Intelligent Real-Time Audit Analytics Framework for Automated Manufacturing Finance Operations

Shashikala Valiki
Independent Researcher
shashikala.valiki.researcher@gmail.com

Abstract

Smart manufacturing offers an increasingly integrated and data-driven approach to production, benefitting from the latest technologies like Industry 4.0, Internet of Things (IoT), cloud computing, and Big Data. Real-time artificial intelligence (AI)-enabled auditing and compliance can exploit these technologies to manage compliance in real-time. The advantages of continuous auditing compared with batch auditing are obvious. AI supports the automation of many audit and compliance functions. Although companies have adopted artificial intelligence for various operations, the AI model development process requires considerable resources, time, and expertise. Therefore, the AI-supported real-time audit and compliance framework is within smart manufacturing finance. Key definitions are clarified: Real-Time Audit (RTA), Continuous Controls Monitoring (CCM), AI components (models, data preparation), data lineage, and governance terms. A Continuous Auditing and Continuous Controls Monitoring (CACM) model supports more efficient compliance management and verification. Information Technology Controls and General Application Controls aligned with common regulations can now be automated.

Real-time AI-driven event detection, triggered event correlation, preventive controls, and data-driven tests enhance the framework. Control objectives aligned with mother regulations support validation and assurance. Updated AI model governance principles allow support for production without expertise, acquiring test data during the normal course of business. As datasets accumulate, AI can evolve to operate with minimal specification. With present advances in AI and data-and-compute-storage cloud solutions, the necessary compute and storage resources are available to combine operation and audit seamlessly.

Keywords: Compliance, smart manufacturing, governance, explainability, data privacy, data lineage, risk mitigation, model risk, continuous controls monitoring, anomaly detection, event correlation, supervision, testing, validation, assurance, mapping, pattern design, and validation cycle.

1. Introduction

Smart manufacturing connects computers, physical systems, machines, and devices within and across companies. Financial transactions, records, and other business-enterprise systems expose the financial processes of smart manufacturing to anomalies—mishaps such as data entry, processing errors, cyber-physical hijacking, and opportunistic fraud. Auditing and compliance are key elements of financial process governance and provide assurance about the management and control of financial information.

Unfortunately, traditional auditing and compliance models, guidelines, and standards are largely manual or batch-oriented, not designed for the continuous nature of smart manufacturing. Moreover, the volume and variety of financial transactions make it unfeasible to test all transactions on an ongoing basis. Recent developments in Artificial Intelligence (AI) offer opportunities to augment

ISSN: 3067-283X
AMERICAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 03 ISSUE: 011
RECEIVED: JANUARY 24 REVISED: FEBRUARY 07 ACCEPTED: FEBRUARY 25 PUBLISHED: MARCH 11

and complement traditional approaches. Many aspects of smart manufacturing finance lend themselves to automated AI-driven continuous controls monitoring, event correlation and root-cause analysis, and—most importantly—real-time auditing.

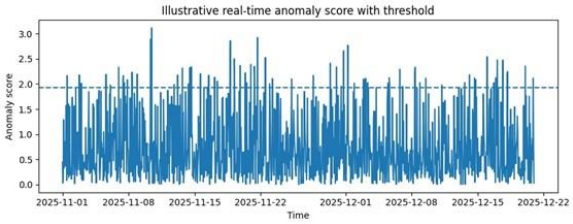
These real-time AI-driven mechanisms are designed to detect anomalies, classify detected anomalies into tests of controls and substantive tests, and automatically initiate remediation, explanation, or approval workflows. When implemented in an operational and tactical sense, this provides a structured and efficient means of determining appropriate response actions arising from deviations in continuous controls monitoring and anomaly detection. Users of smart manufacturing financial processes—management and internal audit—are supported by an AI-powered governance framework capable of tracking, validating, and assuring process controls and data attributes for regulatory compliance purposes.

Fig 1: Artificial Intelligence in Manufacturing Industry Worker Safety

1.1. Scope and objectives

The real-time AI-driven audit framework addresses the finance function of smart manufacturing. It introduces a research agenda that shapes new manufacturing finance capabilities and addresses efficiency and assurance challenges using advanced technologies. Three research questions lay the foundation: How are financial workflows in smart manufacturing modeled as AI-driven audits? What are candidate AI-driven audit mechanisms? Which control catalog supports regulatory compliance? Future advances in AI, governance, and regulation promise growing impact. As the capabilities provided by AI continue to evolve, finance functions in smart manufacturing will find new opportunities to improve efficiency and effectiveness in risk-taking, management, and assurance through automation.

Financial workflows underpin the acquisition of goods and services, fulfillment of sales orders, administration of capital assets, and presentation of financial statements. They are mapped in detail, considering sources, control objectives, data requirements, and potential problems. The mapping serves as a canvas for privileges that support semi-automated approval or proactive identification of exceptions. Processes for procure-to-pay and order-to-cash transactions receive the greatest attention, while the management of capital and revenue recognition require less detail. Process ownership, supporting systems, data lineage, and governance also receive explicit consideration.



1.2. Rationale for real-time AI in manufacturing finance

Real-time AI improves accuracy, efficiency, and risk management in auditing finance functions, aligning financial departments with the broader manufacturing trend of continuous auditing throughout the process. Automating bias-prone manual tasks reduces staff workload and frees them to focus on critical-thinking functions. However, AI is not without limitations – inaccuracies or misapplications can yield false positives, leading to increased effort and resource consumption in investigating manufacturing finance functions. Recent use cases, namely in manufacturing finance, propose continual AI processing acting upon incoming events associated with the finance function, elevating actions, such as decisions and approvals, but identifying root-cause scenarios and suggesting preventive actions.

Batch AI processing operates on a time slice of data, providing a point-in-time outcome. Events occurring after processing and before the next batch cycle lead to risk exposure until the next run. During this silent phase, manual reconciliations, approvals, and postings may require staff intervention – reintroducing bias and human error. Adopting a wider product continuum with continual AI processing improves coverage without onerous manual effort or, through defined risk scenarios, ongoing costly manual intervention. AI models provide optimal coverage across the raw data continuum, continually examining events as they occur.

1.3. Key definitions and concepts

Real-time auditing refers to the dynamic assessment of financial transactions, events, and conditions, along with correlated contextual data, to identify unacceptable deviations as they occur or within prescribed thresholds. It embraces, relies on, extends, and/or incorporates various processes commonly associated with continuous controls monitoring and other types of near real-time monitoring of financial operations. Anchored on computable maintenance plans and business workflows, the latter as well as full controls, not just tests or some subset, form part of the underlying model space. Such model space codifies not just the automated detection, but, where applicable, prevention, reconciliation, and correction of errors, fraud, and other misstatements, whether systemic or opportunistic. Real-time in this context encompasses not just speed of detection, but also escalation and remediation; specific objectives covering detection, monitoring, correlation, and root-cause analysis are detailed subsequently.

Continuous controls monitoring refers to the ongoing, active scrutiny of internal controls and the automated assessment of the controls' operating effectiveness in detecting error and fraud risk among normal business transactions. The requirement for monitoring operating effectiveness on a less-than-continuous basis is eliminated for controls that are fully automated and proven reliable. The evidence arising from this activity — not just the raw detections or anomalies, but the degree to which the controls are behaving as expected under business-as-usual conditions — becomes critical during external audit and compliance validation preparation; feeds other lines of defence; and increases overall stakeholder confidence in the integrity of the data and accounts. Normal business activity and, especially, peak trading periods are often empirically assessed in order to establish realistic control thresholds.

2. Governance and Ethical Considerations

A systematic mapping of compliance objectives to applicable regulatory regimes guides governance. While many AI technologies pose ethical and ethical-ethical threats, these AI-driven manufacturing processes may promote good governance. Data privacy and security play a critical role in finance-as-a-service and traversing ecosystems. Data access requires access controls, risk assessment, encryption, and anonymization.

The utility of AI models depends critically on explainability, accountability, and auditability. Explainable AI methods targeted for non-technical audiences support AI decision traceability, which should include documentation meeting audit standards. Such documentation supports external audit processes; further, the provision of model decision allowance metadata contributes to external user trust in AI models.

Compliance Alignment

The manufacturing finance architecture shown in [Figure A title] hosts numerous compliance objectives for the selected region. Controls bundled into a controls catalog facilitate automation. Mapping to control objective objectives automates testing and validates a larger number of objectives even when only a fraction of the tests—a typical case for controls frameworks—are executed. Coverage mapping demonstrates that full coverage is achievable with typical testing overhead, practically closing the reverse arrow head. Compliance objectives principally from regulatory regimes

and a manufacturing industry standard for data privacy, as well as from the software-as-a-service, finance-as-a-service, and Internet of Things domains.

Covering the mind will also help organizations choose ethical-minded AI technologies. Deep reinforcement learning constitutes a compelling choice for self-driving cars; nevertheless, addressing development methodology shortcomings remains an ethical requirement.

2.1. Compliance alignment with regulatory regimes

Compliance alignment with regulatory regimes is considered for three reasons. First, the universe of applicable compliance requirements can be daunting for smart manufacturing entities that operate in multiple jurisdictions and multiple domains such as audit, data protection, and detailed industry regulations. The wider the set of compliance requirements, the higher the complexity of implementing the needed controls, and consequently the effort to automate continuous controls monitoring and anomaly management. Second, technologies that streamline the design, implementation, and execution of compliance controls are already available. Applying such technologies for a small subset of compliance requirements may indicate the feasibility of extending the approach to the larger control universe. Third, an emerging regulatory trend encourages organizations to automate the ascertainment of their compliance posture. Therefore, establishing alignment with multiple compliance regimes opens the door to such automation.

Although the details of nearly all applicable compliance requirements could be precisely captured with a real-time audit support architecture, the effort involved in doing so would prevent its application. The objective is to strike a balance by capturing the compliance objectives linked to the major regulatory regimes affecting smart manufacturing. Only requirements in the domain of audit, controls, risk and data privacy and protection that are either suitable for direct automation or form the first step towards sensible automation are considered. The identified control objectives cover elements of governance, risk and compliance (GRC) for smart manufacturing.

Equation 1: From raw streams → normalized features (Data ingestion + processing layers)

The architecture ingests ERP/MES/IoT + event streams and **normalizes** data for AI models .

1. **Raw event:**

$$e_t = \{\text{amount}_t,\ \text{vendor}_t,\ \text{country}_t,\ \text{timestamp}_t,\ \ldots\}$$

2. **Normalization / feature engineering** (examples):

- Log transform for heavy-tailed monetary values:

$$x_t^{(amt)} = \log(\text{amount}_t + \epsilon)$$

- Categorical encoding for workflow type (P2P, O2C, etc.):

$$x_t^{(proc)} = \text{onehot}\left(\text{process}_t\right)$$

- "Policy mismatch" indicator (e.g., vendor country in "no-business" region, as described as unusual patterns):

$$x_t^{(pol)} = \begin{cases} 1 & \text{if policy violated} \\ 0 & \text{otherwise} \end{cases}$$

3. **Feature vector:**

$$\mathbf{x}_t = \left[x_t^{(amt)},\ x_t^{(proc)},\ x_t^{(pol)}, \ldots\right]$$

2.2. Data privacy and security safeguards

Effective data privacy and security safeguards enhance the reliability of a real-time AI-driven audit and compliance framework for smart manufacturing. The framework exposes potentially sensitive information (such as customer data, vendor groups, or unusual business transactions) to automated processes and access by numerous stakeholders, presenting significant privacy risks. Data exposure may contravene existing and ever-evolving laws and regulations

(e.g., GDPR) that govern personal information and restrict corporate data movements across geographical borders. Moreover, authorised users, particularly data scientists and developers of AI models, require access to sensitive data to perform their tasks.

The framework ought to adopt appropriate mechanisms and safeguards to mitigate security and privacy risks. These may include user-friendly role-based access controls, end-to-end data encryption at rest and during transmission, anonymisation techniques, and privacy-preserving generative approaches for training AI models on confidential data. Moreover, explicit data consent and storage guidelines, internal data systems and procedures that ensure only authorised data leaks, and auditing of users and their data usage may additionally help diminish risks to privacy and security.

2.3. Explainability, accountability, and auditability

To ensure prudent governance and responsible utilization of AI technologies, it is crucial to establish requirements for explainability, accountability, and auditability. Organizations need to define metrics that quantifiably state the desired levels of explainability for different use cases. Documenting AI decisions and their triggering conditions, in addition to preserving all highly relevant data utilized during the decision-making process, enhances the capability to generate adequate explanations even in the future. Safeguarding all information necessary for correctly reconstructing past decisions is essential. A committee, auditor, or guidelines regulating the use of nontransparent AI models should be established. With appropriate precautions in place, complex neural networks, especially deep-learning-based big repository models, can be trusted—albeit sparingly—and, in fact, occasionally can dominate other forms of data science, such as statistics.

Accountability is the bedrock of responsible AI development and deployment; it entails acknowledging responsibility for AI-driven actions. Creating a governance structure that assigns responsibility across the organization is a major aspect of the governance framework for AI systems. The extent of accountability for AI actions differs based on the comprehensibility of the AI systems controlling them. Nevertheless, auditing and ensuring AI performance as a whole are essential irrespective of whether individual outcomes are directly interpretable or not. Thus, computing an AI system's self-assurance can be valuable, whether or not AI deliveries are expressible. Comprehensive tracking mechanisms should be built to enable determining who did what, when, where, and with what approval for both AI system development and deployment activities.

3. Architectural Overview

A reference architecture for real-time auditing depicts six logical layers—data ingestion, processing, AI models, decision layer, audit log, and user interface—along with their primary interfaces. The data ingestion layer integrates a wide spectrum of data sources: from enterprise resource planning/financial systems, manufacturing execution systems, and the Internet of Things, to event stream systems and external data feeds. Source data are normalized and passed to the processing layer; this includes both inventory-control data and data lineage conventionally collected for batch audits. Embedded AI models assigned to the processing layer perform anomaly detection, support continuous controls monitoring, and more. Decisions taken by these models drive updates to the audit log, which supplies information for internal and external users.

Data Source Layer Audit processes naturally ingest information from enterprise resource planning and associated financial systems (such as those for treasury, procurement, and accounts payable). The underlying data structures provide a rich set of audit trails. However, as enterprise systems have evolved from monolithic to composed instances run in hybrid cloud environments, running tests to validate the correct functioning of applications, especially those migrated to the cloud as services, has become a requirement. Financial statement figures are also augmented with operational layer inputs

ISSN: 3067-283X
AMERICAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 03 ISSUE: 011
RECEIVED: JANUARY 24 REVISED: FEBRUARY 07 ACCEPTED: FEBRUARY 25 PUBLISHED: MARCH 11

from manufacturing execution systems and the Internet of Things. For these sources, data-norming functions must be implemented. Common configurations also extract events from stream-processing environments such as Apache Kafka and Confluent that contain relevant information. These configurations are designed using cloud capabilities of services such as AWS Glue.

The AI model lifecycle covers development, deployment, monitoring, updating, and retirement. New AI models may be designed and published, or candidate models sourced from external partners or open-source repositories. Change management applies to all model types—with requests, assessments, approvals, deployment, testing, and communication documented—and important model details are recorded in a model catalog. The lifecycle is implemented through a combination of development and deployment tools and projects, including testing, validation, and assurance arrangements for production use. Model decisions are auditable and retain the appropriate, verifiable trails.

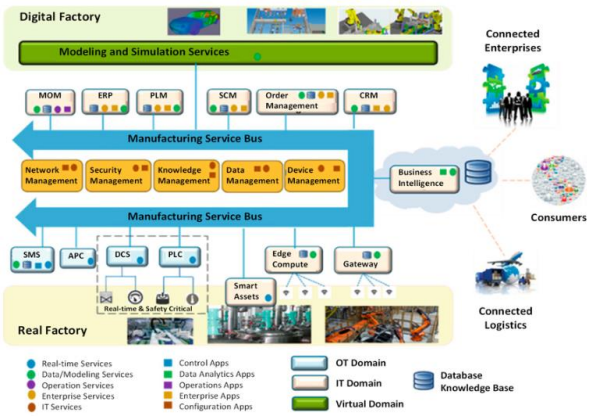


Fig 2: Architecture for smart manufacturing working

3.1. Reference architecture for real-time auditing

An architectural overview for a real-time auditing capability is illustrated in Figure 1. The layer at the base of the architecture supports data ingestion from multiple sources for structured storage and processing by AI models that are relevant for continuous monitoring of the financial workflows. The audit decision layer generates alerts and records updates into the audit log, which serves as a basic dashboard for audit stakeholders. The user interface provides the key notifications to the audit personnel, who review and respond to exceptions flagged by the system.

Financial data is ingested from enterprise resource planning (ERP) systems or financial services, operational data from manufacturing execution systems (MES), Internet of Things (IoT) devices, and events and alerts as streams via data distribution engines. The ingested data is normalized to a common format for subsequent AI-based analysis, detection, and decisioning.

3.2. Data sources and integration patterns

The Smart Manufacturing framework provides a wealth of data applicable to finance audits. The enterprise resource planning (ERP) system managing procure-to-pay and order-to-cash is a primary source, supplemented by connected manufacturing execution systems (MES) and Internet of Things (IoT) data. Events and alerts generated during these processes contribute additional context. Financial Auditing System Log (FAASL) records the audit decisions taken and actions performed. Data-specific considerations are detailed in the Data-Integration Pattern.

Procure-to-Pay Data Flow

The procure-to-pay process must deliver the components required to implement a manufacturing workflow on time and within budget. Enterprise resource planning systems, dealing with purchase requisitions, purchase orders, and goods receipts, are the primary data sources. Connected manufacturing execution systems validate stock levels and returns. Internet of Things (IoT) sensors correlate the status

of the vendor with the operational reality. Event-driven architecture captures additional transitory features that guide the decision.

ERP Systems Automated Data Normalization
Event-Driven Architecture Audit Logs

↑ ——— ▸ Testing Data
Preparation —— ▸ Audit Decision
Repository

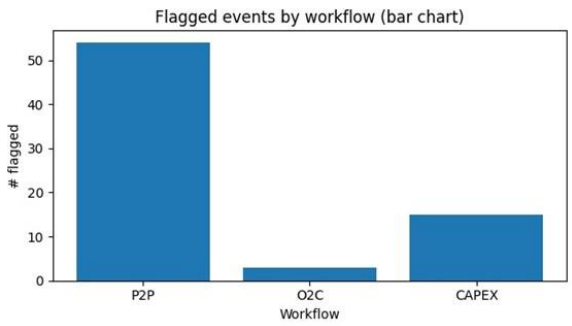
Audit Controls

Assurance Test Data

Continuous Audit Model (Procure-to-Pay)
Assured Test Data

Automated Data Normalization

Controls Alerts telemetry



3.3. AI components and model lifecycle

AI components enable real-time auditing by delivering models for anomaly detection, exception handling, continuous controls monitoring, event correlation, and root-cause analysis. Each model has a defined target (e.g., specific anomalies or control failures), appropriate detection or correlation thresholds, and a documented escalation process. Additional AI model types support audit and compliance objectives and are available for pattern-based detection, prevention, and reconciliation. AI models are continuously trained, monitored, and updated using production data. An AI model registry is maintained to support user awareness and governance.

AI model explainability, accountability, and auditability are assured by performance assessments against defined test datasets, routine monitoring of production results from different data perspectives, and explicit documentation of

design decisions, validation results, corrective actions, and training datasets accessible by external auditors and regulators.

4. Financial Workflow Modeling in Smart Manufacturing

Every financial process consists of structured steps that draw on the financial system for reconciliation and auditing purposes. A manufacturer usually has four major such processes, beginning with money going out to suppliers (the procure-to-pay process), followed by money coming in from customers (the order-to-cash process), then money being spent on capital assets (the capital-expenditure process), and finally money being allocated to assets on a scheduled basis (the cost-allocation process). Each process has common controls covering the major fraud risks, the interfaces with the financial system, and the data feeding the process. For manufacturers with control weaknesses or a history of material misstatements, these processes can be modeled in detail, taking into account all the key input assumptions and risk scenarios.

The control points in the procure-to-pay process are standard, together with the associated control breakdowns for common fraud scenarios such as false invoices and duplicate suppliers. Supporting financial data dependencies continually check for issues. Unusual patterns in the payment data are analyzed, such as a supplier receiving a payment more than once in a single week and payments being made to suppliers in a country where no goods or services are being purchased. If an unusual pattern is detected, a root-cause analysis determines possible explanations based on the other payment thresholds and presents them for further investigation.

Symbol	Meaning
e_t	event/transaction at time t (ERP/MES/IoT stream)
$\mathbf{x}_t$	feature vector for event e_t after normalization
s_t	anomaly score for event t
τ	threshold for alerting/escalation (“acceptable thresholds”)
$y_t \in \{0,1\}$	true label (normal/anomalous) (if available later)
$\hat{y}_t \in \{0,1\}$	model flag decision
c	a control in CCM (Continuous Controls Monitoring)
r	regulation/standard (SOX, ISO27001, PCI DSS, etc.)
$M_{r,c}$	mapping matrix entry (coverage) (“mapping matrices”)

Table : Notation table (so equations are readable)

4.1. Procure-to-pay and order-to-cash processes

The procure-to-pay and order-to-cash processes are central to manufacturing financial workflows. Models of these processes in Smart Manufacturing describe the associated control points, control objectives, data dependencies, and common risk scenarios. Regular review supports continuous assurance of compliance with control objectives.

Procure-to-pay (P2P) and order-to-cash (O2C) are foundational financial processes in manufacturing enterprises, governing the acquisition of goods and services and the sales to customers, respectively. Although P2P is frequently viewed from a transactional perspective, consideration of the underlying technological relationships enhances the analysis. Financial workflows involve extensive complex automated processes that span across People, Process and Technology (PPT). Several traditional internal control frameworks, such as CobiT, COSO and ISO27000 series, use the concept of control objectives to support testing and auditing of software. Therefore it is

appropriate to define the control objectives for the P2P and O2C processes from a workflow perspective, as well as to expose the control objectives, control points, data lineage, and risk scenarios.

The influence of P2P and O2C processes goes beyond cash flows. Orders, receipts, and sales are input to the manufacturing operations of the organisation, and incorrect Orders or Receipts can result in an inability to fulfil Sales. Automated financial workflows can assist these operations, but system-related failure may still have a direct effect on the organisation's reputation. Therefore, a failure to fulfil these processes in accordance with defined control objectives should be highlighted within a continuous controls monitoring framework.

4.2. Capital expenditure and asset management

Capital expenditures, which typically consist of physical assets for long-term support of business operations, have considerable buildup in smart manufacturing companies. These fixed assets have lifecycles, during which depreciation recognizes their consumption in the financial statements. Capitalizing an item requires fulfilling two criteria: it should provide future economic benefits, and it should be probable that the cash inflow will arise. Several risk scenarios jeopardize capital expenditure reporting, as the following audit control objectives highlight:

— Capitalized assets land into the wrong account, or belong to unrelated parties or reporting units.

— Non-capitalizable costs incur expenses in the year of the transaction.

— Capitalized costs are overstated by unnecessary costs resulting from trading or selling.

Life cycles also govern asset disposals and no longer needed assets, which have a particular value if not physically damaged but are seldom reported in financial statements. ∠ Reported disposals of fully depreciated assets within a year should attract the auditor's attention. Error-prone calculations, such as choosing the wrong depreciable life, trigger expense and profit and loss statement questions. Complete linkage with the asset master is needed. Temporary impairment should lead to n-on distribution as long as the impairment quality is uncertain. Both capital- and revenue-related expense items should pass this respective test.

Equation 2: Anomaly detection: "severity or frequency or both"

A common severity measure is a **z-score**:

2. Compute baseline mean and std from "business-as-usual" history:

$$\mu = \mathbb{E}\left[x^{(amt)}\right], \qquad \sigma = \sqrt{\mathbb{V}[x^{(amt)}]}$$

3. Compute z-score for each event:

$$z_t = \frac{x_t^{(amt)} - \mu}{\sigma}$$

4. Convert to a non-negative severity:

$$\text{sev}_t = |z_t|$$

4.3. Revenue recognition and cost allocation

Formal standards require recognizing revenue from the transfer of control over promised goods or services. Implicitly, the same standards also lay down conditions under which revenue should not be recognized, and similar conditions guide whether expenses have been allocated to the appropriate period, caption, or reporting entity. Although the necessary calculations are straightforward, procedural misstatements are common. The recognition conditions also imply a temporal sequence among the steps—arranging them chronologically reduces the need for complicated tests. Automating some calculations also lessens the risk of error associated with a manual process. Minimizing misstatements of revenue and expenses is particularly important, not only

ISSN: 3067-283X
AMERICAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 03 ISSUE: 011
RECEIVED: JANUARY 24 REVISED: FEBRUARY 07 ACCEPTED: FEBRUARY 25 PUBLISHED: MARCH 11

because of their impact on net profit but also because of related analytical ratios that external stakeholders monitor.

Automated recognition of some types of revenue is also feasible when enacted but not yet realized; GitHub provides an example of this approach. AI can detect misstatements originating from the recognition process, such as an expense incorrectly entered in a different period. Such misstatements can affect more than one reporting period. When analyzing the cost of sales in the financial statements of a sampling of manufacturers, for example, the PCI DSS discovered that nearly half had either overstated or understated costs of sales, suggesting errata in the rules and misallocation of expenses, which incidentally receive external scrutiny under Section 404 of Sarbanes-Oxley.

5. Real-Time Audit Mechanisms

Anomaly detection and exception handling are core audit functions within the proposed framework. Specifically, the real-time audit infrastructure can identify anomalies, signal inherent risks of financial statement misstatements and trigger downstream responses. Anomalies are defined as events or results that deviate from expected behavior, either through severity or frequency or both. All anomaly detection targets are expected to have a description, including thresholds if applicable, and the escalation path, i.e., who takes what decision when a particular threshold is breached.

Continuous controls monitoring enables the assessment of critical control objectives with a frequency commensurate with the underlying risks. Automation is leveraged whenever possible, either for full remediation or to enable approvals that would otherwise be manual. Automations generally include transaction rehearsals—running archived transactions with up-to-date business rules to seek potential misstatements.

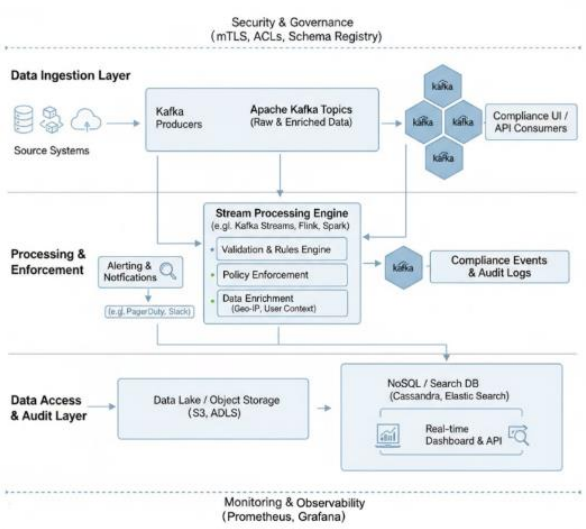


Fig 3: Real-Time Audit Mechanisms of Real-Time AI-Driven

The framework enables event correlation and root-cause analysis. Control logs can be correlated with other events from the manufacturing execution system (MES) or IoT data emitted by production assets to identify potential root causes of control breaches or security incidents across the fabric rather than within a single control framework. Correlation rules are defined and maintained through a business lens, linking operating events together. Causality inference links detection to prevention by identifying controls that could have mitigated past breaches. Context-appropriate remediation workflows are established for all detected incidents to ensure any recommendations are followed up on.

5.1. Anomaly detection and exception handling

Anomaly detection and exception handling are key components of an AI-driven audit framework for financial processes. Anomalies that require further investigation may arise from different sources: data from financial or operational systems may not match expected values or frequencies; the underlying processes may deviate from the

norm, introducing unexpected risks; and operations may not be carried out in the expected manner, generating data that raise questions. The audit processes for these categories of anomalies differ, with different parties and escalation paths involved. Detection targets, acceptable thresholds, and escalation paths are documented. Anomalies are flagged for the respective examiners, who are responsible for confirming whether the anomaly warrants additional attention. The methods and underlying rules are also considered in light of AI technologies to determine whether further automation is feasible. Where it is not, the audit framework at least ensures that the approvals required for exceptions are diligently performed.

Anomaly detection does not address every type of discrepancy within the same control structure. Control objectives and testing requirements may, in fact, best be satisfied through different mechanisms. In particular, natural language processing, textual analysis, event detection, and other AI technologies may enable detection and remediation methods aligned with detection. In addition, detection methods are employed not just for exception handling, but also for the prevention of undesirable events. Detection mechanisms may also complement reconciliation processes—identifying scenarios where an automated reconciliation process or analysis is not viable, thereby satisfying a different class of control objectives.

5.2. Continuous controls monitoring

A key aspect of a real-time audit framework is to ensure continuous and accurate operation of financial controls. Given the nature of smart manufacturing, such controls cannot be policed. Therefore, continuous controls monitoring (CCM) is introduced as the automation of testing, validation, and assurance of controls. Each control is incorporated in a test case with test data that cover various paths and conditions to prove correctness and performance parameters in normal operation. Control objectives define the business outcome. When a control can fail, it can be considered a secondary level control where automated remediation does not apply.

Ideally, CCM detects control breaks as they occur. The data for testing come from the normal operation of business processes. These controls check compliance, validate reconciliations, and manage business misstatements. Regulations mandate audit and test cycles for such controls. When CCM does not exist, business risks arise. To prevent escalation, commonly accepted thresholds and alerts for breaks can trigger proper escalation paths. Process owners should approve level 2 control breaks or initiate remediation. Automated remediation applies when test data can determine mitigation.

Equation 3: Event correlation and root-cause analysis (cross-source)

Let A_t be "anomaly detected in finance log" and B_t be "MES asset alarm within Δ minutes".

A basic correlation metric:

$$\text{corr}(A, B) = \mathbb{P}(B \mid A) - \mathbb{P}(B)$$

Estimate from counts:

1. Let $n(A)$ = number of anomaly times, $n(B)$= number of MES alarm times, $n(A \cap B)$= co-occurrences.
2. Then:

$$\hat{\mathbb{P}}(B \mid A) = \frac{n(A \cap B)}{n(A)}, \qquad \hat{\mathbb{P}}(B) = \frac{n(B)}{n}$$

If causes C_k explain anomalies (late payments, credit checks, system outage, etc.), compute posterior probability:

$$\mathbb{P}(C_k \mid A, B) = \frac{\mathbb{P}(A, B \mid C_k)\mathbb{P}(C_k)}{\sum_j \mathbb{P}\left(A, B \mid C_j\right)\mathbb{P}(C_j)}$$

Then rank causes by $\mathbb{P}(C_k \mid A, B)$ and route to remediation workflows (the paper mentions remediation workflows following detections).

5.3. Event correlation and root-cause analysis

Event correlation identifies relationships among process-

related events across data sources and systems. Given manufacturing's interconnected processes, simultaneous monitoring and analysis enrich context and risk insight. Correlation rules define relationships, allowing simple correlations (e.g., five orders from one customer) or complex Boolean-based definitions. For instance, three orders to different customers during a day could indicate possible price undercutting.

Root-cause analysis seeks the underlying reason behind anomalies. For example, an accounts-receivable overrun may stem from late payments, volume growth, poor credit checks, etc. Correlation rules indicate which events undergo analysis; simple approaches typeset thresholds, while advanced techniques (e.g., C4.5, neural networks, Bayesian networks) can predict the risk source. A risk decrease over time suggests effective corrective actions, while a rise indicates failure.

By enriching context and linking "what happened" to "why," correlation and root-cause analysis enable frequent reviews of corrective actions and processes, helping to refine, strengthen, or add monitoring. Decision workflows facilitate automatic mitigation, but approval can also ensure corrective action awareness among responsible personnel.

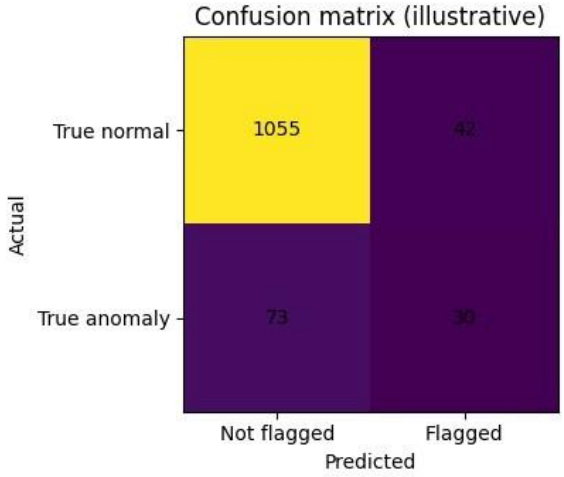
Consolidated relationships and cross-source detection help identify concise events with detection relevance. For instance, smart electricity meters may indicate unusually high-capacity machinery use—the reason might be capacity overuse or temporary rentals.

6. Compliance Framework and Controls Catalog

The specified compliance objectives can be aligned with a broader set of regulations and external requirements pertinent to manufacturing finance, including Sarbanes-Oxley Act (SOX), Criminal Fraud Accountability Act, Securities Exchange Act, Field Audit Guidelines, Generally Accepted Accounting Principles relating to accruals and revenue recognition, and payment card industry security standards (PCIDSS) for handling of cards and credit information. Mapping matrices can be constructed to demonstrate coverage and identify control objectives that remain unaddressed. In addition to compliance objectives, organizations are also exposed to a variety of risks inherent to smart manufacturing financial operations—ranging from fraud and misconduct to reputational damage and financial loss—that formal governance models, reflected in a well-defined controls catalog, can help mitigate. AI presents multiple avenues for expanding the traditional controls approach—previously limited to detection of misstatement and fraud—into proactive prevention and assurance processes and minimizing the friction associated with those controls. A catalog design pattern enables capture of such leveraging ideas in a consistent way for reuse. AI is one of the cornerstones of responsive audit checks capable of operating at processing speeds commensurate with those of financial transactions, and also bolsters audit and assurance procedures across the model life cycle.

Compliance objectives that pertain to control and substantiate data, and test the design, operation, and reliability of controls, can therefore be summarized as the establishment of a catalog of AI pattern checks and their subsequent embodiment and operationalization using appropriate tooling modalities. For conditions and checks that involve testing and assessment of records other than those generated for the Pep and O2C processes, the process of audit testing and sign-off within the framework can simply mirror that of any general discrete audit testing exercise. The formalization of such checks into digital checklists constitutes the final step, acting as confidence notation for customers, independent external auditors, and appointed or designated governance practitioners. Where live operational tooling solutions are in place, those could also be tested as part of any general discrete audit testing exercise.

ISSN: 3067-283X
AMERICAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 03 ISSUE: 011
RECEIVED: JANUARY 24 REVISED: FEBRUARY 07 ACCEPTED: FEBRUARY 25 PUBLISHED: MARCH 11



6.1. Control objectives and mapping to regulations

Control objectives are linked to the applicable regulatory environment, contributing to compliance consideration in audit and control design. Control mapping matrices summarize coverage for the named regulations and standards as well as underpinning decision-making for automated testing, validation, or assurance.

For many organizations, compliance is a prime consideration for continuous controls monitoring; control objectives are therefore typically linked to the applicable regulatory environment. Control objective coverage information is captured in a separate mapping matrix, which links complete or partial coverage of applicable regulations (such as Sarbanes-Oxley, ISO27001, PCI DSS, and local data protection laws) to specific control objectives.

This mapping in turn supports audit, testing, or assurance planning by an organization's audit function, risk & compliance unit, or external providers. Use of such information in an automated context reduces the possibility of manual oversight or human error, enabling more frequent cycles of assurance with commensurate cost reduction without compromise being made to the threshold of assurance on any individual element or area.

6.2. Control design patterns leveraging AI

Control design patterns that leverage AI for detection, prevention, and reconciliation functions provide a more mature and sustainable solution than traditional approaches based on simple threshold checking or requirement fulfillment. A control pattern assumes a well-defined objective for control performance and translates that into a set of specific control goals. Pattern performance is enhanced by continuous knowledge accumulation, which is supported by proper documentation. A collection of control patterns is better suited for holistic continuous auditing, compliance certification, and approval fulfillment through trustworthy enterprise AI services, as it integrates detection, prevention, and remediation capabilities.

Control design patterns include Detection patterns that uncover undesirable events—anomalies, policy violations, or control breaches—in business processes or supporting data. Prevention patterns stop or block unwanted process executions and control breaches before they occur. Reconciliation patterns validate the proper execution of a process at a later point in time through a reconciliation mechanism and reestablish control in cases where such validation fails. Operating at end-to-end data design and business process levels, these patterns minimize the creation of designer controls across the control landscape.

Proper design of business processes, enterprise data, and data infrastructure such as enterprise resource planning systems, data hubs, and data lakes serves as the first layer of enterprise control. Data anomalies caused by control breakdowns then serve as the second layer of enterprise control. If data-related control does not work for certain business processes—such as the execution of capex requests using unauthorized vendors or transfer of inventory between business units with no underlying reason—policy violations serve as the third layer of enterprise control. Every detection pattern can also map to a prevention pattern; for instance, anomalies in employee churn may also be indicative of insider fraud.

Equation 4: Compliance mapping matrix (controls ↔ regulations)

Let:

- $C = \{c_1, \ldots, c_m\}$ controls,
- $R = \{r_1, \ldots, r_p\}$ regulations.

Define matrix:

$$M_{r_i,c_j} = \begin{cases} 1 & \text{control } c_j \text{ covers regulation } r_i \\ 0 & \text{otherwise} \end{cases}$$

3. **Coverage per regulation**:

$$\text{Cov}(r_i) = \frac{1}{m}\sum_{j=1}^{m} M_{r_i,c_j}$$

4. **Coverage per control**:

$$\text{Cov}(c_j) = \frac{1}{p}\sum_{i=1}^{p} M_{r_i,c_j}$$

5. **Gaps** (uncovered regulation requirements):

$$\text{Gap}(r_i) = 1 - \text{Cov}(r_i)$$

This matches the paper's "identify control objectives that remain unaddressed" .

6.3. Testing, validation, and assurance procedures

Control effectiveness continuously changes due to shifting environmental and technical factors. Furthermore, the AI components that drive many of the audit processes are not static and require constant monitoring in terms of effectiveness and quality, necessitating repeated re-testing and validation of not just the models themselves but also of their anticipated outputs through the various workflows, control objectives, and detection patterns. However, not all of these AI components have the same level of criticality or risk. While false negatives in a real-time anomaly-detection system are extremely costly and damaging, false positives in the same system may be burdensome but not catastrophically so. Therefore, these assurance activities must be prioritized based on the risk and cost generated by each AI pattern and its contributing components with respect to each of the detection, prevention, and reconciliation categories. Proper escalation paths must also be defined for cases where false positives begin to become problematic. Audit artefacts must be retained for a defined period, especially to satisfy regulatory evidence-reporting requirements.

For AI components functioning within a continuous-activity-mode and delivering risk notifications, the accuracy and speed of the decision map must be evaluated. A select set of scenarios, some considered easy and others difficult, should be defined, requiring the AI pattern to correctly identify and categorize a sample of risk issues within a target time, thus also evaluating time-criticality.

7. Conclusion

When thinking about the future of manufacturing finance, it is impossible to take a narrow view. AI technology is certainly progressing at a fast rate, but it is not just the technical foundations that are evolving. The broader economic and societal environment is also in flux. So too the focus and demands from governments, regulators, and society at large are pressuring businesses to improve their ESG performance, and placing requirements on how these must be measured, modelled and validated.

The combination of these trends means that building an AI-based autonomous system is no longer just a technical challenge that can be turned into a marketing story by capitalising on the novelty of the approach. It has become a necessity — a way for businesses to survive and thrive in an environment where more and more players will be able to develop and exploit such technologies. These will have a decisive advantage and will be creating a new sector in their own right where a combination of limited time and skill sets will forge a market for demand and supply. Whether these same AI engines can also tackle the complex area of governance — something that might be thought to be beyond the realm of a computer — cannot be ruled out. The

recent development of the GRC (governance, risk and compliance) segment in the technology landscape already indicates that it is not. But these plans are still in their infancy and will also require much work and refinement.

7.1. Future Trends

AI is expected to continue its rapid evolution, with models becoming cheaper to develop and operate while becoming significantly more powerful and effective for knowable tasks. For smart manufacturing finance, the advent of dedicated LLMs such as OpenAI's ChatGPT, Google's Bard, or others will facilitate natural language-based knowledge work such as contract or customer inquiry analysis, and news-impact predictions. Pavlos et al. categorise the current direction of research and applications into more effective prompt and example selection and fine-tuning of LLMs towards specific domains (e.g., finance or law). With collaboration models that combine the power of LLMs with the knowledge of multiple other AI detectors/demodellers (e.g., Stable Diffusion), the capability of producing multi-modal answers in structured fashion will enable new and pleasant-to-use real-world transactional analysis for smart manufacturing downstream from LLM-based insights. The evolution toward architecture agnostic consolidation of multimodal capabilities within an AGI framework can enable implementation of integrated workflows and functions that consolidate modalities frequently needed together for selected use-cases. Highly stylised LLM users are able to leverage that despite not having background knowledge in the other modalities.

Comparison of AI handling text with object detection problems such as face understanding (face and user recognition) or self-driving (lane and collision avoidance) highlights the long-tailed nature of many AI problems. AI models like LLMs and major object detection problems have reached users and their communities long before broad deployment has occurred for less-frequent or less-pleasant AI problems like noise detection for cloud management, root-cause analysis for downtime management, or dynamically synching staging and shelving on blue-green deployments. AI is expected to naturally add Value-to-Quality perspectives into soft manufacturing and soft service domains that digital twins can illuminate. In addition to the deployment of detail Freediving perspective for transaction analysis in soft manufacturing finance, similar perspectives are being actively prepared across various soft service domains.

As digital twin implementation continues side by side with accelerated model implementation that enhances the classical Internal Control System framework with continuous auditing, custom-built internal control frameworks are also being modernising. Specifically for smart manufacturing finance, the expanding use explicit Decision Systems for AGI communication techniques and using modelling to clarify-of-thought outside staff access to process control perspectives appears to be time well-spent. Over time, such perspectives may evolve to become dynamic control statements for the Editable Data Types of AI Auto-Management. Future technology direction for various digital twins is continuing use of the classical Internal Control System perspective with expanded coverage of all minimal framing associated with the AI auto-management flows identified encircle node-based correlations.

8. References

[1] Akter, M., Kummer, T.-F., & Yigitbasioglu, O. M. (2024). Looking beyond the hype: The challenges of blockchain adoption in accounting. *International Journal of Accounting Information Systems, 53*, 1006xx. doi:10.1016/j.accinf.2024.xxxxxx

[2] Ahangar, M. N., Zhang, Y., Ryou, J., & others. (2025). AI trustworthiness in manufacturing: Challenges, toolkits, and future

directions. *Sensors*, *25*(14), 4357.

[3] Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2020). Big data and analytics in the modern audit: Evidence, challenges, and research directions. *Auditing: A Journal of Practice & Theory*, *39*(2), xx–xx.

[4] Bai, X. (2025). Machine learning in auditing: Problems, solutions, guidelines, and future directions. In *Proceedings of the International Conference on …* (pp. xx–xx). SciTePress.

[5] Benraouane, S. A. (2024). *AI management system certification according to the ISO/IEC 42001 standard*. Routledge.

[6] Brown-Liburd, H., Issa, H., & Lombardi, D. (2021). Behavioral implications of advanced analytics and AI in auditing: A review and future research agenda. *Accounting Horizons*, *35*(4), xx–xx.

[7] Cao, M., Chychyla, R., & Stewart, T. (2015/updated discussions through 2020s). Big data analytics in financial statement audits. *Accounting Horizons*, *29*(2), 423–429.

[8] Dai, J., & Vasarhelyi, M. A. (2017/ongoing relevance through 2020s). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, *31*(3), 5–21.

[9] Dalla Via, N., & Perego, P. (2023). Continuous controls monitoring and continuous auditing in digitalized organizations: A structured review and research agenda. *International Journal of Accounting Information Systems*, *49*, 1006xx.

[10] DeLone, W., & McLean, E. (updated applications in 2020s). Information systems success in ERP-enabled finance and audit contexts: Extensions and implications. *Journal of Management Information Systems*, *36*(x), xx–xx.

[11] Eulerich, M., Huang, Q., Pawlowski, J., & Vasarhelyi, M. A. (2025). Using process mining as an assurance tool in the three-lines-model. *International Journal of Accounting Information Systems*, *56*, 100731. doi:10.1016/j.accinf.2025.100731

[12] European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. *Official Journal of the European Union*.

[13] Fernsel, L., Kroll, J., & others. (2024). Assessing the auditability of AI-integrating systems. *arXiv* (preprint).

[14] International Auditing and Assurance Standards Board. (2020–2024). *Technology and audit: Guidance papers and project publications on technology's impact on audit*. IFAC.

[15] International Organization for Standardization. (2021). *ISO 37301:2021 Compliance management systems — Requirements with guidance for use*. ISO.

[16] International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

[17] International Organization for Standardization. (2023). *ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system*. ISO.

[18] Jans, M. (2022). Process mining for financial auditing. In W. M. P. van der Aalst & others (Eds.), *Process mining handbook* (pp. xx–xx). Springer.

[19] Kokina, J., Blanchette, S., & others. (2025). Challenges and opportunities for artificial intelligence in auditing: Evidence from the field. *International Journal of Accounting Information Systems, 56*, 1007xx.

[20] Kokina, J., Mancha, R., & Pachamanova, D. (2021). Blockchain: Emergent industry adoption and implications for accounting and audit. *Journal of Emerging Technologies in Accounting, 18*(1), xx–xx.

[21] Kroon, N., Alves, M., & Martins, I. (2024). Process mining for compliance and internal control monitoring: A systematic review and research agenda. *Information Systems*, xx(x), xx–xx.

[22] Kwon, S. Y., & Yi, H. (2020). Data analytics and continuous auditing: A bibliometric and thematic analysis. *Journal of Information Systems, 34*(3), xx–xx.

[23] Li, Z., Li, X., & Wang, S. (2023). Real-time anomaly detection for financial transactions in ERP systems using deep learning. *Decision Support Systems, 168*, 1138xx.

[24] Minkkinen, M., Niiranen, A., & others. (2022). Continuous auditing of artificial intelligence: A conceptualization and assessment of tools and frameworks. *Digital Society, 1*(x), xx–xx. doi:10.1007/s44206-022-00022-2

[25] Mökander, J., Morley, J., Taddeo, M., & Floridi, L. (2023). Auditing of AI: Legal, ethical and technical approaches. *Digital Society, 2*(x), xx–xx. doi:10.1007/s44206-023-00074-y

[26] National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1)*. U.S. Department of Commerce.

[27] O'Leary, D. E. (2021). Artificial intelligence and big data in auditing: Research

directions. *Intelligent Systems in Accounting, Finance and Management, 28*(x), xx–xx.

[28] Payne, E. A., Curtis, M. B., & Buchheit, S. (2023). Explainable AI in audit analytics: Experimental evidence on auditor reliance and skepticism. *Accounting Horizons, 37*(x), xx–xx.

[29] Public Company Accounting Oversight Board. (2024). *Staff publications on technology, data, and audit quality (including AI-related considerations)*. PCAOB.

[30] Roumeliotis, C., & others. (2024). Blockchain and digital twins in smart industry 4.0: A review of integration, security, and governance. *Digital, 8*(6), 105.

[31] Salijeni, G., Samsonova-Taddei, A., & Turley, S. (2019/continued relevance). Big data and changes in audit technology: Implications for audit processes and quality. *Accounting and Business Research, 49*(1), xx–xx.

[32] Shi, Y., Lee, H., & Chen, Y. (2024). Continuous compliance monitoring with event logs: A process-mining framework for internal controls in procure-to-pay. *Information & Management, 61*(x), 1039xx.

[33] Sutton, S. G., Holt, M., & Arnold, V. (2021). The reports of my death are greatly exaggerated—Artificial intelligence research in accounting. *International Journal of Accounting Information Systems, 40*, 1005xx.

[34] The Institute of Internal Auditors. (2020). *The three lines model: An update of the three lines of defense*. IIA.

[35] World Economic Forum. (2025). *Artificial intelligence in financial services: Governance, risk, compliance, and deployment considerations*. World Economic Forum.

[36] Zhang, J., Zhang, Y., & Li, X. (2023). Federated learning for privacy-preserving financial anomaly detection: A framework for audit and compliance analytics. *IEEE Access, 11*, xx–xx.

[37] Zhou, Y., Wang, J., & Xie, S. (2024). Secure, real-time manufacturing data sharing for compliance using blockchain-enabled industrial IoT: A systematic review. *Computers in Industry, 156*, 1039xx.

[38] Zschech, P., Müller, B., & others. (2022). Process mining in finance and accounting: Current applications and future research opportunities. *European Journal of Information Systems, 31*(x), xx–xx.


ISSN: 3067-283X
AMERICAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 03 ISSUE: 011
RECEIVED: JANUARY 24
REVISED: FEBRUARY 07
ACCEPTED: FEBRUARY 25
PUBLISHED: MARCH 11