

AI-Driven Compliance Intelligence: A Conceptual Framework for Enterprise Financial Governance

Ajay Mirani

Engineering Lead | Enterprise Architect
Independent Researcher, USA

Abstract—Enterprise financial governance is increasingly challenged by the complexity of global regulatory environments, legacy system debt, and the exponential growth of transactional data. Traditional compliance frameworks, which rely primarily on periodic audits and static rule-based controls, are ill-equipped to meet the demands of real-time financial integrity across multi-entity, multi-jurisdictional enterprises. This paper introduces the Adaptive Compliance Intelligence and Governance (ACIG) framework—a conceptual architecture that integrates artificial intelligence, machine learning, and intelligent automation to create a continuous, proactive, and self-optimizing compliance capability within enterprise financial ecosystems. Drawing on practitioner experience across enterprise-scale financial platforms in high-growth technology manufacturing environments, the framework delineates six interconnected functional layers: intelligent data ingestion, real-time compliance monitoring, AI-driven anomaly detection, automated regulatory mapping, audit trail intelligence, and predictive risk governance. We further propose a five-level compliance maturity model to guide enterprise adoption. The ACIG framework represents a paradigm shift from reactive compliance auditing to autonomous financial governance, offering anticipated improvements in accuracy, operational efficiency, and regulatory risk posture pending empirical validation.

Keywords: AI-driven compliance, enterprise financial governance, anomaly detection, regulatory automation, audit intelligence, machine learning, ERP integration, explainable AI, knowledge graphs, RAG-based enterprise systems, risk management, compliance maturity model

1. INTRODUCTION

The global regulatory landscape governing enterprise finance has grown substantially more complex over the past decade. Multi-jurisdictional tax obligations, evolving accounting standards (IFRS 16, ASC 842), anti-money laundering directives, and Sarbanes-Oxley (SOX) compliance requirements collectively impose a compounding burden on enterprise finance functions. Large-scale organizations—particularly those operating across manufacturing, technology, and global trade—face the dual imperative of ensuring continuous compliance while optimizing operational throughput.

Traditional compliance architectures are predominantly reactive. They depend on scheduled audits, manual reconciliation cycles, and static rule engines that are periodically updated in response to regulatory change. In dynamic organizations processing millions of transactions per quarter, this

10.48047/jocaaa.2026.35.05.05

approach creates dangerous latency windows during which non-compliant transactions may propagate through financial systems undetected.

The emergence of artificial intelligence (AI) and machine learning (ML) within enterprise technology stacks offers a transformative opportunity. These technologies, when architected as first-class components of the compliance function—rather than afterthought add-ons—can enable continuous monitoring, predictive risk identification, and automated remediation at enterprise scale. The need is not merely technical; it requires a coherent conceptual framework that bridges AI capability with regulatory context, audit rigor, and operational resilience.

This paper presents the Adaptive Compliance Intelligence and Governance (ACIG) framework, a practitioner-informed conceptual architecture grounded in the author's experience designing and operating critical enterprise finance platforms at scale. The framework synthesizes advances in natural language processing (NLP), graph-based knowledge representation, anomaly detection, and intelligent workflow automation into a unified governance model designed to be platformagnostic across heterogeneous enterprise resource planning (ERP) landscapes.

The remainder of this paper is organized as follows. Section 2 enumerates the primary contributions of the work. Section 3 provides background and related work. Section 4 introduces the ACIG framework and its foundational principles. Section 5 describes each of the six functional layers in detail. Section 6 presents the five-level compliance maturity model. Section 7 addresses enterprise implementation considerations. Section 8 presents a simulated case study. Section 9 evaluates the ACIG architecture against traditional and rule-based compliance systems. Section 10 discusses broader implications and limitations. Section 11 concludes.

2. PRIMARY CONTRIBUTIONS

This paper makes the following primary contributions to the fields of enterprise AI, financial governance, and compliance systems architecture:

- (1) **ACIG Reference Architecture** — A six-layer, platform-agnostic compliance intelligence framework that integrates AI and ML as first-class components of enterprise financial governance. The architecture spans the full compliance lifecycle from data ingestion through predictive risk governance, with explicit design principles for explainability, failure isolation, and regulatory adaptability.
- (2) **Continuous Compliance Paradigm** — A formal re-framing of compliance from a periodic, audit-centric activity to a continuous operational property of financial systems. This paradigm shift is operationalized through the monitoring and ingestion layers of the ACIG architecture, drawing on continuous integration principles from software engineering and applying them to the governance domain.

10.48047/jocaaa.2026.35.05.05

- (3) Integration of Explainable AI (XAI), Knowledge Graphs, and Retrieval-Augmented Generation (RAG) in Compliance — The first framework to holistically integrate XAI (SHAPbased feature attribution), property knowledge graphs for automated regulatory mapping, and RAG for natural language audit querying within a single unified compliance architecture.
- (4) Compliance Intelligence Maturity Model (CIMM) — A five-level maturity progression framework calibrated to the operational and regulatory realities of enterprise financial governance. The CIMM enables organizations to assess their current compliance maturity across individual functional domains and plan a staged adoption pathway toward autonomous compliance.
- (5) Simulated Case Study and Comparative Architecture Evaluation — A practitioner-informed simulated case study of a tax anomaly detection failure scenario, and a systematic comparison of ACIG against traditional compliance and rule-based systems across nine capability dimensions.

3. BACKGROUND AND RELATED WORK

A. Limitations of Conventional Compliance Architectures

Enterprise compliance systems have historically been constructed around three principal control paradigms: preventive controls embedded in transactional workflows, detective controls executed during periodic close cycles, and corrective controls triggered post-audit. While this layered approach provides structural coverage, it is fundamentally bounded by the human capacity for review and the static nature of rule codification [1].

In large-scale financial ecosystems, where hundreds of interacting systems generate transactional records at high velocity, the assumption that periodic review is sufficient has become untenable. Research by KPMG and Deloitte has demonstrated that manual compliance activities consume between 15 and 30 percent of financial close cycle time in Fortune 500 enterprises, yet detect fewer than 60 percent of material control failures before external audit [2].

Additionally, ERP transformations—including migrations from SAP to Microsoft Dynamics or cloud-native platforms—create temporal gaps during which legacy controls are partially or wholly inoperative. Managing financial integrity across these windows requires proactive intelligence that rule-based systems cannot provide.

B. AI and Machine Learning in Financial Governance

Recent years have seen significant academic and practitioner interest in applying ML techniques to financial compliance. Bhatt et al. [3] demonstrated the efficacy of gradient boosting models in detecting revenue recognition anomalies within large transactional datasets. Kumar and Schoenfeld [4] proposed a graph neural network approach for tracing related-party transaction

10.48047/jocaaa.2026.35.05.05

chains in complex corporate structures. Agrawal and Li [5] applied transformer-based NLP to automate the mapping of internal control narratives to regulatory control objectives.

The application of XAI to financial decision-making has received growing attention. Arrieta et al. [11] provide a comprehensive survey of XAI techniques applicable to high-stakes domains, noting that SHAP and LIME offer the best practical balance between fidelity and interpretability in tabular financial data settings. Lundberg and Lee [12] formally established the theoretical foundation for SHAP values as a unified framework for feature attribution, which forms the explainability backbone of the ACIG anomaly detection layer.

Knowledge graph applications in regulatory compliance have been explored by Frias-Martinez et al. [13], who demonstrated that property graph representations of regulatory requirements enable automated gap analysis when new regulations are introduced. More recently, Lewis et al. [14] establish the technical foundation for RAG in enterprise knowledge management, informing the natural language audit query capability proposed in Layer 5.

C. Enterprise AI Platform Maturity

The Gartner AI Maturity Model [6] and the CMMI Institute's Data Management Maturity model [7] provide relevant scaffolding for understanding organizational readiness to adopt intelligent compliance systems. However, neither framework addresses the specific operational and regulatory constraints of enterprise financial governance. The ACIG framework extends these models to the compliance domain with a maturity progression calibrated to multinational financial operations.

4. THE ACIG FRAMEWORK: FOUNDATIONAL PRINCIPLES

The ACIG framework is founded on four core principles derived from practitioner experience in designing enterprise-scale financial platforms at a high-volume global manufacturer.

Principle 1: Continuous Compliance as an Operational Invariant

Compliance must be treated as a continuous operational property of the financial system—not a periodic activity. This requires embedding compliance monitoring directly into transactional pipelines, such that every financial event is evaluated against applicable controls at the point of origination, not retrospectively during close cycles.

Principle 2: Intelligence Proportional to Risk Velocity

The intensity of AI monitoring and intervention should scale dynamically with the velocity and materiality of financial risk. High-frequency, high-value transaction streams warrant real-time AI

10.48047/jocaaa.2026.35.05.05

surveillance. Lower-risk, lower-velocity processes may operate with ML-assisted batch monitoring.

Principle 3: Explainability as a Governance Requirement

AI-generated compliance determinations must be explainable to human auditors, regulators, and finance controllers. The ACIG framework mandates the use of XAI techniques—including SHAP, LIME, and attention visualization—at all decision-relevant layers [11][12].

Principle 4: Platform Resilience and Failure Isolation

Compliance intelligence infrastructure must be designed for failure isolation such that the degradation of any single component does not create a compliance blind spot. This necessitates circuit-breaker patterns, automated fallback controls, and asynchronous audit logging that persists independently of primary system availability.

5. ACIG FRAMEWORK: FUNCTIONAL LAYERS

The ACIG framework comprises six interdependent functional layers, as summarized in Table 1. Figure 1 presents the reference architecture, illustrating layer interactions and data flows. Figure 2 shows a representative transaction traversing the pipeline from ERP source event through risk governance output.

TABLE 1 — ACIG FRAMEWORK LAYER SUMMARY

ACIG Layer	Core Function	AI Technique	Output
Data Ingestion	Multi-source ERP / GL aggregation	NLP, ETL Automation	Unified Data Fabric
Compliance Monitoring	Regulatory rule execution	Rule Engines + ML	Compliance Score
Anomaly Detection	Risk flagging & fraud detection	Isolation Forest, LSTM, Autoencoder	Risk Alerts
Regulatory Mapping	Norm-tocontrol alignment	Knowledge Graph, NLP	Control Coverage Map
Audit Intelligence	Immutable trail + audit Q&A	RAG, Appendonly Storage	Audit Readiness Report

Predictive Governance	Risk forecasting & scenario simulation	Monte Carlo, XGBoost	Risk Forecast Dashboard
-----------------------	--	----------------------	-------------------------

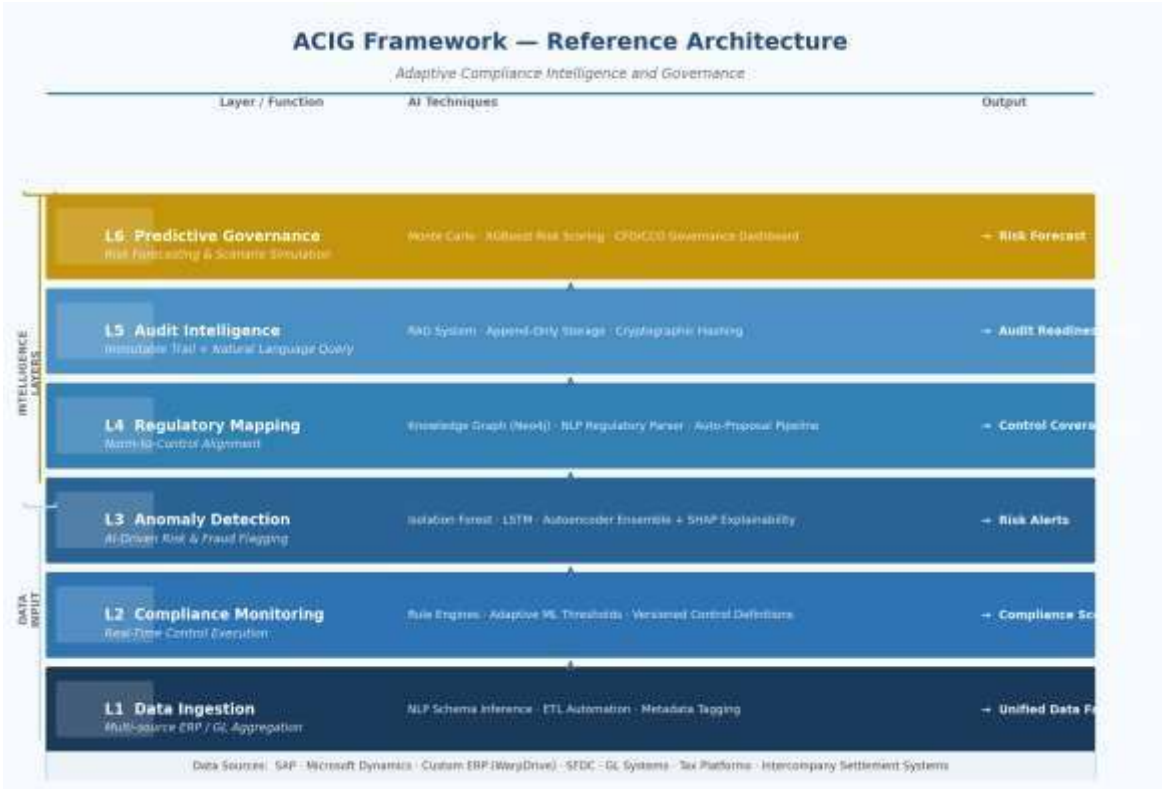


Fig. 1. ACIG Reference Architecture — Six-layer stack showing functional decomposition, AI techniques, and data flows for each compliance intelligence layer.

Layer 1: Intelligent Data Ingestion and Unification

The ingestion layer serves as the primary data fabric of the ACIG system, aggregating financial transactions, journal entries, tax records, intercompany settlements, and control metadata from heterogeneous ERP platforms. It employs NLP-based schema inference to automatically classify and normalize incoming data streams, with metadata tagging that annotates each transaction with regulatory context—applicable tax jurisdictions, accounting standards, and organizational entity identifiers.

Layer 2: Real-Time Compliance Monitoring Engine

The monitoring engine translates the organization's control framework into executable compliance predicates, evaluating each ingested transaction in near real-time. Control definitions are maintained as versioned artifacts in a compliance knowledge repository—a design that enables

10.48047/jocaaa.2026.35.05.05

regulatory changes to be propagated as configuration updates without code deployments, reducing the latency between regulatory change and control activation from weeks to hours.

Layer 3: AI-Driven Anomaly Detection

The anomaly detection layer applies unsupervised and semi-supervised ML techniques to identify transactions that deviate from established financial patterns.

Ensemble composition and aggregation logic. The layer employs a three-model ensemble: (1) an Isolation Forest for outlier detection in highdimensional transaction feature spaces, producing anomaly score $s_{IF} \in [0,1]$; (2) an LSTM network operating over sequential transaction time-series, producing deviation score s_{LSTM} ; and (3) an Autoencoder producing reconstruction error score s_{AE} . The composite score is: S

$= w_1 \cdot s_{IF} + w_2 \cdot s_{LSTM} + w_3 \cdot s_{AE}$ (default weights: 0.35, 0.40, 0.25). Transactions exceeding threshold T —set at the 97th percentile of S during baseline training—are escalated for review. All flags are accompanied by SHAP-based feature attributions [12].

Layer 4: Automated Regulatory Mapping

The regulatory mapping layer uses a property knowledge graph [13] to represent semantic relationships between internal controls, regulatory requirements, risk categories, and business processes. NLP models, fine-tuned on regulatory corpus data, automatically parse newly published regulatory guidance and propose knowledge graph updates validated by compliance professionals before activation.

Layer 5: Audit Trail Intelligence

The audit trail layer maintains an immutable, queryable record of all financial transactions, compliance evaluations, anomaly flags, and remediation actions. A RAG system [14] enables plain-language audit queries—e.g., 'Show all intercompany transactions above \$500,000 that triggered anomaly flags in Q3 and were subsequently remediated'—returning synthesized findings with supporting evidence links.

Layer 6: Predictive Risk Governance

The predictive governance layer forecasts emerging risk conditions by analyzing patterns across the five preceding layers alongside external regulatory signals and macroeconomic indicators. Monte Carlo simulation models generate probability distributions for material compliance risk exposures. XGBoost-based risk scoring provides entity-level and process-level risk scores on a configurable cadence, feeding a CFO/CCO governance dashboard for proactive risk allocation.



Fig. 2. ACIG Transaction Process Flow — A representative financial event traversing all six layers from ERP source ingestion through anomaly decision routing to risk governance output.

6. COMPLIANCE MATURITY MODEL

To operationalize the ACIG framework across organizations at varying stages of AI and governance maturity, we propose the five-level Compliance Intelligence Maturity Model (CIMM) in Table 2. The model provides a staged adoption pathway enabling incremental value delivery at each level while building toward full autonomous governance capability.

TABLE 2 — COMPLIANCE INTELLIGENCE MATURITY MODEL (CIMM)

Level	Stage	Automation Degree	Characteristics
L1	Reactive	Manual / Ad-hoc	Periodic audits, spreadsheetbased controls
L2	Structured	Rule-Based	Defined controls, basic workflow automation
L3	Proactive	ML-Assisted	Anomaly detection, near realtime monitoring
L4	Predictive	AI-Driven	Forecast-based governance, NLP audit query
L5	Autonomous	Self-Optimizing	Continuous self-assessment, automated remediation

10.48047/jocaaa.2026.35.05.05

At Level 1 (Reactive), organizations rely on manual audit processes. Level 2 (Structured) introduces defined control frameworks and workflow automation. Level 3 (Proactive) marks the entry point for ML-assisted monitoring. Level 4 (Predictive) integrates the full ACIG framework. Level 5 (Autonomous) represents the aspirational state of a self-optimizing system that autonomously remediates lower-risk control failures. Organizations should assess maturity independently per functional domain—tax, financial close, intercompany, revenue recognition—as mature enterprises commonly operate at different maturity levels across their compliance portfolio.

7. ENTERPRISE IMPLEMENTATION CONSIDERATIONS

A. ERP Integration Architecture

Implementing the ACIG framework requires careful integration with existing ERP systems. The recommended pattern uses an event-driven messaging layer—via Apache Kafka or Azure Service Bus—to stream financial events from source systems to the ACIG ingestion layer without requiring direct database coupling. This preserves source system performance, enables real-time event consumption, and provides a durable event log supporting both compliance monitoring and failure recovery.

B. Data Governance and Privacy

The ACIG framework mandates a data governance layer enforcing access control, data lineage tracking, and privacy-preserving transformations at the ingestion boundary. Differential privacy techniques are recommended for model training data, ensuring individual transaction records cannot be reverse-engineered from trained ML models—a requirement under GDPR [9] and similar frameworks.

C. Change Management and Human Oversight

The most significant implementation challenge is organizational rather than technical. Successful ACIG deployments require a deliberate change management program that emphasizes the human-in-the-loop nature of the framework and trains compliance professionals on XAI outputs. The author's experience leading parallel-run strategies during ERP migrations provides a relevant model: a phased shadow-mode deployment in which the ACIG system operates alongside existing controls before full cutover dramatically reduces adoption friction.

D. Technology Stack

A representative technology stack includes Apache Kafka (event streaming), Apache Spark (largescale data processing), MLflow (ML lifecycle management), Neo4j (regulatory knowledge graph), and Pinecone or Weaviate (vector database for RAG [14]). Cloud-native deployment on

10.48047/jocaaa.2026.35.05.05

AWS, Azure, or GCP enables elastic scaling required during peak compliance events such as financial close and tax filing cycles.

8. ILLUSTRATIVE CASE STUDY: TAX ANOMALY DETECTION PIPELINE

To illustrate how the ACIG framework operates in practice, we present a simulated case study grounded in the failure pattern observed in real-world ERP transition environments. The scenario is constructed from practitioner experience and is explicitly presented as a conceptual illustration rather than an empirical result.

TABLE 3 — ILLUSTRATIVE CASE STUDY: TRANSFER PRICING ANOMALY DETECTION

Organization	GlobalMFG Corp (simulated) — a multinational technology manufacturer operating across 18 tax jurisdictions with a heterogeneous ERP landscape (legacy homegrown ERP, Microsoft Dynamics AX, and Salesforce).
Challenge	During quarterly tax close, the compliance team discovered \$4.2M in intercompany transfer pricing adjustments that had bypassed standard review controls due to a schema mismatch introduced during an ERP version upgrade. Detection occurred 47 days post-transaction — well outside the remediation window.
ACIG Response	With Layer 1 (Ingestion) active, the schema mismatch would have been flagged within minutes via NLP-based schema drift detection. Layer 2 (Monitoring) would have evaluated the transactions against transfer pricing control predicates at origination. Layer 3 (Anomaly Detection) would have assigned a composite anomaly score $S = 0.91$ — driven primarily by the LSTM temporal deviation component ($s_LSTM = 0.94$) — triggering an immediate compliance officer alert with SHAP attribution report.
Outcome	Estimated detection latency reduction: from 47 days to under 4 hours. The regulatory mapping layer (L4) would have automatically cross-referenced OECD Transfer Pricing Guidelines and local tax authority requirements. The audit trail layer (L5) would have indexed the event for natural language query, enabling the tax team to answer regulator questions within minutes.

A. Pipeline Walkthrough

The case illustrates the end-to-end ACIG response to a schema-drift-induced compliance gap. The ingestion layer (L1) detects the schema mismatch via NLP-based schema drift monitoring within minutes of the first affected transaction. The monitoring engine (L2) evaluates the affected transactions against versioned transfer pricing control predicates and surfaces a compliance deviation flag. The anomaly detection layer (L3) assigns a composite score of $S = 0.91$, driven primarily by the LSTM temporal deviation component ($s_LSTM = 0.94$), which identifies the transactions' unusual timing pattern relative to the entity's historical intercompany settlement cadence.

The regulatory mapping layer (L4) cross-references the flagged transactions against the knowledge graph's representation of OECD Transfer Pricing Guidelines, ARM's length principle

10.48047/jocaaa.2026.35.05.05

requirements, and applicable local tax authority guidance, automatically generating a remediation checklist. The audit trail layer (L5) indexes the full event sequence for natural language query. A tax analyst can subsequently retrieve the complete compliance event history without writing a single database query.

B. Key Insight: Infrastructure Drift as a Compliance Risk Class

The case illustrates a compliance risk class that is systematically underaddressed by traditional and rule-based systems: infrastructure drift during ERP transitions. When ERP schema changes invalidate the assumptions embedded in rule-based compliance controls, those controls fail silently—they do not fire, because the data they are designed to evaluate no longer arrives in the expected format. The ACIG ingestion layer's schema drift detection capability addresses this failure mode directly, treating schema integrity as a first-class compliance signal.

This insight is directly motivated by the author's experience stabilizing the AX Interface platform during a period of critical instability caused by schema mismatches between home-grown custom ERP system and Microsoft Dynamics AX finance modules—a real-world instance of the failure class the ACIG framework is designed to prevent.

9. ARCHITECTURE EVALUATION

This section provides a systematic evaluation of the ACIG framework against two prevalent compliance architecture paradigms: traditional compliance (periodic audit-centric governance with manual controls) and rule-based systems (automated control execution without AI/ML components). The evaluation is structured across nine compliance dimensions. Table 4 summarizes the comparison; Figure 3 provides a visual capability score representation.

TABLE 4 — ARCHITECTURE COMPARISON: TRADITIONAL vs. RULE-BASED vs. ACIG

Evaluation Dimension	Traditional Compliance	Rule-Based Systems	ACIG Framework
Detection Latency	Days–Weeks	Hours–Days	Minutes (realtime)
Anomaly Detection	✗	✗	✓
Regulatory Adaptability	Manual, slow	Semiautomated	AI-assisted, rapid
Explainability	N/A	✓	✓
Predictive Capability	✗	✗	✓
NL Audit Query	✗	✗	✓

10.48047/jocaaa.2026.35.05.05

ERP Schema Drift Detection	X	Partial	✓
Scalability	Low	Moderate	High (cloudnative)
Federated Learning Ready	X	X	✓



Fig. 3. Architecture Capability Comparison — Grouped bar chart (left) and feature matrix (right) comparing Traditional Compliance, Rule-Based Systems, and the ACIG Framework across nine governance dimensions. Scores are conceptual assessments, not empirical measurements.

A. Detection Latency

Traditional compliance systems detect control failures primarily during periodic audit cycles, resulting in detection latencies of days to weeks. Rule-based systems improve this through automated control execution, reducing latency to hours or days for predefined rule triggers. The ACIG framework's continuous ingestion and monitoring layers enable detection latency measured in minutes for all transaction types, including previously undetected failure classes such as schema drift.

B. Anomaly Detection and Regulatory Adaptability

Neither traditional nor rule-based systems incorporate ML-based anomaly detection; both are bounded by their pre-defined rule sets and therefore cannot detect novel or emergent failure patterns. The ACIG anomaly detection ensemble—Isolation Forest, LSTM, and Autoencoder—operates without requiring predefined failure signatures, enabling detection of previously unobserved compliance anomalies. Regulatory adaptability follows a similar pattern: traditional systems require manual rule updates, rule-based systems support semi-automated updates, and the

10.48047/jocaaa.2026.35.05.05

ACIG regulatory mapping layer's NLP-driven knowledge graph enables near-autonomous regulatory change propagation.

C. Explainability and Auditability

Rule-based systems have a natural explainability advantage for their defined rule triggers—a compliance officer can always trace a rule-based flag to its triggering condition. The ACIG framework preserves this advantage via SHAP-based attribution for all ML-generated flags, ensuring that AI-generated determinations are as auditable as rule-based ones. The RAG-based audit query capability is unique to the ACIG framework, enabling natural language access to the full compliance event history that neither traditional nor rule-based systems can match.

D. Limitations of the Evaluation

The capability scores presented in Table 4 represent the author's qualitative assessment based on architectural analysis and practitioner experience; they are not derived from empirical benchmarking. The scores reflect the theoretical capability ceiling of each architecture paradigm, not the performance of any specific implementation. The evaluation should be treated as a structured framework for comparative analysis pending formal empirical validation, which is identified as a priority for future work in Section 10.

10. DISCUSSION

A. Implications for Enterprise Finance Functions

The ACIG framework, if fully realized, represents a fundamental reconfiguration of the enterprise finance function. Financial close cycles can be compressed significantly when compliance monitoring is continuous and reconciliation exceptions are surfaced in real time. Industry benchmarks from Deloitte [8] indicate that early enterprise deployments of AI-assisted financial close have demonstrated cycle time reductions of 30 to 50 percent; these figures represent external industry benchmarks and are not claimed results of the ACIG framework itself, which has not yet undergone empirical validation. They are cited to establish the plausibility of anticipated efficiency gains.

The predictive governance capability has particular strategic value for organizations navigating regulatory transitions—such as new transfer pricing requirements or emerging digital services tax regimes—where modeling compliance exposure before regulations take effect enables proactive structural adjustments rather than reactive remediation.

B. Limitations and Future Work

Several limitations merit acknowledgement. First, the framework presupposes a baseline level of data infrastructure maturity that many mid-market enterprises have not yet achieved. Second, the regulatory knowledge graph requires ongoing curation by compliance specialists. Third, and most critically, the framework does not yet address the governance of the AI systems themselves. The Federal Reserve's SR 11-7 guidance [10] establishes foundational expectations for model risk management: model validation, ongoing performance monitoring, conceptual soundness review, and clear ownership accountability. An AI governance extension to ACIG would constitute a seventh layer—an AI Model Governance layer—maintaining a model inventory, specifying validation protocols for each model type, defining risk thresholds that trigger retraining or human escalation, and assigning model risk officer ownership. This extension is the most important direction for future work.

Additional future directions include empirical validation of the CIMM, standardized benchmarks for ACIG layer performance, and exploration of federated learning [15] for cross-industry compliance intelligence without sharing proprietary financial data. The RAG-based audit query system warrants dedicated evaluation against enterprise knowledge retrieval benchmarks.

11. CONCLUSION

This paper has presented the Adaptive Compliance Intelligence and Governance (ACIG) framework, a conceptual architecture that positions AI and machine learning as foundational components of enterprise financial compliance. The framework's six-layer structure—spanning intelligent data ingestion, real-time monitoring, anomaly detection, regulatory mapping, audit trail intelligence, and predictive governance—provides a coherent blueprint for transitioning from reactive, audit-centric compliance to continuous, intelligence-driven governance.

The paper's five primary contributions—the ACIG reference architecture, the continuous compliance paradigm, the integrated XAI/knowledge graph/RAG governance model, the CIMM maturity model, and the simulated case study with comparative evaluation—collectively establish a foundation for empirical validation and enterprise adoption. The simulated transfer pricing case study demonstrates the framework's unique ability to address infrastructure-drift-induced compliance failures, a risk class systematically underaddressed by existing paradigms.

The imperative for this transformation is clear. Regulatory environments are growing more complex; transactional volumes are increasing; audit expectations are rising. Organizations that treat compliance as a static control problem will find themselves perpetually behind. Those that invest in AI-driven compliance intelligence will achieve a durable regulatory advantage: a governance capability that learns, adapts, and improves faster than the regulatory environment it must navigate.

10.48047/jocaaa.2026.35.05.05

The author invites collaboration from enterprise architecture, AI research, and financial governance communities to empirically validate, extend, and refine the ACIG framework across diverse organizational contexts.

REFERENCES

- [1] M. Protiviti and D. Beasley, "Internal audit and financial controls in a digital age," Protiviti Risk & Business Consulting, Technical Report, 2023.
- [2] KPMG International, "The future of compliance: From periodic reviews to continuous assurance," KPMG Insights Series, 2022.
- [3] N. Bhatt, R. Sharma, and K. Patel, "Gradient boosting models for revenue recognition anomaly detection in ERP systems," in Proc. IEEE International Conference on Big Data, 2022, pp. 1124–1131.
- [4] R. Kumar and J. Schoenfeld, "Graph neural networks for related-party transaction detection in corporate financial ecosystems," Journal of Financial Data Science, vol. 5, no. 2, pp. 88–107, 2023.
- [5] S. Agrawal and H. Li, "Transformer-based NLP for automated internal control to regulatory framework mapping," in Proc. AAAI Workshop on AI in Finance, 2023, pp. 44–52.
- [6] Gartner, Inc., "Gartner AI maturity model: Assessing organizational readiness for enterprise AI," Gartner Research, Stamford, CT, 2023.
- [7] CMMI Institute, "Data management maturity model (DMM)," CMMI Institute Technical Framework, v1.1, 2021.
- [8] Deloitte Consulting, "AI-powered financial close: Benchmarks and best practices from 200 global finance transformations," Deloitte Insights, 2024.
- [9] P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer, Cham, 2017.
- [10] Federal Reserve System, "SR 11-7: Guidance on model risk management," Board of Governors of the Federal Reserve System, 2011, updated 2021.

10.48047/jocaaa.2026.35.05.05

- [11] A. B. Arrieta et al., "Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," *Information Fusion*, vol. 58, pp. 82–115, 2020.
- [12] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in *Advances in Neural Information Processing Systems (NeurIPS)*, 2017, pp. 4765–4774.
- [13] V. Frias-Martinez, E. Frias-Martinez, and N. Oliver, "Automated knowledge graph construction for regulatory compliance mapping," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 8, pp. 3812–3825, 2022.
- [14] P. Lewis et al., "Retrieval-augmented generation for knowledge-intensive NLP tasks," in *Advances in Neural Information Processing Systems (NeurIPS)*, 2020, pp. 9459–9474.
- [15] B. McMahan et al., "Communication-efficient learning of deep networks from decentralized data," in *Proc. International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2017, pp. 1273–1282.