Decision Accountability Is the Missing Control

Why Security Programs Pass Compliance but Fail Audit

By Jessica S. Marosi

Contents

Abstract

Security programs operating in regulated and high-consequence environments routinely demonstrate formal compliance with established frameworks while continuing to experience audit findings, post-incident scrutiny, and recurring governance challenges. These failures are commonly attributed to deficiencies in controls, tooling, or implementation quality. This paper advances a more fundamental diagnosis: that the most persistent and underexamined failure is the erosion of decision rationale over time. When the reasoning behind critical security decisions is not preserved, systems lose their ability to explain themselves. As a result, they become increasingly difficult to defend, govern, and evaluate fairly—even when they remain technically compliant with prescribed requirements.

Drawing on operational experience within complex, long-lived systems, this analysis examines how contemporary compliance frameworks emphasize control presence and procedural completion while leaving decision context implicit, fragmented, and fragile. Security decisions are made under constraint—shaped by mission urgency, legacy dependencies, staffing realities, and risk tradeoffs that rarely align with idealized guidance. As personnel change and conditions evolve, undocumented assumptions, justifications, and accepted risks disappear. What remains are outcomes detached from intent, inviting retrospective judgment and audit reinterpretation based on present-day expectations rather than historical reality. This dynamic produces a recurring and structural disconnect between compliance and defensibility.

This paper reframes decision accountability as a first-class governance control, equal in importance to technical safeguards and procedural mechanisms. It distinguishes compliance, which verifies that requirements have been met, from defensibility, which reflects an organization’s capacity to articulate why its systems, controls, and risk posture look the way they do. The analysis further demonstrates how automation and artificial intelligence do not resolve this gap, but instead amplify existing governance conditions—strengthening accountability where decision rationale is explicit and accelerating failure where it is absent. In critical-infrastructure and national-security contexts, where systems persist across decades and consequences are often irreversible, preserving decision rationale is not an administrative convenience. It is a prerequisite for resilience, institutional credibility, and responsible stewardship.

Purpose, Context, and Boundaries of Analysis

Security programs operating in regulated and high-consequence environments repeatedly confront a persistent paradox: systems that formally satisfy compliance requirements nonetheless falter during audits, incident reviews, or periods of leadership transition. This paper addresses that paradox directly—not as a theoretical shortcoming of governance models, but as an operational condition repeatedly observed in systems shaped by mission urgency, legacy architecture, and layered institutional oversight. Its purpose is to explain why compliance artifacts so often fail to translate into defensible outcomes when scrutiny intensifies. The argument advanced here is not that controls are absent or misunderstood, but that the reasoning behind critical security decisions is routinely allowed to erode or vanish, leaving systems technically intact yet narratively indefensible.

The context for this analysis is environments where security decisions are made under sustained pressure and constraint. In such settings, choices are governed by uptime requirements, staffing limitations, budgetary boundaries, regulatory timelines, and inherited technical debt. Decisions are rarely idealized or optimal; they are situational, negotiated, and pragmatic. Over time, these decisions accumulate into a system posture defined less by deliberate design than by managed compromise. When the rationale behind those decisions is not preserved, later reviewers encounter outcomes without context and are forced to evaluate past actions through the lens of present assumptions rather than historical conditions.

This analysis reflects direct exposure to systems that required explanation long after their original architects, operators, and authorizing officials had departed. In those circumstances, failures did not stem from ignorance of standards or disregard for policy. Instead, they emerged when no durable record existed to explain why a control was tailored, why an exception was granted, or why a particular risk was deemed acceptable at the time. When explanation is absent, accountability becomes diffuse, intent is inferred rather than known, and defensibility collapses under retrospective scrutiny.

The boundaries of this paper are intentionally disciplined. It does not propose new frameworks, advocate specific tools, or critique existing standards, all of which remain foundational to security governance. It relies on publicly observable patterns rather than classified or proprietary detail. Its focus is narrower and more consequential: identifying a governance blind spot that persists even within mature, compliant programs. Systems cannot be considered secure, resilient, or responsibly governed if the decisions that shaped them cannot be explained, defended, and attributed over time.

Executive Summary

Security programs across government and critical-infrastructure sectors frequently demonstrate formal compliance with established frameworks while continuing to experience audit findings, post-incident scrutiny, and governance failures[1]. These outcomes often occur where controls are implemented as specified and authorizing officials have approved system operation. The persistence of these failures indicates that compliance alone does not guarantee defensibility. In practice, systems fail review not because controls were absent, but because the decisions that shaped those controls were insufficiently documented.

Audits and oversight reviews do not evaluate systems solely by verifying technical configuration. They reconstruct decision histories to determine whether actions were reasonable

[1] Government Accountability Office. (2021). Information technology: Agencies need to address persistent weaknesses in management and oversight

given the information, constraints, and risks known at the time[2]. When organizations cannot answer these questions with contemporaneous evidence, even technically sound decisions are vulnerable to misinterpretation. The absence of preserved decision rationale forces organizations to explain past actions using present-day assumptions.

This pattern is reinforced by governance practice. While frameworks emphasize risk-based decision-making, they do not consistently require preservation of reasoning beyond summary approvals. Over time, personnel changes and evolving threat models erode informal knowledge. What remains is a record of outcomes divorced from context. This paper argues that decision accountability must be treated as a first-class governance control. Decisions shape system risk as directly as technical configurations do, and their rationale must therefore be preserved with equal rigor. In regulated environments, defensibility is not optional; it is foundational to credibility and resilience.

The Compliance–Audit Disconnect

Compliance and audit evaluate different dimensions of governance. Compliance verifies whether prescribed controls exist and meet criteria, while audit evaluates whether decisions were reasonable and justified at the time they were made[3]. This distinction becomes consequential when systems are examined retrospectively. At that point, the question is no longer whether controls were present, but whether decisions were defensible under real conditions. Auditors reconstruct decision histories to understand why controls were selected, alternatives rejected, or deviations accepted. These inquiries arise when outcomes are imperfect. When organizations cannot produce contemporaneous rationale, reviewers must infer intent after the fact. That inference almost always disadvantages the system.

Operational experience shows this disconnect is not caused by disregard for governance, but by how governance is practiced. Risk acceptances are approved and exceptions documented, yet reasoning is often informal or fragmented. Over time, that reasoning disappears. Oversight findings consistently reflect this pattern, citing gaps in accountability rather than technical incapacity[4]. The compliance–audit disconnect is therefore not a failure of frameworks, but a failure to preserve the reasoning that bridges policy and practice.

[2] National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations

[3] Government Accountability Office. (2021). Information technology: Agencies need to address persistent weaknesses in management and oversight

[4] Government Accountability Office. (2019). High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas; Department of Homeland Security, Office of Inspector General. (2020). Management Challenges Facing the Department of Homeland Security.

What Existing Frameworks Capture—and What They Leave Behind

Security frameworks provide indispensable structure, shared language, and process discipline across complex organizations[5]. They define how risk is identified, how controls are selected, and how systems are authorized. Their absence would immediately degrade security posture. Their strength lies in standardization, not preservation of lived decision context.

Frameworks capture control state effectively. They document whether safeguards exist and whether they operate as intended. However, control state is not decision state. Frameworks can confirm that a decision occurred without preserving the reasoning that made it appropriate.

In real systems, decisions are shaped by constraints such as legacy architecture and mission urgency. Frameworks acknowledge risk-based decision-making but do not require that these constraints be preserved as auditable context. Over time, constraints fade while outcomes remain. Frameworks also create incentives that prioritize checklist-satisfying artifacts. This produces compliance theater: governance that appears complete but cannot explain itself. The limitation is not a flaw in design, but a consequence of scope. When oversight arrives, defensibility suffers.

Institutional Memory Loss as a Security Liability

Institutional memory loss is a systemic security liability in long-lived systems[6]. When decision rationale is not preserved as an organizational artifact, continuity depends on individual recollection. Over time, this creates silent fragility. Decisions made to accommodate constraints remain embedded in system behavior long after context fades. New teams inherit configurations without understanding intent. Inherited risk is misinterpreted as design failure, driving unnecessary remediation and repeated findings.

Institutional memory loss undermines incident response. Teams must determine whether behavior reflects accepted tradeoff or emergent vulnerability. Without preserved rationale, response slows and risk increases[7]. Turnover accelerates loss, but even stable teams experience memory decay. When explanation is absent, auditors interpret deviation as lack of control. Preserving rationale reframes documentation as resilience infrastructure.

Decision Accountability as a Governance Control

Decision accountability is a governance control that shapes how risk is perceived and accepted[8]. Decisions are where policy meets reality, and they determine system behavior as directly as

[5] National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations

[6] Government Accountability Office. (2019). High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas

[7] Department of Homeland Security, Office of Inspector General. (2020). Management Challenges Facing the Department of Homeland Security.

[8] National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations

technical configurations. When rationale is not preserved, outcomes remain while logic disappears. Treating accountability as a control changes behavior upstream. Assumptions are surfaced, constraints acknowledged, and tradeoffs made explicit. Research on high-reliability organizations shows that visible reasoning improves resilience[9].

Accountability must be distinguished from blame. Accountability preserves context for fair evaluation, while blame assigns fault without regard to conditions[10]. Clear accountability enables responsible risk acceptance. Preserved rationale anchors governance across time. Mature programs are not those that eliminate risk, but those that can explain risk acceptance coherently. A system that can explain itself is more resilient than one that merely produces artifacts.

Why Automation and Tooling Are Insufficient

Automation captures actions, not reasoning. Workflow systems record what happened, not why. When accountability is undefined, automation preserves outcomes while discarding context[11]. Workflow substitution for judgment creates false rigor. Complex tradeoffs are reduced to checkboxes, producing records that cannot answer audit questions. This workflow laundering masks accountability gaps.

Automation also scales inconsistency. Without standards defining decision records, documentation varies across teams and time. The result is institutional noise rather than memory. Decision accountability must precede automation. Tools can preserve judgment, but they cannot supply it.

Artificial Intelligence as an Amplifier of Accountability—and of Risk

AI enters governance amid optimism and unease. It promises synthesis and scale but raises fears of opacity and displaced responsibility[12]. AI does not create governance risk; it amplifies the posture already present. Where governance is strong, AI supports human judgment by surfacing patterns and reconciling fragmented records. Research shows decision quality improves when automation remains subordinate to accountable humans[13]. In these contexts, AI strengthens institutional memory.

Where governance is weak, AI magnifies failure. Model outputs obscure assumptions and uncertainty. When accepted without preserved human rationale, accountability collapses[14]. AI

[9] Weick, K. E., & Sutcliffe, K. M. (2015). Managing the unexpected: Sustained performance in a complex world (3rd ed.). Wiley.

[10] Government Accountability Office. (2021). Information technology: Agencies need to address persistent weaknesses in management and oversight

[11] Government Accountability Office. (2021). Information technology: Agencies need to address persistent weaknesses in management and oversight

[12] Endsley, M. R. (2017). From here to autonomy: Lessons learned from human–automation research. Human Factors, 59(1), 5–27; National Institute of Standards and Technology. (2023). AI Risk Management Framework

[13] Endsley, M. R. (2017). From here to autonomy: Lessons learned from human–automation research. Human Factors

[14] National Institute of Standards and Technology. (2023). AI Risk Management Framework

also introduces continuity risk when models change. Without preserved reasoning, organizations inherit AI-driven outcomes without explanation. AI is therefore a force multiplier for governance quality.

Implications for Critical Infrastructure and National Security

Critical-infrastructure and national-security systems persist across decades and threat landscapes[15]. Early decisions shape risk long after conditions change. When rationale is lost, stewardship credibility erodes. Infrastructure operates in dense dependency networks where failure cascades. Decisions made to prevent downstream disruption may later appear misaligned if context is lost, increasing systemic risk[16].

National-security systems add irreversibility. Certain decisions cannot be undone without unacceptable cost[17]. Lost rationale drives compliance maximalism that weakens resilience. Decision accountability anchors evaluation to historical reality. It enables oversight to assess judgment rather than infer intent, preserving legitimacy in high-consequence environments.

From Compliance to Defensibility

Compliance establishes baseline expectations but does not determine resilience[18]. Defensibility emerges when systems are required to explain themselves under pressure—during audits, incidents, leadership changes, or public scrutiny. Unlike compliance, which measures adherence to prescribed requirements, defensibility evaluates the quality of judgment exercised in shaping a system over time. Organizations that preserve decision rationale demonstrate continuity of intent and reasoning across changing conditions. Those that do not are left to construct hindsight narratives that reinterpret past decisions through present assumptions, often to their disadvantage.

Prioritizing defensibility reshapes governance behavior upstream. When decision rationale is expected to endure, decisions become more deliberate, assumptions are surfaced rather than implied, and tradeoffs are acknowledged rather than obscured. Authority is exercised with an awareness that future reviewers will evaluate not only outcomes, but the reasoning that produced them. Far from slowing systems, this clarity reduces rework, mitigates repeated findings, and enables adaptation without repudiation.

Ultimately, decisions themselves must be treated as security-relevant artifacts. Technical controls show what was implemented, but decision records explain why it was implemented in that form. Compliance confirms that requirements were met. Defensibility demonstrates that judgment was

[15] Government Accountability Office. (2019). High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas

[16] Government Accountability Office. (2019). High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas

[17] Office of Management and Budget. (2016). OMB Circular A-130: Managing Information as a Strategic Resource

[18] National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations

exercised. In regulated and high-consequence environments, this distinction is not merely theoretical. It is the clearest indicator of whether an institution understands its own systems, governs them responsibly, and is prepared to stand behind its choices over time.