Lifecycle-Based Information Security Governance: A Unified Model

Jonathan Doberenz

American Public University

ISSC680: Information Security Management

Dr. Janet Durgin

March 1, 2026

Introduction

Information security governance has become a central concern for modern organizations as digital infrastructures expand, regulatory expectations increase, and cyber threats grow more sophisticated. Governance is no longer limited to technical safeguards or compliance checklists; it requires a structured system of policies, controls, and oversight mechanisms that guide how information assets are protected throughout their lifecycle. According to Calder and Watkins, effective governance depends on aligning leadership responsibilities, organizational processes, and security controls so that confidentiality, integrity, and availability are maintained across all systems (Calder & Watkins, 2023). The findings reflect a broader shift in the field: security must be embedded into the way organizations plan, build, operate, and retire systems rather than treated as an isolated technical function.

Despite the maturity of international standards and models, many organizations continue to struggle with fragmented governance practices. Controls are often implemented inconsistently, risk management is disconnected from daily operations, and development teams frequently operate independently from compliance and monitoring functions. Research across multiple sectors shows that these structural weaknesses undermine the effectiveness of governance programs and create gaps that adversaries can exploit. The problem is not a lack of standards; it is the absence of a unified governance model that integrates risk, compliance, development, monitoring, and continuity across the entire system lifecycle.

This paper examines the literature surrounding information security governance, identifies the structural and operational challenges that contribute to fragmentation, and proposes a lifecycle-based governance model that unifies key security functions. By analyzing standards,

organizational studies, and sector-specific research, the paper demonstrates why lifecycle integration is essential for improving risk posture, compliance alignment, and long-term resilience.

Background and Literature Foundations

Governance Standards and Frameworks

International standards such as ISO/IEC 27001 and ISO/IEC 27002 provide foundational expectations for information security governance and outline how organizations should structure their security programs across the system lifecycle. Calder and Watkins explain that these standards require organizations to establish governance processes that span system acquisition, development, maintenance, and retirement to ensure consistent protection of information assets (Calder & Watkins, 2023). ISO/IEC 27005 extends this idea by outlining how risk management should operate as a continuous activity throughout the system lifecycle, ensuring that risk identification, assessment, and treatment remain aligned with operational realities (International Organization for Standardization, 2018).

NIST frameworks reinforce these lifecycle principles. According to the National Institute of Standards and Technology, NIST SP 800-37 presents the Risk Management Framework as a lifecycle approach that integrates security and privacy activities into every phase of development and operation (National Institute of Standards and Technology, 2018). NIST CSF 2.0 expands on this by emphasizing governance outcomes, organizational cohesion, and continuous improvement as core components of effective cybersecurity programs (National Institute of Standards and Technology, 2024). Together, these standards highlight the importance of structured, integrated governance that evolves alongside the systems it protects.

Organizational Challenges Identified in Literature

While standards provide clear expectations, organizational studies reveal persistent challenges in implementing them. Layton notes that many organizations adopt controls in a reactive or isolated manner, focusing on technical fixes rather than embedding governance into strategic decision making (Layton, 2006). Peltier adds that risk assessment is often treated as an occasional task rather than a routine operational activity, which leads to inconsistent control implementation and oversight gaps (Peltier, 2013).

Structural issues also contribute to governance weaknesses. Research from the Electronics and Computer Science Department at the University of Southampton uses the Viable System Model to show how unclear responsibilities, weak communication channels, and disconnected operational processes undermine governance effectiveness (Alqurashi et al., 2013). This suggests that governance failures often stem from organizational design rather than technical limitations, reinforcing the need for clearer roles and stronger communication structures.

Sector-Specific Findings

Sector-specific research further illustrates the complexity of governance implementation. A comparative study published in *IEEE Access* shows that industrial organizations face significant inconsistencies across cybersecurity standards, creating confusion and duplicated effort for companies operating in multiple regulatory environments (Djebbar & Nordström, 2023). These inconsistencies make it difficult for organizations to maintain uniform governance practices, especially when they must comply with overlapping or conflicting requirements.

In the public sector, research published in the *International Journal of Information Security* reports that government agencies struggle to align policy, risk management, and operational security despite having formal governance requirements (Magnusson et al., 2025). This work highlights how bureaucratic structures, unclear responsibilities, and uneven implementation practices continue to undermine governance maturity even in highly regulated environments.

Federal guidance reinforces these findings. According to the Cybersecurity and Infrastructure Security Agency, effective governance in federal environments requires strong leadership involvement, clear accountability, and coordinated communication across organizational groups (Cybersecurity and Infrastructure Security Agency, 2023). Together, these studies demonstrate that governance challenges are widespread and persistent across sectors, reinforcing the need for a unified, lifecycle-based approach.

Analysis of Literature: Relations, Contradictions, and Gaps

Points of Convergence

Across the literature, several themes consistently emerge. Major standards and approaches emphasize the need for integrated governance that spans the entire system lifecycle. Guidance from ISO/IEC 27005, NIST SP 800-37, and NIST CSF 2.0 outlines the importance of continuous risk management, structured oversight, and alignment between technical and organizational processes (International Organization for Standardization, 2018; National Institute of Standards and Technology, 2018; National Institute of Standards and Technology, 2024).

The literature also agrees that governance must be proactive rather than reactive. Peltier explains that security should be embedded into early planning and development activities so that governance influences decisions before systems are built or deployed (Peltier, 2013).

Finally, leadership involvement and organizational structure are repeatedly identified as critical enablers of effective governance. Studies across sectors show that without clear roles, accountability mechanisms, and coordinated communication, even well-designed governance structures fail to achieve consistent implementation (Alqurashi et al., 2013).

Contradictions and Tensions

Despite the areas of agreement across the literature, several contradictions also emerge. Standards consistently call for integrated governance, yet many organizations continue to implement controls in fragmented ways. Layton notes that operational teams often work independently, resulting in inconsistent practices and uneven oversight (Layton, 2006).

Research published in *IEEE Access* finds contradictions between standards themselves, noting that differences in terminology, structure, and control expectations create confusion for organizations attempting to harmonize requirements across multiple frameworks (Djebbar & Nordström, 2023). These inconsistencies make it difficult for organizations to maintain uniform governance practices, especially in sectors with overlapping regulatory obligations.

Even in highly regulated environments, governance maturity varies widely. A study published in the *International Journal of Information Security* shows that government agencies continue to struggle with aligning policy, risk management, and operational security, suggesting that compliance alone does not guarantee effective integration (Magnusson et al., 2025).

Identified Gaps

The literature identifies several gaps that contribute to ongoing governance challenges. First, few studies present a unified governance model that integrates risk, compliance, development, monitoring, and continuity across the entire lifecycle. Second, cross-department communication and accountability mechanisms are often underdeveloped, limiting the effectiveness of governance structures. Third, while standards describe what organizations should do, they provide limited instruction on how to operationalize lifecycle integration in complex environments. Overall, these gaps highlight the need for a governance model that is both comprehensive and practical, especially for organizations operating across multiple regulatory and operational contexts.

Core Problem: Fragmentation in Governance Practices

Siloed Organizational Structures

Fragmentation is the central governance weakness identified across the literature. Many organizations maintain separate teams for risk management, compliance, development, monitoring, and continuity planning, which prevents governance activities from functioning as a coordinated system. Layton explains that this siloed structure leads to inconsistent control adoption and weak oversight because teams often operate without shared priorities or communication pathways (Layton, 2006). Federal guidance points out this concern by noting that governance failures frequently stem from a lack of coordination between organizational groups, especially when leadership, accountability, and communication mechanisms are not clearly defined (Cybersecurity and Infrastructure Security Agency, 2023). Together, these perspectives

show that structural separation across teams is one of the primary drivers of fragmented governance.

Impact on Security Outcomes

Fragmentation has significant consequences for organizational security. When risk assessments are disconnected from development activities, vulnerabilities often emerge early in the lifecycle and persist into production environments. When compliance functions operate independently from operational teams, organizations struggle to maintain consistent control implementation and oversight. The National Institute of Standards and Technology explains that fragmented practices increase vulnerabilities, complicate compliance efforts, and weaken overall resilience by preventing governance activities from functioning as a coordinated system (National Institute of Standards and Technology, 2020). This evidence shows that structural separation across teams directly contributes to gaps in protection and reduces an organization's ability to respond effectively to evolving threats.

Why Lifecycle Integration Matters

Lifecycle-based governance addresses these weaknesses by ensuring that security activities remain aligned with system evolution rather than functioning as isolated tasks. According to the National Institute of Standards and Technology, NIST SP 800-37 reports that integrating security into each lifecycle phase improves continuity, reduces vulnerabilities, and supports proactive risk management (National Institute of Standards and Technology, 2018). NIST's guidance demonstrates that lifecycle integration is essential for maintaining consistent oversight and adapting governance activities as systems change over time.

Toward a Lifecycle-Based Governance Model

Conceptual Model Overview

A lifecycle-based governance model unifies risk management, compliance, development, monitoring, and continuity into a single, coordinated structure. This model draws on ISO/IEC 27005's emphasis on continuous risk management to ensure that risk identification, assessment, and treatment remain aligned with system evolution (International Organization for Standardization, 2018). It also incorporates the lifecycle integration principles outlined in NIST SP 800-37, which position security and privacy activities as essential components of every phase of system development and operation (National Institute of Standards and Technology, 2018). In addition, the model reflects systems engineering concepts from the MITRE Systems Engineering Guide, a widely used resource in federal and defense environments that stresses the importance of coordination across teams and lifecycle phases to maintain consistency and control (MITRE, n.d.). Together, these references provide the conceptual foundation for a governance model that is structured, integrated, and adaptable across organizational contexts.

Key Components of the Proposed Model

The model includes several core components:

- **Integrated risk management** embedded into planning, development, and operations
- **Embedded compliance** aligned with standards and regulatory requirements
- **Secure development practices** supported by structured requirements and change control
- **Continuous monitoring** to maintain situational awareness
- **Lifecycle-aligned change management** to ensure governance adapts as systems evolve

- **Resilience planning** that incorporates continuity and recovery considerations

These components ensure that governance remains consistent and effective across the system lifecycle.

Organizational Enablers

Successful implementation requires several organizational enablers. Leadership commitment is essential for establishing priorities and allocating resources, while clearly defined roles and responsibilities ensure accountability across teams. Cross-functional communication structures also support coordination by helping risk, compliance, development, and operations groups work toward shared objectives. Research from the University of Southampton's Electronics and Computer Science Department shows that governance effectiveness depends as much on organizational design and communication structures as on technical capability (Alqurashi et al., 2013). This demonstrates that strong governance requires both structural alignment and sustained leadership engagement.

Solutions and Implementation Strategies

Governance Integration Approaches

Organizations can unify governance by establishing cross-functional governance committees, mapping controls across standards, and aligning risk and compliance activities with development workflows. The National Institute of Standards and Technology supports these practices as NIST CSF 2.0 indicates the importance of governance structures that coordinate activities across organizational units (National Institute of Standards and Technology, 2024).

This guidance indicates that effective governance integration depends on both structural coordination and consistent security practices across operational and development processes.

Process Improvements

Embedding risk assessments into development workflows, strengthening feedback mechanisms, and improving documentation practices can enhance governance effectiveness by ensuring that security activities remain connected to operational realities. The National Institute of Standards and Technology emphasizes the importance of continuous evaluation and iterative improvement, noting that governance processes must adapt as systems evolve and new risks emerge (National Institute of Standards and Technology, 2018). This approach helps organizations maintain consistent oversight and support a more proactive approach to managing security throughout the system lifecycle.

Cultural and Structural Adjustments

Reducing silos requires both cultural change and structural adjustments. Organizations must promote systems thinking, encourage collaboration, and ensure that governance responsibilities are understood across teams so that security activities are not treated as isolated tasks. Research from the University of Southampton's Electronics and Computer Science Department argues that communication and accountability are essential for sustaining governance maturity over time (Alqurashi et al., 2013). This finding suggests that cultural alignment and structural clarity are equally important for building governance practices that remain effective as systems and organizational needs evolve.

Alignment with Regulatory and Industry Requirements

A lifecycle-based governance model helps organizations harmonize requirements across multiple standards, reducing duplicated effort and improving compliance efficiency. Research published in *IEEE Access*, a well-regarded engineering and technology journal, shows that harmonization is increasingly important for organizations operating in complex regulatory environments where overlapping standards can create confusion and inconsistent implementation (Djebbar & Nordström, 2023). Aligning governance activities with lifecycle processes helps organizations resolve overlapping requirements and maintain consistent oversight across technical and organizational domains.

Conclusion

The literature consistently shows that fragmentation is a central weakness in modern information security governance. Despite the availability of mature standards and frameworks, organizations continue to struggle with inconsistent control implementation, disconnected risk management practices, and weak cross-functional coordination. A lifecycle-based governance model addresses these challenges by integrating risk, compliance, development, monitoring, and continuity into a unified structure that evolves alongside the systems it protects.

Organizations that adopt lifecycle-aligned processes, strengthen communication, and coordinate requirements across standards tend to improve their risk posture, achieve better compliance alignment, and build long-term resilience. As digital infrastructures continue to expand and systems grow more complex, lifecycle-based governance will become increasingly essential for maintaining secure, reliable, and adaptable environments.

References

Alqurashi, E., Wills, G., & Gilbert, L. (2013). *A viable system model for information security governance: Establishing a baseline of the current information security operations system*. In L. J. Janczewski, H. B. Wolfe, & S. Shenoi (Eds.), *Security and privacy protection in information processing systems* (IFIP Advances in Information and Communication Technology, Vol. 405, pp. 245–256). Springer. https://doi.org/10.1007/978-3-642-39218-4_21

Calder, A., & Watkins, S. (2023). *IT governance: An international guide to data security and ISO 27001/ISO 27002* (8th ed.). IT Governance Publishing.

Cybersecurity and Infrastructure Security Agency. (2023). *Cybersecurity governance*. https://www.cisa.gov/cybersecurity-governance

Djebbar, F., & Nordström, K. (2023). A comparative analysis of industrial cybersecurity standards. *IEEE Access, 11*, 85315–85329. https://doi.org/10.1109/ACCESS.2023.3303205

International Organization for Standardization. (2018). *ISO/IEC 27005:2018 – Information technology — Security techniques — Information security risk management*. https://www.iso.org/standard/75281.html

Layton, T. P. (2006). *Information security: Design, implementation, measurement & compliance*. Auerbach Publications.

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: Investigations, approaches, measures, and trends. *International Journal of Information Security, 24*, 177–193. https://doi.org/10.1007/s10207-025-01097-x

MITRE. (n.d.). *Systems engineering guide*. https://www.mitre.org/publications/technical-papers/systems-engineering-guide

National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST SP 800-37 Rev. 2). https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Peltier, T. R. (2013). *Information security fundamentals* (2nd ed.). CRC Press.