International Journal of Technology, Management and Humanities Volume 12, Issue 3, 2026

AI Governance Scan Engines for Enterprise Data Ecosystems: A RAG-Driven Architecture for Continuous Compliance and Risk Detection

Sharanya Varatharajan

Astrosoft Technologies/ Swiss school of business management USA

Abstract

The reliance of enterprises on complex data ecosystems has grown, enabling them to power their artificial intelligence (AI), machine learning (ML), analytics and automated decision-making processes. Flaws in data quality, privacy concerns, biases, inconsistent data quality, and incomplete data lineage, as well as broken governance practices and changing compliance regulations can taint the trustworthiness and accountability of AI systems. To support on-going compliance assessment and enterprise risk detection, this paper introduces an AI Governance Scan Engine that utilizes Retrieval-Augmented Generation (RAG). The architecture proposed combines metadata catalogs, lineage graphs, policy repositories, vector stores, governance-centric large language models, automatic scan orchestration, enforcement, and reporting. The engine continuously scans for policy violations, fairness, privacy risks, lineage integrity, data quality and model input governance in enterprise data lakes, warehouses and machine-learning pipelines. A multi-dimensional risk scoring system that ties severity, likelihood, governance impact, and confidence to identify findings and take the appropriate remediation. The framework can accommodate scheduled, event-driven, and pipeline-integrated governance scans, and audit evidence is provided, along with the ability to have human oversight on high-impact decisions. The proposed approach establishes a scalable framework for proactive, explainable and ongoing AI governance by linking organizational policies to enterprise data context via RAG. Moves enterprise governance beyond the reactive audit to intelligent, automated and risk-aware monitoring of AI-driven data ecosystems.

Keywords: AI governance, Retrieval-Augmented Generation, enterprise data ecosystems, continuous compliance, risk detection, data governance, responsible AI, large language models, policy enforcement, data lineage, AI risk management, automated governance.

International Journal of Technology, Management and Humanities (2026) DOI:10.21590/ijtmh.12.01.418

Introduction

Large, distributed, and evolving data ecosystems have become more critical to the operations of organizations as a result of the rapid adoption of artificial intelligence (AI), generative AI, and machine learning. Today, data lakes, data warehouses, cloud platforms, ERP systems, and analytical pipelines are all linked together and used as the building blocks for automated decision making and intelligent business processes. As a result, reliable, secure, traceable and properly controlled information is crucial for the smooth operation of AI systems, and effective data governance has been deemed essential for that. While leveraging enterprise workflows including data governance and intelligent automation. Generative AI also presents challenges in terms of governance and security needs (Yuvaraj & Kumar, 2023; Saravanan, 2025).

Traditional governance methods typically rely on periodic audits, manual policy reviews, disorganized metadata, and manual compliance interpretation. These methods often fall short when it comes to recognizing new issues like undocumented data, missing lineage, sharing of sensitive data, violations of model inputs, and shifting compliance concerns that happen at the rate of today's enterprise data usage. With this in mind, enterprise generative AI needs to

Corresponding Author: Sharanya Varatharajan , Astrosoft Technologies/ Swiss school of business management USA, e-mail: varatharajansharanya@gmail.com

How to cite this article: Varatharajan, S. (2026). AI Governance Scan Engines for Enterprise Data Ecosystems: A RAG-Driven Architecture for Continuous Compliance and Risk Detection. *International Journal of Technology, Management and Humanities,* 12(3), 51-59.

Source of support: Nil

Conflict of interest: None

be governed in a way that can sustain itself across various data environments that are often heterogeneous (Biswas, 2024; Rah, 2026).

One way to tackle this challenge is through the use of Retrieval-Augmented Generation (RAG), which allows AI models to refer to relevant policies, metadata, governance rules, and enterprise context before assessing. Rah and Hahues (2026) and Muthusamy (2025) suggest that RAG and generative AI can aid in integrated governance prioritization, explainable analysis, and risk-aware decision-making. Likewise, the governance-driven approach to generative AI can link intelligent insights from data with organizational controls and enterprise systems (Joshi, 2025).

In this context, this study aims to propose an AI Governance Scan Engine based on RAG, combined with vectorized policy repositories, metadata and lineage graphs, automated risk scoring, and continuous scanning. The architecture provides a means to assess compliance, privacy, bias, lineage integrity, data quality, and input governance of the model, as well as automated alerting, remediation, and human oversight. This strategy can enhance enterprise decision support and foster more responsible use of AI (Valiki, 2026).

Background, Motivation, and Governance Challenges

Governance Challenges in Modern Data Ecosystems

Today's businesses span multiple data lakes, data warehouses, cloud ecosystems, enterprise resource planning systems, APIs, and machine-learning pipelines. This distributed environment makes it harder to ensure consistency of governance due to the ability of datasets to be duplicated, transformed, transferred, or consumed without adequate documentation. These factors can result in governance and operational risks due to shadow datasets, incomplete lineage, inconsistent metadata, unauthorized access, and weak data-quality controls. These challenges are exacerbated by enterprise AI applications relying on vast amounts of potentially sensitive and diverse data, as well as the need for generative AI to provide more accurate and useful information. Yuvaraj and Kumar (2023) stress the need for intelligent automation and enterprise data governance, and Saravanan (2025) points to secure governance needs in the cloud-native generative AI world.

Bias and fairness represent another major concern. Training and operational datasets may contain demographic imbalances, historical biases, or proxy variables that influence AI decisions. Consequently, governance mechanisms must examine not only whether data is available, but also whether it is appropriate, representative, and responsibly used. Explainable generative AI can strengthen this process by providing greater visibility into governance assessments and data-modernization decisions (Muthusamy, 2025).

Privacy is equally important because enterprise datasets may contain personally identifiable information, confidential business records, financial information, or other sensitive attributes. Generative AI systems can increase the risk of inappropriate data exposure when access controls, data classification, and usage policies are poorly implemented. Rah (2026) identifies security and governance as central concerns in enterprise generative AI adoption, reinforcing

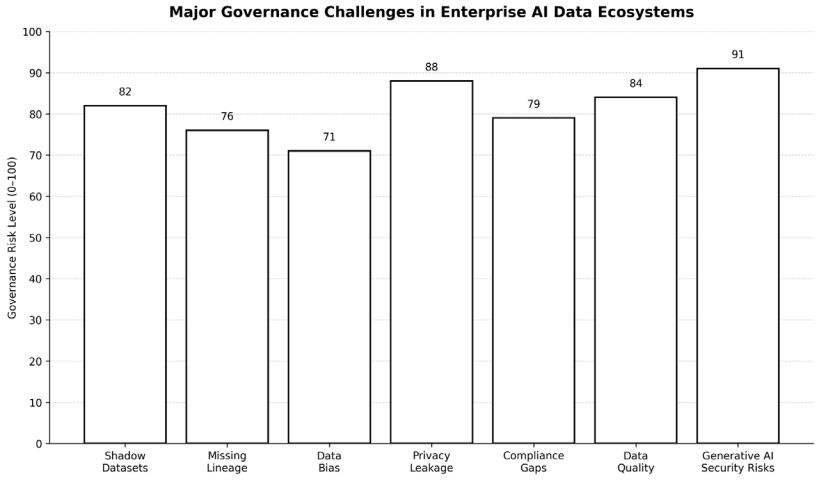

Fig 1: The evaluation framework uses normalized indicators to assess governance effectiveness. Higher values indicate stronger performance for detection, lineage completeness, privacy detection, bias detection, and governance coverage, while lower values are preferable for false-positive rate and remediation time. Continuous evaluation supports current policies, traceable evidence, and adaptation to changing enterprise data and regulatory requirements (Rah & Hahues, 2026).

Table 1: Background Governance Challenges and AI-Driven Responses

Governance Challenge	*Enterprise Implication*	*AI-Driven Governance Response*
Shadow datasets	Undocumented or unauthorized data usage	Automated asset discovery and scanning
Missing lineage	Limited traceability and auditability	Metadata and lineage-graph validation
Data bias	Unfair or unreliable AI outcomes	Bias, fairness, and proxy-variable analysis
Privacy leakage	Exposure of sensitive enterprise information	PII detection and policy-aware monitoring
Compliance gaps	Regulatory and organizational violations	RAG-based policy retrieval and compliance mapping
Data-quality problems	Unreliable analytics and AI outputs	Automated quality and schema-drift assessment
Rapid AI change	Governance controls become outdated	Continuous and event-triggered scanning
Generative AI security risks	Data leakage and unauthorized model use	Security monitoring and governance controls

the need for continuous monitoring rather than isolated compliance reviews.

Rise of AI-Driven Governance

Traditional governance approaches often depend on periodic audits, manually maintained documentation, and rule-based validation. These mechanisms can become inadequate when enterprise data and AI systems change rapidly. AI-driven governance introduces policy-aware LLMs, semantic retrieval, automated risk assessment, and intelligent decision support to improve the speed and contextual accuracy of governance activities.

RAG is particularly relevant because it allows an LLM to retrieve authoritative governance policies, metadata, regulatory requirements, and enterprise context before producing an assessment. This reduces dependence on static model knowledge and enables governance decisions to be grounded in organization-specific evidence. Rah and Hahues (2026) position RAG, generative AI, and agentic AI as complementary technologies for enterprise governance prioritization.

Generative AI can also support enterprise workflow automation and data modernization when governance controls are embedded within the architecture rather than applied after processing has occurred. Biswas (2024) similarly emphasizes the importance of well-architected patterns for scaling enterprise generative AI responsibly. Governance-anchored generative AI can further connect AI-generated insights with organizational controls and enterprise systems such as ERP platforms (Joshi, 2025).

Regulatory and Enterprise Drivers

The increasing deployment of AI has strengthened the need for structured governance frameworks addressing risk management, accountability, transparency, privacy, security, and documentation. The proposed Governance Scan Engine can operationalize these requirements by continuously retrieving applicable policies, evaluating enterprise data assets, identifying governance deviations, and generating auditable evidence.

The architecture is particularly suited to environments where AI-powered decision support is becoming integrated into enterprise operations. Valiki (2026) demonstrates the broader role of AI-powered decision support in modern enterprises, while Rah and Hahues (2026) emphasize prioritizing governance activities according to risk. Accordingly, the proposed scan engine treats governance as a continuous operational capability rather than a one-time compliance exercise.

Governance Scan Methodologies

Policy Compliance Scan

The policy compliance scan evaluates enterprise data assets, AI workflows, and model operations against organizational policies, regulatory requirements, and established governance controls. A Retrieval-Augmented Generation (RAG) mechanism retrieves relevant policy documents and governance rules before the language model interprets their applicability to specific datasets or processes. This enables the engine to map requirements to data assets, identify control gaps, and generate evidence-based compliance findings. Governance-anchored generative AI can strengthen the alignment between enterprise data insights and organizational policies (Joshi, 2025). Similarly, RAG-based governance architectures can prioritize controls according to organizational risk and regulatory importance (Rah & Hahues, 2026).

Bias and Fairness Scan

The bias and fairness scan assesses whether datasets contain demographic imbalances, protected attributes, or proxy variables that could contribute to discriminatory AI outcomes. The methodology can examine representation, distributional differences, and appropriate statistical fairness indicators across relevant groups. Findings are incorporated into the governance risk profile and routed for human review where necessary. Explainable generative AI can support this process by providing understandable reasoning behind identified governance concerns rather than producing unexplained

Table 2: Components of the RAG-Driven Governance Engine

Architecture Component	*Core Function*	*Key Governance Output*
Retrieval Layer	Retrieves policies, metadata, lineage, logs, and governance evidence	Contextual governance evidence
Vector Store	Stores semantic representations of policies and enterprise assets	Relevant policies and controls
Governance LLM	Performs policy interpretation and risk reasoning	Compliance findings and explanations
Scan Orchestration	Executes scheduled, event-driven, and pipeline scans	Continuous scan results
Enforcement Layer	Applies governance controls based on risk	Alerts, masking, quarantine, or blocking
Reporting Layer	Presents findings and audit evidence	Dashboards, reports, and risk heatmaps

classifications (Muthusamy, 2025). This is particularly important because enterprise generative AI systems require systematic governance and risk controls throughout their lifecycle (Rah, 2026).

Lineage Integrity Scan

The lineage integrity scan verifies whether data can be traced from its original source through transformations, storage locations, analytical processes, and model inputs. It identifies missing lineage relationships, undocumented transformations, shadow datasets, and unauthorized pipeline activities. Continuous metadata monitoring can improve visibility across enterprise data environments and strengthen the reliability of automated governance processes (Yuvaraj & Kumar, 2023). Cloud-native approaches further support integration of governance checks within automated enterprise workflows (Saravanan, 2025).

Privacy and Sensitive Data Scan

The privacy scan detects personally identifiable information (PII), confidential records, sensitive attributes, and other restricted data elements within enterprise repositories and AI pipelines. It also evaluates whether appropriate consent, access, classification, and processing metadata are available. Identified exposures can trigger masking, access restrictions, quarantine, or governance alerts. Security and privacy risks are particularly significant in enterprise generative AI because data can move across multiple applications, services, and processing layers (Rah, 2026; Biswas, 2024).

Data Quality Scan

The data quality scan evaluates datasets according to completeness, accuracy, consistency, validity, uniqueness, and timeliness. It also detects schema drift, unexpected distribution changes, duplicate records, missing values, and invalid data types. Quality findings are incorporated into governance scores to prevent unreliable datasets from entering AI training or inference pipelines. Integrating governance into automated enterprise workflows can enable these checks to occur continuously rather than only during periodic audits (Saravanan, 2025; Yuvaraj & Kumar, 2023).

Model Input Governance Scan

The model input governance scan determines whether data entering an AI model satisfies predefined governance, security, privacy, and quality requirements. Each input can be evaluated for classification, authorization, lineage, sensitive-data exposure, and compliance status before

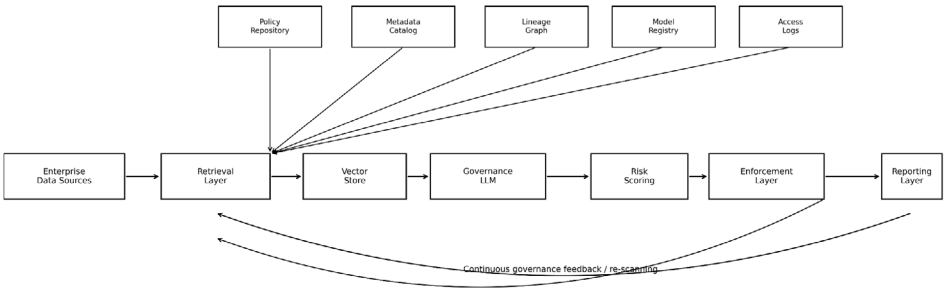

Fig 2: The architecture illustrates a RAG-driven governance process in which enterprise data and governance metadata are retrieved, evaluated by a governance LLM, assigned risk scores, enforced through controls, and continuously refined through reporting and feedback mechanisms.

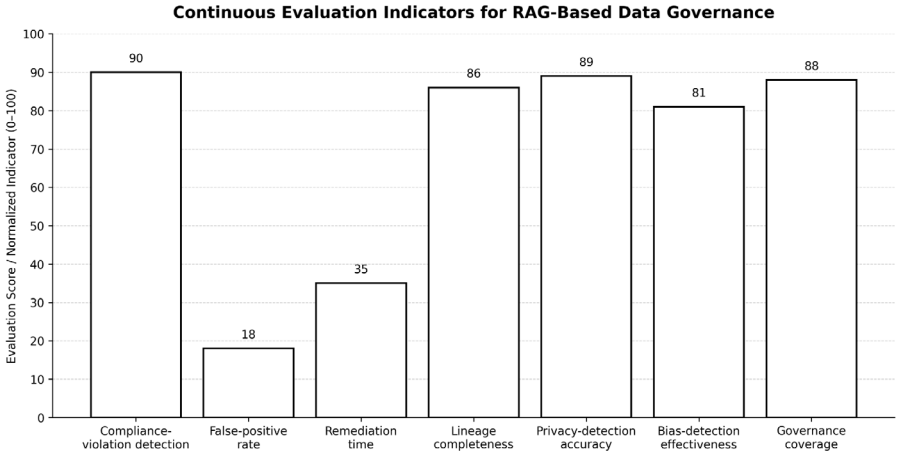

Fig 3: The evaluation framework uses normalized indicators to assess governance effectiveness. Higher values indicate stronger performance for detection, lineage completeness, privacy detection, bias detection, and governance coverage, while lower values are preferable for false-positive rate and remediation time. Continuous evaluation supports current policies, traceable evidence, and adaptation to changing enterprise data and regulatory requirements (Rah & Hahues, 2026).

model execution. Governance rules can therefore be embedded directly into AI workflows, allowing high-risk inputs to be rejected or escalated. AI-powered decision-support approaches reinforce the importance of structured governance mechanisms for reliable enterprise AI operations (Valiki, 2026). A well-architected generative AI environment similarly requires governance controls to be integrated across enterprise AI components rather than applied as an isolated control function (Biswas, 2024).

Overall, these methodologies transform governance from a predominantly reactive audit activity into a continuous scanning process. By combining RAG-based policy interpretation, enterprise metadata, automated analytics, and explainable AI, the Governance Scan Engine can continuously identify and prioritize compliance, privacy, fairness, lineage, quality, and model-input risks (Muthusamy, 2025; Rah & Hahues, 2026).

RAG-Driven Governance Engine Architecture

The proposed RAG-driven Governance Engine Architecture integrates enterprise data governance with retrieval-augmented generative AI to provide continuous, context-aware monitoring of data and AI assets. The architecture connects metadata catalogs, lineage repositories, policy documents, access logs, and governance rules to a retrieval layer that supplies relevant evidence to the governance LLM. This reduces reliance on unsupported model reasoning and enables governance decisions to be grounded in enterprise-specific policies and data context (Rah & Hahues, 2026). RAG-based governance is particularly valuable because enterprise generative AI requires mechanisms that address security, accountability, and policy enforcement throughout the AI lifecycle (Rah, 2026).

Retrieval Layer

The retrieval layer ser information with enterprise workflows can improve continuity, traceability, and automated decision-making (Yuvaraj & Kumar, 2023).

Vector Store

The vector store maintains embeddings representing policies, regulatory requirements, governance controls, datasets, metadata, and enterprise rules. Semantic retrieval enables the engine to locate policies and controls that are contextually relevant to a specific dataset, model, or processing activity. This approach supports scalable enterprise generative AI architectures by enabling information retrieval without requiring every governance rule to be explicitly hard-coded (Biswas, 2024).

Governance LLM

The governance LLM interprets retrieved evidence and performs policy interpretation, compliance reasoning, risk assessment, and remediation recommendation. Rather than allowing the LLM to operate independently, retrieved policies and metadata constrain its reasoning. Explainability is important because governance decisions must be understandable to data stewards, auditors, and compliance teams; explainable generative AI can therefore strengthen

Table 3: Enterprise AI Governance Risk-Scoring and Implementation Framework

Risk Dimension	*Key Assessment Indicator*	*Example Risk Response*	*Governance Owner*
Compliance	Policy or regulatory violation	Escalation, remediation, or pipeline block	Compliance team
Privacy	PII/sensitive-data exposure	Masking, restriction, or quarantine	Privacy/security team
Bias & Fairness	Distributional disparity or proxy variables	Dataset review and remediation	AI governance team
Lineage Integrity	Missing or inconsistent lineage	Traceability correction and validation	Data steward
Data Quality	Completeness, accuracy, or schema failure	Data correction or rejection	Data engineering team
Model Input Governance	Unapproved or high-risk model input	Input restriction or execution block	ML/AI owner
Overall Risk	Combined weighted risk score	Monitoring, remediation, or escalation	Governance committee

trust in enterprise modernization and governance processes (Muthusamy, 2025). AI-powered decision support can further extend this layer by transforming governance findings into actionable enterprise recommendations (Valiki, 2026).

Scan Orchestration Layer

The orchestration layer coordinates scheduled, event-triggered, and pipeline-integrated scans. A scan can automatically start when a dataset changes, a new model is deployed, a policy is updated, or an anomalous governance condition is detected. Cloud-native orchestration supports scalable automation and secure governance across distributed enterprise environments (Saravanan, 2025).

Enforcement Layer

The enforcement layer converts scan findings into governance actions. Depending on the risk level, it can trigger access restrictions, data masking, quarantine, policy gates, alerts, or pipeline blocking. Governance-anchored architectures are particularly relevant for ensuring that generative AI-driven insights remain consistent with organizational policies and enterprise controls (Joshi, 2025).

Reporting Layer

The reporting layer provides compliance dashboards, risk heatmaps, audit trails, governance alerts, and remediation status reports. These outputs enable data stewards, security teams, compliance officers, and governance committees to monitor the overall condition of enterprise AI ecosystems. The integration of automated governance intelligence with enterprise decision support can improve visibility and facilitate faster responses to emerging risks (Valiki, 2026).

Risk Scoring, Implementation, and Enterprise Governance

Risk Dimensions and Scoring Methodology

The proposed AI Governance Scan Engine should evaluate risk across compliance, privacy, bias, lineage integrity, data quality, and model-input governance. Each dimension can be assigned a weighted score based on the severity of the identified issue, likelihood of occurrence, potential business impact, and confidence of the scan result. This multidimensional approach enables organizations to prioritize critical governance issues rather than treating all violations equally. RAG strengthens the process by retrieving relevant policies and governance evidence before the LLM generates its assessment, supporting more context-aware governance prioritization (Rah & Hahues, 2026). Explainable generative AI can further improve the transparency of risk assessments and support enterprise data modernization (Muthusamy, 2025).

Risk Classification and Thresholds

Risk results can be classified into low, medium, and high categories. Low-risk findings may require monitoring, medium-risk findings should trigger documented remediation, while high-risk findings can activate pipeline restrictions, data quarantine, access controls, or escalation to governance authorities. Automated decision support can help organizations interpret these results and prioritize actions across complex enterprise environments (Valiki, 2026). However, high-impact decisions should retain human review because generative AI systems may produce incorrect or insufficiently supported conclusions.

Implementation and Workflow Integration

Implementation should integrate the scan engine with DataOps, MLOps, DevOps, data catalogs, cloud platforms, ERP systems, and enterprise workflow systems. Scheduled and event-driven scans can continuously evaluate changes in datasets, policies, schemas, models, and pipelines. Cloud-native implementation can support scalable governance automation and secure data management across distributed enterprise environments (Saravanan, 2025). Governance controls should also be embedded into enterprise workflows so that compliance becomes an operational process rather than a separate auditing activity (Yuvaraj & Kumar, 2023).

Enterprise Governance and Human Oversight

Effective implementation requires clearly defined responsibilities for data stewards, AI owners, security teams, compliance officers, and governance committees. Governance policies should specify approval requirements, escalation procedures, documentation standards, audit evidence, and remediation responsibilities. Governance-anchored generative AI can help align AI-driven data insights with organizational controls and enterprise processes (Joshi, 2025). A well-architected enterprise generative AI environment should additionally incorporate security, accountability, monitoring, and controlled deployment practices (Biswas, 2024; Rah, 2026).

Continuous Evaluation

The implementation should be evaluated using indicators such as compliance-violation detection rate, false-positive rate, remediation time, lineage completeness, privacy-detection accuracy, bias-detection effectiveness, and governance coverage. Continuous evaluation is particularly important because enterprise data, policies, models, and regulatory obligations change over time. RAG-based governance should therefore maintain current policy sources and provide traceable evidence supporting each significant risk finding (Rah & Hahues, 2026).

Discussion and Conclusion

Discussion

The proposed AI Governance Scan Engine provides a proactive approach to managing governance risks across enterprise data ecosystems by combining RAG, vectorized policy stores, metadata, lineage information, automated scanning, and risk scoring. Unlike periodic governance assessments, the architecture enables continuous monitoring of data assets, pipelines, and AI model inputs. This supports the transition from reactive compliance management toward intelligent and operational governance. The integration of generative AI with enterprise data governance can strengthen workflow continuity and automate governance-related activities (Yuvaraj & Kumar, 2023).

RAG is particularly valuable because governance decisions can be grounded in retrieved organizational policies, regulatory requirements, metadata, and lineage evidence. This reduces dependence on the LLM's internal knowledge and enables governance assessments to reflect changing enterprise requirements. An integrated governance architecture combining RAG, generative AI, and agentic capabilities can further support prioritization and coordination of governance activities (Rah & Hahues, 2026). Cloud-native implementation can also improve scalability by allowing governance scans to operate across distributed enterprise data and workflow environments (Saravanan, 2025).

Nevertheless, several limitations require attention. LLM-based governance can produce inaccurate interpretations, retrieval errors, hallucinations, or inconsistent recommendations when policy documents are incomplete or ambiguous. Generative AI also introduces security and governance risks that organizations must continuously monitor (Rah, 2026). Consequently, automated findings should be supported by evidence, confidence indicators, audit trails, and human review for high-risk decisions. Explainable generative AI can strengthen transparency by helping governance teams understand how findings and recommendations are produced (Muthusamy, 2025).

The framework also highlights the importance of organizational governance. Technology alone cannot establish responsible AI practices. Data stewards, AI owners, security professionals, compliance teams, and governance committees must define accountability, risk thresholds, escalation mechanisms, and remediation responsibilities. Governance-anchored generative AI provides a foundation for connecting AI-driven insights with organizational controls and enterprise processes (Joshi, 2025). Similarly, enterprise generative AI architectures require deliberate attention to security, reliability, monitoring, and responsible deployment practices (Biswas, 2024).

Conclusion

The AI Governance Scan Engine provides a scalable architecture for ongoing compliance, risk identification and responsible governance of enterprise AI data ecosystems. Organizations can continuously detect and prioritize governance risks with the combination of RAG and policy repositories, vector stores, metadata catalogs, lineage graphs, governance LLMs, automated orchestration, and enforcement tools.

The proposed risk-scoring approach offers a structured approach to risk evaluation that includes risks associated with compliance, privacy, bias, lineage integrity, data quality, and model-input risks. By seamlessly integrating with enterprise workflows, governance controls are no longer a one-off audit exercise, but a part of regular data and AI usage. AI assisted decision support tools can improve this capability to better understand governance results and prioritize the corrective actions (Valiki, 2026).

Finally, there has to be a balance between automation and human responsibility in the context of AI governance. The world of scale, consistency, and responsiveness is enhanced with RAG-driven scanning, but high impact governance decisions ought to be overseen by humans appropriately. Going forward, adaptive risk scoring, explainable governance agents, cross-cloud governance, autonomous remediation and increased security controls are key areas that should be prioritized. These can help to build AI governance as a unified, evidence-based capability for trustworthy enterprise data and AI operations.

References

[1] Yuvaraj, N., & Kumar, M. S. (2023). Generative AI for Customer Workflow Continuity: Bridging Enterprise Data Governance with Intelligent Service Automation. *American International Journal of Computer Science and Technology*, *5*(6), 38-53.

[2] Saravanan, K. (2025). Cloud-Native Generative AI Frameworks for Enterprise Workflow Automation and Secure Data Governance. *International Journal of Computer Technology and Electronics Communication*, *8*(6), 11952-11961.

[3] Muthusamy, M. (2025). Enhancing Federated Cloud with Explainable Generative Artificial Intelligence for Enterprise Data Modernization and Governance. *International Journal of Computer Technology and Electronics Communication*, *8*(5), 11586-11591.

[4] Valiki, S. V. S. (2026). AI-Powered Decision Support for Modern Enterprises. *The American Journal of Analytics and Artificial Intelligence (AJAAI)*, *4*(01).

[5] Joshi, C. (2025). Governance-Anchored Framework for Generative AI-Driven Data Insight in ERP Systems. *Available at SSRN 5683982*.

[6] Rah, A. (2026). Enterprise generative AI: A systematic review of security risks and governance. *Available at SSRN 6869661*.

[7] Biswas, S. (2024). *Enterprise GENERATIVE AI Well-Architected Framework & Patterns: An Architect's Real-life Guide to Adopting Generative AI in Enterprises at Scale*. Packt Publishing Ltd.

[8] Rah, A., & Hahues, S. (2026). Retrieval-augmented generation (RAG), generative AI, and agentic AI governance: An integrated enterprise governance prioritization architecture. *Generative AI, and Agentic AI Governance: An Integrated Enterprise Governance Prioritization Architecture (June 11, 2026)*.

[9] Ezeagwuna, D. (2026). AI-Driven Intrusion Detection Systems for Cybersecurity. *Journal of Science Technology and Social Transformation*, *2*(02), 37-51.

[10] Mukherjee, C. (2026). AI-Based Detection of Deepfakes and Misinformation on Social Media. *Euro Vantage journals of Artificial intelligence*, *3*(2), 9-30.

[11] Awodire, M. (2026). Researching Business Processes and Enterprise Architecture in Public Transit Dispatch Operations. *Journal of Integrated Science, Technology and Management*, *2*(03), 1-13.

[12] Begum, S., Akbar, Z., Islam, M. S., Rahman, M. A., Rahman, M. M., Hossen, B., ... & Raj, M. W. Z. (2026, February). IHPO-XGBoost for ESG Performance Prediction: A High-Accuracy Machine Learning Framework. In *2026 5th International Conference on Sentiment Analysis and Deep Learning (ICSADL)* (pp. 1558-1564). IEEE.

[13] Oloruntoba, O., Odum, P., Audu, K., Adepoju, S., Ugboko, R., & Tiamiyu, O. R. (2026). Resilient geospatial data management: a comparative analysis of cloud-native and distributed ledger technology synchronization models for multi-cloud environments. *Journal of Cloud Computing*, *15*(1), 87.

[14] Oloruntoba, O., Odum, P., Audu, K., Adepoju, S., Ugboko, R., & Tiamiyu, O. R. (2026). Resilient geospatial data management: a comparative analysis of cloud-native and distributed ledger technology synchronization models for multi-cloud environments. *Journal of Cloud Computing*, *15*(1), 87.

[15] Jobiullah, M. I., Begum, S., Ali, M. M., Rahman, M. M., Emon, M. S. A., & Fatima, K. (2026, April). A Machine Learning-based National Startup Capital Readiness Scoring Platform: Design, Implementation, and Comparative Evaluation. In *2026 9th International Conference on Inventive Computation Technologies (ICICT)* (pp. 1893-1899). IEEE.

[16] Kola, J. N. (2026, June). Secure Financial Analytics Platforms for Regulatory Compliance and Risk Management. In *2026 IEEE 18th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 794-801). IEEE.

[17] Awodire, M. (2026). Demystifying important issues concerning management of global IT resources in the Public Transit Sector in the US. *Journal of Science Technology and Social Transformation*, *2*(03), 1-15.

[18] Kola, J. N. (2026). Enterprise Business Intelligence and Financial Analytics with a focus on Enterprise Data Architecture and Predictive Risk Integration. *Adhyayan: A Journal of Management Sciences*, *16*(01), 20-28.

[19] Begum, S., Akbar, Z., Islam, M. S., Rahman, M. A., Rahman, M. M., Hossen, B., ... & Raj, M. W. Z. (2026, February). IHPO-XGBoost for ESG Performance Prediction: A High-Accuracy Machine Learning Framework. In *2026 5th International Conference on Sentiment Analysis and Deep Learning (ICSADL)* (pp. 1558-1564). IEEE.

[20] Awodire, M. (2026). Responsible AI governance frameworks: bias mitigation, fairness, and compliance in production AI deployments. *Journal of Science Technology and Social Transformation*, *2*(03), 26-35.

[21] Areghan, E. (2025). Cyber Resilience in Digital Twin and Smart Manufacturing Environments: Challenges, Strategies, and Future Direction. *Journal of Computational Analysis and Applications*, *34*(8), 573-593.

[22] Sanusi, B. O. (2025). Smart Infrastructure: Leveraging IoT and AI for predictive maintenance in urban facilities. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *17*(02), 26-37.

[23] Awodire, M. (2025). Data governance and privacy-by-design frameworks (GDPR/HIPAA) in multi-cloud data pipelines. *Journal of Data Analysis and Critical Management*, *1*(02), 116-126.

[24] Areghan, E. (2025). Emerging Frontiers in Cybersecurity: Navigating AI-Powered Threats, Quantum Risks, and the Rise of Zero-Trust Architectures. *International Journal of Advanced Trends in Computer Science and Engineering 14 (3). 120*, *136*.

[25] Ojuri, M. A. (2025). Ethical AI and QA-Driven Cybersecurity Risk Mitigation for Critical Infrastructure. *Euro Vantage journals of Artificial intelligence*, *2*(1), 60-75.

[26] Omolayo, O., Oloruntoba, O., Adepoju, S., & Audu, K. (2025). Comparative Analysis of Graph Partitioning Strategies for Enhancing Scalability and Performance in Distributed Graph Databases.

[27] Awodire, M. (2025). Master Data Management (MDM) integration strategies in hybrid cloud environments. *Journal of Data Analysis and Critical Management*, *1*(04), 41-50.

[28] Ezeagwuna, D. (2025). Artificial Intelligence for IT Service Management: Developing a Framework for ROI Optimization Using Service Now and Machine Learning Technologies. *Well Testing Journal*, *34*(S4), 394-419.

[29] Chukwu, M., Huang, X., Audu, K., Wang, H., & Subasish, D. (2025). Unequal paths to nature: Mobile-phone insights into park visits in nine major cities in the United States. *Urban Forestry & Urban Greening*, 129196.

[30] Ojuri, M. A. (2025). Quality Metrics for Cybersecurity Testing: Defining Benchmarks for Secure Code. *Well Testing Journal*, *34*(S3), 786-801.

[31] Adepoju, S. A., & Adepoju, M. A. (2024). From Portals to Case Graphs: A Reference Architecture and Benchmark for Safety

Investigation Operations with Agentic Orchestration.
[32] Awodire, M. (2024). Zero-trust and least-privilege IAM design in federal/regulated cloud deployments. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, *14*(02), 84-93.
[33] Khan, H. A. (2024). DATA-DRIVEN EPIDEMIOLOGICAL MODELING USING MACHINE LEARNING FOR DISEASE SPREAD FORECASTING AND PUBLIC HEALTH DECISION SUPPORT IN THE UNITED STATES. *International Journal of Applied Mathematics*, *37*(6s), 178-192.
[34] Sanusi, B. O. (2024). The role of data-driven decision-making in reducing project delays and cost overruns in civil engineering projects. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *16*(04), 182-192.
[35] Areghan, E., & Ndibe, O. S. (2024). Explainable AI for autonomous threat detection in critical infrastructure systems. *Journal of Computational Analysis and Applications*, *33*(8), 6841-6857.
[36] Ojuri, M. A. (2024). Cybersecurity Vulnerability Testing as a Core Component of Quality Assurance. *Pioneer Research Journal of Computing Science*, *1*(3), 122-138.
[37] Begum, S. (2025). AI at scale: Predictive analytics as a strategic engine for national competitiveness in US startup and small business financing. *International Journal of Progressive Research in Engineering Management and Science Development*, *2582*, 7421.
[38] Kola, J. N. (2024). Longitudinal Cohort Intelligence for Self-Insured Employer Groups: A Predictive Framework for Healthcare Cost Trajectory Modeling and Proactive Risk Intervention. *Journal of Information Systems Engineering & Management*, *10*.
[39] Ojuri, M. A. (2024). Integrating Cybersecurity Standards into Software Quality Assurance Frameworks: A Holistic Approach. *Journal of Computer Science and Technology Studies*, *6*(1), 258-271.
[40] Sanusi, B. O. (2024). Integration of nature-based solutions in urban planning: policy, governance, and institutional frameworks. *Journal of Mechanical, Civil and Industrial Engineering*, *5*(2), 10-25.
[41] Areghan, E., & Onwuegbuchi, O. (2024). Predictive Cyber Threat Analysis in Cloud Platforms Using Artificial Intelligence and Machine Learning Algorithms. *Applied Science, Computing, and Energy*, *1*(1), 197-205.
[42] Ojuri, M. A. (2023). Risk-Driven QA Frameworks for Cybersecurity in IoT-Enabled Smart Cities. *Journal of Computer Science and Technology Studies*, *5*(1), 90-100.
[43] Areghan, E. (2023). From Data Breaches to Deepfakes: A Comprehensive Review of Evolving Cyber Threats and Online Risk Management. *Communication in Physical Sciences*, *9*(4), 538-553.
[44] Awodire, M. (2023). Cost optimization strategies (tagging, rightsizing, capacity planning) in enterprise cloud operations. *International Journal of Technology, Management and Humanities*, *9*(04), 307-317.
[45] SANUSI, B. O. (2023). Performance monitoring and adaptive management of as-built green infrastructure systems. *Well Testing Journal*, *32*(2), 224-237.
[46] Ojuri, M. A. (2023). AI-Driven Quality Assurance for Secure Software Development Lifecycles. *International Journal of Technology, Management and Humanities*, *9*(01), 25-35.
[47] Aremu, A., & Anifowose, K. (2026). Global Marketing Strategies for Biotech-Based Consumer Products: Opportunities and Challenges. *Well Testing Journal*, *35*(3), 163-178.
[48] Gamba, K., & Ogar, A. (2026). Mental Health Awareness and Comprehension of Substance Use Consequences: An Analysis of students in the Department of Medicine & Surgery at University of Abuja, Nigeria. Journal of Medical and Health Studies, *7*(4), 15-35.
[49] Moetiara, E. (2025). Enhancing Contractor Health Risk Governance in High-Hazard Industries: A Risk-Based Prequalification and Monitoring Model from the Oil and Gas Sector. *Journal of Science Technology and Social Transformation*, *1*(02), 17-25.
[50] Ojuri, M. A. (2021). Measuring Software Resilience: A QA Approach to Cybersecurity Incident Response Readiness. *Multidisciplinary Innovations & Research Analysis*, *2*(4), 1-24.
[51] Awodire, M. (2022). Trend Analysis in Recurring IT Security Findings: What Repeated Vulnerabilities Reveal About Systemic Control Weaknesses. *International Journal of Technology, Management and Humanities*, *8*(04), 119-145.
[52] Akinyemi, A. (2021). Cybersecurity Risks and Threats in the Era of Pandemic-Induced Digital Transformation. *International Journal of Technology, Management and Humanities*, *7*(04), 51-62.
[53] Ojuri, M. A. (2022). The Role of QA in Strengthening Cybersecurity for Nigeria's Digital Banking Transformation. *Well Testing Journal*, *31*(1), 214-223.
[54] Akinyemi, A. (2022). Zero Trust Security Architecture: Principles and Early Adoption. *International Journal of Technology, Management and Humanities*, *8*(02), 11-22.
[55] Ojuri, M. A. (2022). Cybersecurity Maturity Models as a QA Tool for African Telecommunication Networks. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *14*(04), 155-161.
[56] SANUSI, B. O. (2022). Sustainable Stormwater Management: Evaluating the Effectiveness of Green Infrastructure in Midwestern Cities. *Well Testing Journal*, *31*(2), 74-96.
[57] Begum, S. (2022). Optimizing capital deployment in post-pandemic America: AI-powered predictive analytics for startup resilience and growth. *International Journal of Computer Applications Technology and Research*, *11*(12), 700-710.
[58] Akinyemi, A. (2022). Securing Critical Infrastructure Against Cyber Attacks. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *14*(04), 201-209.
[59] Ojuri, M. A. (2021). Evaluating Cybersecurity Patch Management through QA Performance Indicators. *International Journal of Technology, Management and Humanities*, *7*(04), 30-40.
[60] Kola, J. N. (2023). Measuring the Business Value of Analytics-Driven Decisions: A Decision Impact Attribution Framework for Enterprise Environments. *Journal of Information Systems Engineering & Management*, 1-9.