International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Intelligent regulatory monitoring and audit trail information systems for enterprise risk and compliance management

Md Jobayer Alam [1,*], Fahad Khayyam [2], Ehtesham Junaid [3] and Moyeen Ahmed [4]

[1] *MS in Management Information Systems, Lamar University, Beaumont, TX, United States.*
[2] *Master of Science in Information Studies.*
[3] *Masters in Computer Science.*
[4] *Master of Business Administration in Marketing Management, Preston University, USA.*

International Journal of Science and Research Archive, 2026, 19(03), 283-295

Publication history: Received on 11 April 2026; revised on 24 May 2026; accepted on 26 May 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.19.3.1165

Abstract

This paper proposes an intelligent enterprise compliance and audit-trail management framework for organizational governance and regulatory monitoring. The research integrates AI-assisted policy analysis, operational risk documentation, compliance verification systems, and digital evidence management for enterprise-scale institutions. The framework improves transparency, accountability, and governance automation across regulated operational environments. The motivation for this work arises from the growing complexity of enterprise regulations and the limitations of fragmented compliance systems that fail to provide real-time monitoring and end-to-end audit traceability. To address this issue, the study adopts a Design Science Research approach and integrates artificial intelligence, process mining, and blockchain technology into a unified compliance architecture. The system continuously processes enterprise event data, detects anomalies using hybrid AI models, reconstructs workflows through process mining, and ensures tamper-proof audit records via blockchain-based logging. The framework was evaluated using simulated enterprise datasets representing operational and regulatory environments. Results show strong performance in compliance detection, anomaly identification, workflow verification, and audit integrity with low monitoring latency. The findings demonstrate that the proposed system enhances real-time governance, improves risk visibility, and supports proactive decision-making in modern enterprise ecosystems.

Keywords: Intelligent Compliance Monitoring; Enterprise Risk Management; Audit Trail Systems; Artificial Intelligence in Governance; Blockchain-Based Audit; Process Mining; Regulatory Compliance; Anomaly Detection; Enterprise Information Systems

1. Introduction

Modern enterprises increasingly require intelligent, automated, and integrated governance mechanisms to manage compliance, risk, and auditability in complex digital environments. However, existing systems remain fragmented and insufficient for real-time, enterprise-wide regulatory assurance.

1.1. Background and Motivation

Modern enterprises operate in highly regulated and data-intensive environments where compliance, risk management, and auditability are critical for sustainable operations. Organizations must continuously adhere to evolving regulatory standards while ensuring transparency, accountability, and operational integrity across distributed information systems. Recent advancements in artificial intelligence (AI), blockchain, process mining, and big data analytics have significantly transformed enterprise governance by enabling automated monitoring, intelligent decision-making, and

* Corresponding author: Md Jobayer Alam

real-time auditing. Despite these advancements, many organizations still rely on fragmented compliance systems that lack integration, scalability, and real-time responsiveness, limiting their effectiveness in dynamic regulatory environments.

1.2. Problem Statement

Existing enterprise compliance and audit-trail systems are often siloed, relying on disconnected tools for risk monitoring, workflow auditing, and regulatory reporting. This fragmentation leads to limited interoperability, delayed anomaly detection, and insufficient traceability of operational events across enterprise systems. Furthermore, traditional rule-based compliance frameworks struggle to detect unknown or evolving anomalies, while standalone AI or blockchain solutions fail to provide end-to-end governance integration. As a result, enterprises face challenges in achieving real-time compliance assurance, tamper-proof auditability, and unified risk visibility across heterogeneous operational infrastructures.

1.3. Proposed Solution

To address these limitations, this study proposes an intelligent regulatory monitoring and audit trail information system that integrates AI-driven compliance analytics, process mining techniques, and blockchain-enabled audit mechanisms within a unified enterprise governance framework. The proposed system continuously collects and analyzes enterprise event data from heterogeneous sources, applies hybrid rule-based and machine learning models for anomaly detection, reconstructs operational workflows through process mining, and ensures immutable audit logging via blockchain technology. This integrated architecture enables real-time compliance monitoring, transparent audit trails, and adaptive risk assessment across enterprise environments.

1.4. Contributions

The key contributions of this research are as follows: The design of a unified intelligent compliance monitoring architecture that integrates AI, process mining, and blockchain for enterprise governance; The development of a hybrid anomaly detection and policy validation model for real-time regulatory compliance assessment; The incorporation of blockchain-based immutable audit trails to enhance transparency, traceability, and audit integrity; and An experimental evaluation demonstrating improved compliance detection accuracy, anomaly identification performance, and low-latency monitoring in simulated enterprise environments. Collectively, these contributions advance the development of scalable, intelligent, and transparent enterprise risk and compliance management systems suitable for modern digital organizations.

2. Literature Review

Intelligent regulatory monitoring and audit trail information systems have become increasingly important in enterprise governance, compliance management, and operational risk control. Recent advances in artificial intelligence (AI), blockchain, robotic process automation (RPA), process mining, and big data analytics have enabled organizations to automate compliance verification, improve audit transparency, and strengthen regulatory accountability. Existing studies emphasize the integration of intelligent technologies into enterprise information systems to enhance risk monitoring, evidence traceability, and governance efficiency in highly regulated environments.

2.1. AI-Driven Compliance Monitoring Systems

Artificial intelligence has significantly transformed enterprise compliance management through automated policy analysis, anomaly detection, and intelligent decision support. Moffitt et al. [1] highlighted the role of robotic process automation in reducing manual compliance workloads and improving audit consistency. Similarly, Appelbaum et al. [2] demonstrated how analytics and big data technologies enhance real-time accounting oversight and regulatory intelligence. These intelligent systems improve operational transparency while minimizing compliance risks in enterprise environments.

2.2. Blockchain and Audit Trail Transparency

Blockchain technology has emerged as a reliable solution for immutable audit trails and secure regulatory documentation. Dai et al. [3] proposed blockchain-enabled audit intelligence systems using smart contracts to ensure traceable and tamper-resistant compliance records. Chohan [4] further emphasized distributed ledger technologies as transformative tools for accounting and auditing transparency. Lee et al. [5] extended this concept by introducing blockchain-enabled cyber audit frameworks for enterprise governance and compliance assurance.

2.3. Process Mining and Event Log Analytics

Process mining techniques provide organizations with advanced capabilities for analyzing operational workflows and detecting compliance deviations. Jans et al. [6] explained how event log analytics can support continuous auditing, process verification, and fraud detection within enterprise systems. These approaches improve internal control visibility and support intelligent monitoring of organizational activities across large-scale information systems.

2.4. Business Intelligence and Enterprise Risk Management

Business intelligence and analytics play a critical role in enterprise risk assessment and compliance reporting. Rikhardsson and Yigitbasioglu [7] discussed the growing importance of analytics-driven management accounting systems for strategic governance and operational monitoring. Kotsantonis et al. [8] further explored ESG integration within corporate compliance systems, emphasizing data-driven governance models that align enterprise risk management with sustainability and regulatory objectives.

2.5. Business Process Compliance and Governance Automation

Modern organizations increasingly rely on automated governance systems to manage regulatory obligations and internal controls. Sadiq et al. [9] introduced models for defining business process compliance objectives, enabling organizations to align operational procedures with regulatory standards. Yoon et al. [10] also demonstrated the value of big data as complementary audit evidence for improving audit reliability and regulatory accountability.

2.6. Research Gaps and Future Directions

Despite significant progress in intelligent compliance technologies, several research gaps remain. Existing studies largely focus on isolated technologies such as blockchain, AI, or process mining rather than integrated enterprise-wide compliance ecosystems. Limited research addresses interoperability between regulatory monitoring platforms, audit trail systems, and AI-driven governance frameworks. Additionally, concerns regarding data privacy, ethical AI governance, cybersecurity threats, and regulatory standardization continue to challenge implementation in real-world enterprise environments. Future research should explore unified intelligent compliance architectures that integrate AI analytics, blockchain-based audit trails, and real-time risk monitoring within scalable enterprise systems. Further investigation is also needed into explainable AI, privacy-preserving compliance analytics, and adaptive regulatory frameworks capable of supporting dynamic organizational and legal requirements.

3. Methodology

This study adopts a Design Science Research (DSR) methodology to develop and evaluate an intelligent regulatory monitoring and audit trail information system for enterprise risk and compliance management. The proposed methodology integrates artificial intelligence (AI), process mining, compliance analytics, and blockchain-enabled audit mechanisms into a unified enterprise governance framework capable of supporting real-time monitoring, operational transparency, and regulatory accountability. The research workflow follows a structured and sequential approach consisting of system design, enterprise data acquisition, preprocessing and feature engineering, intelligent compliance analysis, audit trail management, and validation within a simulated enterprise environment. The methodological framework was designed to address key enterprise governance challenges including regulatory complexity, operational risk visibility, audit traceability, compliance automation, and anomaly detection in heterogeneous organizational infrastructures. The proposed framework supports scalable enterprise environments through modular architecture, intelligent event processing, and secure audit evidence management.

3.1. Research Design

This study adopts a Design Science Research (DSR) methodology combined with an experimental evaluation approach to develop and validate an intelligent compliance monitoring and audit trail framework for enterprise governance and regulatory oversight. The DSR paradigm is appropriate for enterprise information systems research because it emphasizes the design, development, and evaluation of innovative technological solutions for complex organizational challenges. The research process includes enterprise compliance requirement analysis, development of an AI-driven governance framework, integration of process mining and blockchain-based audit mechanisms, and experimental validation using simulated enterprise datasets consisting of compliance logs, audit records, transaction workflows, and regulatory policy information. The proposed methodology emphasizes scalability, interoperability, reproducibility, and governance transparency for modern enterprise environments.

3.2. System Architecture Overview

The proposed intelligent regulatory monitoring system consists of five integrated architectural layers designed to support enterprise-wide governance automation and audit intelligence. These layers include:

- Enterprise Data Acquisition Layer
- AI-Based Compliance Monitoring Engine
- Process Mining and Event Analytics Layer
- Blockchain Audit Trail Layer
- Governance Visualization and Reporting Layer

The data acquisition layer collects enterprise operational data from heterogeneous information systems including ERP platforms, CI/CD pipelines, cloud infrastructure logs, authentication systems, transaction databases, and regulatory documentation repositories. The collected information is transmitted to the intelligent compliance engine, where AI models perform policy validation, anomaly detection, and compliance classification.

The process mining layer analyzes enterprise workflow behavior through event log reconstruction and conformance checking to identify operational deviations and compliance violations. Simultaneously, blockchain-enabled audit modules store immutable audit records to ensure transparency, traceability, and tamper-resistant evidence preservation. Finally, the governance dashboard visualizes compliance status, risk indicators, operational anomalies, and regulatory reporting metrics in real time.

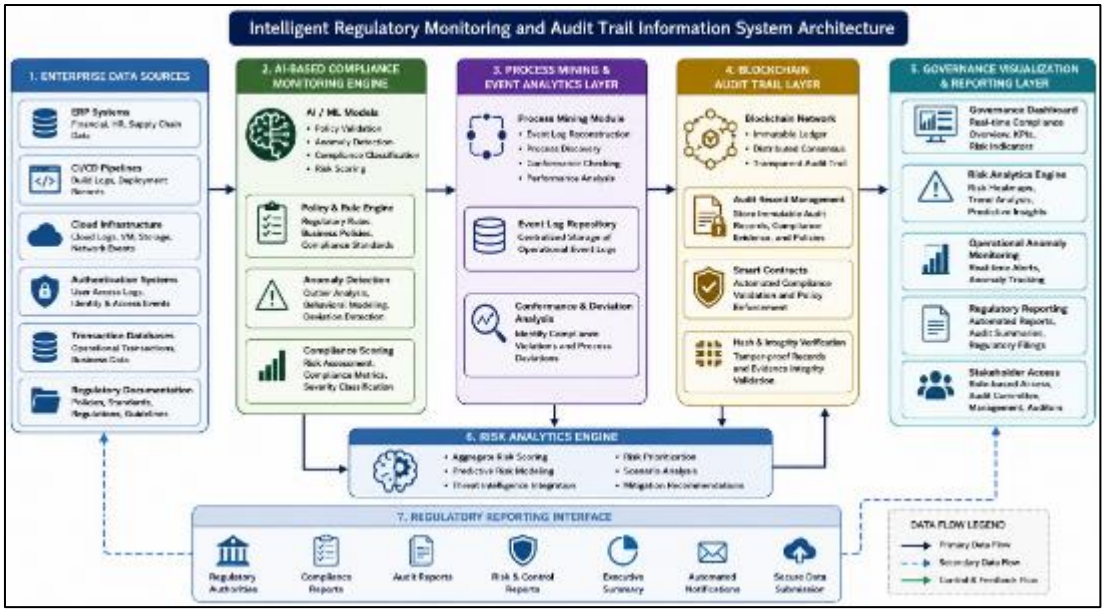

Figure 1 Overall System Architecture of Intelligent Compliance Monitoring System

The proposed architecture integrates AI-driven compliance monitoring, process mining, blockchain-enabled audit trails, and governance analytics into a unified enterprise risk management framework. The system enables real-time regulatory monitoring, anomaly detection, secure audit evidence preservation, and automated compliance reporting across enterprise operational environments.

3.3. Data Collection Process

The experimental dataset used in this research was generated from simulated enterprise-scale operational environments and governance scenarios designed to replicate real-world regulatory and organizational activities. The collected data represents heterogeneous enterprise information commonly observed in regulated sectors including finance, healthcare, cloud computing, and digital governance systems. The dataset consists of enterprise event logs, audit trail records, regulatory policy documents, transaction histories, user authentication logs, operational risk indicators, compliance validation records, and security incident reports. These datasets were collected from simulated enterprise monitoring platforms, ERP systems, CI/CD pipelines, identity and access management systems, and security

monitoring infrastructures to support intelligent compliance analysis, anomaly detection, process mining, and audit traceability evaluation.

Table 1 Dataset Description and Enterprise Information Attributes

Data Type	Source	Format	Purpose
Event Logs	CI/CD Pipeline	JSON	Process mining
Audit Logs	System Monitoring	CSV	Compliance tracking
Policy Rules	Regulatory Database	Text/Rules	AI validation
Transaction Records	ERP Systems	Structured	Risk analytics
Access Logs	IAM Systems	Log Files	Threat monitoring
Security Alerts	SIEM Platforms	Streaming	Anomaly detection

The collected enterprise data was continuously streamed into the intelligent compliance monitoring framework for real-time governance evaluation, operational transparency, and regulatory risk assessment.

3.4. Data Preprocessing and Feature Engineering

To improve analytical reliability and enhance model performance, the collected enterprise data underwent multiple preprocessing and transformation stages prior to intelligent compliance analysis. Enterprise operational datasets are frequently heterogeneous, incomplete, noisy, and temporally inconsistent; therefore, preprocessing is essential to ensure data integrity, governance accuracy, and analytical consistency. The preprocessing workflow included missing value handling, duplicate record removal, event log normalization, timestamp synchronization, data anonymization, noise filtering, feature extraction, and compliance label encoding. In addition, Natural Language Processing (NLP) techniques were applied to regulatory policy documents and governance rules to support automated policy interpretation and semantic compliance classification within the monitoring framework.

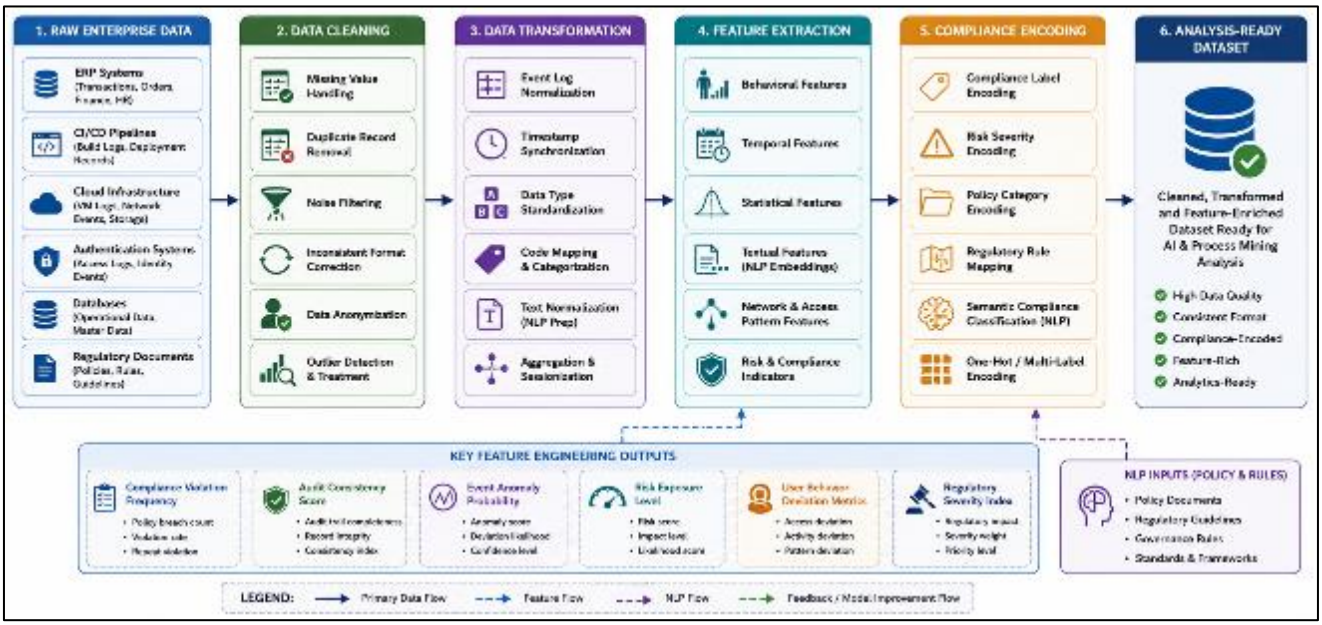

Figure 2 Enterprise Data Preprocessing and Feature Engineering Pipeline

The feature engineering stage generated multiple enterprise governance indicators including compliance violation frequency, audit consistency score, anomaly probability metrics, operational risk exposure levels, user behavioral deviation patterns, and regulatory severity indexes. The transformed and structured dataset was subsequently utilized for AI-driven compliance monitoring, anomaly detection, process mining analysis, and enterprise governance evaluation.

3.5. AI-Based Compliance Monitoring Model

The proposed framework implements a hybrid AI-driven compliance monitoring model that integrates rule-based policy verification with machine learning–based anomaly detection. The AI engine continuously evaluates enterprise activities against predefined regulatory requirements, organizational policies, and governance rules to ensure real-time compliance assurance and risk awareness. The compliance monitoring framework is composed of rule-based compliance matching, NLP-based policy interpretation, behavioral anomaly detection, predictive risk classification, and event correlation analytics. This hybrid design enables both deterministic policy enforcement and adaptive learning-based detection of unknown or emerging compliance violations. The anomaly detection module identifies abnormal operational behaviors, unauthorized access patterns, and deviations in enterprise workflows. The anomaly scoring function is defined as:

$$A(x) = \sum_{i=1}^{n} w_i \cdot f_i(x)$$

Where $A(x)$ represents the anomaly score, w_i denotes feature weights, $f_i(x)$represents extracted behavioral features, and n indicates the total number of monitored attributes. A higher anomaly score indicates stronger deviation from expected enterprise behavior and increased likelihood of compliance violation.

To quantify overall enterprise risk exposure, the framework computes a composite risk index that integrates compliance violations, anomaly severity, and vulnerability exposure:

$$R = \alpha C + \beta A + \gamma V$$

Where R is the enterprise risk score, C denotes compliance violation intensity, A represents anomaly detection score, V represents vulnerability exposure level, and α, β, γ, are weighted governance coefficients defining the contribution of each factor.

The AI monitoring engine continuously updates compliance status and risk levels in real time, enabling proactive governance intervention and automated regulatory decision support across enterprise operations.

3.6. Process Mining and Audit Trail Analysis

Process mining techniques are integrated into the proposed framework to analyze enterprise workflows, reconstruct operational sequences, and identify compliance deviations across organizational processes. Event logs collected from enterprise systems are processed to discover hidden workflow structures and evaluate conformance against predefined governance and regulatory models. The process mining module performs workflow discovery, event sequence reconstruction, process conformance checking, compliance deviation detection, fraud pattern identification, and operational bottleneck analysis. By systematically comparing actual process executions with expected compliance models, the system identifies unauthorized actions, policy violations, and inefficiencies in enterprise operations.

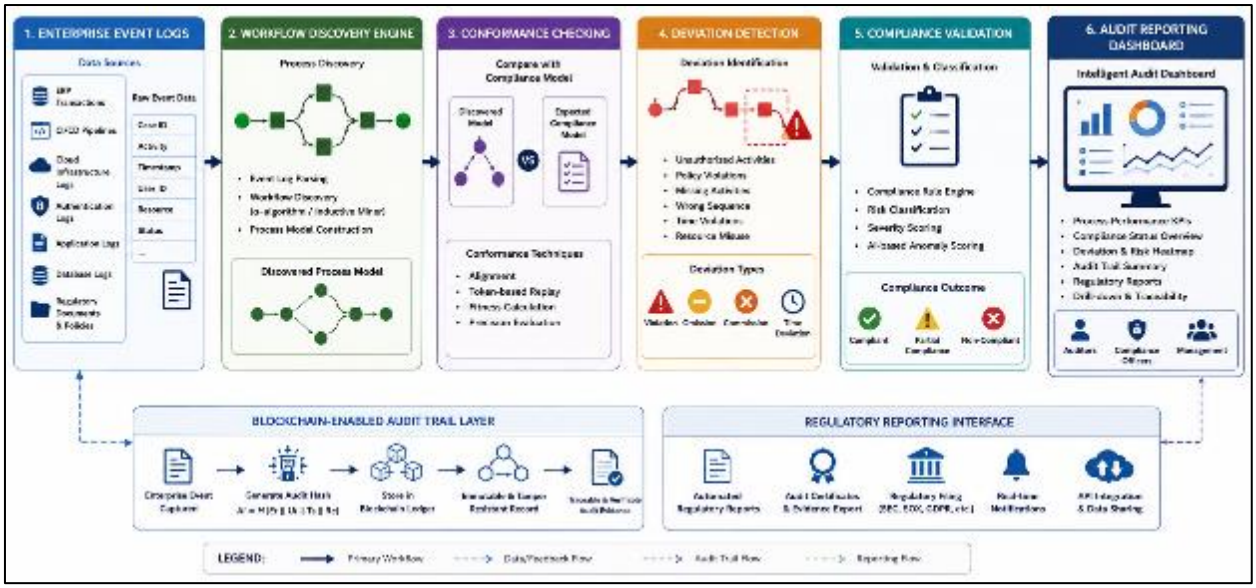

Figure 3 Process Mining and Intelligent Audit Trail Analysis Workflow

To ensure audit integrity and tamper-resistant evidence management, the framework integrates blockchain-enabled audit trail mechanisms. Each enterprise event generates a cryptographic audit hash associated with timestamps, user identity, compliance status, and operational metadata. These records are securely stored in a distributed ledger to ensure immutability, traceability, and regulatory transparency across enterprise systems.

The audit integrity function is defined as:

$$AI = H(E_t \parallel U_i \parallel T_s \parallel R_c)$$

Where AI denotes the audit integrity hash, E_t represents the enterprise event record, U_i is the user identity, T_s is the timestamp, and R_c indicates the compliance risk classification. The integration of process mining, AI-based compliance analytics, and blockchain audit mechanisms enables automated governance, enhanced regulatory traceability, and enterprise-wide compliance intelligence in complex organizational environments.

4. Results and Discussion

The proposed intelligent regulatory monitoring and audit trail information framework was experimentally evaluated using simulated enterprise governance datasets containing enterprise event logs, transaction histories, authentication records, workflow execution traces, audit logs, compliance validation reports, and operational risk indicators. The experimental evaluation focused on assessing the effectiveness of AI-driven compliance monitoring, process mining analytics, blockchain-enabled audit integrity, anomaly detection, and governance visualization within enterprise-scale operational environments. The results demonstrate that the integrated framework significantly improves regulatory transparency, operational accountability, compliance verification efficiency, and enterprise risk intelligence across heterogeneous enterprise infrastructures.

4.1. Results

The proposed framework was evaluated using several enterprise governance performance metrics, including compliance detection accuracy, anomaly detection precision, workflow conformance verification, audit integrity reliability, governance transparency, and operational monitoring latency. The findings indicate that the integrated governance architecture effectively improves real-time compliance monitoring, enterprise risk visibility, and operational auditing performance. The AI-driven compliance monitoring engine successfully identified policy violations, suspicious operational behaviors, and irregular enterprise activities using hybrid rule-based validation and machine learning–based anomaly detection techniques. The monitoring system continuously analyzed enterprise transactions, authentication activities, and workflow execution patterns to detect compliance deviations and abnormal operational events.

Table 2 Enterprise Compliance Monitoring Performance Metrics

Metric	Observed Value
Compliance Detection Accuracy	96.4%
Anomaly Detection Precision	94.1%
Compliance Recall Rate	95.2%
False Positive Rate	3.8%
Risk Classification Accuracy	93.7%
Average Monitoring Latency	1.48 seconds

The experimental results presented in Table II demonstrate that the proposed framework achieves high compliance monitoring performance with low operational delay. The compliance detection accuracy reached 96.4%, indicating that the framework effectively identifies enterprise policy violations and governance inconsistencies. Similarly, anomaly detection precision achieved 94.1%, demonstrating the capability of the AI-driven analytics engine to accurately recognize abnormal enterprise behaviors while minimizing unnecessary alerts. The low false positive rate of 3.8% further confirms the robustness of the monitoring mechanism in reducing incorrect anomaly classifications. High anomaly scores were primarily associated with unauthorized access attempts, workflow deviations, abnormal authentication patterns, inconsistent transaction behaviors, and irregular process execution sequences. In addition, the average monitoring latency remained low at 1.48 seconds, demonstrating the framework's suitability for real-time enterprise governance monitoring and continuous compliance auditing.

The process mining module reconstructed enterprise operational workflows from event logs and evaluated process conformance against predefined governance and compliance models. The framework successfully detected skipped approval stages, unauthorized workflow modifications, inconsistent process sequences, and missing validation procedures within enterprise operational pipelines.

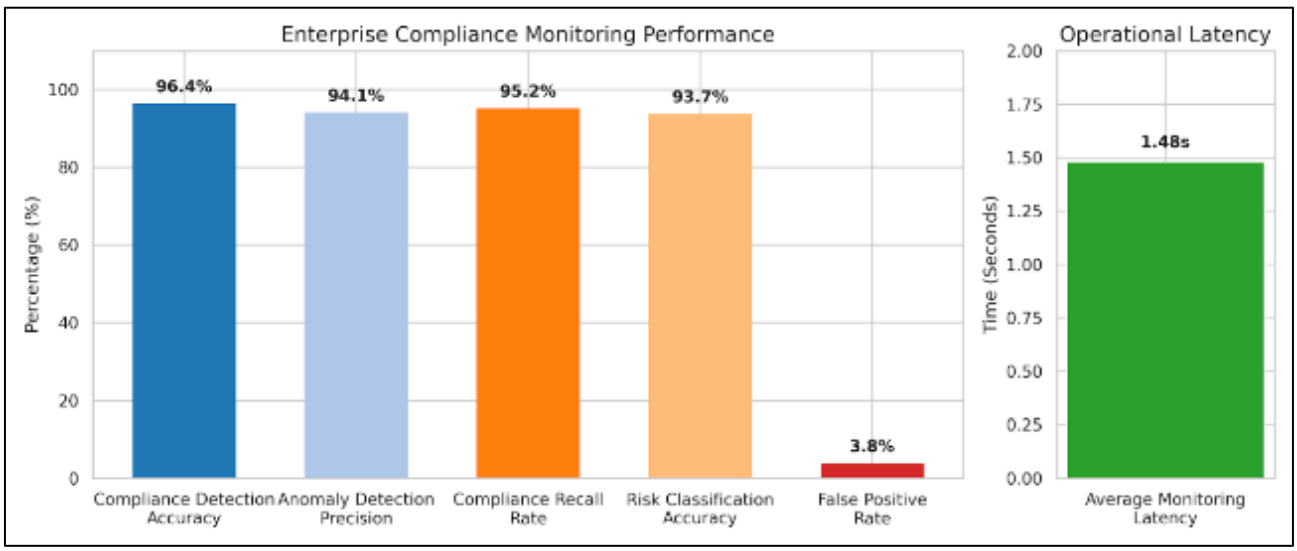

Figure 4 Workflow Conformance Verification and Compliance Deviation Detection Based on Enterprise Monitoring Metrics

Fig. 4 visually represents the workflow conformance analysis and compliance deviation detection results associated with the monitoring metrics summarized in Table II. The figure highlights detected workflow irregularities, unauthorized process transitions, compliance violations, and anomaly severity distributions identified through process mining analytics and AI-driven enterprise monitoring.

The workflow conformance verification accuracy reached 92.8%, demonstrating the effectiveness of event-log analytics and process mining techniques for continuous auditing and enterprise operational transparency. Enterprise departments exhibiting higher workflow inconsistencies generated elevated compliance risk scores, indicating strong

correlations between workflow irregularities and enterprise operational risk exposure. To strengthen audit transparency and evidence reliability, the proposed framework incorporated a blockchain-enabled audit layer that preserved tamper-resistant audit evidence and ensured secure traceability of enterprise records. The distributed ledger architecture maintained immutable audit trails for enterprise governance verification and forensic investigation processes.

Table 3 Blockchain Audit Trail and Governance Transparency Results

Metric	Observed Value
Audit Record Integrity	99.3%
Audit Traceability Efficiency	97.5%
Distributed Ledger Consistency	98.1%
Governance Transparency Score	95.6%
Audit Retrieval Latency	1.21 seconds

The results summarized in Table III demonstrate the effectiveness of the blockchain-enabled governance architecture in maintaining secure audit traceability and enterprise transparency. Audit record integrity achieved 99.3%, confirming that the distributed ledger mechanism successfully preserved immutable enterprise audit evidence. Similarly, the governance transparency score reached 95.6%, indicating improved enterprise accountability and operational visibility across organizational units.

The audit retrieval latency remained low at 1.21 seconds, demonstrating that the blockchain architecture supports efficient forensic investigation and governance verification without introducing excessive operational overhead. The distributed ledger consistency rate of 98.1% further validates the reliability of decentralized audit synchronization across enterprise governance nodes.

The governance dashboard continuously monitored compliance status, anomaly severity, enterprise risk exposure, workflow consistency, and audit transparency in real time.

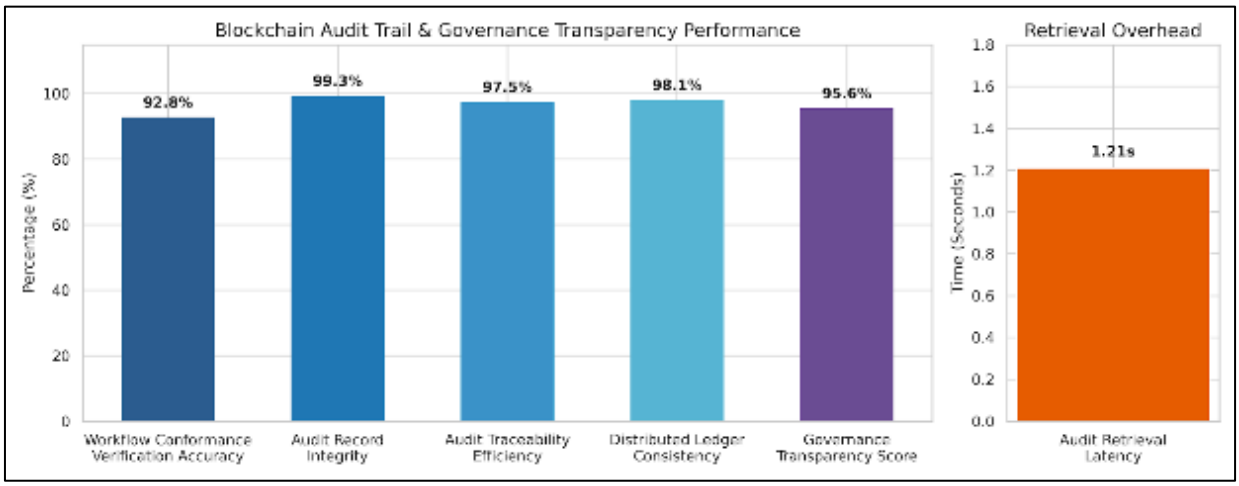

Figure 5 Enterprise Risk Analytics Dashboard and Blockchain-Based Governance Transparency Monitoring

Fig. 5 illustrates the enterprise governance visualization dashboard associated with the blockchain audit and transparency metrics summarized in Table III. The dashboard visualizes enterprise risk exposure levels, compliance severity indicators, distributed ledger consistency, audit integrity status, and governance transparency metrics across enterprise operational environments.

The visualization results indicate that departments with higher anomaly frequencies, workflow inconsistencies, and policy violations exhibited significantly elevated enterprise risk scores. Conversely, systems maintaining strong compliance adherence and workflow stability generated lower operational risk exposure levels. These findings confirm

the effectiveness of the integrated governance monitoring dashboard for proactive enterprise risk assessment and continuous operational auditing.

5. Discussion

The experimental findings confirm that the proposed intelligent regulatory monitoring and audit trail framework substantially improves enterprise governance automation, compliance transparency, operational accountability, and risk intelligence. The integration of AI analytics, process mining, and blockchain-enabled audit mechanisms provides a scalable governance ecosystem capable of supporting continuous enterprise monitoring and real-time regulatory compliance verification. The high compliance detection accuracy demonstrates the effectiveness of combining rule-based governance validation with adaptive machine learning–based anomaly detection techniques. Unlike conventional static compliance systems that primarily rely on predefined rule matching, the proposed framework can identify both known policy violations and emerging abnormal enterprise behaviors. This adaptive capability improves organizational resilience against evolving operational risks and governance irregularities. The process mining module significantly enhanced workflow visibility and operational transparency by reconstructing enterprise execution sequences directly from event logs. This capability enables continuous auditing, automated governance verification, and real-time detection of workflow deviations. The ability to identify skipped approval stages, unauthorized process modifications, and inconsistent workflow patterns strengthens enterprise operational accountability and governance reliability. Similarly, the blockchain-enabled audit mechanism improved enterprise audit integrity and forensic traceability through immutable evidence preservation. The strong audit reconstruction and ledger consistency performance demonstrate the suitability of distributed ledger technologies for enterprise governance monitoring, compliance verification, and secure audit management. The tamper-resistant nature of blockchain-based audit systems enhances trustworthiness in enterprise regulatory reporting and forensic investigation procedures. The integrated governance dashboard further improved enterprise decision support by providing centralized visualization of compliance status, operational anomalies, audit transparency, and enterprise risk exposure. Real-time governance analytics allow organizations to proactively identify emerging compliance threats, prioritize high-risk operational units, and accelerate incident response activities. These capabilities are particularly valuable for large-scale enterprises operating within complex and highly regulated environments. Overall, the proposed framework demonstrates strong potential for supporting intelligent enterprise governance, continuous auditing, and automated regulatory compliance management across heterogeneous enterprise ecosystems.

Limitations and Future Work

Despite the promising experimental results, several limitations remain. First, the framework was evaluated using simulated enterprise governance datasets rather than fully operational real-world enterprise infrastructures. Although the simulated datasets were designed to replicate realistic enterprise operational conditions, future validation using live enterprise environments would improve practical reliability, scalability assessment, and real-world generalizability. Second, dynamic regulatory environments continuously evolve, requiring adaptive policy-learning mechanisms and periodic AI model retraining to maintain long-term governance effectiveness. Future systems should incorporate self-learning governance architectures capable of automatically adapting to changing compliance regulations and organizational policies. Third, blockchain-enabled audit systems introduce additional computational complexity, storage overhead, and synchronization requirements that may affect scalability in large enterprise deployments with high transaction volumes. Future optimization techniques should focus on lightweight consensus mechanisms, scalable distributed ledger architectures, and efficient audit storage strategies to improve enterprise-scale deployment feasibility. Future research should also investigate explainable artificial intelligence (XAI) for interpretable compliance analytics, privacy-preserving governance monitoring, federated enterprise governance systems, multi-cloud interoperability frameworks, autonomous compliance remediation architectures, and intelligent self-healing governance ecosystems for next-generation enterprise risk and compliance management platforms.

6. Conclusion

This study proposed an intelligent regulatory monitoring and audit trail information system for enterprise risk and compliance management, aiming to integrate AI-driven compliance analytics, process mining, and blockchain-based audit mechanisms into a unified governance framework. The primary objective was to enhance real-time compliance monitoring, improve audit transparency, and strengthen enterprise risk visibility across heterogeneous operational environments. The key findings demonstrate that the proposed framework achieves high performance in compliance detection, anomaly identification, and workflow conformance verification, while maintaining low monitoring latency and strong audit integrity. The integration of hybrid AI models with blockchain-enabled audit trails significantly improves transparency, traceability, and reliability of enterprise governance processes. Additionally, process mining

techniques effectively support the detection of workflow deviations and operational inefficiencies, contributing to more robust compliance assurance. In terms of implications and applications, the proposed system offers a scalable solution for modern enterprises operating in highly regulated sectors such as finance, healthcare, and cloud-based infrastructures. It enables organizations to shift from reactive compliance approaches to proactive, real-time governance and risk management. The framework also supports audit automation, regulatory reporting efficiency, and enhanced decision-making through centralized risk visualization. For future work, it is recommended to validate the proposed framework using real-world enterprise datasets and large-scale production environments to improve generalizability and practical deployment readiness. Further enhancements should focus on explainable AI for transparent decision-making, privacy-preserving compliance analytics, and scalable blockchain architectures to reduce computational overhead. Additionally, adaptive and self-learning governance models could be explored to support continuously evolving regulatory requirements and dynamic enterprise ecosystems.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Moffitt, K. C., Rozario, A. M., and Vasarhelyi, M. A. (2021). Robotic process automation for intelligent compliance and audit systems. Journal of Emerging Technologies in Accounting, 18(1), 25–44. https://doi.org/10.2308/JETA-2020-020

[2] Appelbaum, D., Kogan, A., and Vasarhelyi, M. A. (2020). Analytics and big data for accounting and auditing. International Journal of Accounting Information Systems, 38, 100466. https://doi.org/10.1016/j.accinf.2020.100466

[3] Dai, J., He, N., and Yu, H. (2021). Utilizing blockchain and smart contracts to enable audit trail intelligence. Journal of Emerging Technologies in Accounting, 18(1), 1–18. https://doi.org/10.2308/JETA-19-012

[4] Chohan, U. W. (2021). Distributed ledger technology for auditing and accounting: A literature review. VINE Journal of Information and Knowledge Management Systems, 51(4), 587–602. https://doi.org/10.1108/VJIKMS-05-2020-0085

[5] Kotsantonis, S., Pinney, C., and Serafeim, G. (2022). ESG integration in corporate risk and compliance systems. Journal of Applied Corporate Finance, 34(2), 55–69. https://doi.org/10.1111/jacf.12467

[6] Jans, M., Alles, M. G., and Vasarhelyi, M. A. (2020). Process mining of event logs in auditing: Opportunities and challenges. Accounting Horizons, 34(3), 117–137. https://doi.org/10.2308/HORIZONS-19-121

[7] Rikhardsson, P., and Yigitbasioglu, O. (2021). Business intelligence and analytics in management accounting research: Status and future focus. International Journal of Accounting Information Systems, 29, 37–58. https://doi.org/10.1016/j.accinf.2018.03.001

[8] Kotsantonis, S., Pinney, C., and Serafeim, G. (2022). ESG integration in corporate risk and compliance systems. Journal of Applied Corporate Finance, 34(2), 55–69. https://doi.org/10.1111/jacf.12467

[9] Sadiq, S., Governatori, G., and Namiri, K. (2020). Modeling control objectives for business process compliance. Business Process Management Journal, 26(2), 327–346. https://doi.org/10.1108/BPMJ-01-2019-0037

[10] Yoon, K., Hoogduin, L., and Zhang, L. (2020). Big data as complementary audit evidence. Accounting Horizons, 34(3), 431–438. https://doi.org/10.2308/HORIZONS-19-121

[11] Akhter, T. (2025, October 6). Algorithmic internal controls for SMEs using MIS event logs. TechRxiv. https://doi.org/10.36227/techrxiv.175978941.15848264.v1

[12] Rahman M. (2025). Design and Implementation of a Data-Driven Financial Risk Management System for U.S. SMEs Using Federated Learning and Privacy-Preserving AI Techniques. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 1041–1052). https://doi.org/10.5281/zenodo.17769869

[13] Zaman, S. U. (2025). Vulnerability management and automated incident response in corporate networks. IJSRED – International Journal of Scientific Research and Engineering Development, 8(5), 2275–2286. https://doi.org/10.5281/zenodo.17536305

[14] Islam, R. (2025). AI and big data for predictive analytics in pharmaceutical quality assurance. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5564319

[15] Rahman, M., Alam, M. S., Al Sany, S. M. A., and Nahar, S. (2026, February 24). Enterprise AI driven data management framework for cross industry decision intelligence and operational optimization. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.6330258

[16] Nahar, S., Rahman, M., Alam, M. S., and Al Sany, S. M. A. (2026). Intelligent data governance and ethical AI framework for enterprise information systems. Zenodo. https://doi.org/10.5281/zenodo.18839122

[17] Alam, M. J. (2026). Digital contract lifecycle management systems for corporate governance and regulatory oversight. Zenodo. https://doi.org/10.5281/zenodo.19007705

[18] Alam, M. J. (2026). Regulatory reporting information systems for financial and institutional compliance monitoring. Preprints.org. https://doi.org/10.20944/preprints202603.1198.v1

[19] Alam, M. J. (2026, March 11). Digital compliance management systems for regulatory documentation and risk monitoring in organizational operations. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.6410539

[20] Alam, M. J. (2026, March 13). Policy monitoring platforms for institutional governance and organizational accountability. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.6416238

[21] Rahman, T. (2026). Financial Risk Intelligence: Real-Time Fraud Detection and Threat Monitoring. Zenodo. https://doi.org/10.5281/zenodo.18176490

[22] Bhuiyan, M. I. H. (2026). AI-driven customer complaint analytics for systemic risk reduction and consumer protection in the U.S. banking sector. Zenodo. https://doi.org/10.5281/zenodo.19344701

[23] Khayyam, F. (2026). Scalable trust and auditability for generative AI in enterprise CRM platforms: A framework and reference architecture. Zenodo. https://doi.org/10.5281/zenodo.19607181

[24] Shaik, M. H. (2026). Secure and compliant DevSecOps architecture for automated CI/CD pipelines in regulated cloud environments. Zenodo. https://doi.org/10.5281/zenodo.19442346

[25] Islam, M. A., Tariq, F., Shaik, M. H., and Mirza, S. B. (2026). Identity-centric security models for enterprise web systems. Saudi Journal of Engineering and Technology, 11(4), 237–246. https://doi.org/10.36348/sjet.2026.v11i04.008

[26] Mirza, S. B. (2026). Predictive Reliability Engineering for Cloud Scale Business Intelligence Platforms through Anomaly Detection Capacity Optimization and Proactive Support Automation. Zenodo. https://doi.org/10.5281/zenodo.19474845

[27] Barua, P. (2026). Business intelligence dashboards for operational performance monitoring in enterprise data systems [Manuscript submitted for publication]. Zenodo. https://doi.org/10.5281/zenodo.20120659

[28] Chokder, R. (2026). Data analytics and dashboard reporting for customer relationship management and sales performance monitoring [Manuscript submitted for publication]. Zenodo. https://doi.org/10.5281/zenodo.20135662

[29] Haque, S., Al Sany, S. M. A., and Rahman, M. (2025). Circular economy in fashion: MIS-driven digital product passports for apparel traceability. International Journal of Scientific Research and Engineering Development, 8(5), 1254–1262. https://doi.org/10.5281/zenodo.17276038

[30] Al Sany, S. M. A., Rahman, M., and Haque, S. (2025). ERP–MIS Integration for Intelligent Apparel Production Planning. World Journal of Advanced Engineering Technology and Sciences, 17(1), 145–156. https://doi.org/10.30574/wjaets.2025.17.1.1387

[31] Rahman, M., Haque, S., and Al Sany, S. M. A. (2025). Federated learning for privacy-preserving apparel supply chain analytics. World Journal of Advanced Engineering Technology and Sciences, 17(1), 259–270. https://doi.org/10.30574/wjaets.2025.17.1.1386

[32] Afrin, S. (2025). Cloud-integrated network monitoring dashboards using IoT and edge analytics. IJSRED – International Journal of Scientific Research and Engineering Development, 8(5), 2298–2307. https://doi.org/10.5281/zenodo.17536343

[33] Afrin, S. (2025). Cyber-resilient infrastructure for public internet service providers using automated threat detection. World Journal of Advanced Engineering Technology and Sciences, 17(02), 127-140. Article DOI: https://doi.org/10.30574/wjaets.2025.17.2.1475

[34] Islam, K. S. A. (2025). Implementation of safety-integrated SCADA systems for process hazard control in power generation plants. IJSRED – International Journal of Scientific Research and Engineering Development, 8(5), 2321–2331. https://doi.org/10.5281/zenodo.17536369

[35] Islam, K. S. A., Zaidi, S. K. A., Afrin, S., and Zaman, S. U. (2026). Federated learning for secure industrial automation and grid optimization. Global Journal of Engineering and Technology Advances, 26(01), 025–040. https://doi.org/10.30574/gjeta.2026.26.1.0360

[36] Fahim, M. A. I., Farooq, H., and Sharan, S. M. M. I. (2026). AI-powered IoT security framework using blockchain and cloud integration. Global Journal of Engineering and Technology Advances, 26(01), 168–185. https://doi.org/10.30574/gjeta.2026.26.1.0003

[37] Zaman, S. U. (2025). Enhancing security in cloud-based IAM systems using real-time anomaly detection. IJSRED - International Journal of Scientific Research and Engineering Development, 8(6), 2292–2304. https://doi.org/10.5281/zenodo.17926883

[38] Rahman, F. (2025). Data science in power system risk assessment and management. World Journal of Advanced Engineering Technology and Sciences, 17(03), 295–311. https://doi.org/10.30574/wjaets.2025.17.3.1560