International Journal of Advanced Engineering and Management Research

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Cross-Domain Variability in Governance Systems: A Comparative Analysis of Governance Capability Across Critical Sectors

Dr. Robb Shawe

Departments of Cyber Leadership, Sustainability and Critical Infrastructure, Capitol Technology University, 11301 Springfield Road, Laurel, MD, USA

doi.org/10.51505/ijaemr.2026.11327 URL: http://dx.doi.org/10.51505/ijaemr.2026.11327

Received: May 23, 2026 Accepted: Jun 01, 2026 Online Published: Jun 10, 2026

Abstract

Governance systems across sectors exhibit significant variability in their ability to integrate artificial intelligence, real-time monitoring, and adaptive oversight. While some sectors demonstrate advanced governance maturity—characterized by continuous sensing, predictive analytics, and event-validated learning—others remain anchored in reactive, compliance-centric oversight models. This manuscript presents a cross-domain comparative analysis of governance capability across four major sectors: critical infrastructure, healthcare, finance, and public administration. Using the Governance Maturity Model (GMM) as an evaluative framework, the study identifies sector-specific patterns in governance readiness, oversight integration, and adaptive capacity. Findings reveal that governance variability is shaped by environmental complexity, regulatory intensity, technological integration, and organizational culture. The analysis further demonstrates that governance variability reflects broader differences in governance observability, operational intelligence integration, adaptive oversight capability, institutional learning maturity, and resilience modernization across interconnected socio-technical ecosystems. This manuscript extends the Adaptive Governance Systems Framework (AGSF), the AI-Enabled Governance Oversight Model (AIGOM), and the Governance Maturity Model (GMM) by providing a comparative foundation for cross-sector governance transformation.

Keywords: cross-domain governance; governance variability; adaptive oversight; governance maturity; sectoral analysis; AI-enabled governance; socio-technical systems

1. Introduction

Governance systems do not evolve uniformly across sectors. While some domains—such as finance and critical infrastructure—have adopted advanced monitoring, predictive analytics, and AI-enabled oversight, others continue to rely on manual processes, retrospective audits, and static compliance frameworks (Power, 2007; National Institute of Standards and Technology [NIST], 2024). This variability has significant implications for institutional resilience, regulatory alignment, and risk management. These differences reflect more than technological disparities

Vol. 11, No. 03; 2026

ISSN: 2456-3676

alone. They reveal underlying asymmetries in governance observability, adaptive oversight capability, decision-support intelligence integration, and institutional resilience maturation across sectors operating under different operational, regulatory, and socio-technical conditions (Dekker, 2011; Endsley, 2017; Woods, 2018).

This manuscript examines **cross-domain governance variability** using the Governance Maturity Model (GMM) (Shawe, 2026). By comparing governance capability across critical infrastructure, healthcare, finance, and public administration, the study identifies sector-specific strengths, limitations, and modernization pathways.

1.1 Methodological Orientation

This manuscript employs a conceptual comparative-analysis methodology grounded in governance ecosystem evaluation, adaptive governance synthesis, interdisciplinary socio-technical framework integration, and comparative governance capability assessment (Jabareen, 2009; Torraco, 2005). The cross-domain analysis was developed through structured evaluation of governance maturity characteristics, operational intelligence integration, adaptive oversight capability, institutional learning capacity, and resilience modernization patterns across critical infrastructure, healthcare, finance, and public administration environments.

Rather than functioning as an empirical benchmarking investigation, the manuscript operationalizes a comparative governance ecosystem synthesis approach designed to identify sector-specific governance modernization asymmetries, adaptive oversight variations, governance observability differences, and institutional capability distributions across interconnected socio-technical ecosystems (Meadows, 2008; von Bertalanffy, 1968). The analysis integrates governance modernization principles established by AGSF, AIGOM, GMM, and EVG into a unified comparative governance framework that supports cross-domain governance transformation analysis and resilience-oriented modernization planning.

Sources were selected for their relevance to governance modernization, adaptive governance, governance maturity, resilience engineering, operational intelligence integration, regulatory oversight, and institutional learning in complex socio-technical environments. Priority was given to peer-reviewed journal articles, foundational theoretical works, government and regulatory frameworks, governance standards, and contemporary literature addressing governance transformation across critical infrastructure, healthcare, finance, and public administration sectors.

The comparative analysis employed explicit inclusion and exclusion criteria. Included sources were required to address governance capability, adaptive oversight, organizational resilience, governance modernization, operational observability, regulatory governance, or AI-enabled governance integration. Sources focused exclusively on narrow technical implementation issues, sector-specific operational procedures without governance implications, or isolated technological performance outcomes were excluded from the comparative synthesis.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

The selection of critical infrastructure, healthcare, finance, and public administration was intentional because these sectors represent distinct combinations of operational complexity, regulatory intensity, technological integration, institutional accountability requirements, and public-impact consequences. Collectively, these domains provide a representative cross-section of governance environments characterized by varying modernization trajectories and profiles of governance capability.

Governance maturity evaluations were informed by the Governance Maturity Model (GMM) and were derived through comparative assessment of recurring governance characteristics identified throughout the reviewed literature. Sector evaluations considered evidence of governance observability, real-time monitoring capability, adaptive oversight integration, institutional learning mechanisms, operational intelligence utilization, resilience-management practices, and governance modernization maturity. The maturity ranges presented in Figure 1 are therefore conceptual comparative assessments rather than quantitative performance scores, and are intended to illustrate relative patterns of governance capability observed across sectors.

The resulting comparative synthesis provides a structured governance analysis framework through which sector-specific modernization strengths, governance capability asymmetries, and adaptive oversight differences can be evaluated from a common perspective on governance maturity. This approach supports comparative governance learning while preserving the unique operational and regulatory characteristics of each sector.

2. Results of Comparative Governance Synthesis

2.1 Emergent Governance Variability Themes

The comparative governance synthesis identified five recurring dimensions that consistently differentiated governance capability across critical infrastructure, healthcare, finance, and public administration environments. Although sector-specific operational conditions varied substantially, the reviewed literature demonstrated significant convergence regarding the institutional capabilities associated with governance modernization and adaptive oversight effectiveness (Hollnagel, 2014; Kaplan & Mikes, 2012; Woods, 2018).

The first recurring dimension involved governance observability, defined as the ability of organizations to monitor operational conditions, collect performance information, and maintain awareness of emerging risks. The second dimension centered on adaptive oversight capability, reflecting the extent to which governance systems can respond dynamically to changing operational conditions. The third dimension involved operational intelligence integration, including the incorporation of AI-enabled analytics, predictive monitoring, and decision-support systems into governance processes. The fourth dimension focused on institutional learning capacity, including the ability to transform operational experience into governance adaptation and organizational improvement. The fifth dimension emphasized resilience modernization,

Vol. 11, No. 03; 2026

ISSN: 2456-3676

reflecting the extent to which governance systems support anticipation, adaptation, recovery, and continuous improvement within complex socio-technical environments.

Collectively, these dimensions appeared consistently across the sectors reviewed and emerged as the primary governance capability indicators that distinguish higher-maturity governance environments from more reactive or compliance-oriented oversight structures.

2.2 Cross-Domain Governance Capability Outcome

The comparative analysis revealed substantial variability in governance maturity across sectors. Critical infrastructure and finance demonstrated the highest levels of governance modernization due to extensive real-time monitoring, advanced integration of operational intelligence, strong regulatory oversight, and mature institutional learning mechanisms. Healthcare exhibited intermediate governance maturity, characterized by increasing technological integration and the development of adaptive oversight, although governance capability remained uneven across organizations. Public administration demonstrated the greatest variability due to fragmented information systems, limited operational observability, and slower adoption of adaptive governance technologies.

The synthesis further revealed that governance maturity is influenced by the interplay among operational complexity, regulatory intensity, technological integration, organizational culture, and institutional learning capability, rather than by any single modernization factor. These findings suggest that governance capability should be understood as an ecosystem-level phenomenon shaped by multiple reinforcing institutional conditions.

The maturity ranges presented in Figure 1 reflect the relative governance capability patterns identified through the comparative synthesis and provide a conceptual framework for understanding sector-specific governance modernization trajectories across diverse operational environments.

The recurring governance capability patterns identified through the synthesis process provide the conceptual foundation for the comparative governance framework presented in the following sections and establish the basis for evaluating governance variability across critical sectors.

3. Cross-Domain Governance Variability: Conceptual Overview

Governance variability arises from four primary drivers. Collectively, these drivers shape the emergence of governance-ecosystem asymmetries that influence institutional modernization trajectories, operational resilience capabilities, governance-intelligence integration, and adaptive-oversight maturity across sectors (Endsley, 2017; Hollnagel, 2014; Woods, 2018).

Vol. 11, No. 03; 2026

ISSN: 2456-3676

3.1 Environmental Complexity

Sectors with high operational complexity require more advanced governance systems (Rasmussen, 1997).

3.2 Regulatory Intensity

Highly regulated sectors often exhibit more structured governance processes (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017).

3.3 Technological Integration

AI-enabled monitoring and cyber-physical systems influence governance capability (NIST, 2023).

3.4 Organizational Culture

Governance maturity is shaped by leadership priorities, risk tolerance, and institutional learning norms (Kaplan & Mikes, 2012).

4. Comparative Governance Analysis Across Sectors

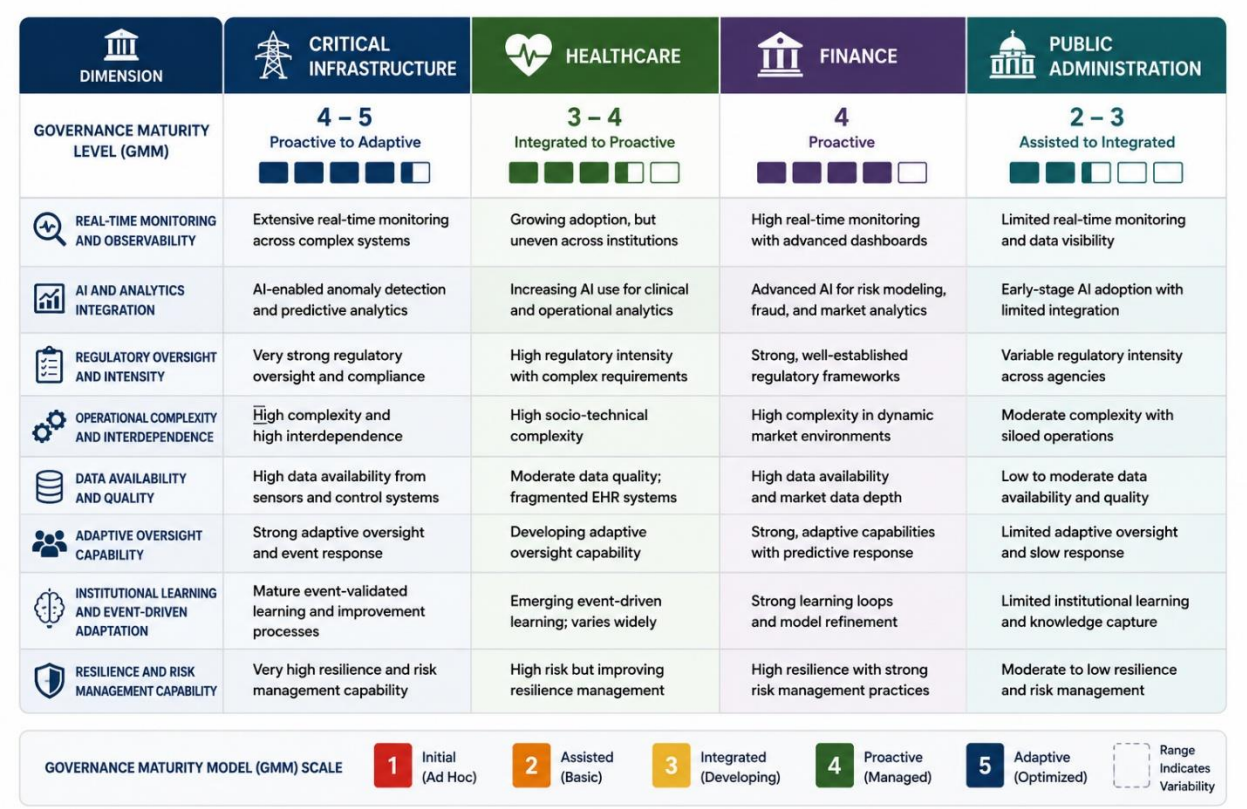
Building upon the constitutional governance architecture established through the Adaptive Governance Systems Framework (AGSF), the operational intelligence architecture operationalized through the AI-Enabled Governance Oversight Model (AIGOM), the governance evolution architecture established through the Governance Maturity Model (GMM), and the adaptive validation architecture operationalized through Event-Validated Governance (EVG), this comparative analysis examines how governance modernization capability, adaptive oversight maturity, and decision-support intelligence integration vary across major operational ecosystems (Leveson, 2011; Dekker, 2011). Figure 1 illustrates cross-domain differences in governance maturity, governance observability, adaptive oversight capability, governance-relevant insight, institutional learning maturity, and resilience modernization across critical infrastructure, healthcare, finance, and public administration.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Figure 1

Cross-Domain Governance Variability Across Sectors



Note. Author created. The figure illustrates cross-domain variability in governance maturity across critical infrastructure, healthcare, finance, and public administration, highlighting differences in governance observability, adaptive oversight capability, governance-relevant insight, and institutional resilience modernization, as measured by the Governance Maturity Model (GMM). Governance maturity ranges represent conceptual comparative assessments derived from governance observability, adaptive oversight capability, operational intelligence integration, institutional learning capacity, regulatory coordination, and resilience-management characteristics identified through the comparative synthesis.

As illustrated in Figure 1, governance modernization does not evolve uniformly across sectors. Instead, governance capability emerges from ecosystem-specific interactions among operational complexity, regulatory intensity, technological integration, institutional learning capacity, and adaptive oversight maturity, which collectively shape governance observability, resilience modernization, and governance-relevant insight across interconnected socio-technical environments.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Importantly, the comparative analysis suggests that governance modernization should not be viewed as a universal progression toward a single governance ideal. Rather, governance maturity emerges through sector-specific interactions among regulatory requirements, technological capabilities, organizational culture, operational complexity, and resilience-management priorities. Consequently, effective governance transformation requires context-sensitive modernization strategies that adapt to the unique demands of individual operational ecosystems.
Moreover, the comparative maturity ranges presented in Figure 1 should not be interpreted as fixed performance rankings or absolute indicators of governance effectiveness. Rather, they represent conceptual assessments of relative governance capability derived from recurring patterns identified throughout the comparative synthesis. The framework illustrates how governance modernization emerges from different combinations of governance observability, adaptive oversight capability, operational intelligence integration, institutional learning capacity, and resilience management practices. This perspective emphasizes that governance maturity is shaped by ecosystem-specific operational conditions rather than by any single technological, regulatory, or organizational characteristic.

Figure 1 further demonstrates that governance variability reflects differences in modernization trajectories rather than differences in institutional importance or mission criticality. Sectors operating under similar regulatory expectations may nevertheless exhibit substantially different governance capabilities depending upon technological integration, operational complexity, information availability, and organizational learning mechanisms. Consequently, the framework should be understood as a comparative governance-learning tool designed to support sector-sensitive modernization planning rather than as a universal governance scoring system.

4.1 Critical Infrastructure

Governance Maturity Level: 4–5 (Proactive to Adaptive)

Characteristics:

- Extensive real-time monitoring
- AI-enabled anomaly detection
- Strong regulatory oversight
- High operational interdependence

Critical infrastructure demonstrates the highest governance maturity due to technological integration, extensive regulatory oversight, and mature operational risk-management requirements that support continuous monitoring and governance observability (National Institute of Standards and Technology [NIST], 2024; Occupational Safety and Health Administration [OSHA], 2024).

4.2 Healthcare

Governance Maturity Level: 3–4 (Integrated to Proactive)

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Characteristics:

- Strong socio-technical complexity
- Increasing adoption of AI-enabled monitoring
- High stakes for safety and reliability
- Fragmented governance across institutions

Healthcare governance is improving but remains uneven across organizations (Carayon et al., 2015).

4.3 Finance

Governance Maturity Level: 4 (Proactive)

Characteristics:

- Advanced risk modeling
- Predictive analytics for fraud and market anomalies
- Strong regulatory frameworks
- High data availability

Finance demonstrates strong governance capability but faces challenges related to model risk and algorithmic transparency (Kaplan & Mikes, 2012).

4.4 Public Administration

Governance Maturity Level: 2–3 (Assisted to Integrated)

Characteristics:

- Limited real-time monitoring
- Fragmented data systems
- Variable regulatory environments
- Slow adoption of AI-enabled oversight

Public administration exhibits the greatest variability in governance due to resource constraints and legacy systems (Wachter et al., 2017).

5. Cross-Domain Patterns and Insights

The comparative analysis reveals that governance modernization does not progress uniformly across sectors. Instead, governance capability evolves through sector-specific interactions among operational complexity, regulatory intensity, technological integration, institutional learning capacity, and adaptive oversight maturity (Perrow, 1984; Woods, 2018).

Vol. 11, No. 03; 2026

ISSN: 2456-3676

5.1 Technological Integration Drives Governance Maturity

Sectors with advanced digital infrastructure exhibit higher governance capability.

5.2 Regulatory Pressure Accelerates Governance Modernization

Compliance requirements drive adoption of structured oversight mechanisms.

5.3 Socio-Technical Complexity Requires Adaptive Governance

Complex environments benefit most from integrating AGSF and AIGOM.

5.4 Organizational Culture Influences Governance Readiness

Leadership commitment to modernization is a critical determinant of governance maturity.

5.5 Illustrative Cross-Domain Governance Comparison Scenario

To illustrate cross-domain governance variability, consider how a cybersecurity anomaly affecting operational continuity may be managed differently across critical infrastructure, healthcare, finance, and public administration environments.

Within critical infrastructure systems, AI-enabled monitoring architectures and real-time telemetry integration may rapidly detect operational anomalies, initiate automated escalation protocols, and support coordinated adaptive oversight processes through mature governance observability mechanisms. In healthcare environments, governance responses may involve partial AI-enabled monitoring combined with human-centered clinical escalation procedures, resulting in more variable adaptive coordination outcomes depending on institutional maturity levels.

Financial institutions may use predictive analytics, fraud-detection systems, and structured **decision-support intelligence integration processes** to assess operational deviations and rapidly implement evidence-driven recalibration mechanisms. Conversely, public administration environments operating with fragmented data systems and limited operational observability may experience delayed anomaly interpretation, slower escalation coordination, and reduced responsiveness of adaptive oversight. The scenario further illustrates how sector-sensitive governance modernization strategies may strengthen resilience coordination, adaptive oversight capabilities, integration of institutional learning, and governance effectiveness across diverse operational ecosystems (Shneiderman, 2022; Parasuraman et al., 2000).

6. Implications for Governance Modernization

The findings suggest that governance modernization strategies must account for ecosystem-specific variability in governance observability, institutional adaptability, operational intelligence integration, and resilience capability development rather than relying on uniform governance

Vol. 11, No. 03; 2026

ISSN: 2456-3676

transformation models (Organisation for Economic Co-operation and Development [OECD], 2024; World Economic Forum, 2023).

6.1 Sector-Sensitive Governance Strategies

Governance modernization must align with sector-specific constraints and capabilities.

6.2 Targeted Capability Development

The GMM provides a roadmap for advancing governance maturity.

6.3 Cross-Sector Learning Opportunities

High-maturity sectors can serve as models for governance transformation.

6.4 Integration of AI-Enabled Oversight

AIGOM supports real-time governance across all sectors.

6.5 Governance Implementation Implications

The comparative findings presented in this manuscript provide organizations with a governance modernization analysis framework that supports sector-sensitive governance transformation planning across diverse operational ecosystems. Executive leadership may utilize the framework to evaluate institutional governance maturity relative to sector-specific modernization expectations, identify governance capability asymmetries, and prioritize adaptive oversight investments aligned with operational complexity and resilience objectives.

Regulators and governance authorities may apply the comparative framework to identify sector-specific governance modernization disparities, strengthen expectations for adaptive oversight, improve governance observability standards, and support evidence-driven governance modernization initiatives across interconnected AI-enabled operational environments (OECD, 2024).

Operational governance teams may use the framework to evaluate governance capability gaps, strengthen cross-domain governance-learning integration, improve coordination of institutional modernization, and align adaptive governance strategies with sector-specific operational conditions and resilience requirements.

7. Discussion

7.1 Theoretical Implications

The comparative findings presented in this manuscript contribute to governance scholarship by demonstrating that governance maturity should not be understood as a universal organizational condition but rather as an ecosystem-dependent capability shaped by interactions among

Vol. 11, No. 03; 2026

ISSN: 2456-3676

operational complexity, regulatory intensity, technological integration, institutional learning capacity, and adaptive oversight maturity. The analysis extends adaptive governance theory, socio-technical systems theory, resilience engineering, and governance modernization research by illustrating how governance capability evolves differently across operational domains despite exposure to many of the same technological and regulatory pressures.

The findings further suggest that governance variability is best conceptualized as a dynamic institutional phenomenon rather than a simple measure of organizational performance. Differences in governance maturity reflect distinct modernization trajectories, resource constraints, information architectures, accountability structures, and resilience-development mechanisms that emerge across sectors operating under unique environmental conditions (Carayon, 2006; Hollnagel, 2014; Meadows, 2008).

The increasing emphasis on anticipatory governance, resilience-oriented oversight, adaptive regulation, and responsible AI integration within contemporary governance scholarship further reinforces the need for governance architectures capable of continuous learning, dynamic adaptation, and evidence-informed institutional decision-making (National Institute of Standards and Technology [NIST], 2024; Organisation for Economic Co-operation and Development [OECD], 2024; World Economic Forum, 2023).

7.2 Governance Modernization Challenges

Although governance modernization remains a strategic objective across sectors, the comparative analysis demonstrates that organizations frequently encounter barriers that limit the development of advanced governance capability. Common challenges include fragmented information systems, uneven technological integration, workforce resistance to organizational change, limited governance observability, regulatory complexity, and resource constraints. These barriers may contribute to latent organizational vulnerabilities that remain undetected until operational failures expose weaknesses in governance structures and decision-making processes (Reason, 1997).

The findings suggest that governance transformation initiatives cannot rely solely on technological modernization. Sustainable advancement in governance capability requires simultaneous investment in institutional learning, leadership development, adaptive oversight processes, governance transparency, and resilience-management practices. Consequently, modernization strategies should be tailored to the specific operational and regulatory realities of individual sectors rather than applied uniformly across governance environments.

7.3 Stakeholder Implications

The implications of governance variability differ across stakeholder groups. Executive leadership may utilize comparative governance assessments to identify modernization priorities, allocate resources, and strengthen governance capability development. Regulators may apply governance

Vol. 11, No. 03; 2026

ISSN: 2456-3676

maturity concepts to improve oversight expectations and encourage adaptive governance practices within regulated industries.

Operational governance teams may use comparative governance frameworks to identify capability gaps, improve governance observability, strengthen institutional learning processes, and support modernization planning. Technology leaders may leverage governance maturity assessments to align AI-enabled monitoring systems, operational analytics, and decision-support capabilities with broader governance objectives and accountability requirements.

7.4 Limitations and Future Research

This manuscript presents a conceptual comparative analysis and does not include empirical benchmarking, longitudinal governance-maturity assessment, sector-specific quantitative validation, or large-scale organizational performance measurement. Although the framework is grounded in governance scholarship and comparative synthesis, the maturity assessments presented in Figure 1 remain conceptual evaluations intended to support comparative analysis rather than definitive sector rankings.

Future research should examine sector-specific governance indicators, modernization trajectories, governance-performance metrics, resilience outcomes, and adaptive oversight effectiveness across diverse operational environments. Additional studies may develop empirical governance benchmarking instruments, sector-specific maturity assessment methodologies, governance observability measures, and comparative validation approaches to support quantitative evaluation of governance capability development.

Particular attention should be given to developing quantitative governance-maturity indicators, sector-specific benchmarking instruments, governance observability metrics, and adaptive-oversight measurement criteria that support empirical validation of cross-domain governance modernization trajectories and institutional resilience outcomes.

8. Conclusion

This manuscript advances governance scholarship by providing a comparative framework for evaluating variability in governance capability across critical infrastructure, healthcare, finance, and public administration environments. The analysis demonstrates that governance modernization trajectories differ substantially across sectors due to variations in operational complexity, regulatory intensity, technological integration, institutional learning capacity, and adaptive oversight capability.

The findings contribute to governance modernization research by reconceptualizing governance variability as a dynamic ecosystem phenomenon rather than a collection of isolated sector-specific differences. This perspective highlights the importance of sector-sensitive governance transformation strategies that align modernization initiatives with unique operational realities, regulatory conditions, and resilience requirements.

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Although conceptual in nature, the framework provides a foundation for future empirical benchmarking, governance maturity assessment, comparative sector studies, and governance modernization planning. Future research should examine sector-specific governance indicators, modernization trajectories, resilience outcomes, and governance capability transitions across diverse operational ecosystems.

References

Carayon, P. (2006). Human factors of complex sociotechnical systems. *Applied Ergonomics, 37*(4), 525–535.

Carayon, P., Schoofs Hundt, A., Karsh, B. T., Gurses, A. P., Alvarado, C. J., Smith, M., & Flatley Brennan, P. (2006). Work system design for patient safety: The SEIPS model. *Quality and Safety in Health Care, 15*(Suppl. 1), i50–i58. https://doi.org/10.1136/qshc.2005.015842

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

Dekker, S. (2011). *Drift into failure: From hunting broken components to understanding complex systems*. Ashgate Publishing.

Endsley, M. R. (2017). From here to autonomy: Lessons learned from human-automation research. *Human Factors, 59*(1), 5–27. https://doi.org/10.1177/0018720816681350

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Ashgate.

Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods, 8*(4), 49–62. https://doi.org/10.1177/160940690900800406

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review, 90*(6), 48–60.

Leveson, N. G. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press.

Meadows, D. H. (2008). *Thinking in systems: A primer*. Chelsea Green Publishing.

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0).* U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

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

Occupational Safety and Health Administration. (2024). *Occupational safety and health standards (29 CFR Part 1910).* U.S. Department of Labor.

Organisation for Economic Co-operation and Development. (2024). *Framework for anticipatory governance of emerging technologies*. OECD Publishing.

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 30*(3), 286–297. https://doi.org/10.1109/3468.844354

Vol. 11, No. 03; 2026

ISSN: 2456-3676

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Princeton University Press.

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science, 27*(2–3), 183–213.

Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.

Shawe, R. (2026). *From probabilistic compliance to event-validated resilience*. International Journal of Advanced Engineering and Management Research.

Shneiderman, B. (2022). *Human-centered AI*. Oxford University Press.

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review, 4*(3), 356–367. https://doi.org/10.1177/1534484305278283

von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*. George Braziller.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Wickens, C. D., Lee, J. D., Liu, Y., & Gordon-Becker, S. (2015). *An introduction to human factors engineering* (2nd ed.). Pearson.

Woods, D. D. (2018). The theory of graceful extensibility: Basic rules that govern adaptive systems. *Environment Systems and Decisions, 38*(4), 433–457. https://doi.org/10.1007/s10669-018-9708-3

World Economic Forum. (2023). *The Global Risks Report 2023* (18th ed.). World Economic Forum.