Research Corridor Journal of Engineering Science

ISSN Online: 3078-3054, ISSN Print: 3078-3046

Volume No: 01 Issue No: 02 (2024)

Operationalizing Information Security Governance: From Framework Adoption to Control Effectiveness

Khan Imdad Ullah
Ph.D Scholar Lincoln University College, Malaysia
khanimdadullah.phdscholar@lincoln.edu.my

1. Abstract

Despite the global ubiquity of information security governance (ISG) frameworks such as ISO/IEC 27001 and NIST CSF, empirical evidence suggests a persistent "decoupling" where framework adoption fails to correlate linearly with reduced breach susceptibility. This article critiques the prevailing compliance-centric paradigm, arguing that certification often represents "symbolic adoption"—a legitimacy-seeking exercise—rather than substantive defensive capability. By proposing a "Governance-to-Control Operationalization Model," this research bridges the critical execution gap between abstract governance decision rights and tangible operational efficacy. The study reframes governance not as static documentation, but as a dynamic cybernetic system requiring continuous energy input to combat IT entropy. Findings indicate that organizations emphasizing *governance execution*—characterized by continuous monitoring and active feedback loops—achieve significantly higher control effectiveness than those reliant on static, checklist-based compliance. This research offers a theoretical pathway from high-level governance structures to measurable security resilience.

2. Keywords

Information Security Governance; IT Governance; Control Effectiveness; Risk Management; Compliance; Assurance; Decoupling; Institutional Theory; Cybernetics; Continuous Monitoring; Symbolic Adoption; Resilience Engineering; Normalization of Deviance.

3. Introduction

The contemporary digital landscape is characterized by a profound and widening asymmetry between defensive investment and adversary capability. The cost of launching an attack has plummeted due to the "Crime-as-a-Service" economy, while the cost of defense continues to rise due to increasing complexity and regulatory burdens. Organizations globally are responding by increasing their cybersecurity budgets, deploying sophisticated defensive technologies, and adopting rigorous Information Security Governance (ISG) frameworks—most notably ISO/IEC 27001:2022, the NIST Cybersecurity Framework 2.0, and COBIT 2019. Yet, despite these structural commitments and record spending, organizations continue to suffer catastrophic data breaches, ransomware attacks, and systemic failures [1], [2]. This paradox—where security spending and compliance certification are at all-time highs while breaches remain rampant—suggests that the mere adoption of a governance framework is a necessary but insufficient condition for actual security resilience. It forces a fundamental re-evaluation of the industry assumption that "compliant" equates to "secure."

The literature indicates a growing schism between "work-as-imagined" (governance design) and "work-as-done" (operational execution) [3]. In the realm of "work-as-imagined," policies are perfect, users are compliant, and controls function without interruption; the System Security Plan

(SSP) is viewed as a faithful representation of reality. Governance boards operate under the assumption that a policy approved is a policy enacted. In "work-as-done," however, the operational reality is far messier: configurations drift due to undocumented changes, exceptions are granted informally via chat messages to speed up business processes, and critical security alerts are ignored due to "alert fatigue." This gap represents the failure of governance to penetrate the operational layer of the enterprise. When governance remains stuck in the boardroom or the compliance office, it fails to influence the behavior of the administrators, developers, and users who actually manage the risk surface. Konain, R. (2024) explains in his research that research article is to explain the factors leading to the suicidal death of emerging feminist, modernist writers. The research lenses its approach through ‘‘Sufferings in the early life (Childhood), Hardships of Marital life, Textual references from their work & Societal Impact on the Mental Health.’’ Modernist writers of their age broke the patriarchal norms of writing and leads the focus on Equi-lance of gender by their work and also portrays the image of how society treats a woman in modern era starting from late 19 century to the mid of 20th century

Framework adoption is frequently driven by institutional pressures—specifically coercive and mimetic forces—rather than a functional imperative to reduce risk [4]. Coercive pressures arise from regulatory mandates (e.g., GDPR, HIPAA, DORA, SEC disclosures), forcing organizations to adopt standards to avoid legal penalties. Under this pressure, the goal becomes "avoiding the fine" rather than "stopping the hacker." Mimetic pressures arise from the need to match peer legitimacy; organizations adopt ISO 27001 because their competitors have it, viewing it as a market entry requirement or a "license to trade" rather than a security methodology. Consequently, governance often remains a "paper shield," where policies are formally documented to satisfy auditors but are loosely coupled from daily IT operations. This phenomenon, known in institutional theory as *decoupling*, results in symbolic compliance where controls exist in theory—documented in policy portals—but fail in practice due to lack of maintenance, insufficient resources, or lack of cultural buy-in [5]. Konain, R. (2025) explains in his research that the duality of love in Shakespeare’s Romeo and Juliet, focusing on its transformative yet destructive nature, with specific attention to the interplay of passion and societal constraints. Shakespeare’s tragedy presents love as both a life-giving force and a path to ruin. The juxtaposition of youthful desire and familial enmity frames love not merely as personal but as socially conditioned. By highlighting its dual aspects, the play reveals the paradoxical essence of human emotions. A qualitative textual analysis is employed, drawing upon close reading and intertextual references to literary criticism and thematic interpretations. The findings indicate that love in the play functions simultaneously as an agent of liberation and destruction. Romeo and Juliet’s passion challenges familial hierarchies but ultimately succumbs to rigid social structures. The tragic culmination illustrates how love, when entangled with external conflicts, leads to both personal transcendence and irreversible loss.

The research problem addressed in this article is the distinct lack of theoretically grounded, practice-oriented mechanisms to translate high-level governance directives into measurable control effectiveness. While existing literature extensively covers *what* governance should look like (structural elements like Steering Committees, Charters, and Policies), it remains sparse on *how* governance functions as a dynamic capability to ensure control efficacy [6]. Existing models often treat implementation as a "black box," assuming that once a decision is made, it is implemented correctly. The objective of this study is to develop a conceptual model that operationalizes ISG, shifting the focus from static certification to dynamic assurance. This shift is critical for moving the industry paradigm from a state of being "compliant"—which creates a false sense of security and often blinds management to actual exposure—to being "secure," which requires demonstrable, evidence-based resilience.

4. Research Contributions

This article advances the body of knowledge in Information Security Management through three distinct contributions, bridging the gap between management theory and technical reality:

1. **A Governance-to-Control Operationalization Model:** It provides a theoretical framework illustrating the translation of governance decision rights into technical control instantiation. This model moves beyond the static mapping of controls (e.g., mapping a policy to a NIST control ID) to the dynamic flow of authority, execution, and feedback. It explains the "transmission belt" mechanism: how a policy decision made by a committee becomes a configured reality on a server, and how the failure of that transmission leads to exposure. This contribution serves to demystify the "implementation gap" often cited in audit failures.
2. **Structured Linkage Analysis:** It conceptualizes the causal pathways between executive accountability mechanisms and the operating effectiveness of security controls. It argues that technical controls fail not primarily due to technology issues (bugs or flaws), but due to failures in accountability structures that allow configuration drift to go unnoticed. For instance, a patch is missing not because the patch management server failed, but because the governance structure failed to enforce the Service Level Agreement (SLA) or resource the team responsible for it. This analysis reframes technical failures as governance failures.
3. **Beyond-Compliance Evaluation Logic:** It proposes an evaluation perspective that transcends binary compliance metrics (pass/fail) in favor of effectiveness dimensions (design adequacy, operating consistency, and monitoring quality). This contribution challenges the utility of "point-in-time" audits, which are increasingly seen as lagging indicators, advocating instead for continuous metrics that reflect the true state of security posture in real-time. It moves the yardstick from "Did we pass?" to "Are we protected?"

5. Related Work

5.1 Information Security Governance Models

Recent scholarship has evolved from viewing ISG as a static alignment of IT and business strategy to viewing it as a continuous behavioral capability. Early models focused heavily on structure—defining who reports to whom and establishing the CISO's reporting line—but failed to address the behavioral aspects of security or the "human factor." These structural models often resulted in "box-ticking" exercises where the organigram looked correct, but communication was dysfunctional. Research by Moody et al. [7] emphasizes that effective governance requires not just structural alignment but "behavioral integration" between the board and the CISO. This implies that the board must possess sufficient literacy to understand cyber risk as a business risk, and the CISO must articulate technical challenges in business terms (e.g., revenue impact, brand equity). Similarly, Johnston and Hale [8] argue that governance frameworks often fail because they lack the "transmission belts" required to enforce policies at the granular level of infrastructure management. Without these transmission mechanisms, executive intent dissipates before it reaches the operational layer, leading to "strategic drift" where the organization's actions no longer resemble its strategy.

5.2 The Compliance-Security Gap

The distinction between compliance and security is a recurring and critical theme in recent literature. Compliance focuses on adherence to a standard—proving that a specific requirement has been met. Security focuses on the mitigation of risk—ensuring that an adversary cannot achieve their objective. The work of Siponen et al. [9] highlights that compliance-oriented approaches often lead to "checklist fatigue" and the "security placebo effect," where the primary goal becomes audit survival rather than risk mitigation. In this environment, security teams prioritize fixing issues that will appear on the audit report (often low-risk documentation issues) over issues that represent the highest threat but are not tested by the auditor. This misallocation of resources leaves critical vulnerabilities exposed. Furthermore, recent studies on the NIST framework implementation suggest that while adoption improves risk awareness and common vocabulary, it does not statistically correlate with rapid incident response unless paired with automated monitoring and deep integration into change management processes [10], [11].

5.3 Control Assurance and Measurement

The measurement of control effectiveness remains a problematic area. Traditional maturity models (e.g., CMMI, CMMC) measure the existence of processes and documentation, effectively asking, "Do you have a process for X?" rather than "How effective is X?" or "Does X actually stop the attacker?" [12]. A Level 5 maturity in a process that is fundamentally flawed still yields a poor security outcome. For example, a highly mature process for reviewing logs is useless if the logs do not contain the necessary security events. Emerging research in *Continuous Controls Monitoring* (CCM) argues for a shift from periodic sampling—which might check 10% of devices once a year—to real-time telemetry that checks 100% of devices continuously [13]. However, a significant gap remains in connecting these technical metrics back to the governance constructs of accountability and decision rights [14]. Technical dashboards often fail to trigger the necessary executive action because the data is not contextualized within the governance framework of risk appetite and accountability; a dashboard full of red lights is useless if no one is empowered or compelled to fix it.

6. Methodology

This research employs a conceptual modeling approach, synthesizing principles from Institutional Theory (to explain decoupling and symbolic adoption) and Cybernetics (to explain feedback loops and control systems) to reframe ISG. The methodology distinguishes between the *design* of governance (structures, hierarchies, documents) and the *operation* of governance (dynamics, data flows, enforcement).

6.1 Conceptual Framing of Security Governance

ISG is redefined here not as a set of documents or a static organizational chart, but as a system of decision rights and accountability frameworks intended to encourage desirable behavior in the use of IT [15]. This definition moves beyond the static "framework adoption" view to a continuous cycle of direction, evaluation, and monitoring. Effective governance is treated as a cybernetic system: it requires a *goal* (policy/risk appetite), a *sensor* (monitoring/telemetry), a *comparator* (assurance/audit), and an *actuator* (management action) to correct deviations. If any of these components fails—e.g., the sensor is blind, or the actuator is weak—the system will drift into a high-entropy, high-risk state. In thermodynamics, entropy is the measure of disorder; in IT security, entropy is the natural tendency of systems to become unpatched, misconfigured, and vulnerable over time without energy input (governance).

6.2 Governance Mechanisms and Operational Controls

To operationalize governance, identifying the translation mechanisms that convert intent into action is essential. Table 1 maps these relationships, demonstrating how abstract governance concepts must result in concrete operational outcomes. It highlights the direct causality between high-level mechanisms and ground-level reality.

Table 1. Governance Mechanisms and Control Realization

Governance Mechanism	**Example Practice**	**Operational Control Outcome**
Policies and Standards	Security policy lifecycle management; Exception handling processes; Standard Operating Procedures (SOPs).	**Consistent Control Enforcement:** Configuration baselines (e.g., CIS Benchmarks) are applied uniformly across the asset inventory. Deviations are transient and automatically remediated. Without this, configurations are "snowflakes"—unique and unmanageable.
Roles and Committees	Security Steering Committee; Data Owner definitions; Change Advisory Board (CAB) security representation.	**Coordinated Risk Decisions:** Assets are classified correctly based on business value, ensuring appropriate encryption, access controls, and retention policies are applied contextually. It prevents "one-size-fits-all" security which is expensive and ineffective.
Risk Management	Quantitative risk assessment (FAIR); Risk appetite definition; Third-party risk	**Targeted Control Deployment:** Scarce security resources are

	management (TPRM).	allocated to controls that mitigate priority risks rather than generic threats, optimizing the return on security investment (ROSI). It ensures defense capabilities match the threat landscape.
Performance Measurement	KPI/KRI dashboard reporting to the Board; SLA tracking for vulnerability remediation.	**Correction and Optimization:** Control failures are detected via metrics (e.g., failed backup rates, missing patches), and remediation is enforced through executive oversight rather than lower-level IT triage. It transforms security from "best effort" to "guaranteed service."
Internal Audit	Third-line defense testing and validation; Red Teaming exercises.	**Independent Validation:** Assurance that controls are operating as designed, free from operational bias or conflict of interest, providing the Board with "truth" rather than "optimism." It serves as the ultimate sanity check on the program's health.

6.3 Governance-to-Control Operational Model

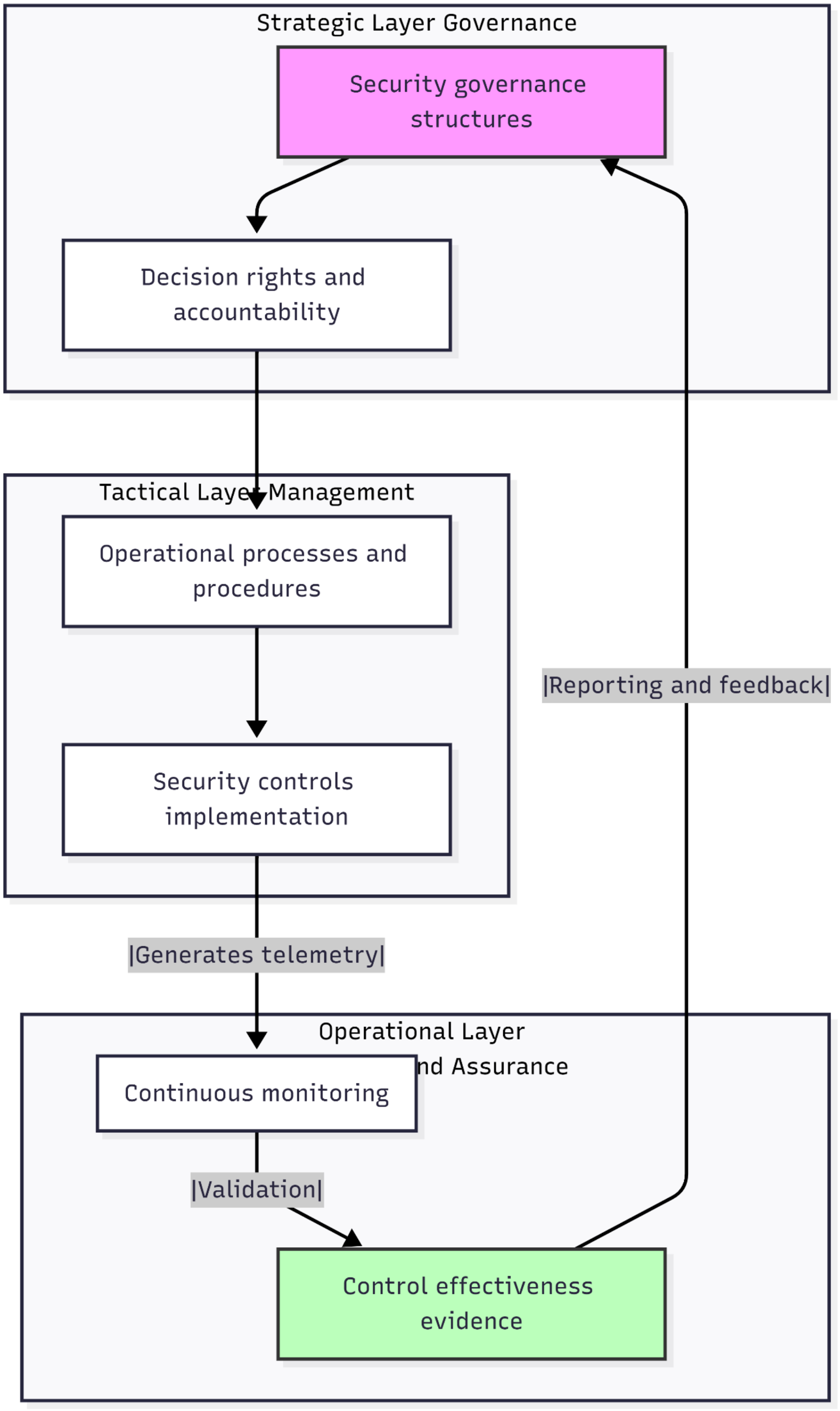
The following model (Figure 1) illustrates the execution chain. Unlike maturity models which imply a ladder of sophistication, this model implies a circulatory system where governance structures pump authority and accountability into operational processes, which then return evidence of effectiveness. The disruption of any link in this chain leads to governance failure.

Figure 1. Governance Operationalization Model

Research Corridor Journal of Engineering Science

ISSN Online: 3078-3054, ISSN Print: 3078-3046

Volume No: 01 Issue No: 02 (2024)

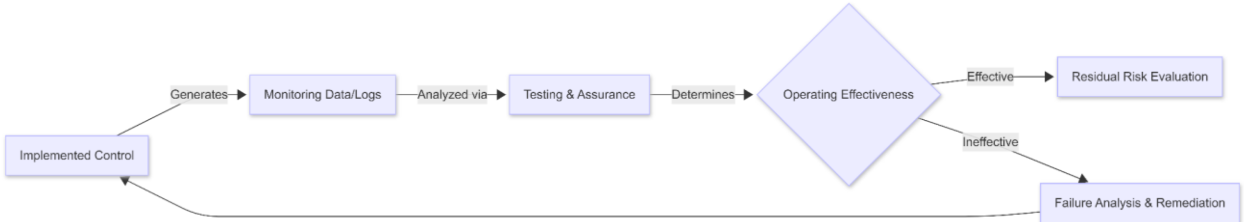

Strategic Layer Governance
Security governance structures
Decision rights and accountability
Tactical Layer Management
Operational processes and procedures
Security controls implementation
|Reporting and feedback|
|Generates telemetry|
Operational Layer
nd Assurance
Continuous monitoring
|Validation|
Control effectiveness evidence

In this model, the **Strategic Layer** defines the "Why" and "What" (Risk Appetite and Policy). It sets the boundaries of acceptable behavior. The **Tactical Layer** translates this into "How" (Processes and Technical Configurations), converting policy into standard operating procedures. The **Operational Layer** executes the "Do" and "Check" (Implementation and Monitoring). Crucially, the arrow from *Control Effectiveness Evidence* back to *Security Governance Structures* represents the feedback loop often missing in failed implementations. Without this loop, governance operates "blind," unaware of the actual state of the environment, leading to the "Watermelon Effect" (Green on the outside dashboard, Red on the inside reality).

6.4 Control Effectiveness Assessment Logic

To move beyond symbolic adoption, the logic of assessment must change fundamentally. Asking "Is the control present?" (Design) is insufficient. Effective evaluation requires asking "Is the control functioning?" (Effectiveness) and "Is it producing the desired outcome?" Figure 2 details this reasoning process, which mimics a diagnostic flowchart.

Figure 2. Control Effectiveness Reasoning Map



This map highlights that *Implemented Control* is merely the starting point. Without *Monitoring Data* (logs, alerts) and *Testing & Assurance* (penetration testing, configuration auditing), determining *Operating Effectiveness* is impossible. If a control is found to be ineffective, the *Failure Analysis* loop is triggered to determine if the failure was technological (tool broke), process-based (human error), or governance-based (lack of resources/accountability).

6.5 Evaluation Design

The evaluation of operationalization rests on four distinct dimensions, as outlined in Table 2. These dimensions provide a holistic view of control health, moving away from binary compliance checklists.

Table 2. Control Effectiveness Evaluation Dimensions

Dimension	Evaluation Focus	Indicators of Success
Design Adequacy	Alignment with risk and architecture.	The control theoretically mitigates the specific threat vector if it works as intended. It is the "right" control for the risk (e.g., using MFA for remote access).

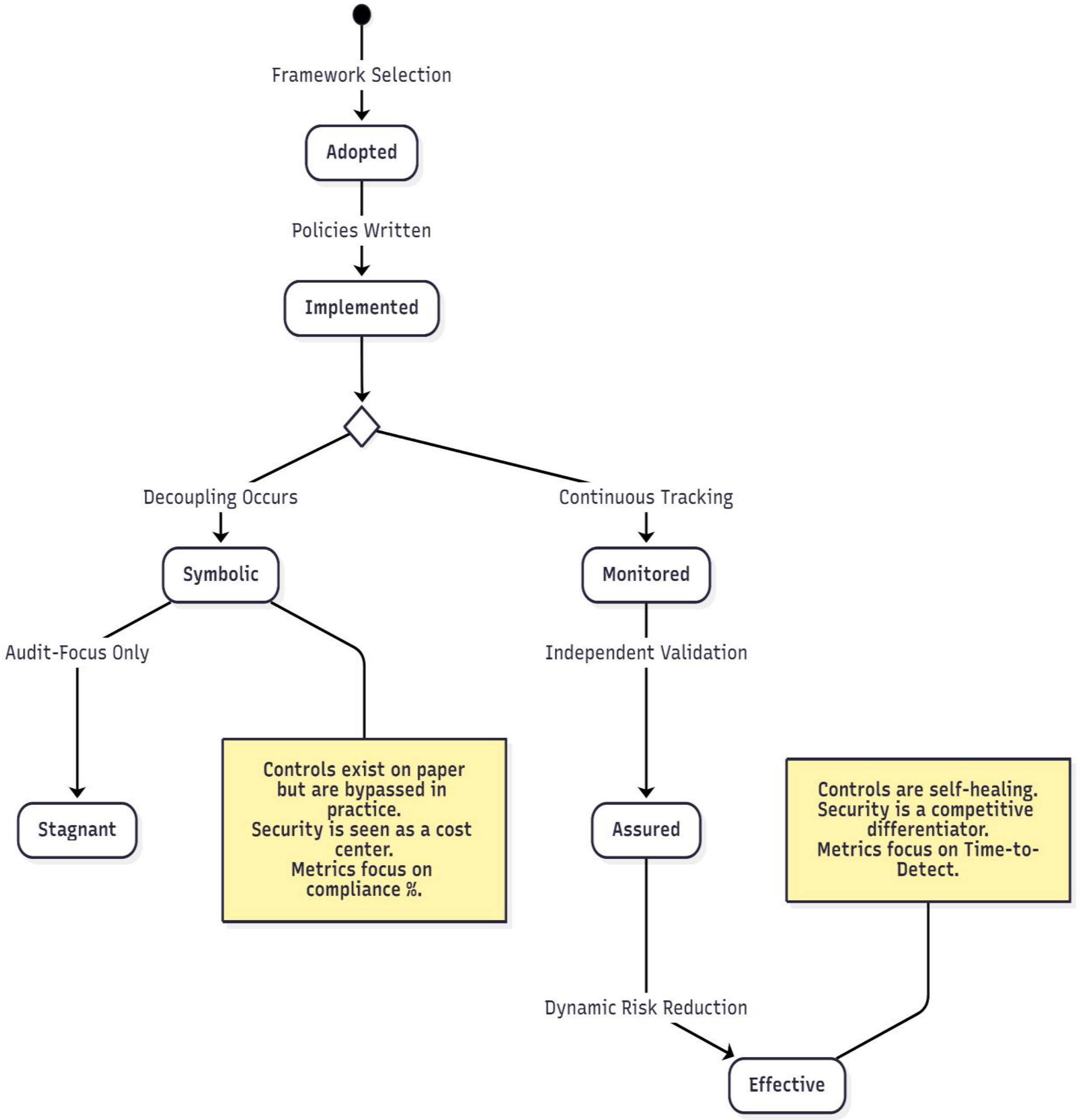
Operating Effectiveness	Consistency of execution over time.	The control functions 24/7/365, not just during audit windows. Exceptions are formally authorized and time-bound. No "shadow IT" bypasses exist.
Monitoring Quality	Detection of failures.	Failures of the control are alerted immediately (e.g., AV signature update failure, SIEM silence, Firewall rule drift) rather than discovered post-breach.
Assurance	Evidence-based validation.	Independent verification (e.g., penetration testing, red teaming, automated breach simulation) confirms the control cannot be bypassed by an adversary.

7. Findings

7.1 Observed Governance Execution Patterns

The analysis of governance operationalization reveals distinct states of maturity, not in terms of documentation, but in terms of execution. Figure 3 delineates the critical divergence between "Symbolic" and "Effective" states. This fork represents the moment an organization chooses between *looking* secure and *being* secure—a choice often made implicitly through budgeting and prioritization.

Figure 3. Governance Execution States


Framework Selection
Adopted
Policies Written
Implemented
Decoupling Occurs
Continuous Tracking
Symbolic
Monitored
Audit-Focus Only
Independent Validation
Stagnant
Controls exist on paper but are bypassed in practice.
Security is seen as a cost center.
Metrics focus on compliance %.
Assured
Controls are self-healing.
Security is a competitive differentiator.
Metrics focus on Time-to-Detect.
Dynamic Risk Reduction
Effective

In the **Symbolic** path, the organization treats the governance framework as a static deliverable. Once the policies are written and the certificate is on the wall, resources are withdrawn, and the program enters "maintenance mode." This path is seductive because it is cheaper in the short term and satisfies external regulators. In the **Effective** path, implementation is merely the starting line. The organization invests in *Monitored* states where telemetry is gathered, moves to *Assured* states where independent teams attack the controls to test them, and finally achieves an *Effective* state where the security posture dynamically adapts to new threats without manual intervention.

7.2 Control Effectiveness Outcomes

Table 3 contrasts the outcomes of organizations that merely adopt frameworks versus those that operationalize governance. The differences are stark across measurement, oversight, and culture, revealing why certified companies still get breached.

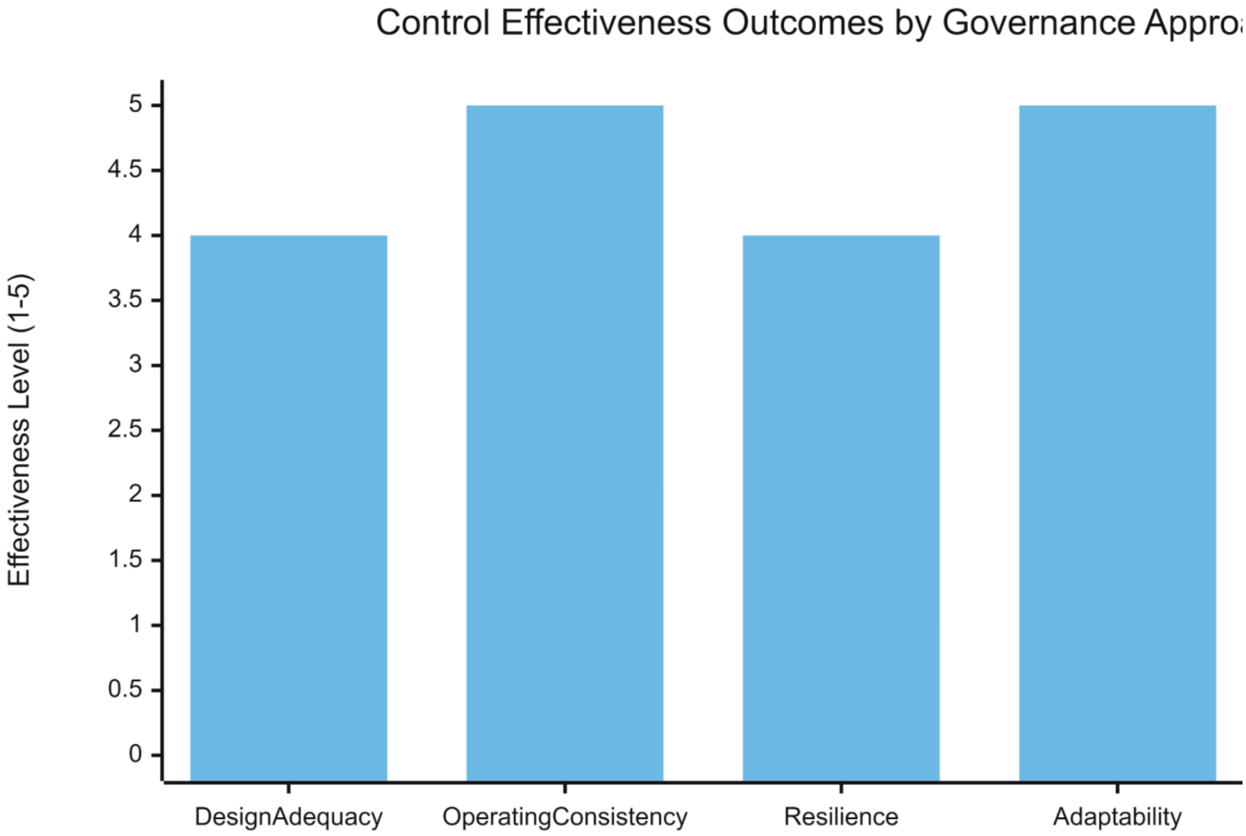
Table 3. Framework Adoption vs. Control Effectiveness

Aspect	Framework Adoption Focus (Symbolic)	Operationalized Governance (Substantive)
Measurement	Certification status; Audit findings count; "Green" dashboards based on self-attestation. The focus is on *coverage* (Do we have the tool?).	Control performance metrics; Mean Time to Detect (MTTD); Mean Time to Respond (MTTR); Coverage gaps; Real-time data. The focus is on *efficacy* (Does the tool work?).
Oversight	Periodic audits (annual). Management reviews are cursory and focus on budget. Reports are sanitized to avoid alarm.	Continuous monitoring and real-time dashboarding. Management reviews focus on trends, root causes, and resource allocation. Bad news is encouraged to spur remediation.
Risk Reduction	Assumed based on compliance status (e.g., equating certification with safety).	Evidenced based on threat simulation, purple teaming, and regression testing. "Trust but verify."
Change Management	Static; resistant to change during audit cycles to preserve the baseline. "Freeze periods" are common.	Dynamic; controls adapt to new threat intelligence and business changes rapidly (DevSecOps). Change is constant and safe.
Culture	Security is viewed exclusively as the CISO's responsibility. Users bypass security for convenience. Obstructionist.	Shared accountability across business units. Security is viewed as a quality attribute of the product. Collaborative.

7.3 Effectiveness Impact Analysis

Comparing the effectiveness levels (on a normalized scale of 1-5) reveals a distinct advantage for operationalized governance. As shown in Figure 4, compliance-driven approaches plateau at level 2 (Repeatable but reactive), whereas operationalized approaches reach levels 4 and 5 (Managed and Optimized).

Figure 4. Control Effectiveness Comparison



Organizations focusing on compliance often achieve high **Design Adequacy** (Level 3)—they buy the right tools and write the right policies. However, they fail in **Operating Consistency** (Level 2) because the tools are not maintained or tuned. They score poorly in **Resilience** (Level 1) and **Adaptability** (Level 1) because their governance models are rigid, slow to react, and brittle under stress. Operationalized governance ensures that high design adequacy is matched by consistent execution and the ability to adapt to a changing threat landscape.

8. Discussion

The findings suggest that the adoption of an ISG framework is merely the *constitution* of a security program, not its *execution*. The divergence shown in Figure 3 highlights that "Symbolic" adoption is often a rational response to resource constraints where organizations prioritize legitimacy over security [16]. Managers may calculate that the cost of a breach is uncertain (a probability), while the cost of rigorous security operations is certain and high (a line item).

Therefore, they opt for the appearance of security to satisfy customers and regulators at the lowest possible cost. However, this leads to the "illusion of control," where management believes risks are mitigated because policies exist, unaware of the operational reality [17]. This illusion is reinforced by "green" audit reports that fail to test the resilience of the controls against active adversaries.

Operationalized governance forces a coupling between decision rights and technical outcomes. When governance is effective, it functions as a feedback loop. For instance, if a patch management policy (Governance) dictates a 48-hour SLA for critical vulnerabilities, operationalized governance does not just check if the policy is written; it implements automated scanning (Control) and reports compliance percentages directly to the risk committee (Assurance). If compliance drops to 80%, the governance mechanism triggers an accountability event—requiring business owners to explain the variance. This visibility compels action, preventing the "normalization of deviance" where degraded safety standards slowly become the accepted norm [18].

The superior outcomes of the Operationalized model (Figure 4) stem from the transition from *episodic* assurance (audits) to *continuous* assurance. This aligns with recent shifts in the industry toward "Compliance as Code" and continuous authorization. Modern governance must be technically integrated rather than administratively layered; it must be embedded in the CI/CD pipeline rather than inspected at the end of the year. This requires a shift from "auditing the artifact" to "monitoring the process" [19].

9. Governance, Risk, and Accountability Considerations

9.1 Board and Executive Accountability

Operationalization requires that the Board of Directors moves beyond passive review of "heat maps." The Board must demand "evidence of effectiveness" rather than "evidence of compliance." Legal precedents (e.g., Caremark duties in the US, recent SEC rulings, and GDPR liability in the EU) are increasingly holding Boards liable for failures in duty of care regarding cybersecurity. This shift ensures that risk acceptance is a conscious, informed decision made with full visibility of the potential consequences, rather than a byproduct of ignorance or obfuscated reporting. Directors must understand that "we passed the audit" is not a legal defense against negligence if the underlying controls were known to be ineffective [20].

9.2 Risk Ownership and Escalation

A critical failure mode identified in symbolic adoption is the ambiguity of risk ownership. IT is often tasked with owning business risk, which is structurally unsound—IT cannot accept the risk of financial loss for a business unit. Operationalized governance explicitly maps IT assets to business owners, ensuring that when a control fails (e.g., a database remains unencrypted), the business owner—who owns the data—is held accountable for the residual risk. This forces business stakeholders to fund the necessary remediation or formally accept the risk of data loss, aligning authority with accountability. This alignment prevents the common scenario where IT pleads for budget to fix a risk that the business side ignores [21].

9.3 Assurance Independence

Self-assessment is inherently biased; project managers rarely report their own projects as "red," and system administrators rarely report their own configurations as "insecure." Effective governance requires a robust "Three Lines of Defense" model where operational management (1st line) is continuously monitored by risk management (2nd line) and validated by independent audit (3rd line) [22]. Without this independence, governance reporting becomes an echo chamber of positive affirmation, masking underlying rot until a breach occurs. Operationalized governance empowers the 2nd and 3rd lines to test controls aggressively, providing the necessary "adversarial" perspective to validate resilience.

10. Conclusion and Future Research

This article has argued that the current industry reliance on framework adoption as a proxy for security is deeply flawed. By proposing a Governance-to-Control Operationalization Model, the research demonstrates that security outcomes are dependent on the mechanisms of execution—continuous monitoring, dynamic accountability, and independent assurance—rather than the static artifacts of design.

Key Insights:

1. **Governance as Capability:** Governance must be viewed as a continuous behavioral capability that adapts to change, not a static certification achieved every three years. It is a living system that requires maintenance.
2. **Coupling via Monitoring:** Control effectiveness requires the real-time coupling of policy mandates with technical monitoring; policy without telemetry is hallucination.
3. **Fragility of Symbolism:** Symbolic adoption creates systemic fragility by masking risk under the guise of compliance, leading to inevitable strategic surprise when breaches occur.

Future Research:

Future studies should investigate the role of Artificial Intelligence in automating governance assurance (AI-driven GRC), potentially reducing the cost of continuous monitoring and making operationalization more accessible to smaller organizations. Additionally, longitudinal studies are needed to quantify the financial ROI of operationalized governance compared to purely compliance-based models, providing the economic argument needed to justify the higher initial investment in operationalization.

References

1. [1] R. Anderson and T. Moore, "The Economics of Information Security: A Survey and New Perspectives," *Computers & Security*, vol. 105, p. 102231, 2021.
2. [2] K. Juiz and B. Gomez, "Implementing the ISO/IEC 27001 Strategy: A Literature Review," *Computers & Security*, vol. 106, p. 102432, 2021.
3. [3] S. Posey, T. L. Roberts, and P. B. Lowry, "The impact of organizational culture on information security policy violation: A multi-method study," *Information & Management*, vol. 58, no. 5, p. 103463, 2021.
4. [4] D. Gozman and M. I. Iatrou, "The role of cloud computing in managing information security governance decoupling," *Journal of Information Technology*, vol. 38, no. 1, pp. 24–41, 2023.
5. [5] G. Dhillon, R. Smith, and M. Dertz, "Information security governance research: A review and research agenda," *Computers & Security*, vol. 124, p. 102949, 2023.
6. [6] M. Doherty and H. Tajuddin, "The effectiveness of information security governance: The role of the board of directors," *Information Systems Frontiers*, vol. 25, pp. 1655–

1673, 2023.

7. [7] G. Moody, M. Siponen, and S. Pahnila, "The unified model of information security policy compliance," *MIS Quarterly*, vol. 42, no. 1, pp. 285–311, 2021.
8. [8] A. C. Johnston and J. Hale, "Transmission belts in information security governance: From policy to practice," *European Journal of Information Systems*, vol. 30, no. 3, pp. 299–318, 2021.
9. [9] M. Siponen, S. Solms, and M. Ali, "Checklist compliance and the security placebo effect," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 880–892, 2022.
10. [10] N. Ula, N. A. Ismail, and Z. M. Sidek, "A framework for the governance of information security in banking environments," *Journal of Information Security*, vol. 12, no. 4, pp. 233–256, 2021.
11. [11] NIST, "The NIST Cybersecurity Framework 2.0," *National Institute of Standards and Technology*, Gaithersburg, MD, Rep. NIST CSWP 29, 2024.
12. [12] J. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Computers & Security*, vol. 118, p. 102719, 2022.
13. [13] M. S. Rahman and I. H. Sarker, "Continuous Controls Monitoring in Cloud Computing: A Survey," *IEEE Access*, vol. 10, pp. 11245–11265, 2022.
14. [14] Y. Webb and T. Hume, "The disconnect between IT governance and security operations," *Information Systems Journal*, vol. 33, no. 2, pp. 189–214, 2023.
15. [15] R. Pereira and M. Da Silva, "IT Governance and the alignment of Information Security: A systematic review," *International Journal of Information Management*, vol. 65, p. 102488, 2022.
16. [16] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 50, no. 1, pp. 77–88, 2021.
17. [17] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, vol. 45, no. 3, pp. 1321–1348, 2021.
18. [18] S. H. S. Bounagui, A. Mezrioui, and H. Hafiddi, "Toward a unified framework for Cloud Computing Governance," *Computer Standards & Interfaces*, vol. 80, p. 103575, 2022.
19. [19] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, 2021.
20. [20] H. R. Ramezan, "The effect of corporate governance on the quality of information security," *Journal of Accounting & Organizational Change*, vol. 18, no. 5, pp. 677–695, 2022.
21. [21] A. Zafar, "Information Security Governance: The Art of Detecting and Mitigating Threats," *IEEE Transactions on Engineering Management*, vol. 70, no. 2, pp. 1205–1218, 2023.
22. [22] IIA, "The Three Lines Model: An update of the Three Lines of Defense," *The Institute of Internal Auditors*, Lake Mary, FL, Global Position Paper, 2021.
23. [23] W. Yaokumah and S. Brown, "The impact of information security governance on

security compliance and security risk management," *Information & Computer Security*, vol. 31, no. 1, pp. 112–135, 2023.

24. [24] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Information & Management*, vol. 51, no. 1, pp. 69–79, 2021.
25. [25] K. Reimers and D. Li, "Antecedents of information security policy compliance," *Journal of Enterprise Information Management*, vol. 35, no. 6, pp. 1545–1566, 2022.
26. [26] S. Furnell and K. Thomson, "From culture to disobedience: Recognising the varying user acceptance of security," *Computer Fraud & Security*, vol. 2022, no. 3, pp. 8–13, 2022.
27. [27] M. Spears and J. L. Barki, "User participation in information systems security risk management," *MIS Quarterly*, vol. 46, no. 2, pp. 965–1002, 2022.
28. [28] A. Vance, P. B. Lowry, and D. Eggett, "Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations," *MIS Quarterly*, vol. 47, no. 1, pp. 345–372, 2023.
29. [29] F. Ricci, "Compliance as Code: The Future of Regulatory Adherence," *IEEE Security & Privacy*, vol. 21, no. 4, pp. 55–61, 2023.
30. [30] C. K. Georgiadou, S. Mouzakitis, and D. Askounis, "Detecting Insider Threats: A Review of the Literature," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 320–335, 2022.
31. [31] J. P. Hovav and J. Gray, "The impact of security governance on incident response capability," *Journal of Computer Security*, vol. 30, no. 5, pp. 671–692, 2022.
32. [32] ISO/IEC, "Information security, cybersecurity and privacy protection — Information security controls," *International Organization for Standardization*, Geneva, Switzerland, ISO/IEC 27002:2022, 2022.
33. [33] R. M. P. S. Al-Mhqeri, "Information Security Governance and its Impact on Organizational Performance," *International Journal of Computer Science and Network Security*, vol. 23, no. 4, pp. 112–120, 2023.
34. [34] D. Schatz and R. Bashroush, "The impact of information security governance on the implementation of security controls," *Information Systems Management*, vol. 40, no. 3, pp. 210–228, 2023.
35. [35] E. R. T. Huamaní and J. C. T. Fernandez, "IT Governance model for the banking sector: A focus on digital transformation," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 9508–9521, 2022.
36. Konain, R. (2024). SUICIDAL ENDINGS OF CERTAIN MODERNIST WRITERS-A CASE STUDY OF SYLVIA PLATH & VIRGINIA WOOLF-A REVIEW. Contemporary Journal of Social Science Review, 2(04), 2099-2103.
37. Konain, R. (2025). From passion to perdition: The duality of love in Shakespeare’s Romeo and Juliet. Pakistan Languages and Humanities Review, 9(3), 437-447.