International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(21s) 2026 pp. 2029-2039
https://doi.org/10.70917/ijcisim-2026-5978
Article

Procurement Governance Innovation Failure Patterns in U.S. State Enterprise Systems: A Cross-Jurisdictional Taxonomy and Capability-Gap Mapping Framework (2014–2024)

Vijaya Bhaskar Reddy Saadhu

Independent Researcher, USA

Abstract: U.S. state governments have spent heavily on enterprise procurement systems. These systems were built to enforce compliance, strengthen oversight, and create reliable audit trails across complex multi-agency environments. Despite this investment, state oversight reports keep documenting the same procurement failures — in the same digitally enabled settings — year after year. This suggests that having capable systems does not automatically produce capable governance.

This paper analyzes eight verified state oversight reports from seven U.S. states over the period 2014 through 2024. Using qualitative comparative document analysis, the study develops a seven-domain procurement-control failure taxonomy. Each domain is mapped to the enterprise governance capability area it reflects. Governance architecture, monitoring, workflow enforcement, and organizational capability failures appeared more consistently across jurisdictions than technical system defects. The largest capability gap — present across all seven states — was organizational governance maturity: the distance between what a system can do and what an organization actually configures, maintains, and enforces.

The paper offers a portable, audit-grounded diagnostic framework for EIS practitioners working on the design, assessment, or remediation of procurement governance systems in regulated environments.

Keywords: Enterprise information systems, Procurement governance, Governance capability gaps, Cross-jurisdictional analysis, Legislative audit evidence, Digital transformation

1. INTRODUCTION

1.1 Public-Sector Procurement Modernization and Its Governance Expectations

U.S. state governments have made large, sustained investments in enterprise procurement modernization over the past two decades. These investments transformed how procurement is managed. California built the Financial Information System for California, known as FI$Cal. Florida replaced its legacy FLAIR system with the cloud-based Florida PALM enterprise resource planning platform. Georgia deployed PeopleSoft-based systems under the TeamWorks and GeorgiaFIRST programs. Arizona integrated its Arizona Financial Information System with the ProcureAZ procurement portal. Each of these investments carried a specific governance expectation.

The expectation was not simply that systems would automate transactions. It was that systems would actively enforce the controls on which public accountability depends. Competitive bidding compliance, proper authorization, accurate data, continuous oversight — these were not afterthoughts. They were the stated rationale for the investment (Bhatnagar & Bonagiri, 2026).

Governance standards make this expectation explicit. The COSO (2013) internal control framework identifies control activities, monitoring, and information integrity as the operational dimensions of effective governance. The

Copyright: © 2026 by the authors

Government Accountability Office (2014) Green Book translates these principles into federal internal control standards applicable to state government settings. Together, these frameworks define what enterprise procurement systems are supposed to deliver in practice.

1.2 The Research Problem

Despite this infrastructure, state oversight reports keep finding the same failures. California's state auditor found that at least $44 billion in contracts were awarded over five years without adequate competitive bidding oversight. The auditor noted that even this figure was an estimate, because data reliability problems made a precise count impossible (California State Auditor, 2017). Arizona's statewide procurement audit found $9.8 billion in annual procurement activity managed without comprehensive spend analysis or risk-based oversight (Arizona Office of the Auditor General, 2015). In Mississippi, emergency procurements went undetected until costs had already risen by $1.2 million per year. Auditors attributed that increase directly to a failure in monitoring capability (Mississippi PEER Committee, 2022).

These are not isolated incidents. They reflect a recurring pattern across states with established, functioning enterprise systems. The systems exist. The failures persist. That gap is the research problem this paper addresses.

Two analytical gaps compound the challenge. EIS governance research has focused heavily on what makes implementations succeed in the first place (Nah et al., 2001; Holland & Light, 1999; Umble et al., 2003). Far less attention has been paid to governance failures that occur in stable, multi-year production environments — well after go-live. No cross-jurisdictional, audit-grounded taxonomy currently exists that classifies these failures by governance capability domain or translates audit evidence into terms practitioners can use for diagnosis and remediation.

1.3 Article Contribution and Structure

This paper makes three contributions. First, it derives a seven-domain procurement-control failure taxonomy from eight verified state oversight reports across seven U.S. states. Each domain is defined by the type of governance capability the failures implicate. Second, it presents a governance-capability mapping framework that links each failure domain to the enterprise capability area it represents. Third, it argues that procurement digitization tends to shift governance risk rather than eliminate it — moving the risk from manual process failures toward failures in how enterprise system controls are configured, maintained, and monitored.

Section 2 reviews the background literature. Section 3 describes the methodology. Section 4 presents the taxonomy and mapping framework. Section 5 discusses the findings. Section 6 concludes.

2. BACKGROUND AND LITERATURE REVIEW

2.1 Enterprise Information Systems and Procurement Governance

ERP adoption research consistently shows that a successful implementation does not guarantee effective governance in the years that follow. Markus et al. (2000) identify post-implementation governance dynamics — configuration drift, user behavior divergence, organizational changes not reflected in system settings — as a persistent challenge extending well beyond the deployment phase. These are not technical system failures. They are organizational failures that happen inside functioning systems.

Critical success factors identified during implementation continue to have governance implications long after go-live (Nah et al., 2001). Top management support, change management, and business process alignment do not become irrelevant once a system is live. They determine whether governance capabilities are actually sustained and enforced over time. Holland and Light (1999) draw a useful distinction between strategic and tactical implementation factors. The strategic dimensions bear directly on the operational governance challenges that emerge in mature production environments. Umble et al. (2003) connect implementation clarity and organizational commitment to long-term governance outcomes.

Davenport (1998) makes the underlying point directly: governance outcomes are shaped more by how organizations deploy and maintain available capabilities than by the capabilities themselves. The cross-jurisdictional evidence in Section 4 reinforces this. COSO (2013) defines the internal control framework applicable to state procurement governance. COSO (2017) extends this to enterprise risk management. ISACA (2019) provides the COBIT 2019 IT governance framework.

Table 1. Summary of EIS governance frameworks and applicability to procurement governance analysis

Framework / Source	Core Governance Concept	Applicability to Procurement Governance Analysis
COSO (2013)	Internal control: control environment, risk assessment, control activities, information, monitoring	Primary standard against which state procurement governance controls are assessed in audit contexts
COSO (2017)	Enterprise risk management integrated with strategy and performance	Frames procurement governance as strategic risk management — grounds Domain 5 (organizational maturity)
Government Accountability Office (2014)	Federal internal control standards — 17 principles across 5 components	Green Book standards define the control objectives each documented failure violates
ISACA (2019)	COBIT 2019: IT governance objectives mapped to enterprise system capabilities	IT governance framework most widely used for ERP governance assessment in practice
ISO/IEC 38500:2015	IT governance principles: responsibility, conformance, performance, human behavior	Provides governance architecture reference for interpreting failure domain dimensions
Bostrom & Heinen (1977)	Sociotechnical systems: technical and organizational processes jointly produce outcomes	Grounds the dual-dimension (technical + organizational) character of each failure domain

2.2 Procurement Governance in State Government Enterprise Environments

Public procurement governance encompasses the controls, policies, and oversight mechanisms that ensure public funds are spent in compliance with applicable law. Thai (2001) categorizes essential procurement oversight criteria as encompassing competitive bidding integrity, operational transparency, fiscal accountability, and demonstrable value for public resources. These are the dimensions that enterprise procurement systems are designed to enforce.

Coggburn (2003) found substantial variation in governance effectiveness across state environments even where comparable systems were deployed. This suggests that organizational governance decisions — not system capability levels — drive the differences in outcomes across jurisdictions. Rendon and Rendon (2016) examine auditability in public procurement and establish the direct connection between internal control design and audit defensibility. This connection underpins the governance-capability mapping framework presented in Section 4. The Government Accountability Office (2014) Green Book sets the federal internal control standard against which each documented failure in Section 4 represents a gap.

2.3 IT Governance Frameworks and Enterprise System Governance

ISO/IEC 38500:2015 establishes the international standard for IT governance. It identifies responsibility, strategy, acquisition, performance, conformance, and human behavior as the core governance principles. These principles serve as a governance architecture reference throughout this analysis. Competitive bidding failures reflect

conformance gaps. Monitoring failures reflect performance governance gaps. Organizational capability failures reflect human behavior governance gaps.

Sociotechnical systems theory, brought into the IS literature by Bostrom and Heinen (1977), provides the theoretical lens for understanding why procurement governance failures are not purely technical. Enterprise systems operate inside sociotechnical contexts. Technical capabilities and organizational processes interact to produce governance outcomes. Each failure domain in the taxonomy spans both technical and organizational dimensions. Neither dimension alone is sufficient to explain the failures — or to fix them.

2.4 Gaps in the Existing Literature

Three gaps motivate this paper. The first is the cross-jurisdictional gap. Existing procurement governance research is mostly single-jurisdiction in scope. This limits the identification of patterns that are truly systemic rather than state-specific.

The second is the audit-evidence gap. State oversight reports are underused in EIS governance research. These reports are independently produced, subject to formal review processes, and represent externally validated evidence of governance failure in live production environments. They are among the most credible primary sources available.

The third is the diagnostic tool gap. No framework currently exists that translates audit-documented procurement-control failures into the governance capability terms practitioners use for diagnosis and investment prioritization. This paper provides that framework.

3. RESEARCH METHODOLOGY

3.1 Qualitative Comparative Document Analysis

This paper uses qualitative comparative document analysis of publicly available official government documents. Yin (2018) establishes document analysis as a rigorous qualitative research method for studying governance phenomena in real-world contexts where controlled experimentation is not feasible. State oversight reports meet the credibility standard for this purpose. They are independently produced, formally reviewed, and directly relevant to governance failure in live enterprise system environments.

The comparative dimension is essential. Eight reports across seven states make cross-jurisdictional pattern recognition possible. Single-jurisdiction analysis cannot produce this.

3.2 Data Sources

The empirical base consists of eight state oversight reports from seven U.S. states, covering 2014 through 2024. The reports are: Arizona Office of the Auditor General (2015), Report No. 15-102; California State Auditor (2017), Report 2016-124; California State Auditor (2024), Report 2023-302; Florida Auditor General (2024), Report No. 2024-138; Georgia Department of Audits and Accounts (2024), Special Examination No. 23-11; Mississippi PEER Committee (2022), Report No. 672; North Carolina Office of the State Auditor (2022), INV-2022-6070; and Texas State Auditor's Office (2015), Report No. 15-019. All reports are publicly available official government documents.

3.3 Analytical Approach

Analysis proceeded in three stages. The first stage involved systematic extraction of procurement-control failure evidence from each report. The second stage involved iterative coding and classification by failure type. This step distinguished technical-system defects from governance architecture and organizational capability gaps. The third stage involved governance-capability mapping: translating each coded failure domain into the enterprise governance capability area it represents. These mappings reflect the author's analytical interpretations, grounded in practitioner expertise in enterprise procurement governance architecture. They are not direct statements from the audit bodies.

4. CROSS-JURISDICTIONAL FAILURE TAXONOMY AND GOVERNANCE-CAPABILITY MAPPING FRAMEWORK

4.1 Overview of the Seven-Domain Taxonomy

Seven procurement-control failure domains emerged from the cross-jurisdictional analysis. Each domain is defined by the type of governance capability the failures implicate. Table 2 presents the complete taxonomy.

The distribution of findings carries an important message. Governance architecture and organizational capability failures dominated the evidence base. They appeared more consistently across jurisdictions than technical system defects. That is the central finding of this analysis.

Table 2. Seven-domain procurement-control failure taxonomy

Domain	Governance Capability Area	States with Evidence (of 7)	Symptom Pattern
1. Competitive Bidding & Authorization Failures	Workflow enforcement	3 (CA, GA, NC)	Procurement bypasses competitive requirements; authorization controls circumvented
2. Contract & Spend Data Integrity Failures	Data governance	4 (FL, MS, AZ, CA)	Inaccurate/incomplete procurement data undermines system-based governance controls
3. Monitoring & Analytics Capability Failures	Compliance analytics	4 (CA, AZ, MS, GA)	No systematic spend analysis or anomaly detection; reactive oversight posture
4. Documentation & Audit Trail Failures	Audit traceability	3 (TX, GA, CA)	Incomplete procurement files; absent vendor evaluation records; audit trail gaps
5. Organizational Governance Maturity Failures	Organizational governance maturity	7 (all states)	System capabilities available but not configured, enforced, or maintained
6. System Configuration & Technical Control Failures	ERP configuration governance	2 (FL, AZ)	Technical controls not properly configured; configuration drift over time
7. Access Governance & SOD Failures	Access governance	3 (FL, NC, TX)	Role-access misalignment; SOD violations; access reviews not conducted

4.2 Domain 1 — Competitive Bidding and Authorization Failures

Three of the seven states showed procurement failures tied to competitive bidding and authorization processes. California's state auditor found that at least $44 billion in contracts were awarded over five years without adequate competitive bidding oversight (California State Auditor, 2017). Georgia's special examination documented purchase-splitting and emergency procurement designations applied without adequate justification (Georgia Department of

Audits and Accounts, 2024). In North Carolina, unauthorized procurement at NC A&T bypassed institutional approval requirements entirely (North Carolina Office of the State Auditor, 2022).

These failures map to a workflow enforcement capability gap. Available system capabilities were not consistently configured or monitored to prevent authorization bypasses — a governance architecture gap rather than a system capability limitation.

4.3 Domain 2 — Contract and Spend Data Integrity Failures

Data integrity failures appeared across four states. Florida's audit found data quality and completeness weaknesses in FLAIR (Florida Auditor General, 2024). Mississippi's review found procurement data quality problems that limited spend analysis and compliance reporting (Mississippi PEER Committee, 2022). Arizona identified spend data reliability issues that undermined statewide analytics (Arizona Office of the Auditor General, 2015). These failures map to a data governance capability gap.

Enterprise systems enforce controls based on the data they contain. When that data is inaccurate, system-based controls operate on a corrupted information foundation. The control environment deteriorates not from technical malfunction but from the unreliable data on which system controls must operate.

4.4 Domain 3 — Monitoring and Analytics Capability Failures

Monitoring and analytics failures were the most fiscally consequential domain. California's auditor documented at least $44 billion in noncompetitive contracts without adequate statewide monitoring (California State Auditor, 2017). Arizona identified $9.8 billion in annual procurement activity operating without comprehensive spend analysis (Arizona Office of the Auditor General, 2015). Mississippi's $1.2 million cost increase was directly attributed to insufficient monitoring capability (Mississippi PEER Committee, 2022). Georgia's review identified deficiencies in oversight coverage spanning several distinct procurement categories, as documented in the Department of Audits and Accounts special examination.

This domain appeared across four states. The fact that this pattern recurred so consistently across different states points to compliance analytics as likely the most systematically neglected governance investment area within U.S. state-level enterprise procurement.

4.5 Domain 4 — Documentation and Audit Trail Failures

Documentation and audit trail failures appeared in three states. The Texas audit uncovered material weaknesses in contract file management, with insufficient documentation to substantiate the basis for procurement decisions and subsequent amendments (Texas State Auditor's Office, 2015). Georgia's special examination found procurement recordkeeping so incomplete that external reviewers could not independently verify whether competitive bidding obligations had been met. California's judicial branch audit found documentation weaknesses that limited oversight capacity (California State Auditor, 2024).

These failures map to an audit traceability capability gap. These organizations had not activated or enforced the documentation controls their systems were already equipped to support.

4.6 Domain 5 — Organizational Governance Maturity Failures

Organizational governance maturity failures appeared across all seven states. This was the most broadly distributed finding in the entire analysis — and the most consequential.

In California, corrective actions prescribed by auditors had not been fully implemented even years after the finding was first documented (California State Auditor, 2017). Florida's 2024 review explicitly drew on unresolved findings from prior audit cycles, indicating that documented weaknesses had persisted without adequate correction (Florida Auditor General, 2024). Georgia exhibited repeated breakdowns in procurement workflow controls even though its enterprise platform possessed the technical features necessary to enforce them. The root cause was not any

deficiency in the platform itself, but the gap between the platform's governance design intent and how it was configured and operated in practice. Mississippi's audit revealed workforce preparation deficiencies alongside a pattern of established procurement policies failing to take effect in day-to-day operations.

The persistent divergence between what enterprise systems are technically capable of and what agencies actually activate and enforce has emerged as the defining governance vulnerability in digitally transformed procurement settings. Deploying advanced technology platforms cannot independently produce the organizational governance maturity required to translate system capabilities into governance outcomes.

4.7 Domain 6 — System Configuration and Technical Control Failures

Technical system configuration failures were the least consistently documented domain. They appeared in two states. Florida's audit identified IT general control weaknesses in FLAIR (Florida Auditor General, 2024). Arizona documented ProcureAZ configuration issues that limited automated control effectiveness (Arizona Office of the Auditor General, 2015).

The relative infrequency of this domain is analytically significant. In these operating environments, the core governance challenge is not an absence of system functionality. It is the failure to consistently activate, maintain, and enforce the controls that the systems already provide. Silic and Back (2014) reach an analogous conclusion in their analysis of shadow IT governance risk.

4.8 Domain 7 — Access Governance and Segregation of Duties Failures

Access governance failures appeared in three states. Florida documented user access weaknesses and segregation of duties violations in FLAIR (Florida Auditor General, 2024). North Carolina's investigative report found access governance failures that contributed directly to unauthorized procurement (North Carolina Office of the State Auditor, 2022). Texas documented access control weaknesses that limited transaction auditability (Texas State Auditor's Office, 2015).

These failures straddle both technical and organizational dimensions. That is consistent with the sociotechnical framing established by Bostrom and Heinen (1977). Neither purely technical remediation nor policy-level directives, taken in isolation, can close access governance gaps. Durable improvement requires coordinated action across both dimensions simultaneously.

4.9 The Governance-Capability Mapping Framework

The seven failure domains map to seven enterprise governance capability areas. Table 3 presents the complete framework. The diagnostic logic is direct: assess the organization's governance against each capability area, identify gaps, and direct remediation at the capability level rather than the symptom level. The result is a unified diagnostic instrument drawn from distributed audit evidence, applicable across any regulated-industry context in which enterprise procurement systems are in operation.

Table 3. Governance-capability mapping framework

Failure Domain	Governance Capability Area	Remediation Focus	Evidence Strength
1. Competitive Bidding & Authorization	Workflow enforcement	Configure and monitor procurement routing, approval thresholds, and bidding enforcement	Moderate (3/7)
2. Contract & Spend Data Integrity	Data governance	Establish active data quality standards for master data, contract records, and transaction	Strong (4/7)

		data across system lifecycle	
3. Monitoring & Analytics Capability	Compliance analytics	Invest in compliance monitoring, anomaly detection, and corrective action tracking as designed governance capabilities	Strong (4/7) — highest fiscal impact
4. Documentation & Audit Trail	Audit traceability	Configure and enforce documentation completeness standards within available system capabilities	Moderate (3/7)
5. Organizational Governance Maturity	Organizational governance maturity	Develop organizational capacity, policy operationalization, and institutional accountability to translate system capabilities into governance outcomes	Broadest (7/7) — highest priority
6. System Configuration & Technical Controls	ERP configuration governance	Actively maintain enterprise system configurations aligned with current policy requirements	Limited (2/7)
7. Access Governance & SOD	Access governance	Conduct access reviews, enforce role-based access alignment, and maintain SOD controls both technically and organizationally	Moderate (3/7)

5. DISCUSSION

5.1 The Central Pattern: Governance Architecture Gaps Dominate Technical Defects

Among the seven failure domains identified, six are rooted in governance architecture weaknesses and organizational shortcomings rather than in technical malfunctions of the enterprise systems themselves. Domain 6 — technical configuration failures — was the least consistently documented across the evidence base (Rekulapalli et al., 2026b).

Enterprise procurement systems across these environments have the capability to enforce competitive bidding requirements. They can maintain data integrity. They can generate audit trails. They can support compliance monitoring. What the cross-jurisdictional evidence documents is not the absence of these capabilities. It is their inconsistent configuration, maintenance, and enforcement.

Markus et al. (2000) describe post-adoption governance dynamics as the under-examined challenge of ERP governance research. This paper documents what those dynamics actually produce across seven state governments over a decade of audit evidence. The picture is consistent: governance breakdowns are not attributable to missing system functionality; they stem from the sustained gap between available system controls and how organizations configure, sustain, and enforce them in practice (Rekulapalli et al., 2026a).

5.2 Procurement Digitization Transforms Rather Than Eliminates Governance Challenges

States with mature, long-established enterprise system investments — California, Florida, Georgia — showed recurring procurement-control weaknesses across multiple audit cycles. This is not what the original governance arguments for these investments predicted 9Gagar, 2024).

The evidence across these jurisdictions indicates that digitizing procurement operations redistributes governance risk rather than eliminating it. Governance exposure migrates away from errors inherent in manual workflows and concentrates instead in the configuration integrity, ongoing maintenance practices, and oversight of automated system controls. This pattern mirrors findings from public sector business process reengineering literature: initiatives that concentrate on building technical capability while underfunding the organizational governance work produce a migration of risk rather than its removal.

5.3 Practical Implications for EIS Practitioners

Four practitioner roles find direct application in the governance-capability mapping framework.

Enterprise architects gain a structured diagnostic checklist — seven capability domains against which any governance architecture can be systematically assessed.

Procurement governance specialists gain cross-jurisdictional benchmarking context. Knowing that Domain 5 failures appeared across all seven states, while Domain 6 failures appeared in only two, changes how specialist attention should be allocated.

ERP implementation and remediation practitioners gain remediation prioritization guidance. The predominance of governance and organizational failures over technical defects directs investment toward governance architecture interventions rather than technical upgrades.

Regulated industry organizations subject to audit gain a pre-audit self-assessment tool. The framework enables proactive identification of capability gaps before auditors find them. Its relevance extends to healthcare, utilities, higher education, and federal contracting organizations (Gaggar, 2025).

5.4 Limitations

Several methodological limitations apply. Enterprise system environments were not directly identified from audit reports for Texas, Mississippi, and North Carolina. These were confirmed through related official sources. The governance-capability mappings are the author's analytical interpretations grounded in practitioner expertise — not direct statements from the audit bodies.

Audit scope varied across states, which limits direct comparability. The absence of a documented finding in a particular domain for a specific state reflects audit scope choices — not confirmed governance adequacy. A state may have a gap that was not audited, not disclosed, or not within the audit's scope.

6. CONCLUSION

Eight state oversight reports from seven U.S. states tell a consistent story. Procurement-control failures across these jurisdictions were driven more by governance architecture deficiencies, monitoring gaps, workflow enforcement failures, and organizational capability shortfalls than by technical system defects. The divergence between the control capabilities that enterprise systems offer and what agencies actually configure, sustain, and enforce proved to be the most pervasively implicated governance dimension across the full body of evidence. It appeared in all seven states.

Two original contributions emerge from this analysis. The seven-domain procurement-control failure taxonomy provides an audit-grounded classification of the governance capability gaps most consistently at risk in enterprise procurement environments. The governance-capability mapping framework translates this taxonomy into a portable diagnostic instrument. EIS practitioners, enterprise architects, and procurement governance specialists can use it to assess, diagnose, and prioritize remediation in any regulated environment where enterprise procurement systems operate.

Digital transformation programs designed to strengthen procurement governance must invest in governance architecture, organizational capability, and monitoring infrastructure with the same priority given to system capability. These are not post-implementation afterthoughts. They are core program workstreams.

Future research should examine the framework's applicability in federal, international public sector, and other regulated industry contexts. Developing quantitative governance maturity measures per capability domain is another productive direction. Investigating the relationship between governance-capability investment and audit finding recurrence rates would produce practically useful evidence for procurement governance investment decisions.

Declaration of Competing Interest

The author declares no competing interests.

Author Contributions (CRediT)

Vijaya Bhaskar Reddy Saadhu: Conceptualization; Data curation; Formal analysis; Investigation; Methodology; Writing — original draft; Writing — review & editing.

REFERENCES

1. Arizona Office of the Auditor General. (2015). Arizona Department of Administration — State-wide procurement (Report No. 15-102). OAG. https://www.azauditor.gov/sites/default/files/2023-11/DOA_15-102_0.pdf
2. Bhatnagar, A., & Bonagiri, V. R. K. (2026). Operational Excellence through Cloud-Native Distributed Systems. International Journal of Computational and Experimental Science and Engineering, 12(2). https://doi.org/10.22399/ijcesen.5207
3. Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. MIS Quarterly, 1(3), 17–32. https://www.jstor.org/stable/248710
4. California State Auditor. (2017). Department of General Services and California Department of Technology: Neither entity has provided the oversight necessary to ensure that state agencies consistently use the competitive bidding process (Report 2016-124). CSA. https://information.auditor.ca.gov/reports/responses/2016-124/5
5. California State Auditor. (2024). Judicial Branch Procurement (Report 2023-302). CSA. https://www.auditor.ca.gov/reports/2023-302/
6. Coggburn, J. D. (2003). Exploring differences in the American states' procurement practices. Journal of Public Procurement, 3(1), 3–28. https://www.emerald.com/jopp/article-abstract/3/1/3/227824/Exploring-differences-in-the-american-states?redirectedFrom=fulltext
7. Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control — Integrated framework. COSO. https://www.coso.org/guidance-on-ic
8. Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management: Integrating with strategy and performance. COSO. https://www.coso.org/guidance-erm
9. Davenport, T. H. (1998). Putting the enterprise into the enterprise system. Harvard Business Review, 76(4), 121–131. https://hbr.org/1998/07/putting-the-enterprise-into-the-enterprise-system
10. Florida Auditor General. (2024). Department of Financial Services — Florida Accounting Information Resource Subsystem and selected information technology general controls (Report No. 2024-138). AG. https://flauditor.gov/pages/pdf_files/2024-138.pdf
11. Gaggar, H. (2024). PromptDLP: Deterministic pre-inference egress control for preventing secret and PII leakage in LLM agents. Journal of Information Systems Engineering and Management.
12. Gaggar, H. (2025). Architecting scalable enterprise AI agent infrastructure for distributed intelligent systems. International Journal of Advances in Signal and Image Sciences, 193–208. https://doi.org/10.29284/da9w0117
13. Georgia Department of Audits and Accounts. (2024). Special Examination Report No. 23-11: State Purchasing — Competitive Bidding. DOAA. https://www.audits.ga.gov/ReportSearch/download/30758
14. Government Accountability Office. (2014). Standards for internal control in the federal government (GAO-14-704G). U.S. Government Accountability Office. https://www.gao.gov/assets/gao-14-704g.pdf
15. Holland, C. P., & Light, B. (1999). A critical success factors model for ERP implementation. IEEE Software, 16(3), 30–36. https://www.researchgate.net/publication/220092133_A_Critical_Success_Factors_Model_for_ERP_Implementation
16. ISACA. (2019). COBIT 2019 framework: Governance and management objectives. ISACA. https://sfia-online.org/en/tools-and-resources/sfia-views/cobit-2019-governance-objectives-and-sfia
17. ISO. (2015). ISO/IEC 38500:2015 — Information technology — Governance of IT for the organization. International Organization for Standardization. https://www.iso.org/standard/81684.html
18. Markus, M. L., Axline, S., Petrie, D., & Tanis, C. (2000). Learning from adopters' experiences with ERP: Problems encountered and success achieved. Journal of Information Technology, 15(4), 245–265.

https://www.researchgate.net/publication/233681020_Learning_from_Adopters'_Experiences_with_ERP_Problems_Encountered_and_Success_Achieved
19. Mississippi Joint Legislative Committee on Performance Evaluation and Expenditure Review. (2022). A review of state agency procurement (Report No. 672). PEER Committee. https://www.peer.ms.gov/sites/default/files/peer_publications/rpt672.pdf
20. Nah, F. F.-H., Lau, J. L.-S., & Kuang, J. (2001). Critical factors for successful implementation of enterprise systems. Business Process Management Journal, 7(3), 285–296. https://www.emerald.com/bpmj/article-abstract/7/3/285/257420/Critical-factors-for-successful-implementation-of?redirectedFrom=fulltext
21. North Carolina Office of the State Auditor. (2022). Investigative Report: North Carolina Agricultural and Technical State University (INV-2022-6070). OSA. https://files.nc.gov/nc-auditor/documents/2022-10/INV-2022-6070.pdf?VersionId=dT4feHm3Ny3k.wQFEsIJFX9aqWPk5Jcb
22. Rekulapalli, K., Kagga, S. R., Ayyagari, V., Akula, A., & Raj Akula, R. (2026). AI in HRM: Enhancing Workforce Competency and Organizational Effectiveness. SSRN, 6762998.
23. Rekulapalli, K., Nilagiri, H., & Vakkanthula, M. (2026). A comparative evaluation of national FHIR Implementation Guides: strategic methodologies for enhancing interoperability, regulatory alignment, and clinical comprehensiveness in global health IT. Health Systems, 1–13.
24. Rendon, R. K., & Rendon, J. M. (2016). Auditability in public procurement: An analysis of internal controls and fraud vulnerability. International Journal of Procurement Management, 9(2), 134–152. https://www.researchgate.net/publication/283837085_Auditability_in_public_procurement_An_analysis_of_internal_controls_and_fraud_vulnerability
25. Silic, M., & Back, A. (2014). Shadow IT — A view from behind the curtain. Computers & Security, 45, 274–283. https://www.researchgate.net/publication/263284725_Shadow_IT_-_A_view_from_behind_the_curtain
26. Texas State Auditor's Office. (2015). A report on recent contracting audits (Report No. 15-019). SAO. https://sao.texas.gov/reports/main/15-019.pdf
27. Umble, E. J., Haft, R. R., & Umble, M. M. (2003). Enterprise resource planning: Implementation procedures and critical success factors. European Journal of Operational Research, 146(2), 241–257. https://ideas.repec.org/a/eee/ejores/v146y2003i2p241-257.html
28. Weerakkody, V., Janssen, M., & Dwivedi, Y. K. (2011). Transformational change and business process reengineering (BPR): Lessons from the British and Dutch public sector. Government Information Quarterly, 28(3), 320–328. https://www.sciencedirect.com/science/article/abs/pii/S0740624X11000323
29. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications. https://uk.sagepub.com/en-gb/eur/case-study-research-and-applications/book250150