Applied Science, Computing and Energy, 2026, 4(5), 740-763

Data Governance, Integrity, and Cybersecurity Frameworks for Predictive Audit Models

Olatunde Ayeomoni*, Sugar Raymond, and Jude Okwuchukwu Ogene
Received: 17 March 2026/Accepted: 19 July 2026/Published: 28 July 2026

Abstract: *The rapid integration of machine learning and artificial intelligence into auditing has transformed traditional periodic assurance into continuous, predictive, and data-intensive processes. While predictive audit models enable population-level risk assessment and early detection of material misstatements, they simultaneously introduce novel vulnerabilities, including data bias, poisoning, concept drift, adversarial attacks, and explainability manipulation. Conventional data governance (DAMA-DMBOK, DCAM, COBIT), integrity, and cybersecurity frameworks (NIST CSF, ISO 27001, MITRE ATT&CK) were not designed for these interdependent risks and fail to satisfy the strict sufficiency, appropriateness, and reliability requirements for audit evidence under ISA 500, ISA 315 (Revised), and SOX. This conceptual paper synthesises existing frameworks, identifies critical gaps, and proposes a novel, audit-centric, three-layer integrated framework that combines immutable data lineage and governance at the core, real-time integrity verification in the middle layer, and zero-trust cybersecurity with adversarial robustness at the perimeter. The framework is operationalised through defined organisational roles, a recommended technology stack, and a five-level maturity model. By bridging longstanding disciplinary silos, it provides practitioners, standard-setters, and regulators with a theoretically grounded yet actionable blueprint for deploying reliable predictive audit analytics while preserving professional scepticism and regulatory compliance.*

Keywords: *Predictive auditing, Continuous auditing, Data governance, Data integrity, Cybersecurity, Adversarial machine learning, Audit evidence reliability, Explainable AI (XAI), Concept drift, Model risk management, ISA 315 (Revised), Audit analytics*

Olatunde Ayeomoni
University of Cincinnati, School of Information Technology, Cincinnati, Ohio, USA.
Email: ayeomooe@mail.uc.edu

Sugar Raymond
University of Cincinnati, School of Information Technology, Cincinnati, Ohio, USA.
Email: Sugarraymond@gmail.com

Jude Okwuchukwu Ogene
Kennesaw State University, College of Computing and Software Engineering, Marietta, Georgia, USA.
Email: Joption7@gmail.com

1. 0 Introduction

The auditing profession is undergoing a profound digital transformation driven by advances in artificial intelligence (AI), machine learning (ML), big data analytics, cloud computing, and automation technologies. These innovations are reshaping traditional audit methodologies and redefining the relationship between professional judgment and technology-enabled assurance services.

The traditional audit has consisted, at least in principle, of a reasonably high-level link between certain procedures and the effects of changes in risk on material misstatement (Kayaga, 2020). Such varied developments from traditional to current times are heavily influenced by emerging technological advancements such as artificial intelligence and machine learning.

The Fourth Industrial Revolution (Industry 4.0) has accelerated the generation of large volumes

Also available @ https://zenodo.org/records/21820920

of structured and unstructured data across organizations. Consequently, auditors are increasingly expected to analyse complete populations of transactions rather than relying solely on sample-based testing. This transition has stimulated the adoption of predictive analytics and continuous auditing systems capable of providing real-time insights into organizational risks, internal control weaknesses, and potential financial misstatements.

The use of data streams, sensor logs, textual disclosures, and even external signals is being harnessed for use in current nexus audit models to build a definition of immediate material misstatements, fraud patterns, and emerging risks for near real-time identification "in near real time" (Aboagye *et al*., 2022). The effectiveness and reliability of predictive audit models depend heavily on the quality, integrity, traceability, and security of the underlying datasets used during model development, validation, and deployment. (Ling *et al*., 2023). The incidents that reveal and expose weighty systemic data manipulation, model poisoning, and adversarial attacks in both financial and non-financial domains suggest that the gaps in data governance and cybersecurity can undermining audit evidence and professional scepticism while putting the organizations or their stakeholders at high financial impact, reputational damage, and regulatory cost (Booth *et al*., 2023).

Traditional auditing has, historically, relied on sampling techniques, manual testing of controls, and performed on static datasets year-ends substantive procedures (Adeyemi, 2023). The birth of continuous auditing came in the early 2000s to represent the first move towards automated exception detection; however, this tool remained predominantly rules-based and backward-looking (Tiron-Tudor & Deliu, 2022). Supervised and unsupervised machine learning algorithms, reinforced by natural-language processing and graph analytics, not only forecast risk hotspots, detect anomalies, but also recommend audit procedures before financial statements are finalized, thus representing a true paradigm shift in the current generation of predictive audit models (Lekkala *et al*., 2022). This is now reflected by specific requirements imposed on the auditor by standards bodies such as IAASB (ISA 315 revised) and PCAOB to address robotics-related risks deriving from automated tools and techniques, as they render data and model governance essential to a high-quality audit (Ilori *et al*., 2022).

Although substantial research has been conducted on data governance, data integrity, cybersecurity, and AI governance frameworks, these domains have largely evolved independently, resulting in fragmented approaches to managing risks in predictive audit environments.Furthermore, existing studies have focused primarily on data management, information security, or AI governance from organizational perspectives, with limited attention to the unique evidentiary requirements imposed by auditing standards such as ISA 315 (Revised) and ISA 500. Consequently, there remains a significant theoretical and practical gap in the development of an integrated framework capable of simultaneously addressing governance, integrity, cybersecurity, explainability, and audit evidence reliability throughout the machine-learning lifecycle. (Aguboshim *et al*., 2023). Similarly, existing frameworks are mostly outdated, being either traditional for the IT environment or non-audit-specific AI systems. However, in predictive auditing, the systemic confluence of risk (simultaneous exposure to data poisoning, adversarial examples, concept drift, and lineage opacity) does not even come close to such stringent sufficiency, appropriateness, and reliability requirements in audit evidence (McGregor & Carpenter, 2020). As an extension of the above statements, audit firms and internal audit functions do not at this point have an integrated theoretically grounded

framework that aligns specifically with the life cycle of predictive audit models data governance, integrity verification, and cybersecurity controls (Pangastuti, 2023).

Therefore, the primary aim of this study is to develop an integrated governance, integrity, and cybersecurity framework capable of enhancing the reliability, transparency, resilience, and regulatory compliance of predictive audit models. Therefore, this conceptual paper pursues three main objectives: (1) synthesise and critique the extant data governance, integrity, and cybersecurity frameworks with respect to predictive audit analytics; (2) develop an integrated, multi-layered approach to directly mitigate data and model risk but still meet audit-proof evidence admissibility; and (3) provide actionable guidance in terms of roles, processes, technologies, and maturity model for audit functions to operationalize in practice the proposed framework.

This study is significant from theoretical, practical, and regulatory perspectives. Theoretically, it contributes to the emerging body of knowledge at the intersection of auditing, artificial intelligence, data governance, and cybersecurity. Practically, the proposed framework provides audit firms and internal audit functions with a structured mechanism for managing AI-related risks and ensuring the reliability of predictive audit outputs. From a regulatory standpoint, the framework supports compliance with professional auditing standards, including ISA 315 (Revised), ISA 500, and Sarbanes-Oxley (SOX) requirements, while addressing emerging concerns regarding AI governance and algorithmic accountability.

The main contribution lies in a novel, audit-centric framework meant to fill silos that had been in place for long periods between data governance, integrity assurance, and cybersecurity and under such conditions fit the unique evidentiary and regulatory demands of predictive auditing (Ilori *et al*., 2022). In this regard, the achieved future map against the gaps identified through continual monitoring and lineage mechanisms may serve as theoretical advancement and practical blueprint of standard-setters, regulators, and practitioners (Hossain & Khan, 2022).

The rest of the paper, therefore, falls into the following form: Section 2 deals with the literature review session; Section 3 presents a risk taxonomy; Section 4 identifies and presents the core components of the integrated framework; Section 5 outlines its architecture and control mappings; Section 6 discusses implementation and maturity considerations while Section 7 concludes with implications for audit quality and future research directions.

2.0 Literature Review

2.1 Predictive audit models and technologies

Predictive audit models have evolved from conventional statistical sampling to adopt various machine learning (ML) capabilities that can process real-time populations of transactions (Huang *et al*., 2022). Supervised algorithms including random forests, gradient boosting machines (XGBoost, LightGBM) and variants of logistic regression lead in applications related to fraud detection and material misstatement prediction (Idowu *et al*., 2026). Increasingly, unsupervised methods such as autoencoders, isolation forests, and clustering find application in anomaly detection for continuous auditing (Abolade, 2023). These models will rely on both structured general-ledger data and unstructured sources such as e-mails, contracts, and management commentary to derive risk scores which guide audit planning and testing scope long before period-end (Batini *et al*., 2021). Deep learning architectures, especially those of recurrent neural networks (RNNs), long short-term memory networks (LSTMs), or even transformer-based models, have generally excelled when the consideration of temporal patterns or textual evidence is imperative (Liu *et al*., 2022). For instance, LSTMs are

implemented to predict going concern issues from sequences of cash-flow indicators, and transformer models such as BERT along with its financial-domain variants (FinBERT) are used to extract risk signals from narrative disclosures and earnings-call transcripts (Hsu & Lee, 2020). Graph neural networks (GNNs) have generated an interest to model entry manipulation schemes in a more complex way, viewing relationships among accounts with respect to entities and counterparties as interconnected nodes in a network (Ademilua, 2021).

Because of increased regulatory and professional requirements to ensure transparency, the deployment of explainable AI (XAI) techniques in auditing has gained momentum (Mehdiyev *et al*., 2021). SHAP (SHapley Additive exPlanations) and other methods such as LIME, integrated gradients, and counterfactual explanations are now embedded in audit analytics engines in order to meet ISA 315 (Revised) requirements on meaningfully understanding how automated tools arrive at conclusions (Areghan 2023). Then, post-hoc XAI methods will be complemented by inherently interpretable models such as generalized additive models and monotonic XGBoost, and by newly emerging audit-specific protocols requiring explanation fidelity in addition to predictive accuracy (Ann, & Deni, 2023). Although predictive audit technologies have demonstrated substantial improvements in risk identification, fraud detection, and audit efficiency, concerns remain regarding transparency, model interpretability, and robustness under changing data environments. Many studies emphasize predictive performance while paying insufficient attention to governance and control mechanisms required to ensure audit evidence reliability.

2.2 Data governance frameworks

The Data Management Body of Knowledge (DAMA-DMBOK2) represents the most extensive reference on data governance, defining ten knowledge areas from data governance and architecture through metadata, to quality management (Thitiphiromlarp & Pongpech, 2023). Its wheel structure emphasizes governance as the central enabling function that coordinates all others (Ademilua & Areghan, 2022). Although DAMA-DMBOK gives a detailed account of its control objectives and activities, it is very much a pre-machine-learning proposition; therefore, its guidance on model-related metadata, training-data lineage, or version control for any datasets used in predictive processes is limited (Iliashenko *et al*., 2022).

The Data Capability Assessment Model (DCAM) developed by the EDM Council offers a maturity-based approach particularly suited to financial services (Chukwudi & Oladunjoye, 2023). Explicit measurement in DCAM is for governance of data, quality of data, integration of data; in its later version analytics governance was included as well (Caballero *et al*., 2023). Nevertheless, the dominant view continues to be toward establishing a data management program from an enterprise perspective rather than the specific evidentiary requirements of audit functions, internal or external, that would withstand regulatory scrutiny (Georgiadis & Poels, 2021).

Adding to the earlier ones are COBIT 2019 (APO13 "Managed Security" and DSS06 "Managed Business Process Controls") and ISO 8000 (standards series on data quality) (Nanfa *et al*., 2022). COBIT aligns IT governance with business objectives and provides management practices for data classification and protection, while ISO 8000-8 addresses information and data quality measures (De Haes *et al*., 2019). Neither standard accounts for the dynamic lifecycle of training, validation, and production datasets employed in predictive audit models, nor do

they set controls for adversarial robustness or concept-drift detection (Tekale & Rahul, 2022). Collectively, existing data governance frameworks provide valuable guidance for enterprise-wide data management; however, they were developed primarily for traditional information systems and do not adequately address machine-learning-specific challenges such as training data lineage, model versioning, concept drift monitoring, and adversarial resilience.

2.3 Data integrity in the audit context

It has been noted that in the traditional sense of auditing that data integrity meant truthfulness, completeness and validity of evidence obtained from client systems (AU-C 500, ISA 500) (No *et al*., 2019) however with predictive models, integrity goes through the entire data pipeline-from source extraction feature engineering to model inference (Ling *et al*., 2023) Anything can fail at some point-whether it is duplicated records, wrong mappings, or undetected manipulation. But that will trigger a systematic chain of events and effect sufficiency and appropriateness of audit evidence in violation of professional standards (Okolo, 2023).

Deliberate integrity attacks, such as data poisoning and backdoor attack, are particularly insidious because they are not detected until triggered (Goldblum *et al*., 2022). This is proven by research that even a small percent of fraudulent training examples can cause fraud-detection models to ignore certain patterns and thus create hidden risk channels whichmight never be discovered through traditional substantive testing (Rahman *et al*., 2023). Checks under Benford's Law and duplicate-transaction tests would cease to suffice when one's adversary had knowledge of the model it'elf (Akinsanya, *et al*., 2022).

The non-malicious integrity threats, that is, concept drift, covariate shift and silent data corruption due to ETL failures are equally dangerous as the above mentioned (Akinsanya *et al*, 2023). However continuous integrity verification and recalibration mechanisms along with robust lineage tracking built into the system should keep them in check so that model predictions do not yield misleading risk scores later on when there will be a change in population features-for example, the introduction of new revenue recognition policies under IFRS 15/ASC 606 (Zhou, 2021). These observations suggest that conventional integrity assurance mechanisms are increasingly inadequate in AI-driven audit environments. Effective predictive auditing requires continuous integrity monitoring, automated anomaly detection, immutable lineage records, and real-time validation of model inputs and outputs.

2.4 Cybersecurity frameworks relevant to audit data

The NIST Cybersecurity Framework (CSF 2.0, 2024) organizes controls into six core functions: "Govern", "Identify", "Protect", "Detect", "Respond", and "Recover", and explicitly added a "Govern" function, which overlaps with data governance (Corbett-Wilkins *et al*., 2023). Its AI-specific profile under the NIST AI Risk Management Framework (2023) specifically addresses adversarial machine learning, although remaining voluntary and generic, which lacks audit-specific mappings to requirements for ensuring reliability of evidence (Tjoa *et al*., 2022).

ISO/IEC 27001:2022 Annex A controls (A.8.24-A.8.28 mainly) describe the cryptographic use-cases, secure development, and vendor relationships but do not define controls regarding the confidentiality of training data and model inversion attacks (Gu *et al*, 2019). Although certification guarantees fair security, it does not signify that audit evidence derived from ML systems is free from compromise, undetected (Anisetti *et al*., 2023). CIS Controls v8 and MITRE ATT&CK provide specific tactical guidance (Möller, 2023). Control 3 on Data Protection and Control 13 on Network Monitoring would

certainly have a direct bearing through several ATT&CK techniques such as "Data Manipulation" (T1565), "Adversary ML"(T1599), and "Model Theft", which provide an analysis of threats that audit teams would use to argue the detection analytics (Akanni *et al*., 2026). However, there is no amalgamating of these strategies with data governance or auditing standards for evidence (Pemmasani & Abd Nasaruddin, 2022). While existing cybersecurity frameworks provide comprehensive guidance for protecting information assets, they do not adequately account for emerging machine-learning threats such as data poisoning, model inversion, adversarial manipulation, and model theft. Consequently, additional controls are required to ensure the trustworthiness of predictive audit systems.

2.5 Identified gaps when applied to predictive audit analytics

A current framework deals with the governance of data, ensures the integrity of the data, and cybersecurity as three distinct disciplines (Lomas, 2020). Predictive auditing models exist within the intersection: one poisoned dataset to compromise integrity, governance (lineage), and cybersecurity objectives (Odozor *et al*., 2025). The existing standard, however, doesn't yet provide an integrated control structure that spans the entire ML lifecycle while preserving the evidentiary chain required by audit standards (Bukhari *et al*., 2021).

Explainability and lineage opacity are another important gap (Carabantes, 2023). Most of all XAI methods provide local or global explanations; however, very few governance or cybersecurity frameworks require the provenance of those explanations to be protected from modification or whether the provenance of the explanation can be traced back to the raw source data because this type of regulation is increasingly being expected from regulators looking at the "black box" audit tools (Charmet *et al*., 2022).

Finally, continuous monitoring and feedback loops are underdeveloped (Eitzinger *et al*., 2019). Periodic assessment is assumed in traditional frameworks, but predictive audit models require detection of real-time drift, adversarial robustness testing, and automated rollback capabilities (Lawal *et al*., 2021). Without integrating these dynamic controls, organizations risk deploying models whose reliability quietly degrades between formal governance reviews, making internal risk assessments vulnerable as well as external audit opinions (Ogunsola *et al*., 2021). The foregoing review demonstrates that no existing framework comprehensively integrates data governance, data integrity, cybersecurity, explainability, and continuous monitoring requirements within a single audit-centric architecture. Addressing this deficiency forms the central motivation for the present study and provides the foundation for the integrated framework proposed in subsequent sections.

3. 0 Risks in Predictive Audit Models

3.1 Data-related risks (bias, poisoning, drift, leakage)

Data-related risks in predictive audit models frequently arise from biases embedded within training datasets, including under-representation of industries, transaction types, economic cycles, and organizational characteristics (Siddique *et al*., 2023). Such biases systematically distort risk scores: for instance, a fraud-detection model would predominantly consist of large public companies and hence might fail to detect aggressive revenue recognition practices of mid-sized entities that result in reduction of substantive testing scope due to auditors overlooking material misstatements (Singh *et al*, 2019).Such biases can undermine model fairness, reduce predictive accuracy, and impair auditors' ability to identify material misstatements across diverse audit environments.

Data poisoning represents one of the most severe integrity threats to predictive audit systems because it intentionally contaminates training or operational datasets to influence model behaviour. (Wang *et al*., 2022). An example in audit would be where the perpetrator gets access to the source systems and creates fictitious but very legitimate journal entries showing a model to learn that such specific red flagged events might involve round-amount transfers just below approval thresholds (Kassem, 2023). Already experimental studies have shown that training data treated as the ground truth by predictive models may create even very low rates of poisoning, as low as 1-3%, into "blind spots" that are persistent with retraining and escape detection by normal audit analytics (Omefe *et al*., 2021). Consequently, organizations require robust data validation procedures, anomaly detection mechanisms, and immutable data lineage controls to mitigate poisoning attacks throughout the machine-learning lifecycle.

Concept drift, covariate drift, and data leakage constitute additional critical threats that may compromise the reliability of predictive audit models over time.(Guo *et al*., 2021). Drift is a phenomenon that occurs when the statistical aspects of production data diverge from those of training data; for example, the shift in expense patterns after the pandemic into remote-work-based expenses would affect the false-positive or false-negative rates quietly (Folorunso *et al*., 2025). Leakage-the accidental inclusion of future information or target variables in a feature-is an artificial inflation of model performance during validation, which produces misleading results in the field of implementation within live audits, more strictly, violating the sufficiency and appropriateness criteria for audit evidence under ISA 500 and AU-C 500 (Li *et al*., 2022). Collectively, these risks highlight the necessity for continuous monitoring, data quality assurance, lineage management, and model validation procedures capable of preserving the reliability and integrity of audit analytics in dynamic business environments.

3.2 Model-specific risks (adversarial attacks, model theft, explainability attacks)

Adversarial attacks exploit vulnerabilities inherent in machine-learning algorithms by manipulating inputs in ways that deceive predictive models while remaining largely undetectable to human observers.(Finlayson *et al*., 2019). The increasing sophistication of adversarial machine learning techniques has elevated cybersecurity concerns in audit analytics, particularly where automated decisions influence risk assessments and audit planning activities.By adding imperceptible perturbations to input transactions (e.g. splitting a fraudulent entry into hundreds of micro-transactions differing by pennies), the attackers can temper a high-risk score to flip to low risk [Naseer *et al*., 2021]. Research has shown that gradient-based attacks, namely FGSM and PGD, along with transfer-based black-box attacks, achieve almost 100% success rate against most standard audit classifiers; thus, making it possible for an insider or a compromised third-party data feed to exit the continuous monitoring controls entirely undetected [Obamuwagun 2023].

Unique to proprietary audit analytics, model theft and reverse-engineering also present additional challenges for intellectual property and security [Booth *et al*., 2023]. Using only query access, attackers can extract hyperparameters, feature importance rankings, or even construct a functionally equivalent model through model extraction or inversion attacks [Onwuegbuchi *et al*., 2023]. Once stolen, the model can be analysed offline for evasion strategies or sold to malicious actors, permanently forfeiting the audit firm's or company's analytical advantage and inducing systemic risk across multiple clients (Chhabra & Prabhakaran 2023). Beyond intellectual property concerns, model theft may expose sensitive audit methodologies and enable

adversaries to design targeted evasion strategies capable of circumventing audit controls.

Explainability attacks target model interpretation mechanisms and seek to manipulate the explanations generated by XAI tools without altering prediction outcomes.(Bordt *et al*., 2022]). Recent studies demonstrate that SHAP and LIME explanations can be manipulated by constructing inputs that preserve model output but lead to misleading feature attributions, causing auditors to focus on irrelevant variables while neglecting true drivers of risk. Such attacks erode professional scepticism and the auditor's ability to demonstrate "understanding of automated tools and techniques," now explicitly required by ISA 315 (Revised 2019) paragraph A147 (Sun *et al*., 2022).

3.3 Regulatory and assurance risks (SOX, GDPR, ISA 315 revised)

Management and external auditors remain ultimately responsible for internal control effectiveness under Sarbanes–Oxley Act Sections 302 and 404, even when the audit engagement draws upon the work of an AI system (Chang *et al*., 2021). Control reliance can seldom be afforded if any predictive audit model used to scope or substantiate control testing suffers from undetected bias, poisoning, or drift. This voids the basis for the CEOs, CFOs, audit committee members, and external auditors to rely on the controls, thereby exposing themselves to potential claims of false certification and possible enforcement actions from the SEC and PCAOB (Singh *et al*., 2019).

Liabilities are further extended for predictive audit models that process personal data by virtue of GDPR (and its emerging equivalents like CCPA and Brazilian LGPD) (Victoria & Omosunlade, 2020). Automated decision-making producing "legal or similarly significant effects" (Article 22) activates rights to meaningful explanation and human intervention (Malgieri, 2022). Failure to ensure training datasets containing personal data were protected against leakage or adversarial manipulation can amount to a reportable breach; conversely, failure to trace a high-risk audit flag back to specific personal data elements contravenes the principles of data-minimization and accountability (Aswathy & Tyagi, 2022).

ISA 315 (Revised 2019) and related technology projects now being undertaken by the IAASB mandate auditors to recognize and evaluate risks arising from the use of automated tools and techniques, including those related to data reliability and its IT dependencies (Barr-Pulliam *et al*., 2022). When the existing documentation frameworks of the governance or cybersecurity types do not properly address ML-specific risks, auditors find themselves facing such documentation and performance gap: they have no way of demonstrating whether their audit evidence was sufficient and appropriate, given that their predictive model may have failed silently; in the extreme, this may put them in a position of giving qualified opinions, regulatory findings, or claims of professional negligence (Kumar *et al*., 2020).

Table 1 – Risk Taxonomy for Predictive Audit Models

Category	Risk Type	Description	Impact on Audit Reliability
Data Governance	Poor metadata management	Inconsistent definitions across source systems	Misleading predictions
Data Integrity	Data poisoning	Malicious injection of training data	False negatives/positives

Cybersecurity	Adversarial examples	Crafted inputs that fool the model	Undetected material errors
Model Governance	Concept drift	Population changes not reflected in model	Outdated risk assessments

Risk taxonomy for predictive audit models (Alles & Gray, 2020)

4.0 Core Components of an Integrated Framework

The proposed framework adopts a layered architecture to address the interdependent risks associated with predictive audit models. The framework recognizes that reliable predictive auditing requires more than isolated governance, integrity, or cybersecurity controls. Instead, it integrates these functions into a cohesive system in which governance establishes accountability and traceability, integrity ensures the accuracy and reliability of data and model outputs, and cybersecurity protects the entire ecosystem from internal and external threats. Together, these layers provide a comprehensive mechanism for preserving audit evidence reliability throughout the machine-learning lifecycle.

4.1 Data Governance layer

The Data Governance Layer constitutes the foundational component of the proposed framework, establishing the policies, accountability structures, standards, and oversight mechanisms necessary for the effective management of predictive audit data assets.. Within predictive audit environments, data governance extends beyond conventional enterprise data management by addressing the unique evidentiary, regulatory, and transparency requirements associated with machine-learning-driven audit processes.(Adepoju *et al*., 2023). This sets definitive authoritative policies for data ownership and classification e.g., “audit-evidence grade” vs. “management information” stewardship roles (Audit Data Steward, Model Owner, Source System Owner) and other metadata attributes as well. Very importantly, every dataset obtained at any stage of a predictive audit model, may it be for training, validation, or live inference, is also accompanied by immutable, cryptographically signed provenance metadata that records origin, transformation history, as well as approval workflow (Booth *et al*., 2023).

A centralized Data Catalog and Lineage Service serves as the source of truth enforcing version control over both raw extracts and derived actualized features (Pimentel *et al*., 2019). Changing definitions for data, mappings, or feature-engineering scripts triggers automated impact analysis identifying downstream predictive models and forcing formal reapproval before production use (Idowu *et al*., 2025). This governance layer also requires developing and maintaining a comprehensive Audit Data Dictionary linking financial statement assertions (existence, completeness, valuation, etc.) with the corresponding underlying data elements and transformations to preserve the evidential chain required by ISA 500 and AU-C 500 (Appelbaum *et al*., 2021).

Governance also reaches into the temporal governance dimension by policies related to data retention, refresh frequency, and decommissioning (Rohde, 2022). An example of such training datasets would be automatically flagged for retirement when older than a "defined horizon" (usually 24 to 36 months unless justified for longer retention) to prevent inadvertent reliance on stale populations. In addition, the layer institutionalizes a cross-functional Predictive Audit Governance Committee consisting of representatives from internal audit, IT, data management, and the "second line" of defense, with quarterly meetings focusing on reviewing lineage completeness, policy adherence, and emerging regulatory expectations (Lehner *et al*., 2022). Consequently, the governance layer

provides the institutional foundation upon which integrity verification and cybersecurity controls operate, ensuring that predictive audit activities remain transparent, accountable, and compliant with professional auditing standards.

4.2 Data Integrity layer

The Data Integrity Layer operates as the second tier of the framework and is responsible for ensuring the accuracy, completeness, consistency, and trustworthiness of data throughout the predictive audit lifecycle.(Nwaimo *et al*., 2023). It operates auto-data-quality gates at ingestion points that enforce Benford analysis, referential integrity, duplication checks, and business rule validations before any record enters the audit analytics environment (Bhaskaran, 2020).

Great Expectations or similar open-source/contractual tools are integrated to create auditable integrity reports that travel with each dataset version. For predictive models, the integrity layer engages two additional real-time engines: (i) a Poisoning and Anomaly Detection Engine that uses statistical-anomaly detection and deep learning (e.g., spectral analysis, autoencoders) to identify outlier batches that deviate from established fingerprints (Feng *et al*., 2019) and (ii) a Drift and Shift Monitoring Engine that continuously compares live distributions against training and recent reference windows, automatically signalling when Kolmogorov-Smirnov or Population Stability Index limits are exceeded (Mehmood *et al*., 2021). All three engines create immutable log entries that are appended into the audit trail.

These controls of integrity culminate in the cryptographic hashing and digital signing of every dataset snapshot and feature store release approved. Every deviation detected at inference time, be it due to transmission errors, 749 nauthorized changes or attacks, automatically invalidates the model run and calls for human review (Jegorova *et al*., 2022). This deterministic but sufficient linkage between data state and model output satisfies regulatory requirements for reproducibility while simultaneously providing defensible proof that the auditor has sufficiently addressed the risk of incorrect or manipulated input data (Enyiorji, 2023). By continuously validating data quality, detecting anomalies, monitoring drift, and preserving immutable records of data transformations, the integrity layer ensures that predictive audit outputs remain reliable, reproducible, and defensible under regulatory scrutiny.

4.3 Cybersecurity layer

The Cybersecurity Layer forms the outer protective boundary of the framework and employs a defence-in-depth strategy designed to safeguard predictive audit systems from evolving cyber threats.Access to training data, feature stores, and deployed models is segregated in a dedicated secure enclave following zero-trust architecture, enforced API gateways, and behavioural analytics (Bayya, 2022). All data in transit and at rest are encrypted using keys managed independently of the analytics platform with model weights and hyperparameters themselves being classified as high business impact assets under CIS Control 3 and ISO 27001 Annex A.8 (Nandakumar *et al*., 2021).

An institution for adversarial robustness is following mandatory red-team tests before each production release with continuous monitoring for evasion attempts in live inference traffic (Mei *et al*., 2023). Tools such as Adversarial Robustness Toolbox (ART) or Counterfit are integrated in CI/CD pipelines whereby gradient-based, decision-based, and transferability attacks are executed, and any models failing predefined robustness thresholds are automatically rejected. Runtime input validation serves to enhance rejection further, transactions with features of known attack patterns (for instance, perturbation norms that exceed historical bounds) (Sánchez *et al*., 2019).

The integration of threat intelligence with MITRE ATT&CK techniques specific to machine learning (e.g., T1565 Data Manipulation, T1599 Adversarial ML) informs proactive updates of controls (Al-Sada *et al*., 2023). Incident response playbooks explicitly encompass model-specific scenarios—poisoning, theft, and explainability attacks—with prioritized containment actions, including the immediate rollback of the model to the last signed golden version and forensic preservation of compromised datasets. Consequently, in wrapping integrity and governance layers in these dynamic, threat-aware controls, the Cybersecurity layer ensures that predictive audit evidence is protected from external attackers and malicious insiders during its entire lifecycle (Juntunen & Virta, 2019).

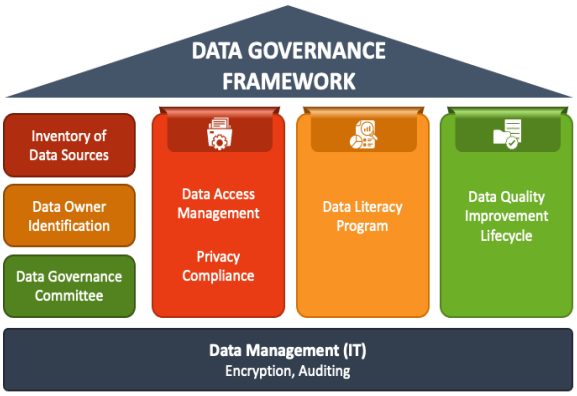

Fig. 1 Integrated Data Governance, Integrity, and Cybersecurity Framework (IBM Global Services 2021).

Table 2 – Mapping of Existing Standards to Predictive Audit Needs

Framework / Standard	Covers Data Governance	Covers Data Integrity	Covers Cybersecurity	Gap for Predictive Models
DAMA-DMBOK	Yes	Partial	No	No model risk or adversarial focus
COBIT 2019 (APO13, DSS06)	Yes	Partial	Partial	Limited AI/ML guidance
NIST AI RMF (2023)	Partial	Partial	Yes	Not audit-specific
ISO/IEC 27001	No	No	Yes	No data quality or lineage
Proposed Integrated Framework	Yes	Yes	Yes	—

4.4 Interaction Among Framework Components

The effectiveness of the proposed framework depends on the interaction among its three layers. The governance layer establishes policies, accountability structures, and lineage requirements. The integrity layer operationalizes these policies through continuous validation, monitoring, and verification mechanisms. The cybersecurity layer protects both governance and integrity processes from malicious interference. Information flows bidirectionally among the layers through automated monitoring systems, incident management processes, and governance review mechanisms, thereby ensuring continuous assurance throughout the predictive audit lifecycle.

5. 0 Implementation Considerations

The successful implementation of the proposed framework requires the alignment of organizational structures, governance

mechanisms, technology infrastructure, and workforce capabilities. This section outlines the critical implementation requirements necessary to operationalize the framework and sustain its effectiveness in predictive audit environments.

5.1 Organizational roles and responsibilities

Effective implementation of the integrated framework requires clearly defined roles, responsibilities, and accountability structures that extend beyond traditional three-lines-of-defence governance models.(Rikhardsson *et al*., 2019). The Data Owner (most often a senior finance or business process owner) holds ultimate accountability for ensuring the accuracy, completeness, and authorization of the source system data that has gone into audit analytics (Akanni *et al*., 2026). This person approves changes to the master data, authorizes data classification, and guarantees that the datasets are still reflective of the whole population that was subjected to audit (Pettus *et al*., 2021).

The Model Owner, who usually would sit in the internal audit or specialist audit analytics function, is accountable for the entire lifecycle of predictive audit modeling, from initial design to training, validation, deployment, performance monitoring, and eventual decommissioning (Raji *et al*., 2020). The Model Owner must document the risk assessment of the predictive audit models, endorse retraining triggers, provide evidence that the model is still performing within accuracy, robustness, and explainability thresholds for reliance as audit evidence according to ISA 315 (Revised) and other standards (Hollenberg *et al*., 2019).

The Chief Audit Executive and Chief Data Officer jointly oversee the Audit Data Steward, who is a cross-layer controls hybrid role, together with the CISO (Burhan *et al*., 2023). The Audit Data Steward is responsible for lineage completeness, metadata quality, integrity rule maintenance, and drift response, while the CISO controls the cybersecurity perimeter, adversarial testing, access controls, and incident playbooks (Adepoju *et al*., 2023). RACI matrices and quarterly joint attestation formalize that no weak link may undermine the predict audit scheme. Collectively, these governance roles ensure accountability, transparency, and segregation of duties throughout the predictive audit lifecycle while minimizing operational and model-related risks.

5.2 Technology stack recommendations

The proposed framework requires an integrated technology ecosystem capable of supporting governance, integrity verification, explainability, cybersecurity, and continuous monitoring functions. A modern, domain-oriented architecture like data mesh is advocated to thwart a centralized bottleneck and enforce accountability at the source (Dibouliya & Jotwani, 2023). Each business domain (for example, Procure-to-Pay, Order-to-Cash) makes audit-relevant data products available through self-service portals, equipped with governance metadata, while the audit function consumes these products within a dedicated analytical domain, ensuring independence and mitigating the chances of transformation (Anomah *et al*., 2021).

For the integrity and quality layer, Great Expectations or Monte Carlo provide declarative data testing and observability, while Alibi Detect and River provide open-source production-grade drift and outlier detection (Guntupalli, 2021). Explainability and adversarial robustness are underpinned by SHAP, InterpretML, and the Adversarial Robustness Toolbox (ART), and the results are automatically featured in an immutable audit trail (via, for example, Apache Atlas or Amundsen for lineage and OpenLineage integrated) (Fidel *et al*., 2020).

Runtime security is fortified using Falco or Sysdig for container and host behavioral monitoring; Trivy/Grype for model container

vulnerability scanning; and implementation of signed model artifacts through Gatekeeper policies in Kubernetes (Gantikow *et al*., 2019). All logs and alerts are channeled to a centralized SIEM/SOAR platform (e.g., Splunk, Elastic, or Microsoft Sentinel) with pre-built playbooks for ML-specific incidents to ensure spill containment and forensic preservation (Victor & Marcel, 2022). The selection of specific technologies should be guided by organizational size, regulatory requirements, audit complexity, and existing digital maturity levels.

5.3 Maturity model (5 levels suggested)

Predictive models are created and deployed by people based on their localized private data sets, (Varma, 2020). These datasets are in the absence of a formal governance structure, integrity checks, or any tighter cybersecurity controls than basic IT access restrictions. The lineage of these models is undocumented. Model output is not acceptable for any purpose as audit evidence.

Policies, roles, and basic tooling (data catalog, Great Expectations tests, simple drift alerts) are established. Lineage is manually or semi-automatically recorded, adversarial robustness testing is conducted pre-deployment, and model usage is allowed only for risk assessment-not direct evidence (Gao *et al*., 2019). Cybersecurity controls were implemented following the standard ISO 27001 scope.

Total framework integration is fully automated-zero touch lineage, real-time drift and poisoning detection, continuous adversarial monitoring, and a data-to-decision pipeline, signed cryptographically. (Coronado *et al*., 2022). Thus, at Level 5, an organization can participate in the standard-setting process (e.g. IAASB technology working groups), rely on generative AI for synthetic poisoning defense, and have their predictive outputs recognized as primary audit evidence by regulators, materially reducing the scope of traditional substantive testing (Spulber, 2019).

Fig. 3 :Maturity Model for Predictive Audit Data Governance (Data Governance Institute, 2023)

6.0 Discussion and Implications

This section evaluates the practical implications of the proposed framework for audit quality, efficiency, regulatory compliance, and organizational adoption while highlighting implementation challenges and future research opportunities.

6.1 Benefits for audit quality and efficiency

The proposed framework has the potential to significantly improve audit quality by enabling

population-level risk assessment, continuous monitoring, and enhanced validation of audit evidence. (Tanvir *et al*., 2020). Each predictive risk score has thus traceability to signed data lineage and real-time drift detection so that a substantial place on reliance can be put on analytical procedures as substantive evidence under ISA 520 and AU-C 520.Test evaluations in early fields of similar continuous-monitoring systems herald reductions of 30-70% in undetected material weaknesses and highly quicker detection of fraud (Acar *et al*.,2021).

Great efficiency gain is further detailed: the first month of an audit is traditionally used for manual data reconciliation and cleansing over weeks. However, now, with automated gateways for integrity and pre-approved data products, such laborious tasks can be sidestepped (Polit *et al*., 2022). Dynamic risk scoring focuses effort on the higher 5-15% of anomalous transactions, or journal entries, thus enabling audit teams to reallocate 40-60% of their routine testing hours from lower-impact areas into more complex judgement areas such as management estimates, related-party relationships, and narrative disclosures-areas where professional scepticism adds maximum value (Ogunsola *et al*., 2021). Beyond efficiency gains, the framework enhances audit transparency, strengthens evidence reliability, and supports more informed professional judgment.

6.2 Regulatory compliance advantages

According to ISA 315 Revised A147–A154, PCAOB AS 1105, and AS 2201, increased expectations arise from regulators and standard-setters with regards to documented comprehension and testing of automated tools. The immovable audit trail of this framework can provide exact reproducibility and transparency that SEC, PCAOB, and FRC inspectors would demand during their firm inspections (Kend & Nguyen, 2020). Several examples of Big-Four approaches cite lineage and drift controls as «best practice» in defending reliance on predictive analytics (Liew *et al*., 2022).

Under GDPR, CCPA, or prospective AI regulations, the framework meets Article 5(2) requirements on accountability and data-protection-by-design through cryptographic provenance, right-to-explanation tooling (SHAP values stored with each flagged transaction) and automatic flags to minimise personal data (Fakeyede *et al*., 2023). This casts the audit function as a compliance leader rather than a laggard, therefore reducing the enterprise risk of being subject to regulatory findings or enforcement actions due to inadequate technology adoption (Celestin, 2020). As regulatory scrutiny of AI-enabled decision systems continues to increase, organizations implementing integrated governance frameworks are likely to be better positioned to demonstrate compliance, accountability, and audit readiness.

6.3 Challenges and barriers to adoption

The greatest barrier remains organizational silos and skill shortages (Watson, 2022). Disputes over data ownership between Finance, IT, and Internal Audit serve to delay the adoption of data mesh principles, and only a very small handful of audit functions have staff trained in both auditing standards and adversarial machine-learning defence (Dibouliya *et al*., 2023). For the larger organizations, this could mean an initial investment of USD 2–5 million for secure enclaves, lineage platforms, and red-team capability, which tends to bring about budgetary resistance in an industry that has always favored spreadsheet-based analytics.

Cultural resistance along with fears of excessive reliance on "black-box" models also remain (Vivek, 2023). Senior audit partners formed by decades of sampling tradition sometimes look at continuous predictive monitoring as a process that reduces, rather than enhances, professional judgment (Alberti *et al*., 2022). The smaller firms and mid-tier

practices are particularly challenged by the fact that the ecosystem of tools that are needed (Great Expectations, Alibi Detect, ART) is predominantly open-source and requires DevOps maturity that many lack. Data privacy concerns, regulatory uncertainty, and the absence of universally accepted standards for AI-enabled auditing may further complicate implementation efforts, particularly across multinational organizations.

6.4 Future research directions

Future research should focus on the empirical validation of the proposed framework through field experiments, quasi-experimental studies, and longitudinal investigations across diverse audit environments.(Huber, 2023). This could include looking at audit quality metrics (like restatement rates, material weakness detection lag, or inspection findings) between adopters and those who have not adopted. Especially longitudinal studies would provide cost-benefit ratios on varying maturity levels for standard setters considering formal uptake of predictive analytics in audits and some further analysis on cost-benefit ratios over time (Rahaman *et al*., 2023).

Integration into the new regulatory frameworks, such as the risk-classification audit models of the EU AI Act or NIST AI RMF governance profiles, and the IAASB's forthcoming technology project on this (De Almeida *et al*., 2021). One can also move towards the creation of adversarial benchmark datasets for auditing, the standardised explainability fidelity metrics acceptable to regulators, and the techniques of generative AI for synthetic poisoning defence-areas that potentially cover the remaining gap between academic research and practical audit assurance in an increasingly algorithmic financial reporting ecosystem (Costanza-Chock *et al*., 2022). Additional research should also investigate the role of generative AI, federated learning, blockchain-enabled audit trails, and explainability assurance metrics in enhancing the reliability and regulatory acceptance of predictive audit systems.

7.0 Conclusion

7.0 Conclusion

This conceptual paper proposed an integrated audit-centric framework that unifies data governance, data integrity, and cybersecurity controls across the lifecycle of predictive audit models. By positioning immutable data lineage and cryptographic provenance at the core, continuous integrity verification as the operational layer, and zero-trust cybersecurity as the protective perimeter, the framework addresses the interconnected risks of bias, data poisoning, concept drift, adversarial attacks, and explainability manipulation that threaten the reliability of AI-driven audit evidence. The proposed framework represents one of the first comprehensive efforts to align governance, integrity, and cybersecurity requirements with the evidentiary expectations of ISA 500, ISA 315 (Revised), and the Sarbanes–Oxley Act (SOX), while accounting for the dynamic characteristics of machine-learning systems. In doing so, it provides a maturity-based implementation roadmap for practitioners and a structured benchmark for regulators and standard-setters to evaluate technology-enabled assurance systems.

Although the framework offers a strong theoretical foundation and practical implementation guidance, its effectiveness must ultimately be validated through empirical application in real-world audit environments. Future research should therefore focus on controlled field experiments, case studies, and longitudinal investigations that assess the framework's impact on audit quality, operational efficiency, regulatory compliance, and model reliability. Additional studies may also explore the integration of emerging technologies such as generative artificial intelligence, federated learning, blockchain-enabled audit trails, and advanced explainability assurance mechanisms. Until

such empirical evidence becomes available, the benefits of predictive auditing will remain accompanied by legitimate concerns regarding data quality, model integrity, and cybersecurity risks. Nevertheless, the proposed framework provides an important foundation for the next generation of predictive audit practices and contributes to the advancement of transparent, resilient, and trustworthy AI-enabled assurance in an increasingly digital financial reporting environment.

8.0 References

Aboagye, E. F., Borketey, B., Danquah, K., Borketey, D. (2022). A Predictive Modeling Approach for Optimal Prediction of the Probability of Credit Card Default. International Research Journal of Modernization in Engineering Technology and Science. 4(8), 2425-2441

Abolade, Y.A. (2023). Bridging Mathematical Foundations and intelligent system: A statistical and machine learning approach. Communications in Physical Sciences, 9(4): 773-783

Acar, D., Gal, G., Öztürk, M. S., & Usul, H. (2021). A case study in the implementation of a continuous monitoring system. *Journal of Emerging Technologies in Accounting*, *18*(1), 17-25.

Ademilua, D. A., & Areghan, E. (2022). AI-Driven Cloud Security Frameworks: Techniques, Challenges, and Lessons from Case Studies. Communication in Physical Sciences, 8(4), 674–688.

Ademilua, D.A. (2021). Cloud Security in the Era of Big Data and IoT: A Review of Emerging Risks and Protective Technologies. Communication in Physical Sciences, 7(4):590-604

Adepoju, A. H., Austin-Gabriel, B. L. E. S. S. I. N. G., Hamza, O. L. A. D. I. M. E. J. I., & Collins, A. N. U. O. L. U. W. A. P. O. (2022). Advancing monitoring and alert systems: A proactive approach to improving reliability in complex data ecosystems. *IRE Journals*, *5*(11), 281-282.

Adepoju, A. H., Austin-Gabriel, B., Eweje, A., & Hamza, O. (2023). A data governance framework for high-impact programs: Reducing redundancy and enhancing data quality at scale. *International Journal of Multidisciplinary Research and Growth Evaluation*, *4*(6), 1141-1154.

Adeyemi, D. S. (2023). Autonomous Response Systems in Cybersecurity: A Systematic Review of AI-Driven Automation Tools. Communication in Physical Sciences, 9(4), 878-898.

Aguboshim, F. C., Obiokafor, I. N., & Emenike, A. O. (2023). Sustainable data governance in the era of global data security challenges in Nigeria: A narrative review. *World J. Adv. Res. Rev*, *17*(2), 378-385.

Akanni, F., Idowu, K., Odozor, L., & Waheed, B. (2026). *Cyber-financial risk analytics: Integrating business intelligence with threat modeling*. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*. https://doi.org/10.32628/CSEIT26121371

Akinsanya, M. O., Adeusi, O. C., Ajanaku, K. B. (2022). A Detailed Review of Contemporary Cyber/Network Security Approaches and Emerging Challenges. Communication in Physical Sciences. 8(4): 707-720

Akinsanya, M. O., Bello, A. B., Adeusi, O. C. (2023). A Comprehensive Review of Edge Computing Approaches for Secure and Efficient Data Processing in IoT Networks. Communication in Physical Sciences. 9(4): 870-720

Alberti, C. T., Bedard, J. C., Bik, O., & Vanstraelen, A. (2022). Audit firm culture: Recent developments and trends in the literature. *European Accounting Review*, *31*(1), 59-109.

Al-Sada, B., Sadighian, A., & Oligeri, G. (2023). Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database. *Ieee Access*, *12*, 1217-1234.

Anisetti, M., Ardagna, C. A., Bena, N., & Damiani, E. (2023). Rethinking certification for trustworthy machine-learning-based applications. *IEEE Internet Computing*, *27*(6), 22-28.

Ann Jo, A., & Deni Raj, E. (2023). Post hoc interpretability: Review on new frontiers of interpretable ai. *Advances in Distributed Computing and Machine Learning: Proceedings of ICADCML 2023*, 261-276.

Anomah, S., Ayeboafo, B., & Aduamoah, M. (2021). An audit risk model for it audit ecosystems and digital transformation (dx) decision making. *Edpacs*, *64*(2), 1-33.

Appelbaum, D., Showalter, D. S., Sun, T., & Vasarhelyi, M. A. (2021). A framework for auditor data literacy: A normative position. *Accounting Horizons*, *35*(2), 5-25.

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). 738-753

Aswathy, S. U., & Tyagi, A. K. (2022). Privacy breaches through cyber vulnerabilities: Critical issues, open challenges, and possible countermeasures for the future. In *Security and privacy-preserving techniques in wireless robotics* (pp. 163-210). CRC Press.

Barr-Pulliam, D., Brown-Liburd, H. L., & Munoko, I. (2022). The effects of person-specific, task, and environmental factors on digital transformation and innovation in auditing: A review of the literature. *Journal of International Financial Management & Accounting*, *33*(2), 337-374.

Batini, C., Bellandi, V., Ceravolo, P., Moiraghi, F., Palmonari, M., & Siccardi, S. (2021, September). Semantic data integration for investigations: lessons learned and open challenges. In *2021 IEEE International Conference on Smart Data Services (SMDS)* (pp. 173-183). IEEE.

Bayya, A. K. (2022). Cutting-Edge Practices for Securing APIs in FinTech: Implementing Adaptive Security Models and Zero Trust Architecture. *International journal of applied engineering and technology (London)*, *4*, 279-298.

Bhaskaran, S. V. (2020). Integrating data quality services (dqs) in big data ecosystems: Challenges, best practices, and opportunities for decision-making. *Journal of Applied Big Data Analytics, Decision-Making, and Predictive Modelling Systems*, *4*(11), 1-12.

Booth, J., Metz, D. W., Tarkhanyan, D. A., & Cheruvu, S. (2023). Machine learning security and trustworthiness. In *Demystifying Intelligent Multimode Security Systems: An Edge-to-Cloud Cybersecurity Solutions Guide* (pp. 137-222). Berkeley, CA: Apress.

Bordt, S., Finck, M., Raidl, E., & Von Luxburg, U. (2022, June). Post-hoc explanations fail to achieve their purpose in adversarial contexts. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 891-905).

Bukhari, T. T., Oladimeji, O., Etim, E. D., & Ajayi, J. O. (2021). Automated control monitoring: A new standard for continuous audit readiness. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *7*(3), 711-735.

Burhan, M., Alam, H., Arsalan, A., Rehman, R. A., Anwar, M., Faheem, M., & Ashraf, M.

W. (2023). A comprehensive survey on the cooperation of fog computing paradigm-based IoT applications: layered architecture, real-time security issues, and solutions. *IEEE Access*, *11*, 73303-73329.

Caballero, I., Gualo, F., Rodríguez, M., & Piattini, M. (2023). Maturity models for data governance. In *Data Governance: From the Fundamentals to Real Cases* (pp. 139-162). Cham: Springer Nature Switzerland.

Carabantes, M. (2023). Why artificial intelligence is not transparent: a critical analysis of its three opacity layers. In *Handbook of Critical Studies of Artificial Intelligence* (pp. 424-434). Edward Elgar Publishing.

Celestin, M. (2020). The effect of regulatory changes on auditing standards: How global compliance rules are reshaping the audit profession. *Brainae Journal of Business, Sciences and Technology*, *4*(1), 34-43.

Chang, S. A., Hussein, M. E., Leung, P. W. Y., & Tam, K. (2021). Modeling and implementing internal control automation in compliance with the Sarbanes-Oxley act. *Pan-Pacific Journal of Business Research*, *12*(1), 29-48.

Charmet, F., Tanuwidjaja, H. C., Ayoubi, S., Gimenez, P. F., Han, Y., Jmila, H., ... & Zhang, Z. (2022). Explainable artificial intelligence for cybersecurity: a literature survey. *Annals of Telecommunications*, *77*(11), 789-812.

Chhabra Roy, N., & Prabhakaran, S. (2023). Sustainable response system building against insider-led cyber frauds in banking sector: a machine learning approach. *Journal of Financial Crime*, *30*(1), 48-85.

Chukwudi, D. C., Oladunjoye M. (2023). Communication In Physical Sciences. Geophysical Exploration of Coastal Saline Water Intrusion: A Study of Ikoyi and Banana Island, Lagos State. 9(4): 834-846

Corbett-Wilkins, R., McLaughlin, C., Taylor, A., Lloyd, S., Bellis, C., Yeend, R., & Paynter, K. (2023). Cyber Risk and Insurance. In *The Global Insurance Market and Change* (pp. 286-332). Informa Law from Routledge.

Coronado, E., Behravesh, R., Subramanya, T., Fernandez-Fernandez, A., Siddiqui, M. S., Costa-Pérez, X., & Riggio, R. (2022). Zero touch management: A survey of network automation solutions for 5G and 6G networks. *IEEE Communications Surveys & Tutorials*, *24*(4), 2535-2578.

Costanza-Chock, S., Raji, I. D., & Buolamwini, J. (2022, June). Who Audits the Auditors? Recommendations from a field scan of the algorithmic auditing ecosystem. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1571-1583).

Dako, O. F., Onalaja, T. A., Nwachukwu, P. S., Bankole, F. A., & Lateefat, T. (2020). Big data analytics improving audit quality, providing deeper financial insights, and strengthening compliance reliability. *Journal of Frontiers in Multidisciplinary Research*, *1*(2), 64-80.

De Almeida, P. G. R., Dos Santos, C. D., & Farias, J. S. (2021). Artificial intelligence regulation: a framework for governance. *Ethics and Information Technology*, *23*(3), 505-525.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2019). COBIT as a Framework for Enterprise Governance of IT. In *Enterprise governance of information technology: Achieving alignment and value in digital organizations* (pp. 125-162). Cham: Springer International Publishing.

Dibouliya, A., & Jotwani, D. V. (2023). Review on data mesh architecture and its impact. *Journal of Harbin Engineering University*, *44*(7), 2353-2363.

Eitzinger, A., Cock, J., Atzmanstorfer, K., Binder, C. R., Läderach, P., Bonilla-Findji, O., ... & Jarvis, A. (2019). GeoFarmer: A monitoring and feedback system for agricultural development projects. *Computers and electronics in agriculture*, *158*, 109-121.

Enyiorji, P. (2023). Blockchain-enforced data lineage architectures with formal verification workflows enabling auditable AI decision chains across regulated fintech compliance regimes and supervisory reporting. *International Journal of Science and Research Archive*, *9*(2), 1201-1217.

Fakeyede, O. G., Okeleke, P. A., Hassan, A., Iwuanyanwu, U., Adaramodu, O. R., & Oyewole, O. O. (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. *International Journal of Research in Engineering and Science*, *11*(11), 45-58.

Feng, F., Liu, X., Yong, B., Zhou, R., & Zhou, Q. (2019). Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. *Ad hoc networks*, *84*, 82-89.

Fidel, G., Bitton, R., & Shabtai, A. (2020, July). When explainability meets adversarial learning: Detecting adversarial examples using shap signatures. In *2020 international joint conference on neural networks (IJCNN)* (pp. 1-8). IEEE.

Finlayson, S. G., Bowers, J. D., Ito, J., Zittrain, J. L., Beam, A. L., & Kohane, I. S. (2019). Adversarial attacks on medical machine learning. *Science*, *363*(6433), 1287-1289.

Folorunso, T. N., Idowu, K., & Balogun, A. (2025). AI-driven financial risk forecasting: A multi-model ensemble approach for enterprise decision intelligence. *Journal of Computational Analysis and Applications, 34*(3). https://eudoxuspress.com/index.php/pub/article/view/5080

Gantikow, H., Reich, C., Knahl, M., & Clarke, N. (2019, May). Rule-based security monitoring of containerized environments. In *International Conference on Cloud Computing and Services Science* (pp. 66-86). Cham: Springer International Publishing.

Gao, X., Boccalini, S., Kitslaar, P. H., Budde, R. P., Tu, S., Lelieveldt, B. P., ... & Reiber, J. H. (2019). A novel software tool for semi-automatic quantification of thoracic aorta dilatation on baseline and follow-up computed tomography angiography. *The international journal of cardiovascular imaging*, *35*(4), 711-723.

Georgiadis, G., & Poels, G. (2021). Enterprise architecture management as a solution for addressing general data protection regulation requirements in a big data context: a systematic mapping study. *Information Systems and e-Business Management*, *19*(1), 313-362.

Goldblum, M., Tsipras, D., Xie, C., Chen, X., Schwarzschild, A., Song, D., ... & Goldstein, T. (2022). Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *45*(2), 1563-1580.

Gu, Z., Jamjoom, H., Su, D., Huang, H., Zhang, J., Ma, T., ... & Molloy, I. (2019, June). Reaching data confidentiality and model accountability on the caltrain. In *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 336-348). IEEE.

Guntupalli, B. (2021). My Approach to Data Validation and Quality Assurance in ETL Pipelines. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(3), 62-73.

Guo, L. L., Pfohl, S. R., Fries, J., Posada, J., Fleming, S. L., Aftandilian, C., ... & Sung, L. (2021). Systematic review of approaches to preserve machine learning performance in the presence of temporal

dataset shift in clinical medicine. *Applied clinical informatics*, *12*(04), 808-815.

Hollenberg, S. M., Warner Stevenson, L., Ahmad, T., Amin, V. J., Bozkurt, B., Butler, J., ... & Storrow, A. B. (2019). 2019 ACC expert consensus decision pathway on risk assessment, management, and clinical trajectory of patients hospitalized with heart failure: a report of the American College of Cardiology Solution Set Oversight Committee. *Journal of the American College of Cardiology*, *74*(15), 1966-2011.

Hossain, M. A., & Khan, M. K. (2022). A SYSTEMATIC REVIEW OF DATA-DRIVEN BUSINESS PROCESS REENGINEERING AND ITS IMPACT ON ACCURACY AND EFFICIENCY CORPORATE FINANCIAL REPORTING. *International Journal of Business and Economics Insights*, *2*(4), 01-41.

Hsu, Y. F., & Lee, W. P. (2020). Evaluation of the going-concern status for companies: An ensemble framework-based model. *Journal of Forecasting*, *39*(4), 687-706.

Huang, F., No, W. G., Vasarhelyi, M. A., & Yan, Z. (2022). Audit data analytics, machine learning, and full population testing. *The Journal of Finance and Data Science*, *8*, 138-144.

Huber, K. (2023). Estimating general equilibrium spillovers of large-scale shocks. *The Review of Financial Studies*, *36*(4), 1548-1584.

Idowu, K., Cherotich, V., Aniebonam, E. E., Odozor, L., & During, A. (2025). *Integrating AI and machine learning into cyber risk management for critical utility systems*. *International Journal of Artificial Intelligence Engineering and Technology*. https://doi.org/10.54660/IJAIET.2025.6.2.32-48

Idowu, K., Leslie, A., Twayana, S., Nitzan, Y., & Waheed, B. O. (2026). *Real-time detection of DDoS and phishing attacks for enhanced banking security*. *International Journal of Scientific Research in Science Engineering and Technology*. https://doi.org/10.32628/IJSRSET2613313

Iliashenko, O., Iliashenko, V., & Shuvalova, A. (2022, April). Development of the Company's IT Infrastructure in the DAMA-DMBOK Standard Implementation. In *International Scientific Conference "Digital Transformation on Manufacturing, Infrastructure & Service"* (pp. 732-744). Cham: Springer Nature Switzerland.

Ilori, O., Lawal, C. I., Friday, S. C., Isibor, N. J., & Chukwuma-Eke, E. C. (2022). Cybersecurity auditing in the digital age: A review of methodologies and regulatory implications. *Journal of Frontiers in Multidisciplinary Research*, *3*(1), 174-187.

Jegorova, M., Kaul, C., Mayor, C., O'Neil, A. Q., Weir, A., Murray-Smith, R., & Tsaftaris, S. A. (2022). Survey: Leakage and privacy at inference time. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *45*(7), 9090-9108.

Juntunen, T., & Virta, S. (2019). Security dynamics: Multilayered security governance in an age of complexity, uncertainty, and resilience. *Leading change in a complex world: Transdisciplinary perspectives*, 67-84.

Kassem, R. (2023). Investigating the black box of external audit practice: the paradox of auditors' failure in detecting and reporting fraud. *Journal of Accounting Literature*, *45*(2), 406-424.

Kend, M., & Nguyen, L. A. (2020). Big data analytics and other emerging technologies: the impact on the Australian audit and assurance

profession. *Australian Accounting Review*, *30*(4), 269-282.

Kumar, R. S. S., Nyström, M., Lambert, J., Marshall, A., Goertzel, M., Comissoneru, A., ... & Xia, S. (2020, May). Adversarial machine learning-industry perspectives. In *2020 IEEE security and privacy workshops (SPW)* (pp. 69-75). IEEE.

Lawal, S. A., Omefe, S., Balogun, A. K., Michael, C., Bello, S. F., Taiwo, I., Ifiora, K. N. (2021). Circular Supply Chains in the Al Era with Renewable Energy Integration and Smart Transport Networks. Communication in Physical Sciences, 7(4): 605-629

Lehner, O. M., Leitner-Hanetseder, S., Eisl, C., & Knoll, C. (2022). Artificial intelligence-driven accounting (AIDA): future insights and organisational implications. In *Artificial Intelligence in Accounting* (pp. 6-34). Routledge.

Lekkala, S., Avula, R., & Gurijala, P. (2022). Big Data and AI/ML in Threat Detection: A New Era of Cybersecurity. *Journal of Artificial Intelligence and Big Data*, *2*(1), 32-48.

Li, Z., Liu, Y., He, X., Yu, N., Backes, M., & Zhang, Y. (2022, November). Auditing membership leakages of multi-exit networks. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1917-1931).

Liew, A., Boxall, P., & Setiawan, D. (2022). The transformation to data analytics in Big-Four financial audit: what, why and how?. *Pacific Accounting Review*, *34*(4), 569-584.

Ling, J., Feng, K., Wang, T., Liao, M., Yang, C., & Liu, Z. (2023). Data modeling techniques for pipeline integrity assessment: A state-of-the-art survey. *IEEE Transactions on Instrumentation and Measurement*, *72*, 1-17.

Liu, J., Chu, X., Wang, Y., & Wang, M. (2022, November). Deep text retrieval models based on DNN, CNN, RNN and transformer: A review. In *2022 IEEE 8th International Conference on Cloud Computing and Intelligent Systems (CCIS)* (pp. 391-400). IEEE.

Lomas, E. (2020). Information governance and cybersecurity: Framework for securing and managing information effectively and ethically. In *Cybersecurity for Information Professionals* (pp. 109-130). Auerbach Publications.

Malgieri, G. (2022). Automated decision-making and data protection in Europe. In *Research Handbook on Privacy and Data Protection Law* (pp. 433-448). Edward Elgar Publishing.

McGregor, D., & Carpenter, R. (2020). Potential threats for the auditing profession, audit firms and audit processes inherent in using emerging technology. *The Business and Management Review*, *11*(2), 45-54.

Mehdiyev, N., Houy, C., Gutermuth, O., Mayer, L., & Fettke, P. (2021, March). Explainable artificial intelligence (XAI) supporting public administration processes–on the potential of XAI in tax audit processes. In *International Conference on Wirtschaftsinformatik* (pp. 413-428). Cham: Springer International Publishing.

Mehmood, H., Kostakos, P., Cortes, M., Anagnostopoulos, T., Pirttikangas, S., & Gilman, E. (2021). Concept drift adaptation techniques in distributed environment for real-world data streams. *Smart Cities*, *4*(1), 349-371.

Mei, A., Levy, S., & Wang, W. (2023, December). ASSERT: Automated safety scenario red teaming for evaluating the robustness of large language models. In *Findings of the Association for Computational Linguistics: EMNLP 2023* (pp. 5831-5847).

Möller, D. P. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 231-271). Cham: Springer Nature Switzerland.

Nandakumar, K., Vinod, V., Akbar Batcha, S. M., Sharma, D. K., Elangovan, M., Poonia, A., ... & Sengan, S. (2021). Securing data in transit using data-in-transit defender architecture for cloud communication. *Soft Computing*, *25*(18), 12343-12356.

Nanfa, C. A., Aminu, M. B., Christopher, S. D., Akudo, E. O., Musa, K. O., Aigbadon, G. O., & Millicent, O. I. (2022). Electric Resistivity for Evaluating Groundwater Potential Along the Drainage Zones In the Part of Jos North, Plateau State, Nigeria. European Journal of Environment and Earth Sciences, 3(6), 59–68. https://doi.org/10.24018/ejgeo.2022.3.6.347

Naseer, M., Khan, S., Hayat, M., Khan, F. S., & Porikli, F. (2021). On generating transferable targeted perturbations. In *Proceedings of the IEEE/CVF International Conference on Computer Vision* (pp. 7708-7717).

No, W. G., Lee, K., Huang, F., & Li, Q. (2019). Multidimensional audit data selection (MADS): A framework for using data analytics in the audit data selection process. *Accounting Horizons*, *33*(3), 127-140.

Nwaimo, C. S., Oluoha, O. M., & Oyedokun, O. (2023). Ethics and governance in data analytics: balancing innovation with responsibility. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *9*(3), 823-856.

Obamuwagun, O. E. (2023). A comprehensive review on mental health, psychological wellbeing, and performance challenges of elite athletes in competitive sports. Communication in Physical Sciences, 9(4), 859-869. https://doi.org/10.4314/cps.v9i4.12

Odozor, L., Berko, S. N., Obu, A. U., & Idowu, K. (2025). Building a resilient U.S. cybersecurity workforce through practical training. *International Journal of Scientific and Management Research, 8*(8), 30–36.

Ogunsola, K. O., Balogun, E. D., & Ogunmokun, A. S. (2021). Enhancing financial integrity through an advanced internal audit risk assessment and governance model. *International Journal of Multidisciplinary Research and Growth Evaluation*, *2*(1), 781-790.

Okolo, J. N. (2023). A Review of Machine and Deep Learning Approaches for Enhancing Cybersecurity and Privacy in the Internet of Devices. Communication in Physical Sciences. 9(4): 754-772.

Omefe, S., Lawal, S. A., Bello, S. F., Balogun, A. K., Taiwo, I., Ifiora, K. N. (2021). AI-Augmented Decision Support System for Sustainable Transportation and Supply Chain Management: A Review. Communication In Physical Sciences. 7(4), 630-642.

Onwuegbuchi, O., Ibiyeye, A. O., Okolo, J. N., Adeniji, S. A. (2023). Cybersecurity Risks in the Fintech Ecosystem: Regulatory and Technological Perspectives. Communication in Physical Sciences, 9(4), 947-967.

Pangastuti, L. A. (2023). The Role of Internal Auditing in Upholding Corporate Governance Standards. *Advances in Managerial Auditing Research*, *1*(3), 114-124.

Pemmasani, P. K., & Abd Nasaruddin, M. A. (2022). Strengthening Public Sector Data Governance: Risk Management Strategies for Government Organizations. *International Journal of Modern Computing*, *5*(1), 108-118.

Pettus, J. A., Pajk, A. L., Glatz, A. C., Petit, C. J., Goldstein, B. H., Qureshi, A. M., ... & McCracken, C. M. (2021). Data quality methods through remote source data verification auditing: results from the Congenital Cardiac Research Collaborative. *Cardiology in the Young*, *31*(11), 1829-1834.

Pimentel, J. F., Freire, J., Murta, L., & Braganholo, V. (2019). A survey on collecting, managing, and analyzing provenance from scripts. *ACM Computing Surveys (CSUR)*, *52*(3), 1-38.

Polit, A. T., Balram-Knutson, S. S., Audi, E., Becker, T., Boynton, W. V., Dean, D., ... & Lauretta, D. S. (2022, March). Science Operations Planning and Implementation for the OSIRIS-REx Mission, Part 1: Process. In *2022 IEEE Aerospace Conference (AERO)* (pp. 1-17). IEEE.

Rahaman, M. M., Hossain, M. M., & Bhuiyan, M. B. U. (2023). Disclosure of key audit matters (KAMs) in financial reporting: evidence from an emerging economy. *Journal of Accounting in Emerging Economies*, *13*(3), 666-702.

Rahman, M. S., Bhowmik, P. K., Hossain, B., Tannier, N. R., Amjad, M. H. H., Chouksey, A., & Hossain, M. (2023). Enhancing Fraud Detection Systems in the USA: A Machine Learning Approach to Identifying Anomalous Transactions. *Journal of Economics, Finance and Accounting Studies*, *5*(5), 145-160.

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., ... & Barnes, P. (2020, January). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 conference on fairness, accountability, and transparency* (pp. 33-44).

Rikhardsson, P., Singh, K., & Best, P. (2019). Exploring continuous auditing solutions and internal auditing: A research note. *Accounting and Management Information Systems*, *18*(4), 614-639.

Rohde, K. (2022). Pervasive Governance–Understand and Secure Your Transaction Data & Content. In *Cybersecurity and Privacy-Bridging the Gap* (pp. 169-188). River Publishers.

Sánchez, C., Schneider, G., Ahrendt, W., Bartocci, E., Bianculli, D., Colombo, C., ... & Weiss, A. (2019). A survey of challenges for runtime verification from advanced application domains (beyond software). *Formal Methods in System Design*, *54*(3), 279-335.

Siddique, S., Haque, M. A., George, R., Gupta, K. D., Gupta, D., & Faruk, M. J. H. (2023). Survey on machine learning biases and mitigation techniques. *Digital*, *4*(1), 1-68.

Singh, N., Lai, K. H., Vejvar, M., & Cheng, T. E. (2019). Data-driven auditing: A predictive modeling approach to fraud detection and classification. *Journal of Corporate Accounting & Finance*, *30*(3), 64-82.

Spulber, D. F. (2019). Standard setting organisations and standard essential patents: Voting and markets. *The Economic Journal*, *129*(619), 1477-1509.

Sun, Y., Jia, W., & Liu, S. (2022, July). Is auditors' professional scepticism a "double-edged sword"?. In *Accounting Forum* (Vol. 46, No. 3, pp. 241-263). Routledge.

Tanvir, A., Juie, B. J. A., Tisha, N. T., & Rahman, M. M. (2020). Synergizing big data and biotechnology for innovation in healthcare, pharmaceutical development, and fungal research. *International Journal of Biological, Physical and Chemical Studies*, *2*(2), 23-32.

Tekale, K. M., & Rahul, N. (2022). AI and Predictive Analytics in Underwriting, 2022 Advancements in Machine Learning for Loss Prediction and Customer Segmentation. *International Journal of*

Artificial Intelligence, Data Science, and Machine Learning, *3*(1), 95-113.

Thitiphiromlarp, P., & Pongpech, W. (2023, August). Data Management Framework for Metaverse. In *2023 IEEE Smart World Congress (SWC)* (pp. 1-8). IEEE.

Tiron-Tudor, A., & Deliu, D. (2022). Reflections on the human-algorithm complex duality perspectives in the auditing process. *Qualitative Research in Accounting & Management*, *19*(3), 255-285.

Tjoa, S., Temper, P. K. M., Temper, M., Zanol, J., Wagner, M., & Holzinger, A. (2022, December). AIRMan: An artificial intelligence (AI) risk management system. In *2022 International Conference on Advanced Enterprise Information System (AEIS)* (pp. 72-81). IEEE.

Varma, Y. (2020). Governance-Driven ML Infrastructure: Ensuring Compliance in AI Model Training. *International Journal of Emerging Research in Engineering and Technology*, *1*(1), 20-30.

Victor, H., & Marcel, P. (2022). Integrating Firewalls with SIEM and SOAR Platforms for Automated Threat Response. *International Journal of Trend in Scientific Research and Development*, *6*(3), 2315-2323.

Victoria, G. T. & Omosunlade, O. S. (2020)., A Qualitative Study of Teachers' Perception on the Need for Reviewing the Senior Secondary School Economics Curriculum in Kosofe Local Government, Lagos State. Al-Hikmah Journal of Education, 7(2). ISSN 2384-7662 E-ISSN 2705-2508

Vivek, R. (2023). Enhancing diversity and reducing bias in recruitment through AI: a review of strategies and challenges. *Информатика. Экономика. Управление/Informatics. Economics. Management*, *2*(4), 0101-0118.

Wang, Z., Ma, J., Wang, X., Hu, J., Qin, Z., & Ren, K. (2022). Threats to training: A survey of poisoning attacks and defenses on machine learning systems. *ACM Computing Surveys*, *55*(7), 1-36.

Watson, A. (2022). How organisations can remove barriers to increase workforce collaboration. *Strategic HR Review*, *21*(1), 31-33.

Zhou, S. (2021, March). Current Income Recognition Principle Analysis of IFRS 15, ASC 606 and CAS 14. In *6th International Conference on Financial Innovation and Economic Development (ICFIED 2021)* (pp. 38-44). Atlantis Press.

Declarations

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Ethical Approval

Not applicable

Informed Consent

Not applicable.

Consent for Publication

Not applicable.

Declaration of Competing Interests

The authors declared no competing interests

Data Availability Statement

Data shall be made available upon request

Conflict of Interest

The authors declared no conflict of interest

Author Contributions

latunde Ayeomoni conceptualized the study, developed the framework, and drafted the manuscript. Sugar Raymond contributed to literature review, framework validation, and manuscript revision. Jude Okwuchukwu Ogene provided cybersecurity expertise, critical review, and editing. All authors interpreted findings, reviewed, approved, and accepted responsibility for the final manuscript

.**Publisher's Note**

The authors are solely responsible for the content and conclusions presented in this study.