains are deliberately broader than a conventional feature scorecard because each one represents a source of institutional value or durable risk.

**Table 1: DIGS decision domains**

| Domain | Decision focus | Required evidence |
|---|---|---|
| Mission and service fit | Problem, populations, outcomes, alternatives | Charter, baseline, outcome owner |
| Architecture and interoperability | Identity, integration, semantics, portability | Architecture/data-flow diagrams, interface and export tests |
| Data governance and privacy | Purpose, authority, access, retention, secondary use | Data inventory, privacy assessment, retention and deletion terms |
| Cybersecurity and resilience | Controls, incident response, recovery, supply chain | HECVAT, independent reports, recovery evidence, subprocessor list |
| Accessibility and equity | Conformance, critical tasks, remediation, inclusive service | ACR/VPAT, assistive-technology tests, remediation commitments |
| Lifecycle economics and viability | Total cost, staffing, pricing, vendor and exit | TCO model, staffing plan, references, viability and exit analysis |
| Implementation and benefits | Migration, adoption, operations, measurable outcomes | Pilot results, acceptance criteria, benefit review plan |

### 4.7.2 Noncompensatory Gates and Weighted Preferences

A critical design principle is that some requirements cannot be offset by strengths elsewhere. A platform that cannot meet a legal obligation, protect restricted data, integrate with authoritative identity, or provide a credible exit path should not prevail because it has a strong interface or a lower initial price. DIGS therefore separates mandatory gates from weighted preferences.

For alternatives that pass all mandatory gates, an institution may calculate an auditable comparative score using Eq. (1):

$$S_j = \Sigma_{i=1}^{n} w_i r_{ij} c_{ij} - \lambda R_j \qquad (1)$$

where S_j is the comparative score for alternative j, w_i is the approved weight of criterion i, r_ij is the normalized performance rating, c_ij is the confidence assigned to the supporting evidence, R_j is residual risk, and λ is the institution's approved risk-penalty factor. Weights sum to one. Confidence prevents an unsupported vendor assertion from being treated as equivalent to a successful scenario test or an independent report. The equation is a decision heuristic, not a predictive model; institutions should publish their scales and conduct sensitivity analysis.

### 4.7.3 Six Stage Gates

The DIGS lifecycle uses six stage gates. A decision can be paused, rejected, or returned for additional evidence at each gate.

**Table 2: DIGS stage-gate record**

| Gate | Decision question | Minimum record |
|---|---|---|
| G0 | Is the problem and authority clear? | Charter, baseline, alternatives, owner, decision rights |
| G1 | Does every mandatory obligation pass? | Pass/exception/reject for legal, privacy, security, accessibility, architecture, funding |
| G2 | Which feasible alternative has strongest evidence? | Scenarios, TCO, references, confidence-adjusted scores, sensitivity |
| G3 | Does the service work under representative conditions? | Pilot tasks, exceptions, accessibility, migration, support and operational results |
| G4 | Are claims enforceable and implementation ready? | Terms, service levels, acceptance tests, governance, migration and adoption plan |

| | | |
|---|---|---|
| G5 | Are value and risk acceptable over time? | Benefits, service, risk, cost, vendor review; renew/remediate/compete/exit |

#### 4.7.4 Evidence Hierarchy and Decision Record

DIGS uses an evidence hierarchy to reduce false precision. Direct institutional testing of a critical scenario is generally stronger than a demonstration; independently verified assurance is stronger than an unqualified assertion; and contractually enforceable obligations are stronger than roadmap statements. Evidence should be dated because certifications, subprocessors, product capabilities, and financial conditions change.

The final record should preserve: the problem charter; stakeholder and decision-rights map; mandatory requirements and exceptions; criteria, weights, ratings, and confidence; scenario scripts and results; architecture and data-flow diagrams; risk register; total-cost assumptions; accessibility and security evidence; reference findings; dissenting views; approvals; contract protections; and review dates. Transparency does not eliminate judgment, but it makes judgment inspectable.

#### 4.7.5 Governance operating model

##### 4.7.5.1 Assign Outcomes, Not Only Tasks

An executive sponsor should own the institutional outcome and accepted residual risk. A service owner should own ongoing performance. Data stewards should define authoritative data and permitted uses. Enterprise architecture should assess integration and lifecycle fit. These assignments reflect governance principles that distinguish direction and accountability from day-to-day management [19] and support strategic alignment between institutional and technology capabilities [21]. Security, privacy, accessibility, legal, procurement, records, finance, and affected operational units should have explicit review or approval roles. Students, faculty, and staff who perform critical tasks should participate in scenario design and pilots.

A committee without clear decision rights can diffuse accountability. The charter should identify who recommends, who must concur, who decides, and who can accept an exception. Exceptions should have an owner, rationale, compensating controls, expiration date, and review trigger.

##### 4.7.5.2 Contract as a Governance Instrument

The contract translates evaluation evidence into enforceable behavior. It should align definitions and remedies with the institution's actual risk. Common provisions include data ownership and permitted use; subprocessor notice; security controls and evidence; incident-notification timing; cooperation and cost allocation; recovery objectives; accessibility conformance and remediation; service levels; audit rights; pricing and renewal protections; model-training restrictions where artificial intelligence is present; data return and deletion; transition assistance; and termination rights.

Contract review should trace each material selection claim to a term, acceptance test, or documented risk decision. If a feature or control materially influenced the award but remains only in a sales presentation, the governance record is incomplete.

*Continuous Review*

Cloud services change continuously. New features, subprocessors, integrations, licensing rules, artificial-intelligence functions, and data uses can alter the original risk profile. Where AI capabilities are introduced, governance should add context-specific impact, measurement, and risk controls consistent with the NIST AI Risk Management Framework [26]. Lifecycle governance should therefore use scheduled reviews and event triggers. Events include a major incident, acquisition, material price change, control-report qualification, accessibility complaint, substantial product redesign, new data category, regulatory change, or failure to meet benefit targets.

*Illustrative application*

Consider a university selecting a cloud-based advising and student-success platform. Gate 0 establishes that the problem is inconsistent referral coordination and limited visibility into case status, not a general desire for analytics. The baseline records referral completion, time to first contact, unresolved cases, staff effort, and student-reported barriers.

At Gate 1, the institution requires single sign-on and automated role deprovisioning, defined data purposes, export of case records and audit history, accessibility evidence for high-frequency workflows, minimum recovery objectives, incident notification, and a feasible termination process. A product that cannot export complete case histories fails regardless of its predictive features.

At Gate 2, remaining alternatives are tested against scripted cases involving a student, advisor, disability-services staff member, supervisor, and integration administrator. Ratings are accompanied by evidence confidence. Total cost includes integration, training, identity work, data cleanup, accessibility remediation, support, and exit. Sensitivity analysis determines whether modest changes in weights reverse the ranking; if they do, the committee examines the contested criteria rather than treating the rank as objective truth.

At Gate 3, a limited pilot tests task completion, screen-reader and keyboard use, referral exceptions, access changes, data reconciliation, alert accuracy, support volume, and staff workload. Gate 4 converts accepted performance and risk controls into contract terms and implementation acceptance criteria. Gate 5 reviews benefits and harms after launch. If referral visibility improves but staff workload and false alerts increase, the institution adjusts configuration and process rather than declaring success based on deployment alone.

The example shows why governance is not an additional layer after selection. Governance supplies the problem definition, evidence rules, accountability, and feedback through which selection becomes a defensible institutional decision.

## 5 DISCUSSION

### 5.1 Contribution to Practice

DIGS contributes a usable translation layer. Existing scholarship explains why transformation and enterprise systems are sociotechnical; standards define important control outcomes; and sector tools collect vendor information. Practitioners still need a way to connect these sources to a sequence of institutional decisions. DIGS does so by pairing domains with gates and by distinguishing mandatory assurance from comparative preference.

Confidence-adjusted scoring is particularly useful. Conventional matrices imply that every number has equal evidentiary status. Recording confidence exposes uncertainty and makes further testing purposeful. Similarly, an explicit exit criterion reframes portability from a distant contracting detail to an architectural requirement.

### 5.2 Implications for Institutional Leaders

Leaders should resist three shortcuts. The first is delegating enterprise risk to a technology committee without outcome authority. The second is allowing time pressure to convert mandatory controls into post-award tasks. The third is assuming that contract signature ends selection. For cloud services, renewal and material change are recurring selection decisions.

Smaller institutions may not be able to perform every assessment independently. They can still preserve the logic of DIGS by pooling expertise, using sector tools such as HECVAT, relying on independently verified evidence, scaling pilots to the highest-risk workflows, and documenting the risks they accept. Proportionality should reduce effort, not erase accountability.

### 5.3 Research Agenda

DIGS creates testable propositions. Comparative case studies could examine whether mandatory gates reduce late-stage disqualification and contract exceptions. Longitudinal studies could test whether evidence confidence predicts implementation surprises. Researchers could evaluate whether exit testing changes contract terms or switching costs, and whether lifecycle reviews improve benefit realization. The framework's domains and weights should also be studied across community colleges, research universities, minority-serving institutions, and multi-campus systems. Such work should examine not only efficiency and adoption but also accessibility, equity, staff labor, student trust, and institutional resilience.

#### *Limitations*

This article synthesizes heterogeneous research and guidance and therefore cannot establish causal effects. The framework has not yet been validated through a multi-institution sample, and its illustrative scoring function should not be interpreted as an optimized model. The U.S. focus limits direct transfer to jurisdictions with different privacy, procurement, and governance regimes. Standards and vendor practices also evolve. Institutions should verify current requirements and adapt thresholds to data sensitivity, service criticality, legal status, and organizational capacity.

The practitioner perspective introduces interpretive judgment. To make that judgment contestable, the framework emphasizes traceable sources, explicit assumptions, confidence ratings, dissent records, and review triggers. Future empirical work is needed to measure reliability, decision quality, implementation outcomes, and unintended effects.

## 6 CONCLUSION

Selecting digital infrastructure and administrative information systems is an exercise in institutional governance. The decision determines how authority, data, risk, labor, and adaptability will be distributed long after procurement ends. Product features and initial price are therefore insufficient foundations for selection.

The DIGS framework offers a lifecycle method grounded in seven domains and six stage gates. It begins with an accountable problem definition, protects noncompensatory obligations, compares alternatives with evidence-aware scoring, requires controlled validation, translates material claims into contract and implementation controls, and continues through benefit and risk review. Its purpose is not to remove judgment but to make judgment explicit, evidence-based, and revisable. That orientation can help U.S. colleges and universities make technology decisions that are more resilient, accessible, transparent, and aligned with mission.

## STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

### *Acknowledgments*

This research was not funded by any grant. The author acknowledges the scholarly and professional communities whose published research, standards, and guidance informed this integrative review.

### *Funding Source*

This research received no external funding.

### *Disclosure of conflict of interest*

Fatema Akter declares no financial or non-financial conflicts of interest.

### *Statement of ethical approval*

The present research work does not contain any studies performed on animals or human subjects by any of the authors.

### *Author contributions*

Conceptualization, methodology, investigation, source identification and evaluation, literature organization and synthesis, resources, formal analysis, framework development, writing—original draft preparation, writing—review and editing, and project administration: Fatema Akter. The author has read and agreed to the submitted version of the manuscript.

### *Use of generative AI and AI-assisted tools*

Fatema Akter conceived the study, selected and evaluated the sources, organized and synthesized the literature, developed the framework and analysis, interpreted the evidence, and authored the substantive manuscript. OpenAI Codex was used only to improve language and readability. The manuscript was placed into the publisher template using document-formatting tools under the author's review. The author reviewed and edited the full manuscript, verified the cited sources, and accepts responsibility for its arguments, interpretations, accuracy, originality, and final text. Earlier AI-assisted schematic figures were removed and are not included in this submission. No confidential institutional data were used.

### *Data availability statement*

No new empirical data were created or analyzed in this study. The publications and standards used in the integrative review are identified in the reference list.

## REFERENCES

[1] G. Vial, "Understanding digital transformation: A review and a research agenda," J. Strategic Inf. Syst., vol. 28, no. 2, pp. 118–144, 2019, doi: 10.1016/j.jsis.2019.01.003.

[2] L. M. Benavides, J. A. Tamayo Arias, M. D. Arango Serna, J. W. Branch Bedoya, and D. Burgos, "Digital transformation in higher education institutions: A systematic literature review," Sensors, vol. 20, no. 11, Art. no. 3291, 2020, doi: 10.3390/s20113291.

[3] M. Alenezi, "Deep dive into digital transformation in higher education institutions," Educ. Sci., vol. 11, no. 12, Art. no. 770, 2021, doi: 10.3390/educsci11120770.

[4] B. R. Aditya, R. Ferdiana, and S. S. Kusumawardani, "Digital transformation in higher education: A barrier framework," in Proc. 3rd Int. Conf. Modern Educ. Technol., 2021, pp. 100–106, doi: 10.1145/3468978.3468995.

[5] N. Pollock and J. Cornford, "ERP systems and the university as a 'unique' organisation," Inf. Technol. People, vol. 17, no. 1, pp. 31–52, 2004, doi: 10.1108/09593840410522161.

[6] C. Campbell, "Behind the curve: Higher education's efforts to implement advanced information systems," J. Emerg. Technol. Accounting, vol. 15, no. 2, pp. 77–91, 2018, doi: 10.2308/jeta-52237.

[7] W. H. DeLone and E. R. McLean, "The DeLone and McLean model of information systems success: A ten-year update," J. Manage. Inf. Syst., vol. 19, no. 4, pp. 9–30, 2003, doi: 10.1080/07421222.2003.11045748.

[8] N. Sultan, "Cloud computing for education: A new dawn?" Int. J. Inf. Manage., vol. 30, no. 2, pp. 109–116, 2010, doi: 10.1016/j.ijinfomgt.2009.09.004.

[9] C. Pascoe, S. Quinn, and K. Scarfone, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2024, doi: 10.6028/NIST.CSWP.29.

[10] National Institute of Standards and Technology, NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management, NIST SP 1305, 2024, doi: 10.6028/NIST.SP.1305.

[11] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST SP 800-161 Rev. 1, 2022, doi: 10.6028/NIST.SP.800-161r1.

[12] EDUCAUSE, "Higher Education Community Vendor Assessment Toolkit," 2026. [Online]. Available: https://www.educause.edu/hecvat. Accessed: Jul. 20, 2026.

[13] National Institute of Standards and Technology, NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, 2020, doi: 10.6028/NIST.CSWP.01162020.

[14] U.S. Department of Education, "Family Educational Rights and Privacy Act regulations," 34 C.F.R. Part 99, 2026.

[15] Federal Trade Commission, "Standards for Safeguarding Customer Information," 16 C.F.R. Part 314, 2026.

[16] World Wide Web Consortium, "Web Content Accessibility Guidelines (WCAG) 2.2," W3C Recommendation, Oct. 5, 2023. [Online]. Available: https://www.w3.org/TR/WCAG22/.

[17] U.S. Department of Justice, "Nondiscrimination on the basis of disability; accessibility of web information and services of state and local government entities," Federal Register, vol. 89, no. 83, pp. 31320–31484, Apr. 24, 2024.

[18] K. Shachmut, "Asking the right questions for procuring inclusive, accessible technology," EDUCAUSE Review, Oct. 25, 2021. [Online]. Available: https://er.educause.edu/articles/2021/10/asking-the-right-questions-for-procuring-inclusive-accessible-technology.

[19] International Organization for Standardization, Governance of IT for the Organization, ISO/IEC 38500:2024, Geneva, Switzerland, 2024.

[20] R. S. Kaplan and D. P. Norton, "The balanced scorecard—Measures that drive performance," Harvard Bus. Rev., vol. 70, no. 1, pp. 71–79, 1992.

[21] J. Luftman, "Assessing business-IT alignment maturity," Commun. Assoc. Inf. Syst., vol. 4, Art. no. 14, 2000, doi: 10.17705/1CAIS.00414.

[22] A. Hevner and S. Chatterjee, Design Research in Information Systems: Theory and Practice. New York, NY, USA: Springer, 2010, doi: 10.1007/978-1-4419-5653-8.

[23] National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5, 2020, doi: 10.6028/NIST.SP.800-53r5.

[24] Cybersecurity and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals," Version 2.0.1, 2023. [Online]. Available: https://www.cisa.gov/cpg.

[25] 1EdTech Consortium, "Learning Tools Interoperability Core Specification," Version 1.3, 2020. [Online]. Available: https://www.imsglobal.org/spec/lti/v1p3/.

[26] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, 2023, doi: 10.6028/NIST.AI.100-1.