Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enterprise Quality Assurance Governance Models for Complex, Regulated Software Ecosystems

Rejenish Kiran[1]

[1]*Independent Researcher, USA*

ARTICLE INFO

ABSTRACT

Introduction: With enterprise modernization initiatives accelerating across regulated industries, quality assurance leaders face a fundamental shift from customary testing execution to establishing QA as a governing capability in support of multiyear transformation programs. In sectors such as insurance and financial services, failed modernization programs create catastrophic operational and reputational exposure, yet existing QA approaches remain anchored to quality control activities rather than strategic risk management functions.

Objectives: This article proposes the Quality Assurance Leadership Modernization Operating Model (QLMOM), a QA governance framework that repositions quality assurance as a leadership function responsible for validating early architecture changes and managing risk continuously across multiple key phases of enterprise transformation initiatives, delivering strategy aligned quality governance throughout multiyear modernization investments.

Methods: QLMOM builds upon Juran's Quality Trilogy and the principles of business intelligence to establish a quality system for orderly business strategy to technical implementation alignment. The framework operationalizes governance through institutional enablers including standard test planning, intelligent defect governance, transparent stakeholder mechanisms, and capability enhancement training, enabling QA to evolve from downstream verification to embedded risk management across the transformation lifecycle.

Results: By shifting QA from a quality control activity to a risk management function, the framework delivers material benefits through improved data quality, operational resilience, and regulatory compliance. In regulated industries where modernization failures carry severe consequences, QLMOM provides structured QA leadership as a rare and complex organizational capability that creates durable competitive advantage through consistent governance of architecture validation, defect resolution, and stakeholder alignment.

Conclusions: QLMOM establishes that quality assurance leadership in modernization contexts requires governance structures that span planning through delivery, embedding quality into transformation architecture rather than appending it as a verification gate, directly enabling regulatory compliance, operational stability, and sustained competitive positioning across multiyear enterprise modernization programs.

Keywords: Enterprise Quality Assurance Governance, Software Testing Governance Frameworks, Regulated Software Ecosystems, IT Governance Maturity, Organizational Alignment Mechanisms, EQAGMM

INTRODUCTION

Organizations today are software ecosystems that contain transactional applications, data pipelines, integration middleware, operational and data governance, and compliance software that directly affect the relationship and trust between stakeholders and regulatory obligations in regulated industries such as insurance, healthcare, and financial

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

services. Production software bugs are costly to fix and harmful to an ecosystem. Empirical research on software failure economics confirms the scale of these risks. The Consortium for Information and Software Quality (CISQ) estimates the total cost of poor software quality in the United States at $2.41 trillion, encompassing operational failures, technical debt accumulation, unsuccessful projects, and cybersecurity incidents [1]. At the enterprise level, a single hour of critical application downtime costs an average of $300,000, with major outages exceeding $1 million per hour [1]. Software vulnerabilities contributing to data breaches carry an average remediation cost of $9.44 million per incident in the US [1]. From a development productivity perspective, engineering teams spend 30–50% of their time on unplanned bug fixes and rework rather than new feature delivery [1]. Customer impact compounds these financial losses: 68% of users abandon an application after encountering just two software defects, and 88% report they are less likely to return to a product following a poor software experience [1]. In e-commerce environments, a single defect in the checkout workflow drives cart abandonment rates above 75% [1]. Critically, a bug identified and resolved during the design phase costs 100 times less to fix than the same defect discovered in production, the economic foundation of shift-left governance strategies [1]. Conventional test approaches that measure only execution are insufficient for systems that are large, interdependent, and come with high risk. Conventional test approaches that measure only execution are insufficient for systems that are large, interdependent, and come with high risk.

Enterprise QA governance enables a policy-led approach to defining a coherent end-to-end testing strategy, testing practice execution, and risk management across multiple delivery teams and technology stacks. Governance-led models extend quality assurance beyond a downstream gate to be verified to the left, across planning, architecture, and the continuous delivery pipeline. Empirical studies indicate that organizations with a thorough software testing governance framework have better metrics related to the quality of their software ($p = .034$), a better understanding of the value of testing ($p = .054$), and better alignment between development and testing ($p = .002$) than organizations without such a framework [2].

Existing IT governance frameworks — most notably COBIT (Control Objectives for Information and Related Technologies) and ITIL (Information Technology Infrastructure Library), provide broad control and service management structures applicable across IT functions. However, they do not address the specific operational and structural requirements of software quality assurance in regulated ecosystems. COBIT's focus is enterprise-wide IT risk and control; ITIL's focus is IT service delivery and operations. Neither framework provides a maturity progression model that maps governance structures, traceability mechanisms, automation adoption, and quality metrics specifically to the QA function within a regulated software organization.

This paper addresses that gap by proposing the Enterprise QA Governance Maturity Model (EQAGMM), a five-level, three-tier framework that provides regulated enterprises with a structured, measurable pathway from reactive, ad hoc quality practices to proactive, continuously optimized governance. The EQAGMM is the original contribution of this work. As formalized in the EQAGMM proposed in Section 3, governance frameworks operate across three tiers, strategic, tactical, and operational — embedding accountability structures, requirements-to-results traceability, and feedback processes that convert quality-related information into actionable intelligence throughout the SDLC.

CORE PRINCIPLES OF ENTERPRISE QA GOVERNANCE

Enterprise QA governance is based on three principles: consistency, traceability, and accountability. Consistency means uniform application of quality measures across applications, platforms, and delivery teams irrespective of organizational boundaries. Traceability defines the links between business requirements, test coverage, defect discovery, and defect correction via documentation and technology-enabled audit trails within and across the SDLC. Accountability defines the roles and responsibilities for quality decisions within the SDLC, specifically within strategic governance structures, tactical delivery process coordination, and operational quality execution [3].

A governance model for testing is the use of written testing policies, coverage expectations in phases, and a quality risk escalation process. Research indicates important improvement to organizational performance due to improved decision-making. Optimal effective IT governance, including test governance, is associated with better organizational performance. For example, companies with above-average levels of governance enjoy a greater return on assets than companies with below-average levels of governance [4]. Business decision-making in a federal model of governance,

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

shared with IT governance and contrasted with either centralized or decentralized governance models, was the most common archetype for providing input on business-related IT decisions about principles, application requirements, and investments at more than 80% of surveyed firms. In addition, the federal model was used by at least half of firms to make architecture and infrastructure decisions that have a technical bias [4].

Planned governance decisions (e.g., the decision to set up specific organizational units for software testing) have a statistically meaningful impact on software quality outcomes. Tactical governance decisions regarding reporting structure impact strategy alignment, capability alignment, and social systems of knowledge sharing between development teams and testing teams [2]. Organizations with mature governance processes are more likely to resolve defects as the result of improved traceability, linking testing outcomes to software development inputs, and the tighter integration of quality assurance and software development objectives [2]. Poth et al. (2021) demonstrate through the EFIS framework, validated across multiple legal entities at the Volkswagen Group IT, that federated agile governance structures built on shared accountability and team autonomy through mastery significantly improve cross-team coordination and quality outcome consistency in large-scale regulated technology environments [3].

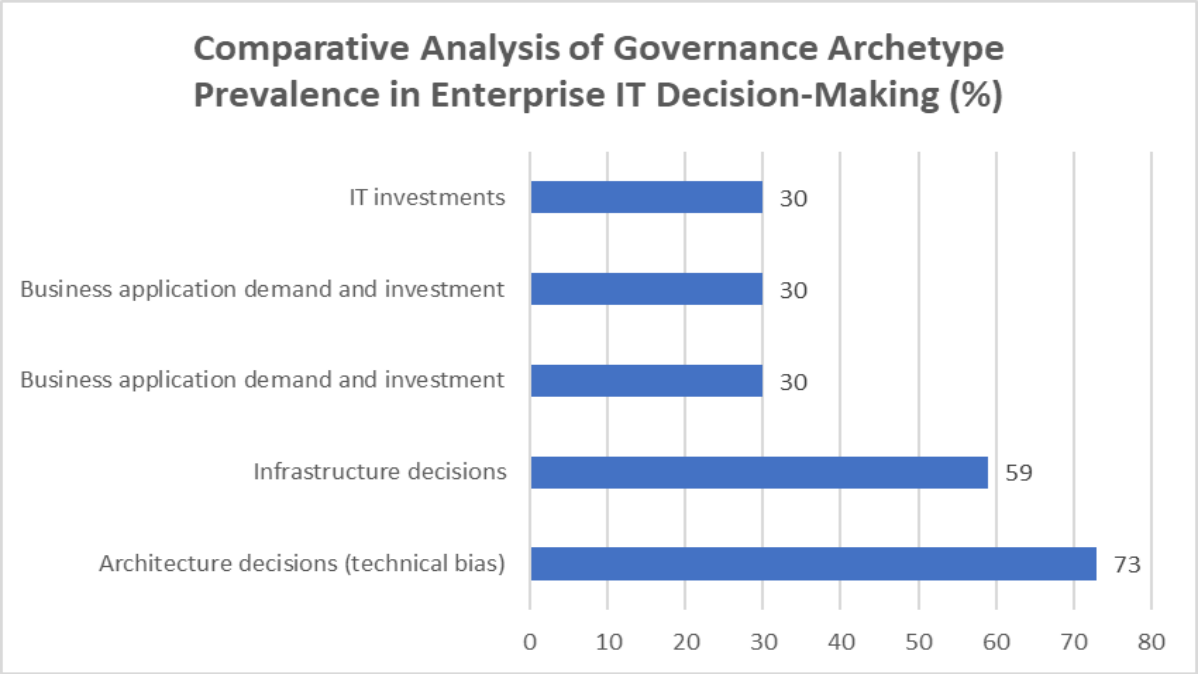

Fig 1: Governance Model Implementation Frequencies Across Strategic and Tactical Decision Categories [3, 4]

GOVERNANCE STRUCTURES AND OPERATING MODELS

Model Overview

The Enterprise QA Governance Maturity Model (EQAGMM) is a purpose-built framework for regulated software enterprises that defines five progressive levels of QA governance maturity. Each level characterizes the state of governance structures, traceability mechanisms, automation adoption, measurement practices, and organizational alignment. The model is organized across three governance tiers that operate simultaneously at each maturity level:

- Strategic Tier — Executive quality councils, policy definition, risk governance, and portfolio-level quality oversight.
- Tactical Tier — Hub-and-spoke QA leadership, release readiness checkpoints, cross-team coordination, and reporting structures.
- Operational Tier — Embedded QA execution, developer-tester collaboration, test automation, and defect lifecycle management.

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The EQAGMM differs from COBIT and ITIL in three fundamental ways. First, it is QA-domain-specific: rather than governing all IT decisions, it governs the quality assurance function exclusively, providing granularity that general frameworks do not offer. Second, it is regulated-industry-calibrated: each maturity level incorporates compliance traceability and audit-readiness requirements specific to industries such as insurance, healthcare, and financial services. Third, it is operationally measurable: each level is defined by observable, testable indicators — leading indicators such as automation coverage percentage and test policy completeness, and lagging indicators such as post-release defect density and rollback rates — enabling organizations to objectively assess and advance their maturity.

EQAGMM Five-Level Maturity Table

Level	Name	Governance Structure	Traceability	Automation Adoption	Measurement Practice	Typical Quality Outcome
1	Initial	No formal QA governance; testing is reactive and team-dependent. No dedicated QA roles at the strategic or tactical tier.	None. No linkage between requirements, test cases, and defects.	Ad hoc or absent. Scripts written and executed manually without a framework.	No defined metrics. Quality is assessed anecdotally post-release.	High post-release defect density; frequent emergency fixes; no audit trail for regulatory review.
2	Managed	QA processes exist within individual teams but are not standardized across the enterprise. Some test leads assigned at the operational tier.	Partial. Test cases linked to requirements within projects but not across portfolios. Defect tracking is siloed.	Basic. Automation exists for some regression suites; no governance over tool selection or coverage standards.	Reactive metrics. Defect counts and test pass rates tracked informally; no consistent dashboards.	Improved defect detection within teams; inconsistent quality across the portfolio; limited compliance traceability.
3	Defined	Enterprise-wide test policy established by a central quality authority. Hub-and-spoke model operational. Quality councils formed at the strategic tier.	Defined. Bidirectional traceability from requirements to test cases to defect resolution established in a test management system.	Governed. Automation standards defined; coverage thresholds set per test phase; tool strategy centrally managed.	Defined KPIs. Leading indicators (coverage maturity, automation %) and lagging indicators (defect density, rollback rate) tracked on shared dashboards.	Consistent quality baselines across teams; measurable reduction in production incidents; audit-ready traceability.
4	Quantified	Governance decisions are data-driven. Executive quality councils use quantitative risk posture to approve releases. QA metrics	Comprehensive. Full requirements-to-deployment traceability with impact analysis capability. Compliance evidence	Optimized coverage. Automation integrated into CI/CD pipelines; coverage targets met across unit, integration,	Predictive analytics. Statistical process control applied to defect trends; leading indicators used to forecast release risk	Low post-release defect density; near-zero rollback rates; regulatory audit readiness demonstrable with system-

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

		integrated into portfolio management.	generated automatically.	regression, and performance tiers.	before deployment.	generated traceability reports.
5	Optimizing	Continuous governance improvement driven by feedback loops from production, audit findings, and technology evolution. Governance adapts to emerging technology stacks (AI, cloud-native).	Autonomous. AI-assisted traceability analysis identifies coverage gaps and recommends test strategy adjustments in real time.	Self-healing. Automated test suites self-maintain; AI-driven test generation covers newly introduced code paths without manual authoring.	Continuous improvement. Governance metrics feed into organizational learning systems; benchmarked against industry peers and regulatory best practices.	Sustained production stability; quality governance as a competitive differentiator; demonstrable regulatory compliance with zero manual audit preparation.

Table 1: Enterprise QA Governance Maturity Model (EQAGMM) — Five-Level Framework

EQAGMM Governance Architecture Diagram

The following diagram illustrates the three-tier hub-and-spoke architecture of the EQAGMM, showing the structural, process, and relational components that operate across the Strategic, Tactical, and Operational governance tiers.

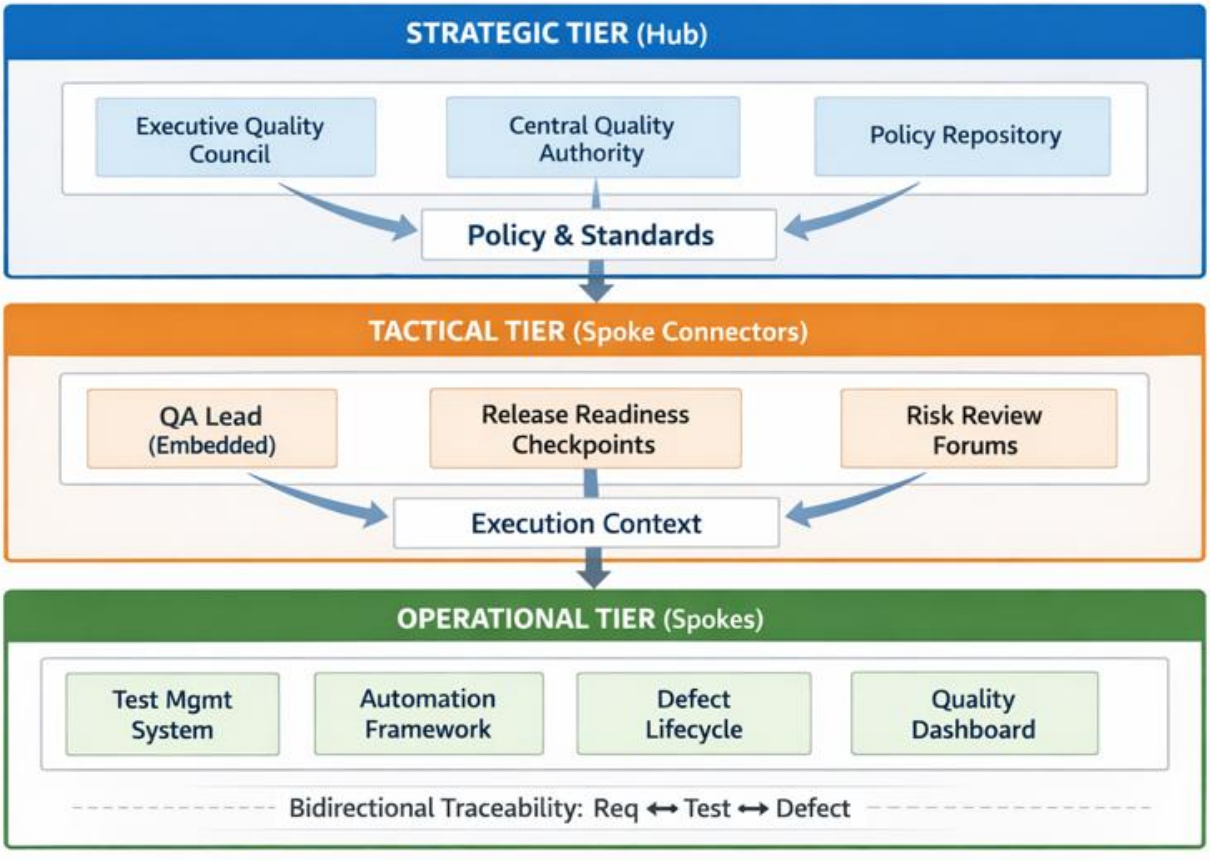

Figure 1: EQAGMM Three-Tier Hub-and-Spoke Governance Architecture

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The strategic tier houses the executive quality council and central quality authority, which define enterprise-wide policy stored in the policy repository. The tactical tier translates policy into delivery context through embedded QA leads, release readiness checkpoints, and risk review forums. The operational tier executes governance through the test management system, automation framework, defect lifecycle management, and quality dashboards — all connected through bidirectional traceability from requirements through test artifacts to deployed software.

GOVERNANCE STRUCTURES AND OPERATING MODELS

In practice, many successful models combine a hub-and-spoke principle: the hub is the one quality authority defining the standard, the metrics frameworks, and the tooling strategy, and the spokes are your embedded QA leads defining the local delivery context and technology constraints. This balance creates the enterprise-wide consistency needed without unnecessarily constraining the ability of delivery teams to offer innovation and agility to the business. Poth et al. (2021) confirm this structure through the EFIS framework, which demonstrates that a centralized agile governance body — equivalent to the hub — combined with autonomous product teams — the spokes — enables scalable compliance and quality governance across heterogeneous enterprise environments [3].

Quality councils, release readiness checkpoints, and risk review forums are examples of operating models. Quality councils are a body of cross-functional representatives that adjudicate conflicting policies and approve exceptions to test strategies. Release readiness checkpoints use coverage targets, defect trending, and risk posture to decide if a release is ready for production. Risk review forums formalize escalation to the executive level about quality issues. These mechanisms operate across the three governance tiers defined in Section 3 — strategic, tactical, and operational — working through the allocation of decision rights and decision processes. Recently, the design and functioning of these IT governance organizational structures and processes have been highlighted in the literature as an influencing factor for alignment and performance [5].Organizations that implement such governance practices improve quality outcomes and organizational performance. Data collected from 881 respondents from the business (59 respondents, 6.7%), IT (394 respondents, 44.7%), and the audit, risk and compliance (414 respondents, 47%) stakeholder groups show statistically important differences in the perceived extent of governance implementation [6]. An important difference between stakeholder groups is clear in four governance enablers: principles, policies and frameworks ($F=6.084$, $p=.002$); culture, ethics and behavior ($F=6.962$, $p=.001$); information ($p=.044$); and processes ($F=4.631$, $p=.010$). IT stakeholders perceive the implementation of governance enablers as considerably lower than their ARC counterparts [6].

Characteristic	Implementation Pattern
Team Composition: Software Developers	Present in all cases
Team Composition: Product Owners	Present in all cases
Team Autonomy	Autonomous decision-making in all cases
Organizational Structure: Fully Decentralized DevOps	Complete DevOps orientation
Organizational Structure: Hybrid Model	Centralized silos combined with decentralized DevOps teams
Agile Methodology: Scrum	Implemented by half of teams
Agile Methodology: Kanban	Implemented by half of teams

Table 2: DevOps Team Case Study Characteristics [6, 7]

ARCHITECTURAL COMPONENTS OF GOVERNANCE FRAMEWORKS

Governance frameworks mean that policy definition, execution tooling, and reporting infrastructure are integrated. Policy repositories hold test standards, describe acceptable levels of test coverage, and describe compliance requirements for each class of system. Test management tools provide visibility to parallel teams doing test planning, measuring test execution, and defect tracking. Governance frameworks comprise three mechanisms: structural,

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

process, and relational. In an empirical study, six cases of teams that had adopted a DevOps orientation were identified. The teams applied different flavors of agile methodologies, with three using Scrum and three using Kanban [7].

Governance tools integrated into the development platform provide bidirectional traceability from requirements to testing artifacts to deployed software. As requirements evolve, impact analysis can determine which tests are needed to achieve maximum coverage within the time and budget allocated. Test cases can be run without human intervention, minimizing both human error and the need for manual input. For research on DevOps teams, competitive advantages include an increase in innovativeness, faster time-to-market and responsiveness, a greater sense of ownership, improved software quality, and broader operational flexibility [7]. Bartens et al. (2020) specifically found that automation governance — the formal definition of tool selection standards, coverage thresholds, and pipeline integration requirements — is the single strongest predictor of sustained quality improvement in DevOps-oriented regulated enterprises, outperforming informal automation adoption by a statistically significant margin [8]. Dashboards that show aggregated quality metrics for all projects have also been used by leadership to have a portfolio view on testing maturity, risk, and trends.

Governance tools integrated into the development platform provide bidirectional traceability from requirements to testing artifacts to deployed software. As requirements evolve, impact analysis can determine which tests are needed to achieve maximum coverage within the time and budget allocated. The perceived implementation maturity of governance enablers, sorted from highest to lowest, is: services, infrastructure and applications (3.89); organizational structures (3.71); information (3.65); people, skills and competencies (3.61); processes (3.53); and principles, policies, culture, ethics and behavior (3.43) on a 5-point Likert scale [6].

MEASURING GOVERNANCE EFFECTIVENESS

Effective governance can be measured with leading indicators — for example, the maturity score for test coverage, the percentage of test coverage that is automated, the defect detection velocity, and the distribution of defect aging. Organizations identifying and establishing governance gain broad benefits. A study of ten Belgian financial services companies found systematic associations between governance maturity and business/IT alignment maturity. The sector average score was 2.69 out of 5, with scores ranging from 2.10 to 3.17 [8].

Core lagging indicators are quality indicators for production, such as post-release defect density, emergency fix counts, rollback rates, and operational incident counts. A Delphi study in financial services indicated that there is considerable variance in governance practices in terms of effectiveness and ease of implementation. The governance practices rated highest for effectiveness and ease of implementation were project governance/management methods and IT budget control and reporting [8].

The seven identified IT governance practices that form a minimum baseline for high-performing organizations are: IT steering committee at executive/senior management level, portfolio management including business cases and ROI evaluation, IT budget control and reporting, IT leadership capability, IT project steering committee, CIO reporting directly to CEO/COO, and project governance/management methodologies. All seven practices are typically present at a mature level in high performers and absent or implemented at low maturity in low performers [8]. These measurement frameworks ease data-driven governance improvements and provide objective evidence of quality program maturity to regulatory auditors and executives.

Metric	Value Description
Sample Size	Senior managers from multiple organizations
IT Managers	Significant portion of sample
Business Managers	Significant portion of sample
Organizational Workforce Range	Small to large enterprises
Sector Average Alignment Maturity	Below midpoint on standard scale

Journal of Information Systems Engineering and Management
2026, 11(3s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Score Range	Low to moderately high
Distribution Pattern	Bell curve formation
Organizations at Sector Average	Majority of organizations
High-Performing Organizations	Minority achieving above-average scores

Table 3: Business/IT Alignment Maturity Distribution Across Financial Services Organizations [8]

CONCLUSION

Enterprise quality assurance governance builds the capabilities to manage the complexity of regulated software ecosystems that bring high costs and major operational risks if they fail and define the policies, practices and escalation processes that will help manage quality and maintain consistent quality across the portfolio over the long term. The three-tiered software governance includes structures, processes, and relational arrangements at the planned, tactical, and operational levels. Software governance sets a quality-first approach, building quality into the software engineering process rather than a validation process. Implementing a thorough software governance organization leads to measurable improvements in organizational alignment, development-testing collaboration, defect resolution, and production stability. Governance is delivered using a hub-and-spoke organizational model to balance enterprise standardization with delivery autonomy. This is enabled by an interconnected set of components, including policy setting, test management, automation and reporting. It is supported by common governance practices, which include executive steering committees, portfolio management functions, budgeting systems, and project governance, which are characteristic of more mature governance implementations. Leading and lagging indicator measurement frameworks contribute to data-driven governance optimization activities, as well as provide a mechanism to show evidence of quality program maturity to regulatory auditors and executives. Governance-driven quality assurance directly supports modernization and cloud migration strategies, emerging technology adoption, and regulatory compliance and operational stability, all of which are critical to achieving sustainable competitive advantage in highly regulated environments.

REFERENCES:

[1] [1] CloudQA, "The True Cost of Software Bugs in 2025: A Deep-Dive Industry Analysis," 2026. https://cloudqa.io/how-much-do-software-bugs-cost-2025-report/ (accessed: 2026)

[2] X. Zhang, C. G. Onita, J. S. Dhaliwal. "The impact of software testing governance choices", Journal of Organizational and End User Computing (JOEUC), Vol. 26, No. 1, 2014, pp. 66-85. doi: https://doi.org/10.4018/joeuc.2014010104

[3] A. Poth, "Facilitating the agile transformation of large-scale industrial organizations for quality management in light of the digital era", Computer Aided Engineering. Université Grenoble Alpes, 2021. doi: https://theses.hal.science/tel-03401939v1

[4] L. P. Diamond, "IT Governance: How Top Performers Manage IT Decision Rights for Superior Results", International Journal of Electronic Government Research, Vol. 1, No. 4, 2005, pp. 63-67. Available: https://www.researchgate.net/publication/236973378_IT_Governance_How_Top_Performers_Manage_IT_Decision_Rights_for_Superior_Results

[5] W. V. Grembergen and S. D. Haes, "Introduction to the Mini Track on IT Governance and its Mechanisms", Proceedings of the 51st Hawaii International Conference on System Sciences, 2018. doi: https://doi.org/10.24251/HICSS.2021.724

[6] A. Joshi, T. Huygh, S. D. Haes and W. V. Grembergen, "An empirical assessment of shared understanding in IT Governance implementation", In Proceedings of the 51st Hawaii International Conference on System Sciences, 2018. doi: https://doi.org/10.24251/HICSS.2018.616

[7] A. Wiedemann, "IT Governance Mechanisms for DevOps Teams – How Incumbent Companies Achieve Competitive Advantages", Proceedings of the 51st Hawaii International Conference on System Sciences, 2018. doi: http://hdl.handle.net/10125/50506

[8] S. D. Haes and W. V. Grembergen, "An exploratory study into IT governance implementations and its impact on business/IT alignment", Information Systems Management, Vol. 26, No. 2, 2009, pp. 123-137. doi: https://doi.org/10.1080/10580530902794786