International Journal of Future Engineering Innovations

Advances in Service Reliability Engineering and Observability for Distributed Financial Data Processing Platforms

Precious Nnamdi Ibe [1], Emmanuel Chukwuma Okeke [2*], Ifeanyichukwu Okwesa [3], Oluranti Ogundapo [4], Olabode Michael Soneye [5], Kofi Okyere Mensah [6]
[1] Cerema, Paris, France
[2] Arcesium, New York, NY, USA
[3] Barclays PLC, United Kingdom
[4] Google, USA
[5] EQ Bank, Toronto, ON, Canada
[6] CIBC Bank USA, USA

* Corresponding Author: **Emmanuel Chukwuma Okeke**

Article Info

ISSN (online): 3049-1215
Volume: 02
Issue: 06
Received: 21-10-2025
Accepted: 23-11-2025
Published: 19-12-2025
Page No: 74-95

Abstract
Distributed financial data processing platforms, which carry payments, trade capture, market data, risk aggregation and regulatory reporting workloads, have long treated reliability as an engineering discipline. Recently that discipline was reshaped by three forces acting at the same time. Regulation turned operational resilience into a supervised, time-boxed obligation: the EU Digital Operational Resilience Act (DORA) became applicable, and the UK operational resilience transition period has ended. Open observability standards matured, with OpenTelemetry adding profiling as a signal type, stabilising database semantic conventions and absorbing eBPF-based zero-code instrumentation, while Apache Kafka 4.0 removed its ZooKeeper dependency. AI-driven site reliability engineering (SRE) agents moved from prototypes to generally available products. Using an integrative review of recent regulatory, technical and industry sources, combined with a thematic synthesis of 205 peer studies on monitoring, risk governance, security operations, payments and AI governance, this paper develops the Integrated Financial Data Reliability (IFDR) model. The model links regulatory, technological and failure-environment drivers to four core capabilities (data-centric service level indicators, a unified telemetry pipeline, governed AI autonomy and telemetry-based regulatory classification) and to three resilience outcomes, and it is expressed as five propositions. A major AWS US-EAST-1 outage is used as an illustrative case. The paper discusses implications for practitioners, supervisors and researchers, sets out its limitations, and proposes a research agenda including financial-domain semantic conventions, correctness observability at scale and the evaluation of AI agents against realistic incident corpora.

DOI: https://doi.org/10.54660/IJFEI.2025.2.6.74-95

Keywords: site reliability engineering, observability, OpenTelemetry, DORA, operational resilience, data reliability, event streaming, Apache Kafka, AIOps, incident management, financial services, conceptual model

1. Introduction

Financial institutions increasingly run their core data flows on distributed platforms: event streaming backbones, stream processors, fleets of microservices, cloud object stores and lakehouse tables, often spread across several cloud regions and on-premises data centres. These platforms move money and the records of money. When they fail, the failure is not always an

outage. A payment can be processed twice, a position file can arrive complete but stale, a risk aggregation can silently omit one desk, or a regulatory report can be filed on time with wrong numbers. In finance, a system that is up but wrong can be more damaging than a system that is down, because the error propagates to counterparties, customers and supervisors before anyone notices.

Site reliability engineering (SRE), as codified by Beyer et al. (2016) [79], gave the industry a vocabulary of service level indicators (SLIs), service level objectives (SLOs), error budgets and blameless postmortems. Observability, built on correlated metrics, logs and traces, gave engineers the means to ask new questions of running systems. Both practices were well established before 2025. What changed during 2025 was the environment around them:

- **Regulation became operational:** DORA applied to EU financial entities from 17 January 2025 (Walkers Global, 2025) [226], with harmonised incident classification and fixed reporting deadlines (Central Bank of Ireland, 2025; Folderit, 2025) [85, 118]. In the UK, firms had to be able to remain within impact tolerances for their important business services by 31 March 2025 (Financial Conduct Authority, n.d.; Sidley Austin LLP, 2025) [212].
- **Open standards matured:** OpenTelemetry added profiling as a fourth signal type in OTLP, stabilised database semantic conventions and accepted a donated eBPF instrumentation project (Bindplane, 2025; Grafana Labs, 2025b; Grafana Labs, 2025c) [80, 121, 122].
- **Streaming infrastructure simplified:** Apache Kafka 4.0, released on 18 March 2025, became the first major release to run entirely without ZooKeeper (Apache Software Foundation, 2025a) [59].
- **AI entered incident response:** Several observability vendors released AI SRE agents that investigate alerts autonomously, with Datadog making its agent generally available in December 2025 (Datadog, 2025b) [88].
- **A major cloud failure tested assumptions:** On 20 October 2025 a DNS failure affecting DynamoDB in AWS US-EAST-1 cascaded across many services and disrupted banks and payment applications (Payment Expert, 2025; Robinson, 2025) [203, 206].

Research on these topics remains fragmented. Studies of compliance monitoring, fraud analytics, security operations, cloud governance and IT service management each address part of the problem, but few connect system reliability, data integrity and regulatory reporting in one frame. This paper addresses three research questions:

RQ1. What were the principal regulatory, technical and operational advances of 2025 affecting reliability and observability for distributed financial data processing platforms?

RQ2. How does existing research on monitoring, risk governance, security operations, payments and AI governance inform reliability practice for these platforms, and where are its gaps?

RQ3. What conceptual model can integrate these advances and findings into a coherent basis for practice and further research?

The paper makes four contributions: (i) a structured synthesis of 2025 developments and of twelve related research streams; (ii) the Integrated Financial Data Reliability (IFDR) model, with a data-centric SLI taxonomy, an autonomy model for AI agents and a reference architecture, expressed as five testable propositions; (iii) an illustrative analysis of the October 2025 AWS outage; and (iv) implications for practitioners, supervisors and researchers together with a research agenda. Section 2 describes the research method. Section 3 presents the results and discussion: the literature synthesis (3.1), the conceptual model (3.2), discussion of the findings and the illustrative case (3.3), implications (3.4), limitations (3.5) and future research (3.6). Section 4 concludes.

1.1. Background: Characteristics of Financial Data Processing Platforms

Financial data platforms share the general properties of large distributed systems, but several domain properties shape how reliability must be defined and measured:

- **Correctness invariants:** Value must be conserved: debits equal credits, positions reconcile to trades, and each instruction is applied exactly once. Idempotency and deduplication are reliability properties, not merely implementation details.
- **Ordering constraints:** Many workloads require strict ordering per key (account, instrument, order) while tolerating reordering across keys. Partition design in streaming systems directly encodes this.
- **Hard temporal deadlines:** Settlement windows, end-of-day batch cut-offs, market open and close, and regulatory filing deadlines create sharp, calendar-driven peaks and non-negotiable completion times. The shortening of US securities settlement to T+1 in 2024 compressed these windows further.
- **Auditability:** Records must be retained, attributable and reproducible for years. Telemetry used as evidence inherits some of these requirements.
- **Deep third-party dependency:** Card networks, central counterparties, market data vendors, messaging networks and, increasingly, a small number of hyperscale cloud providers sit on the critical path.

1.2. SRE and Observability Foundations

Classic SRE frames reliability through user-centred SLIs, typically the proportion of successful requests and the proportion of requests faster than a threshold. An SLO sets a target for an SLI over a window, and the error budget is the permitted shortfall. Error budgets convert reliability into a resource that product and operations teams can negotiate over (Beyer et al., 2016) [79]. The difficulty for financial data platforms is that much of the work is asynchronous and batch-shaped: there is no user request whose latency can be measured, only data that must arrive, completely and correctly, by a deadline.

Observability practice in 2025 rests on OpenTelemetry (OTel), which provides vendor-neutral APIs, SDKs, a wire protocol (OTLP) and the Collector, a pipeline component that receives, processes and exports telemetry. Logs, metrics and traces achieved stability in 2023, and the community announced profiling support in 2024 (Grafana Labs, 2025a) [120]. Semantic conventions, which standardise attribute names such as those describing HTTP calls or database queries, make telemetry from different libraries and languages comparable (Dynatrace, 2025) [99]. Context propagation links spans across process and message boundaries, which for streaming systems means carrying trace context in message headers.

2. Research Method

2.1. Research Design

The study combines an integrative literature review with conceptual model development. An integrative design suits the topic because relevant knowledge is spread across peer-reviewed studies, regulatory texts, open source project documentation, vendor announcements and incident reports, which a narrow systematic review of one database would miss. The review is used to answer RQ1 and RQ2, and its findings are then abstracted into constructs and relationships to answer RQ3. A single, publicly documented incident is used as an illustrative case to test the plausibility of the model rather than to generalise statistically.

2.2. Sources and Search Strategy

Two bodies of evidence were assembled. The first comprises 2025 primary and near-primary sources on the developments in scope: regulatory texts and supervisory guidance on DORA and UK operational resilience, OpenTelemetry and Apache Kafka release notes and project blogs, vendor product announcements for AI SRE agents, conference programmes such as SREcon25, and public reporting on the October 2025 AWS outage. These were located through targeted web searches using combinations of terms such as operational resilience, incident reporting, OpenTelemetry, semantic conventions, Kafka 4.0, KRaft, AI SRE agent and US-EAST-1 outage, and by following links from official announcements to the underlying documents.

The second body is a peer literature set drawn from a consolidated reference list of 1,056 records spanning many subject areas. Records were screened against the inclusion criteria in Table 1. Sources dated after 2025 were excluded so that the evidence base reflects the state of knowledge in the year under review.

Table 1: Review protocol and screening summary

Step	Description and result
Scope	Reliability, observability, monitoring, risk governance, security operations, payments, audit and AI governance relevant to distributed financial data platforms
Inclusion criteria	Directly related (financial monitoring, compliance, fraud, payments, cyber risk, cloud, IT service reliability, AI governance) or semi-related by transferable method (critical infrastructure anomaly detection, high-availability engineering, predictive maintenance)
Exclusion criteria	Off-domain topics (for example clinical, agricultural, construction safety, marketing); duplicates; incomplete bibliographic records; publication after 2025
Screening of peer list	1,056 records screened by title and subject area; 224 retained after relevance screening, duplicate removal and exclusion of incomplete records; 19 excluded as published after 2025; 205 included
2025 primary sources	21 regulatory, project, vendor, conference and incident sources from 2025 (one undated supervisory page), plus one foundational SRE text
Coding	Included studies coded into twelve thematic research streams (Section 3.1.5)

Screening was performed by a single reviewer on titles and bibliographic metadata; see Section 3.5.

2.3. Synthesis and Model Development

Included sources were synthesised thematically. For the 2025 sources, each development was described and its engineering consequence for financial platforms identified. For the peer studies, each record was assigned to one of twelve streams, and the contribution of each stream to reliability practice was summarised. Recurring concepts across both bodies of evidence (for example continuous rather than periodic assurance, telemetry as evidence, and governed automation) were abstracted into constructs. Relationships among drivers, capabilities and outcomes were then specified and stated as propositions, following common practice in conceptual papers that aim to guide subsequent empirical testing.

2.4. Illustrative Case

The 20 October 2025 AWS US-EAST-1 outage was selected because it was large, well documented in public sources, cross-industry and affected banks and payment services. Its timeline and causes were reconstructed from contemporaneous reporting and subsequent technical analyses (Payment Expert, 2025; Reddy, 2025; Robinson, 2025) [203, 205, 206], and the case was examined against each construct of the model to assess whether the model explains the observed impacts and indicates practical responses.

3. Results and Discussion

3.1. Literature Synthesis

This section first reports the 2025 regulatory, technical and industry developments identified in the review (3.1.1 to 3.1.4) and then synthesises the related peer research streams (3.1.5).

3.1.1. Regulatory Drivers in 2025

3.1.1.1. The EU Digital Operational Resilience Act

DORA (Regulation (EU) 2022/2554) became applicable on 17 January 2025 to a broad set of EU financial entities, including banks, insurers, investment firms, payment and e-money institutions and market infrastructures (Folderit, 2025; Walkers Global, 2025) [118, 226]. It harmonises five areas: ICT risk management, incident reporting, resilience testing, ICT third-party risk and information sharing (Folderit, 2025) [118]. National competent authorities began supervision from the application date, and the next significant milestone was the submission of registers of information on ICT third-party arrangements, which competent authorities were due to pass to the European Supervisory Authorities by 30 April 2025 (Walkers Global, 2025) [226].

For reliability engineers, the incident reporting pillar is the most consequential. Major ICT-related incidents must be reported to the competent authority using templates designed by the European Supervisory Authorities (Central Bank of Ireland, 2025) [85]. The reporting sequence follows an initial notification, an intermediate report and a final report, on a timeline commonly summarised as 24 hours, 72 hours and one month (Folderit, 2025) [118]. Classification criteria include the number of affected clients and transactions, duration, geographic spread, data losses, criticality of the services affected and reputational impact; for example, an incident lasting longer than 24 hours or one reflected in the

media can contribute to a major classification (Burke & Price, 2025) [84]. Entities must also inform clients when a major incident affects their financial interests (Burke & Price, 2025) [84].

The engineering consequence is that incident classification is now a measurement problem. To decide within hours whether an incident is major, an organisation must be able to answer, from telemetry, how many clients and transactions were affected, in which member states, for how long and with what data impact. Observability data has become regulatory evidence, and the questions it must answer are fixed in advance by law. This is consistent with research arguing that financial institutions need integrated, data-driven compliance analytics rather than periodic attestation (Akomolafe et al., 2025; Bello et al., 2024; Uchechi et al., 2022) [35, 76, 216].

3.1.1.2. UK Operational Resilience

Under FCA PS21/3 and PRA SS1/21, UK banks, insurers, payment and e-money institutions and other in-scope firms had until 31 March 2025 to identify important business services, set impact tolerances for each and demonstrate that they could remain within those tolerances in severe but plausible scenarios (Financial Conduct Authority, n.d.; Sidley Austin LLP, 2025) [212]. In its observations before the deadline, the FCA noted that most firms had set purely time-bound tolerances and encouraged complementary metrics, and it emphasised that impact tolerances are distinct from recovery time objectives, which are usually set well inside them (Financial Conduct Authority, n.d.). In December 2024 the PRA and FCA also consulted (CP17/24 and CP24/28) on operational incident and third-party reporting, proposing that firms report incidents meeting certain thresholds even where no impact tolerance has been breached (Sidley Austin LLP, 2025) [212].

Impact tolerances map naturally onto the SRE stack. An impact tolerance is an outer boundary of intolerable harm; an SLO is an inner operating target that, if respected, keeps the service well away from that boundary; and the error budget measures how much margin has been consumed. Firms that express both in the same telemetry can show supervisors a continuous, quantitative link between day-to-day engineering and regulatory outcomes, instead of relying on annual scenario tests alone. Research on continuous control and security validation in regulated infrastructures supports the same shift from periodic to continuous assurance (Adebayo, Amadi, et al., 2025; Dosunmu & Ogundele, 2024c) [4, 95].

3.1.1.3. Convergence of SRE and Compliance Practice

The practitioner community ummarized this convergence explicitly. The SREcon25 EMEA call for participation included a dedicated track on high availability in financial systems, inviting talks on how institutions align SRE practices with requirements such as SOX, Basel III and DORA, alongside tracks on observability for data pipelines and silent failures and on AI-assisted incident response (USENIX, 2025) [224]. Table 2 summarises the 2025 regulatory milestones and their engineering implications.

Table 2: Key 2025 regulatory milestones and engineering implications

Date	Milestone	Engineering implication
17 Jan 2025	DORA applicable across EU financial entities; major ICT incident reporting mandatory (Central Bank of Ireland, 2025; Walkers Global, 2025) [85, 226]	Telemetry must support rapid, criteria-based incident classification and evidence retention
31 Mar 2025	End of UK operational resilience transition; firms must remain within impact tolerances (Financial Conduct Authority, n.d.; Sidley Austin LLP, 2025) [212]	Map important business services to SLOs; test tolerances with chaos and failover exercises
30 Apr 2025	DORA registers of information due to the ESAs via competent authorities (Walkers Global, 2025) [226]	Dependency inventories should be derived from, and reconciled with, observed service topology
Through 2025	DORA technical standards in force for incident templates, subcontracting and threat-led penetration testing (Folderit, 2025) [118]	Incident tooling must populate ummarized d fields; resilience testing becomes evidence-driven

Sources as cited. Timelines are ummarized; firms should consult the regulations and their competent authority for definitive obligations.

3.1.2. Advances in Observability Standards and Tooling

3.1.2.1. OpenTelemetry Maturity in 2025

OpenTelemetry made substantial progress in 2025. At KubeCon Europe in April, the project reported that profiling had been added as a new signal type in OTLP version 1.30.0, that the eBPF profiler was enabling low-overhead CPU profiling, and that the Collector supported profiling across a dozen components behind feature flags (Bindplane, 2025) [80]. In May 2025 Grafana Labs announced the donation of Beyla, its eBPF-based zero-code instrumentation tool, to the project as OpenTelemetry eBPF Instrumentation (Grafana Labs, 2025b) [121]. In June 2025 the community marked the database semantic conventions as stable for spans, the operation duration metric and their attributes on MariaDB, Microsoft SQL Server, MySQL and PostgreSQL, with other databases still in development (Grafana Labs, 2025c) [122]. HTTP span conventions had already been declared stable, with messaging conventions nearing stabilisation (Dynatrace, 2025) [99].

Each of these advances matters specifically for financial platforms:

- Stable database conventions allow consistent latency and error SLIs across heterogeneous estates, starting with the four relational databases covered by the 2025 stabilisation, and give a template for extending the same consistency to other stores as their conventions mature (Grafana Labs, 2025c) [122].
- eBPF zero-code instrumentation reaches workloads whose source code cannot be modified, such as vendor core banking packages, third-party payment switches and legacy services, closing long-standing blind spots without application changes.
- Continuous profiling as a correlated signal lets engineers move from a latency or CPU spike directly to the code consuming the resource (Grafana Labs, 2025a) [120]. In pricing, order routing and fraud scoring services, where microseconds and tail latency matter, this shortens the path from detection to root cause.
- Vendor neutrality, reinforced by broad adoption across backends, reduces lock-in risk, which DORA frames as part of ICT third-party and exit-strategy planning.

3.1.2.2. Observing AI Workloads

Financial institutions expanded their use of large language models in 2025 for customer service, document processing, fraud operations and internal tooling. OpenTelemetry's generative AI semantic conventions define standard attributes for prompts, responses, token usage, tool calls and provider metadata, and major backends adopted them; Datadog, for example, announced native support for conventions version 1.37 and later in December 2025 (Datadog, 2025a) [87]. These conventions remain under active development, so teams should expect some churn. For regulated firms, the significance is twofold: AI features become observable with the same pipeline as other services, and the AI agents that firms adopt for operations (Section 3.1.4) can themselves be traced and audited.

3.1.2.3. Telemetry Volume, Cardinality and Cost

Financial workloads generate telemetry with extreme cardinality: account numbers, instrument identifiers, order IDs and message references. Placing such identifiers in metric labels is a well-known route to runaway cost and backend instability. Practice that matured through 2025 favours keeping high-cardinality identifiers in traces and structured logs, using exemplars to link aggregate metrics to representative traces, applying tail-based sampling in the Collector so that errors, slow requests and flagged transactions are always retained, and redacting personal data at the Collector before export. Cost pressure also drove architectural change, with some vendors building on data lake storage and reporting large cost reductions, such as up to 60 percent for one vendor's early customers (Observe, Inc., 2025) [158]; such claims should be validated locally, and research on predictive rightsizing and usage forecasting for cloud resources offers complementary approaches (Ahmed et al., 2020; Upreti & Oteri, 2023) [25, 222]. Retention tiers should be aligned with regulatory record-keeping, distinguishing operational telemetry (short retention) from incident evidence (long retention, immutable); ledger-based audit trails have been proposed for the latter (Anichukwueze et al., 2021; Oshoba et al., 2020) [54, 194].

3.1.3. Advances in Streaming Infrastructure Reliability

Event streaming is the backbone of most modern financial data platforms, and Apache Kafka is its most common implementation. Kafka 4.0, released on 18 March 2025, was the first major release to operate entirely without Apache ZooKeeper, running in KRaft mode by default (Apache Software Foundation, 2025a) [59]. Among its improvements, KIP-996 introduced a pre-vote mechanism to reduce unnecessary KRaft leader elections, KIP-1076 extended client metrics so that application-level metrics can be collected through brokers, KIP-932 provided early access to queue semantics through share groups, and old client protocol API versions and message formats were removed (Apache Software Foundation, 2025a) [59]. Clusters still running ZooKeeper must migrate to KRaft on a 3.x release before upgrading (AutoMQ, 2025) [67]. Kafka 4.1, released in September 2025, promoted Queues for Kafka from early access to preview, while noting it was still not ready for production (Apache Software Foundation, 2025b) [60].

These changes carry several reliability implications, which complement work on scalable cloud messaging architectures (Ahmed & Odejobi, 2018a) [23]:

- **Fewer moving parts:** Removing a separate coordination ensemble eliminates a whole class of failure modes and a second system to monitor, patch and capacity-plan. The controller quorum becomes the critical component, so controller election rate, metadata log lag and quorum health deserve explicit SLIs.
- **Election stability:** Pre-vote reduces disruptive elections caused by transient network partitions, which in a payments backbone can otherwise produce bursts of producer retries and latency spikes.
- **Broker-side visibility of clients:** Client metrics collected via brokers help platform teams observe consumer lag, retries and errors across hundreds of application teams without requiring each team to instrument and export consistently. Consumer lag is the raw material for data freshness SLIs (Section 3.2.2).
- **Queue semantics, with caution:** Share groups suit work-distribution patterns common in payment processing and exception handling. Because the feature was early access in 4.0 and preview in 4.1, it should be evaluated in non-production environments before use on critical flows.
- **Mandatory migrations as risk events:** The ZooKeeper-to-KRaft migration is itself a change with resilience implications. Under DORA and UK rules, it should be planned, tested and evidenced like any significant ICT change, with rollback paths and SLO monitoring throughout.

3.1.4. AI-Assisted Reliability Engineering

3.1.4.1. The 2025 Product Landscape

2025 marked the shift from AI copilots that summarise alerts to agents that investigate incidents autonomously. Datadog launched Bits AI SRE as a generally available on-call agent in December 2025, positioning it to investigate alerts and surface the fastest path to remediation (Datadog, 2025b) [88]. In November 2025 Observe introduced AI SRE agents and reported early customers achieving incident triage up to ten times faster, using a knowledge graph and an MCP server to give agents context (Observe, Inc., 2025) [158]. All performance figures here are vendor-reported. Together these releases mark a move from assistive suggestions toward agents that investigate on their own, extending earlier research on security orchestration and automated incident response in SIEM-centred operations (Dosunmu & Ogundele, 2021; Dosunmu & Ogundele, 2025c; Mbonu, Iwuanyanwu, et al., 2019) [90, 98, 153].

3.1.4.2. Governance Requirements in Regulated Environments

Adopting AI agents in financial incident response raises issues that general-purpose SRE literature does not fully address:

- **Explainability and audit:** Every hypothesis, query and action taken by an agent should be recorded so that the incident timeline can be reconstructed for postmortems and regulatory reports. Recommendations should show their supporting evidence (Elebe & Anunagba, 2025; Ominyi & Anichukwueze, 2024) [108, 188].
- **Third-party and concentration risk:** An AI agent vendor, and any model provider behind it, becomes an ICT third-party provider. Under DORA it belongs in the register of information, with contractual, exit and testing

arrangements (Folderit, 2025; Walkers Global, 2025) [118, 226].

- **Data protection:** Telemetry often contains personal and transactional data. Redaction at the Collector, data residency controls and clear rules on what can be sent to external models are prerequisites.
- **Model risk management:** Agents that influence operational decisions fall naturally within existing model risk frameworks, which require validation, performance monitoring and documented limitations (Ominyi & Anichukwueze, 2023; Ominyi & Anichukwueze, 2024) [187, 188]. Agents with tool access must also be protected against prompt injection, tool poisoning and excessive agency (Nwakamma et al., 2024b) [157].
- **Human factors:** The SREcon25 programme asked whether automation degrades operators' ability to handle incidents the tools cannot (USENIX, 2025) [224]. Organisations should keep humans practised through game days and require human judgement for novel failure modes.

3.1.5. Related Research Streams

The 2025 developments reviewed above sit within a wider body of research on monitoring, risk governance, security operations and data-driven decision making in financial and other regulated environments. This section organises that literature into twelve strands and shows how each informs reliability and observability for financial data platforms.

3.1.5.1. Real-Time Monitoring, Compliance Pipelines and Data Governance

The closest antecedent to data-centric reliability is work on real-time compliance pipelines, which reviews automated risk monitoring tied to enterprise data governance (Uchechi et al., 2022) [216], and on AI-assisted compliance monitoring with anomaly detection for high-volume transactions (Ominyi et al., 2024a) [189]. Automated KPI tracking and continuous performance monitoring (Ogbole, Okoruwa, Babatope, et al., 2021; Tonoyan et al., 2024b) [163, 215], and the embedding of economic evaluation directly into enterprise data pipelines (Ogundairo & Ayivi-Donkor, 2023b) [166], show that pipelines can carry their own quality and value signals. Early-warning predictive risk analytics across technology estates (Okwesa et al., 2024) [176] anticipates the shift from reactive alerting to risk forecasting. Governance architectures for lakehouses, data sensitivity classification and regulatory traceability (Aliliele et al., 2024a; Aliliele et al., 2025b) [44, 47], privacy-preserving analytics under GDPR and HIPAA (Aliliele et al., 2024b; Atakpa & Abolaji, 2022) [45, 65], and studies of data integrity failures and remediation in regulated operations (Aneke et al., 2023) [52] supply the controls side of the picture, together with work on data protection impact assessment in multi-cloud financial infrastructure and cross-border privacy governance (Annan, 2022; Mbonu et al., 2022a; Mbonu, Aliliele, et al., 2019; Ominyi, 2021) [55, 147, 151, 184]. Legal and ethical risk modelling for data protection (Mbonu et al., 2018) [142], risk-based assurance of data availability (Fadayomi et al., 2019) [111], comparative frameworks for data verification and risk screening (Peteranaba et al., 2022) [204], governance architectures for interoperable data backbones (Ilodigwe & Adesemoye, 2021) [124] and studies of trust, privacy and regulatory governance in AI-enabled digital services (Akintola et al., 2025) [28] show that the same governance problems recur across regulated sectors.

3.1.5.2. Operational Reliability and IT Service Management

A second strand addresses reliability as an operational discipline. An operational reliability and service assurance framework for enterprise IT serving large user populations (Olagunju et al., 2025) [179] and a governance model for change, incident and problem management in mission-critical environments (Olagunju et al., 2023) [177] are directly relevant to SRE practice, as are KPI-driven optimisation of IT service delivery (Edivri & Oteri, 2024) [106], performance optimisation for high-demand technology rollouts (Olagunju et al., 2024) [178], predictive capacity planning (Edivri & Oteri, 2022) [105] and maturity models for distributed IT support (Anyanwu, 2019; Wikiri, 2021) [57, 227]. Outside finance, a reliability engineering framework for sustained high availability in 5G core networks (Oteri et al., 2025a) [197], analyses of energy, reliability and latency trade-offs (Asiedu et al., 2025) [62], and general reliability and failure analysis of complex systems (Asibor & Isong, 2019; Gideon et al., 2019) [61, 119] offer transferable methods. Predictive maintenance, digital twins and interpretable failure prediction in energy and e-commerce systems (Adaramola et al., 2018; Komi & Adamolekun, 2021; Mayo et al., 2021; Shittu & Shittu, 2024; Shittu et al., 2023) [1, 128, 141, 208, 211] illustrate how condition monitoring can move from equipment to software platforms. Change management analytics for large organisational transitions (Oteri & Chibwaye, 2025) [196], secure decoupling of IT services after mergers and ownership changes (Fadero et al., 2025) [113], skill transfer between IT operations and new ventures (Anyanwu, 2022) [58] and data-driven lifecycle performance management (Adelanwa et al., 2023a) [11] address the organisational and architectural conditions under which reliability is sustained.

3.1.5.3. Cloud Architecture, Scaling and Software Delivery

Financial data platforms increasingly run on cloud infrastructure, and a substantial literature addresses its resilience and governance. Security design for resilient network architectures in large-scale cloud platforms (Upreti & Oteri, 2025) [223], continuous monitoring of cloud misconfiguration (Aliliele et al., 2023a) [43] and governance of Terraform-based infrastructure as code (Mbonu et al., 2020b) [149] correspond to the configuration-drift and control-plane risks discussed in Section 3.3.1. Machine learning models for cloud resource scaling and rightsizing (Ahmed et al., 2020; Upreti & Oteri, 2023) [25, 222], constraint-based resource allocation (Ahmed et al., 2019) [24] and database optimisation (Odejobi et al., 2019) [159] relate to capacity SLOs and telemetry cost. Migration and multi-cloud strategies (Ladapo et al., 2022; Ladapo et al., 2025; Ukadike, 2024) [131, 133, 220], scalable enterprise messaging (Ahmed & Odejobi, 2018a) [23], and real-time analytics and monitoring architectures (Tonoyan et al., 2024b; Uchechi et al., 2022) [215, 216] are directly relevant to the streaming backbone described in Section 3.1.3. Work on CI/CD, DevOps tooling, integration patterns and AI-assisted software testing (Badmus et al., 2018; Badmus et al., 2019a; Badmus et al., 2020; Badmus et al., 2022b; Borah et al., 2022; Mbonu et al., 2021b; Odejobi et al., 2025) [69, 70, 72, 73, 83, 145, 160], and portable cloud-to-edge runtimes (Ojukwu et al., 2025) [168] complete

the strand. Cloud-based IT service management orchestration on ServiceNow (Oteri et al., 2025b) [198] and malware classification for cloud-native microservices at the edge (Idika et al., 2021) [123] are also relevant to the operating environment of distributed financial platforms.

3.1.5.4. Identity, Zero Trust and Privacy Engineering

Because control-plane identity services proved to be a hidden dependency in the October 2025 outage, research on identity governance is pertinent. It includes identity-centric zero trust architecture for enterprise security governance (Ogbole, Okoruwa, Fadayomi, et al., 2021) [163], optimisation of cloud identity and access governance in large AWS estates (Mbonu et al., 2022b) [152], identity management for distributed and federated systems (Oshoba et al., 2019) [193] and integration strategies for hybrid and multi-cloud environments (Mbonu et al., 2020) [143]. Directory service assessment (Ladapo et al., 2018; Ladapo et al., 2019) [129, 132], privacy-based access control (Ladapo et al., 2023b) [134], privacy-centric security engineering (Okoruwa et al., 2020) [175] and zero trust in healthcare and operational technology (Adebayo, Anunagba, et al., 2025; Ahmed et al., 2021) [5, 26] broaden the evidence base.

3.1.5.5. Security Operations, Detection and Response

Incident response in financial institutions spans reliability and security, and security operations research offers mature models for detection and triage. Enterprise log analytics and automated incident response on SIEM platforms (Mbonu, Iwuanyanwu, et al., 2019) [153], security orchestration and automation for faster detection and response (Dosunmu & Ogundele, 2025c) [98], and incident response and forensics for rapid containment (Dosunmu & Ogundele, 2021) [90] parallel the AI SRE workflows described in Section 3.1.4. Threat intelligence integration and automation (Dosunmu & Ogundele, 2022; Dosunmu & Ogundele, 2023) [91, 92], continuous security validation, breach and attack simulation and threat-informed measurement of control effectiveness (Dosunmu & Ogundele, 2024a; Dosunmu & Ogundele, 2024c; Dosunmu & Ogundele, 2024d) [93, 95, 96], and integrated network and security operations centres (Ladapo et al., 2024) [130] show how evidence-driven assurance can be run continuously. Board-level cyber defence measurement and cyber risk quantification (Adegbite et al., 2025; Dosunmu & Ogundele, 2024b; Dosunmu & Ogundele, 2025b) [10, 94, 97], AI-based posture management for NIST CSF adherence (Amadi et al., 2025a) [49], and work on insider threat, awareness and ransomware economics (Adebayo, Adepoju, et al., 2023; Akeju et al., 2018; Onche et al., 2024; Ozowara et al., 2022; Ozowara, Anunagba, et al., 2025) [3, 27, 192, 200, 201] connect operations to governance. Surveys of enterprise threat evolution (Okoruwa et al., 2024) [174] frame the direction of this work.

3.1.5.6. Critical Infrastructure and Operational Technology Resilience

Payment systems and market infrastructures are designated critical infrastructure in many jurisdictions, and research on industrial and energy systems offers relevant methods for anomaly detection under hard availability constraints. Systematic reviews of machine learning for ICS threat detection (Adebayo, Adegbite, et al., 2023) [2], of SIEM, NDR and anomaly detection architectures for energy-sector SCADA networks (Adegbite et al., 2023) [8] and of vulnerabilities in legacy SCADA (Amadi et al., 2025c) [51], together with comparative deep learning for SCADA anomaly detection (Amadi et al., 2025b) [50] and continuously learning cyber-physical threat prevention (Amadi, 2025) [48], are instructive for detecting faults in legacy financial systems that cannot be instrumented directly. AI-driven SOC architectures for utilities (Adegbite et al., 2024b) [9], IT and OT convergence and NERC CIP compliance (Adegbite et al., 2020; Adegbite et al., 2022) [6, 7], and blockchain-assisted data exchange for control systems (Shittu et al., 2022) [210] align closely with the case for continuous, telemetry-based resilience evidence made in Section 3.1.1. IoT-enabled adaptive protection for cyber-physical resilience in digital substations (Shittu et al., 2024) [208], physics-informed ransomware defence using digital twins in operational technology (Ojukwu et al., 2023) [167], blockchain-assisted secure data exchange for SCADA-controlled systems (Shittu et al., 2022) [210] and security for IoT-driven transport infrastructure (Jimoh, Abolle-Okoyeagu, et al., 2023) [126] offer further designs for resilient operation under attack or failure.

3.1.5.7. Cyber Risk Governance and Regulatory Compliance in Financial Institutions

A large strand addresses governance and compliance in banks and other financial entities, which frames the regulatory context of Section 3.1.1. Frameworks for cybersecurity risk management and regulatory compliance in financial institutions (Bello et al., 2024) [76], for harmonising risk governance, technology infrastructure and compliance in future-ready banking (Okafor, Osuji, et al., 2024) [171], and for data-driven compliance analytics in risk governance (Akomolafe et al., 2025) [35] are directly aligned with DORA's ICT risk management pillar. Integrated governance for financial resilience (Akomolafe & Agu, 2019c) [32], risk-based business intelligence for fintech platforms (Mbonu et al., 2021a) [144], data-driven risk evaluation and compliance risk models for emerging markets (Akomolafe & Agu, 2019b; Akomolafe et al., 2023b) [31, 34], capital adequacy and risk-weighted asset optimisation (Mensah et al., 2019) [156], cyber risk maturity in insurance (Fadero et al., 2021) [114] and post-merger compliance integration (Ominyi, 2020) [183] extend this. Automated governance of operational and systemic risk (Uchechi et al., 2025) [218], the standardisation of compliance controls (Uchechi et al., 2023) [217] and the role of frameworks in cybersecurity governance (Jimoh, Ahmed, et al., 2023) [126] complete the strand. Related work on data-driven tax compliance and financial reporting in banks (Bola-Sadipe et al., 2022) [82], strategic accounting systems and comprehensive reporting models for transparency and accountability (Bola-Sadipe et al., 2019; Medon & Oduleye, 2022) [81, 154], financial governance in smaller enterprises (Eboh et al., 2025) [102], regulatory clearance for cross-border mergers (Ominyi & Anichukwueze, 2020) [185], cybersecurity compliance as competitive advantage (Annan, 2025b) [56], ethics and compliance training for behavioural change (Anichukwueze et al., 2020) [53], and IT risk, procurement risk and vendor risk models embedded in supply chain transformation (Bello et al., 2023; Mbonu et al., 2020a; Tonoyan et al., 2024a) [78, 148, 214] shows how compliance obligations shape technology and third-party arrangements, a theme central to DORA's third-party risk pillar.

3.1.5.8. Audit, Internal Control and Continuous Assurance

Supervisors increasingly expect evidence rather than attestation, which links SRE telemetry to audit research. Work on security audit and enterprise risk assessment for resilient information systems (Dosunmu & Ogundele, 2019) [89], AI-assisted continuous auditing in technology risk and cybersecurity oversight (Aliliele et al., 2025a) [46], AI-enabled IT general controls and SOX automation (Mbonu et al., 2022) [146], and implementation pathways from audit to continuous control (Adebayo, Amadi, et al., 2025) [4] supports the view that observability data can serve as continuous control evidence. Responsible AI in IT auditing with human oversight (Elebe & Anunagba, 2025) [108], auditing of AI-powered financial systems (Fobellah, 2025b) [117], SOX frameworks in cross-border auditing (Agu et al., 2023a) [20], risk-based auditing and internal control models (Akomolafe & Agu, 2018; Akomolafe & Agu, 2019a; Akomolafe et al., 2023a) [29, 30, 33], analytics-driven audit quality (Okoli et al., 2022; Ozowara, Adebayo, et al., 2025) [173, 201], cognitive bias in audit and risk decisions (Fobellah, 2025a) [116] and regulatory technology for fraud reporting (Bello, Elebe, et al., 2025) [75] make up the strand.

3.1.5.9. Fraud, Anti-Money Laundering and Transaction Monitoring

Fraud and AML systems are among the most latency-sensitive and correctness-critical consumers of financial streaming data. An adaptive fraud risk scoring model for real-time transaction monitoring at scale (Fadayomi et al., 2024) [112] and a systematic review of machine learning for fraud detection in banking (Atakpa & Abetoh, 2022) [64] illustrate the performance requirements such systems place on the platform. Predictive AML analytics (Atakpa, 2021) [63], comparative AML and anti-bribery regimes (Ominyi & Anichukwueze, 2021) [186], blockchain-supported KYC and AML (Bello, Oduro, et al., 2025) [74], AI-driven fraud detection in UK digital payments and international payment channels (Adesuyi et al., 2025a; Bello, Oguntola, et al., 2025) [15, 77], cross-border payment risk scoring (Adesuyi et al., 2024) [14], forensic analytics for fraud and compliance monitoring (Ekechi et al., 2022; Mbonu et al., 2021; Ogbole et al., 2025) [107, 144, 165], synthetic identity fraud detection (Elebe et al., 2023) [109], anomaly detection in financial time series (Atakpa & Fobellah, 2023) [66] and investment fraud due diligence (Adelanwa et al., 2023b; Eboh & Aliliele, 2023; Eboh & Aliliele, 2024; Eboh & Aliliele, 2025a) [12, 100, 101, 102] complete the strand.

3.1.5.10. Payment Infrastructure, Cross-Border Flows and Distributed Ledgers

Research on payment systems speaks directly to the reliability of financial data flows. End-to-end monitoring controls for cross-border payment operations and correspondent banking risk (Okafor, Farounbi, et al., 2024) [169] and a resilience and continuity model for global payment infrastructure under geopolitical risk (Adesuyi et al., 2025b) [16] are closely related to the concerns of this paper. Interoperability and standardisation models for ledger-based payments (Adesuyi et al., 2023; Akomolafe et al., 2025b) [13, 41], scalable blockchain payment gateways (Akomolafe et al., 2024a) [38], predictive remittance liquidity optimisation (Akomolafe et al., 2023) [33], regulatory adaptation of payment products (Olaogun et al., 2023) [180], secure payment data sharing (Akomolafe et al., 2025a) [40], smart contract automation and dispute resolution (Akomolafe et al., 2022; Akomolafe et al., 2024b) [36, 39], and tamper-proof blockchain audit trails for configuration management and regulatory recordkeeping (Anichukwueze et al., 2021; Oshoba et al., 2020) [54, 194] suggest mechanisms for immutable incident evidence. High-throughput collections platforms (Osuji et al., 2021) [195], transaction banking transformation (Okafor et al., 2021) [170], customer data platforms (Ukadike, 2022) [219], digital banking and inclusion (Agboada et al., 2022) [18], treasury architecture (Dada et al., 2021a) [86], bank and capital market resilience after the pandemic (Isiekwu et al., 2025) [125] and fintech investment risk monitoring (Eboh & Aliliele, 2025b) [103] broaden the context. Studies of the macroeconomic impact of blockchain-enabled payment adoption (Olaogun et al., 2025) [181], partnership ecosystems in private banking (Agboada et al., 2020) [17], trade finance product design (Agboada et al., 2018) [19] and relationship banking performance (Ezeako et al., 2019) [110] show the business dependence on payment and banking platforms whose reliability this paper addresses.

3.1.5.11. AI Governance, Model Risk and Agentic AI

The governance questions raised by AI SRE agents in Sections 3.1.4 and 3.2.4 are anticipated by work on responsible AI structures for automated decision systems in regulated industries (Ominyi & Anichukwueze, 2024) [188], algorithmic accountability and model risk management in financial services (Ominyi & Anichukwueze, 2023) [187] and organisational readiness for the EU AI Act (Ominyi et al., 2024b) [190]. Securing agentic AI workflows against prompt injection, tool poisoning, memory manipulation and excessive agency (Nwakamma et al., 2024b) [157] is directly relevant to agents granted operational permissions, as are multi-agent quality control for regulated documents (Ominyi et al., 2025a) [191], governance of AI-assisted CRM agents (Badmus et al., 2025) [68], responsible automation brokerage (Alieme et al., 2025) [42], data curation for fine-tuning (Oyesiji et al., 2024) [199] and AI in operational analytics (Rukh et al., 2024) [207].

3.1.5.12. Predictive and Financial Analytics for Decision Systems

Finally, a strand on financial analytics and decision systems informs how reliability data can be used in business decisions such as error budget policy, investment in redundancy and capacity planning. It includes integrated predictive models for financial forecasting (Medon & Oduleye, 2024) [155], analytics-driven decision making in banking (Oluwo et al., 2025) [182], executive dashboards for real-time oversight (Walawalkar et al., 2025) [225], data management for forecasting accuracy (Agu et al., 2023b) [21], Python-based predictive risk assessment (Agu et al., 2025) [22], and models for capital allocation, cost management and strategic alignment (Lawal & Oduleye, 2018a; Lawal & Oduleye, 2018b; Lawal & Oduleye, 2019b; Lawal & Oduleye, 2021a; Lawal & Oduleye, 2021b; Lawal & Oduleye, 2023b; Oduleye & Medon, 2021; Oduleye & Medon, 2023b; Tonoyan et al., 2022c) [135, 136, 137, 138, 139, 140, 161, 162, 213], together with CRM analytics and platform governance in financial and regulated settings (Badmus et al., 2019b; Okoli et al., 2025; Ukadike & Ibeh, 2023) [71, 172, 221].

Across these strands, three gaps stand out. First, most monitoring and compliance work treats data quality and

system reliability separately, whereas this paper argues for a single set of SLIs covering both. Second, few studies connect telemetry to time-boxed regulatory incident classification of the kind DORA requires. Third, the governance of AI agents with operational authority over financial platforms is only beginning to be addressed. The conceptual model in Section 3.2 is designed to address these gaps.

3.2. Conceptual Model

3.2.1 The Integrated Financial Data Reliability (IFDR) Model

The synthesis in Section 3.1 points to a common pattern. Regulatory change, technical advances and a more concentrated failure environment are pushing financial institutions to treat reliability, data integrity and regulatory reporting as one problem rather than three. The IFDR model, shown in Figure 1, organises this pattern into three layers. Drivers are the external forces observed in 2025: regulatory (DORA and UK impact tolerances), technological (OpenTelemetry, Kafka 4.x and AI SRE agents) and the failure environment (cloud concentration, control-plane dependency and silent data failures). Core capabilities are what an institution builds in response: data-centric SLIs (C1), a unified telemetry pipeline (C2), governed AI autonomy (C3) and telemetry-based regulatory classification (C4). Outcomes are the resilience results sought: services kept within impact tolerance with faster and safer recovery (O1), data integrity (O2) and timely, defensible regulatory reporting (O3). Governance maturity, human expertise and third-party arrangements moderate the strength of these relationships.

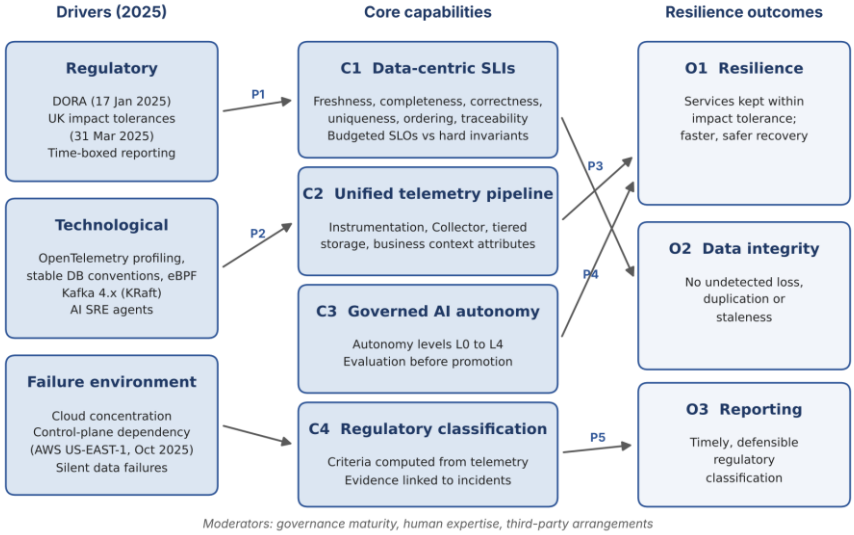


Fig 1: The Integrated Financial Data Reliability (IFDR) model

The following subsections specify each capability in operational terms and then state the relationships as propositions.

3.2.2 Capability C1: Data-Centric Service Level Indicators

Request-centric SLIs capture whether a service answered and how fast. They do not capture whether data arrived on time, completely and correctly, which is what most financial data platforms exist to guarantee. Silent failures in data pipelines were singled out by the SREcon25 programme as a priority topic (USENIX, 2025) [224]. Table 3 extends classic SLIs with data-centric indicators. Each indicator is expressed as a ratio of good events to valid events, consistent with standard SRE practice (Beyer et al., 2016) [79], so that error budgets can be computed uniformly.

Table 3: Data-centric SLI taxonomy for distributed financial data processing platforms

Indicator	Definition	Example measurement	Illustrative target
Availability	Proportion of valid requests or instructions accepted and processed without error	Successful payment API calls divided by valid calls	99.95% monthly
Latency	Proportion of operations completed within a threshold	Authorisations completed in under 300 ms at p99	99% of minutes compliant
Freshness	Age of the newest data available to consumers relative to source	Event time watermark lag; consumer lag converted to seconds	Positions under 60 s old during trading hours
Completeness	Proportion of expected records present by a deadline	Records received versus control totals from the source system	100% of batches complete by cut-off
Correctness	Proportion of records passing invariant and reconciliation checks	Debit and credit totals balance per ledger per interval	Hard invariant: zero tolerance
Uniqueness	Proportion of instructions applied exactly once	Duplicate idempotency keys detected downstream	Hard invariant: zero tolerance
Ordering	Proportion of keyed events processed in order	Sequence gaps or regressions per account	99.999% in order; gaps alerted
Traceability	Proportion of records with complete lineage and trace context	Records carrying source message ID and trace ID end to end	99.9%

Targets are illustrative only and must be derived from business impact analysis and, where applicable, impact tolerances.

Not every indicator should carry an error budget. We distinguish budgeted objectives, such as availability, latency and freshness, where occasional shortfall is tolerable and the budget supports release and change decisions, from hard invariants, such as conservation of value and exactly-once application, where any violation is an incident. Hard invariants are monitored continuously, and a violation should trigger automated containment (pausing the affected flow, diverting to a quarantine topic or engaging a kill switch) before human triage.

Streaming platforms make continuous reconciliation feasible: windowed aggregates computed independently at ingress and egress can be compared every few seconds, and divergence becomes an SLI. Control totals published by upstream systems alongside data (record counts, hash totals, value sums) allow completeness to be measured at each hop. Carrying a durable business identifier, such as an ISO 20022 end-to-end identification or a trade reference, as a trace attribute links data-quality failures to the specific spans and services involved, joining data observability with application observability. Related proposals for real-time transaction monitoring and AI-assisted anomaly detection over high-volume transactions (Atakpa & Fobellah, 2023; Fadayomi et al., 2024; Ominyi et al., 2024a) [66, 112, 189] can consume the same streams. Freshness can be derived from stream processor watermarks or from consumer lag converted to time; broker-side client metrics in Kafka 4.0 (Apache Software Foundation, 2025a) [59] make this easier to compute uniformly across an estate.

3.2.3 Capability C2: Unified Telemetry Pipeline

C2 is the reference architecture in Table 5 (Section 3.2.5). Its defining features are that it collects application, infrastructure and data-quality signals through one open pipeline, attaches business context (important business service, client segment, jurisdiction) at the point of instrumentation, and retains incident evidence immutably. These features allow the same telemetry to serve engineering diagnosis, SLO reporting and regulatory classification.

3.2.4 Capability C3: Governed AI Autonomy

Firms should classify agent capabilities by autonomy level and permit higher levels only for actions whose blast radius and reversibility are well understood. Table 4 sets out the levels.

Table 4: Autonomy levels for AI agents in financial incident response

Level	Name	Permitted behaviour	Typical financial use
L0	Observe	Read telemetry; summarise; no recommendations	Shift handover summaries
L1	Advise	Form hypotheses and recommend actions with evidence	Root cause suggestions during incidents
L2	Prepare	Draft runbook steps, change records and regulatory report fields for human approval	Pre-filling DORA classification criteria
L3	Act with approval	Execute pre-approved, reversible actions after explicit human sign-off	Scaling consumers; failing over read replicas
L4	Act autonomously	Execute bounded, reversible actions without sign-off; notify humans	Restarting stateless pods; quarantining malformed messages

Actions that move money, alter ledgers, communicate with customers or regulators, or are hard to reverse should remain at L2 or below.

Agents should be evaluated before promotion between levels by replaying historical incidents and measuring accuracy of root cause identification, time to useful hypothesis and rate of harmful or misleading recommendations. Evaluation results become part of the evidence that the firm manages ICT risk proportionately.

3.2.5 Capability C4 and the Reference Architecture

C4 is a classification module that pre-computes DORA and UK criteria (affected clients and transactions, duration, jurisdictions, data impact) from telemetry and links each incident record to its supporting evidence. Table 5 shows how C2, C3 and C4 fit together in a layered, vendor-neutral reference architecture.

Table 5: Reference architecture layers

Layer	Components and 2025 advances	Purpose
Instrumentation	OpenTelemetry SDKs with stable HTTP and database conventions; OBI eBPF for unmodifiable workloads; eBPF profiling; Kafka client metrics; data-quality probes emitting control totals	Uniform telemetry across modern, legacy and vendor components, including data-centric signals
Collection	OpenTelemetry Collector in agent and gateway tiers; tail sampling; PII redaction; routing by retention class	Control cost and cardinality; protect personal data; ensure errors and flagged transactions are always kept
Storage	Hot store for operational queries; low-cost lake storage for long retention; immutable evidence store	Balance query speed and cost; meet record-keeping and evidential requirements
Analysis	SLO engine covering Table 3 indicators; continuous reconciliation service; dependency graph builder; AI agents governed per Table 4	Detect budget burn and invariant breaches; map real dependencies; accelerate diagnosis
Response	Incident management; regulatory classification module (C4); customer and supervisor communication workflows	Classify and report within deadlines with evidence linked to telemetry
Governance	Mapping of important business services to SLOs and impact tolerances; third-party register reconciliation; agent evaluation records; testing evidence	Demonstrate to supervisors a continuous link between engineering practice and resilience outcomes

Two design principles cut across the layers. First, independence of the observing system: at least a minimal path for alerting and status must survive the failure of the primary cloud region or provider. Second, business context in telemetry: impact must be aggregable in the terms regulators use without manual mapping during an incident.

3.2.6 Propositions

The relationships in Figure 1 are stated as five propositions for empirical testing:

P1. Regulatory obligations that fix incident classification criteria and deadlines increase the likelihood that institutions adopt data-centric SLIs alongside availability and latency SLIs.

P2. Maturity of open observability standards (stable semantic conventions, eBPF instrumentation, profiling) increases the coverage and consistency of a unified telemetry pipeline, particularly for legacy and vendor components.

P3. Institutions that operate data-centric SLIs with hard invariants and continuous reconciliation over a unified telemetry pipeline experience fewer undetected data integrity failures than those relying on request-centric SLIs and end-of-day reconciliation.

P4. AI agents improve recovery time without increasing operational risk only when their autonomy is governed by explicit levels, evaluation before promotion and human approval for irreversible actions.

P5. Computing regulatory classification criteria directly from telemetry shortens the time to classify and report major incidents and improves the accuracy of reported impact, and this effect is stronger in concentrated failure environments.

3.3. Discussion

3.3.1 Illustrative Case: The 20 October 2025 AWS US-EAST-1 Outage

Early on 20 October 2025, AWS reported increased error rates and latencies for multiple services in its US-EAST-1 region, beginning at 12:11 AM PDT. By 1:26 AM it reported significant error rates on the DynamoDB endpoint, and at 2:01 AM it identified a likely root cause in DNS resolution of the DynamoDB API endpoint. Global features relying on US-EAST-1 endpoints, such as IAM updates and DynamoDB Global Tables, were also affected, and banks and government sites were among those disrupted (Robinson, 2025) [206]. Payment industry coverage described connectivity problems at many banks and warned of knock-on effects on payment flows (Payment Expert, 2025) [203]. Subsequent technical analyses, drawing on AWS's post-event summary, attributed the trigger to a race condition in DynamoDB's automated DNS management in which a delayed process reapplied outdated state, leaving the regional endpoint without valid records. They reported that more than 140 AWS services were affected over roughly 15 hours, with most of that duration spent on recovery rather than on the initial fault, and listed payment and exchange applications among those with stuck payments and delays (Reddy, 2025) [205]. The event illustrates concerns raised in research on the continuity of global payment infrastructure and on end-to-end monitoring of cross-border payment operations (Adesuyi et al., 2025b; Okafor, Farounbi, et al., 2024) [16, 169].

Read through the IFDR model, the case yields seven lessons:

1. **Control planes are hidden single points of failure (failure environment, C2):** Firms with multi-region data planes still suffered if identity, configuration or orchestration depended on a single region. Dependency maps must include control-plane and global-service dependencies, not just where data is stored.
2. **Recovery dominates duration (O1):** Because most of the outage was spent recovering (Reddy, 2025) [205], reliability engineering must cover the return path: backlog draining, retry storms and throttling. Observability should expose queue depth, retry rate and admission control during recovery, and runbooks should include deliberate load shedding.
3. **Static stability beats reactive failover (O1):** Systems that can continue serving with existing capacity and cached credentials when a dependency fails outperform those that must call a failing control plane to fail over.
4. **Monitor from outside the provider (C2):** Telemetry pipelines and alerting hosted in the affected region can fail with it. Synthetic probes and a minimal alerting path independent of the primary provider preserve situational awareness.
5. **Concentration risk is measurable (C2, C4):** DORA registers of information list contracts, but observed traffic reveals actual dependencies. Deriving dependency graphs from traces and network telemetry, and reconciling them with the register, gives a truer picture of concentration.
6. **Classification readiness (C4, P5):** An incident of this kind may meet several DORA major-incident criteria, including duration above 24 hours for some firms and media coverage (Burke & Price, 2025) [84]. Firms that could compute affected clients and transactions from telemetry were better placed to classify and notify quickly.
7. **Data integrity after recovery (C1, P3):** Partial writes, retried instructions and replayed messages during recovery are exactly where duplicate and missing records arise. Post-incident reconciliation should be an explicit recovery step, with hard invariants checked before declaring the incident closed.

3.3.2 Interpreting the 2025 Shift

The synthesis suggests that 2025 marked a change in what reliability means for financial data platforms. In earlier practice, reliability was largely internal: engineering teams set SLOs, compliance teams wrote policies, and the two met mainly in periodic audits. In 2025, regulation fixed the questions that telemetry must answer and the time within which it must answer them, while open standards made it practical to answer those questions consistently across heterogeneous estates. The peer literature reviewed in Section 3.1.5 shows the same movement from periodic to continuous assurance in audit, security validation and compliance monitoring, which supports the central claim of the IFDR model that telemetry is becoming regulatory evidence.

Four tensions qualify this conclusion. Speed versus accuracy: early classification under DORA deadlines may rely on incomplete telemetry, so classification modules must express uncertainty and support revision in intermediate and final reports. Autonomy versus accountability: AI agents shorten diagnosis but complicate attribution of decisions, which is why the model ties autonomy to explicit levels and evidence. Standardisation versus domain specificity: general-purpose semantic conventions improve consistency but do not yet describe payments, ledgers or settlement, leaving each institution to invent its own attributes. Completeness versus cost: retaining all telemetry is unaffordable at financial volumes, yet evidence obligations require that the right records survive; tail sampling and retention tiers manage this tension but do not remove it.

3.4. Implications

3.4.1 Implications for Practice

- Define data-centric SLIs (Table 3) for each important business service, separating budgeted objectives from hard invariants, and wire hard invariant breaches to automated containment.
- Attach business context to telemetry at instrumentation time so that incident impact can be aggregated in regulatory terms without manual mapping.
- Treat the ZooKeeper-to-KRaft migration and other platform changes as evidenced ICT changes with SLO monitoring and rollback paths.
- Adopt AI SRE agents through the autonomy levels in Table 4, starting at L1 or L2 and promoting only after replay-based evaluation; register agent and model providers as ICT third parties.
- Build a minimal, provider-independent alerting path and derive dependency graphs from observed traffic to test concentration assumptions.

3.4.2 Implications for Regulators and Supervisors

- Encourage firms to evidence resilience through continuous telemetry linked to impact tolerances, rather than relying mainly on periodic scenario tests and attestations.
- Recognise data integrity measures (freshness, completeness, correctness) alongside time-based tolerances, consistent with the FCA observation that time-bound tolerances alone are insufficient (Financial Conduct Authority, n.d.).
- Provide guidance on the use of AI agents in incident response, covering autonomy, auditability and third-party treatment of model providers.
- Consider using aggregated, telemetry-derived dependency data to monitor sector-wide concentration on shared cloud providers.

3.4.3 Implications for Research and Theory

For research, the IFDR model reframes reliability in regulated financial settings as a socio-technical capability that spans engineering, data governance and compliance, rather than as a property of individual systems. It offers constructs and propositions that can be operationalised in surveys of institutions, comparative case studies and quantitative analysis of incident data. It also connects previously separate literatures, including continuous auditing, security operations, payment resilience and AI governance, around a shared object: the telemetry that institutions collect about their own operations.

3.5. Limitations

Several limitations apply. First, the evidence on 2025 developments relies partly on vendor announcements and secondary analyses whose performance figures have not been independently verified. Second, screening of the peer literature was conducted by a single reviewer on titles and bibliographic metadata, which introduces a risk of selection bias and means that the characterisation of some studies is based on their stated focus rather than full-text appraisal. Third, the peer list was drawn from a consolidated set rather than a comprehensive database search, so relevant work published elsewhere may have been missed. Fourth, regulatory summaries are simplified and do not constitute legal advice. Fifth, the IFDR model and its propositions are conceptual and have not been empirically validated, and the single illustrative case cannot establish generality. Finally, the review is restricted to sources published up to the end of 2025, so later developments are outside its scope.

3.6. Future Research

The propositions in Section 3.2.6 provide an immediate agenda for empirical testing. Beyond them, the synthesis identifies the following directions:

- **Financial-domain semantic conventions:** OpenTelemetry now has stable conventions for HTTP and databases and evolving ones for messaging and generative AI, but none for payments, securities or ledgers. Shared conventions for attributes such as payment scheme, message type, settlement date and business identifiers would enable comparable SLIs across institutions and vendors.
- **Correctness observability at scale:** Continuous reconciliation over high-volume streams raises open questions about approximate versus exact methods, the cost of maintaining independent aggregates and how to localise a divergence quickly.
- **Evaluating AI agents:** There are no public benchmarks of realistic financial incidents. Privacy-preserving incident corpora, replay harnesses and agreed metrics for agent accuracy and harm would allow firms and supervisors to assess these tools on evidence.
- **Telemetry as regulated data:** Telemetry increasingly falls under data protection, retention and cross-border transfer rules. Techniques for minimisation, pseudonymisation and selective retention that preserve diagnostic value need further work.
- **Quantifying concentration risk:** Methods to compute systemic dependency on shared providers from observed telemetry, rather than from contracts alone, would serve both firms and macroprudential supervisors, building on cyber risk quantification work (Adegbite et al., 2025; Dosunmu & Ogundele, 2024b) [10, 94].
- **Recovery engineering:** The October 2025 outage showed that recovery can take far longer than the fault. Formal models and testing methods for recovery dynamics, including backlog draining and retry storms, deserve more attention than they receive.
- **Human and organisational factors:** As agents take on more diagnosis, keeping engineers skilled and maintaining clear accountability for decisions will require deliberate training, exercise design and role definitions.
- **Validation of the IFDR model:** Multi-case studies across banks, payment institutions and market infrastructures, and surveys measuring capability maturity against incident outcomes, would test and refine the model.

4. Conclusion

In 2025, reliability engineering for financial data platforms stopped being only an internal engineering concern. DORA and the UK operational resilience regime made the ability to measure, classify and report disruption a legal obligation with fixed deadlines. OpenTelemetry's maturation gave institutions a vendor-neutral way to produce the evidence those obligations demand, Kafka 4.0 simplified the streaming backbone on which many platforms depend, and AI SRE agents arrived as generally available products. The October

2025 AWS outage demonstrated that hidden control-plane dependencies and slow recovery, rather than the initial fault, determine much of the impact.

This paper has synthesised these developments with 205 peer studies and proposed the IFDR model, which links drivers to four capabilities and three resilience outcomes through five propositions. Its central argument is that financial institutions should define reliability in terms of data freshness, completeness and correctness as well as availability and latency; express impact tolerances and SLOs in the same telemetry; govern AI agents through explicit autonomy levels; and connect observability pipelines directly to regulatory classification. Institutions that do so will be better placed not only to satisfy supervisors but to prevent the silent, data-level failures that matter most in finance.

References

1. Adaramola TS, Fadero S, Gideon EN. Predictive maintenance and condition monitoring in critical power and energy infrastructure. Iconic Research and Engineering Journals. 2018;2(5):454-477. doi:10.64388/IREV2I5-1722489
2. Adebayo A, Adegbite MP, Ahmed MO. AI augmented threat detection in industrial control systems: A systematic review of machine learning approaches for ICS anomaly detection. International Journal of Engineering and Modern Technology. 2023;9(3):287-340. doi:10.56201/ijcsmt.v9.no3.2023.pg287.340
3. Adebayo A, Adepoju PA, Ozowara DE. Conceptual model for cyber risk pricing and insurance structuring in health technology platforms. Gyanshauryam, International Scientific Refereed Research Journal. 2023;6(6).
4. Adebayo A, Amadi C, Ijagbemi AO. From audit to continuous control: Implementation pathways, governance, and organizational readiness for AI-enabled compliance in critical infrastructure. International Journal of Computer Science and Mathematical Theory. 2025;11(8):88-134. doi:10.56201/ijcsmt.vol.11.no8.2025.pg88.134
5. Adebayo A, Anunagba CO, Ozowara DE. A review of zero trust security models and cost effectiveness in healthcare infrastructure. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2269-2283. doi:10.62225/2583049X.2025.5.6.6051
6. Adegbite MP, Adebayo A, Ahmed MO. Securing operational technology networks in electric utilities: A systematic review of NERC CIP compliance and architectural threat mitigation. International Journal of Engineering and Modern Technology. 2020;6(3):103-146. doi:10.56201/ijemt.vol.6.no3.2020.pg103.146
7. Adegbite MP, Adebayo A, Ahmed MO. A security architecture model for IT and OT convergence in regulated energy networks: Design principles and governance alignment. International Journal of Computer Science and Mathematical Theory. 2022;8(2):81-132. doi:10.56201/ijcsmt.v8.no2.2022.pg81.132
8. Adegbite MP, Adebayo A, Ahmed MO. ICS and SCADA threat detection architectures in energy sector networks: A systematic review of SIEM, NDR, and anomaly detection approaches. World Journal of Innovation and Modern Technology. 2023;7(2):121-182. doi:10.56201/wjimt.v7.no2.2023.pg121.182
9. Adegbite MP, Adebayo A, Ahmed MO. An AI driven security operations architecture for utility sector SOCs: Integrating threat intelligence, behavioral analytics, and automated response. International Journal of Engineering and Modern Technology. 2024;10(11):197-256. doi:10.56201/ijemt.v10.no11.2024.pg197.256
10. Adegbite MP, Adebayo A, Ahmed MO. A cyber risk quantification and governance architecture for critical infrastructure: From posture measurement to executive reporting. International Journal of Computer Science and Mathematical Theory. 2025;11(12):232-293. doi:10.56201/ijcsmt.vol.11.no12.2025.pg232.293
11. Adelanwa A, Basnet A, Anene UN. Data driven digital transformation models for lifecycle performance management in infrastructure delivery. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(6):2646-2662. doi:10.62225/2583049X.2023.3.6.5968
12. Adelanwa A, Basnet A, Anene UN. Predictive analytics models for financial risk detection and fraud prevention in public systems. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(6). doi:10.62225/2583049X.2023.3.6.5969
13. Adesuyi MO, Akomolafe O, Olaogun BO, Ndukwe VU, Sakyi JK. Global interoperability model for distributed ledger-based cross-border payment systems. International Journal of Multidisciplinary Research and Growth Evaluation. 2023;4(6):1291-1300. doi:10.54660/.IJMRGE.2023.4.6.1291-1300
14. Adesuyi MO, Akomolafe O, Olaogun BO, Ndukwe VU, Sakyi JK. AI-driven risk scoring model for global cross-border trade payment transactions. International Journal of Advanced Multidisciplinary Research and Studies. 2024;4(1):1569-1581. doi:10.62225/2583049X.2024.4.1.5281
15. Adesuyi MO, Akomolafe O, Olaogun BO, Ndukwe VU, Sakyi JK. AI-enabled fraud detection ecosystem model for securing international payment channels. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):866-882. doi:10.62225/2583049X.2025.5.6.5284
16. Adesuyi MO, Akomolafe O, Olaogun BO, Ndukwe VU, Sakyi JK. Resilience and continuity model for global payment infrastructure under geopolitical risks. International Journal of Multidisciplinary Research and Growth Evaluation. 2025;6(4):1467-1482. doi:10.54660/.IJMRGE.2025.6.4.1467-1482
17. Agboada P, Anene UN, Ezeako R, Okoli IE. Partnership ecosystems in private banking: A review of advances in non-financial value-proposition design. International Journal of Engineering Technology Research & Management. 2020;4(11):96-115.
18. Agboada P, Anene UN, Obukadata VO, Ezeako R. Financial inclusion and digital banking transformation in Sub-Saharan Africa: A review of advances and policy implications. International Journal of Management and Organizational Research. 2022;1(1):267-282. doi:10.54660/IJMOR.2022.1.1.267-282
19. Agboada P, Ezeako R, Okoli IE, Ibeh AV. Distributorship and trade finance product design: A conceptual framework for new-to-bank growth in emerging markets. Iconic Research and Engineering

Journals. 2018;2(5):552-578. doi:10.64388/IREV2I5-1723312
20. Agu MU, Akomolafe O, Bello A. A comparative review of SOX compliance frameworks in cross-border financial auditing. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(6):2297-2306. doi:10.62225/2583049X.2023.3.6.5362
21. Agu MU, Akomolafe O, Bello A. A review of integrated data management systems for enhancing financial forecasting accuracy. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(6):2335-2344.
22. Agu MU, Akomolafe O, Bello A. Advances in predictive financial risk assessment using Python-based forecasting systems. International Journal of Computer Science and Mathematical Theory. 2025;11(11):131-148. doi:10.56201/ijcsmt.vol.11.no11.2025.pg131.148
23. Ahmed KS, Odejobi OD. Conceptual framework for scalable and secure cloud architectures for enterprise messaging. IRE Journals. 2018;2(1):1-15.
24. Ahmed KS, Odejobi OD, Oshoba TO. Algorithmic model for constraint satisfaction in cloud network resource allocation. IRE Journals. 2019;2(12):516-532.
25. Ahmed KS, Odejobi OD, Oshoba TO. Predictive model for cloud resource scaling using machine learning techniques. Journal of Frontiers in Multidisciplinary Research. 2020;1(1):173-183.
26. Ahmed MO, Adegbite MP, Adebayo A. Zero trust architecture for operational technology in North American critical infrastructure: A framework for implementation and resilience optimization. International Journal of Engineering and Modern Technology. 2021;7(1):66-113. doi:10.56201/ijemt.vol.7.no1.2021.pg66.113
27. Akeju B, Edivri J, Ogbole JI, Okoruwa PO, Fadayomi O, Abolaji TO. Conceptual model for insider threat classification and risk modeling in complex digital systems. Iconic Research and Engineering Journals. 2018;1(9):476-492. doi:10.64388/IREV1I9-1713778
28. Akintola AS, Fawehinmi YO, Aiyenitaju O, Chinemerem B, Emmanuella O. Digital transformation in telehealth: A systematic review of user trust, privacy, and regulatory governance in AI-powered remote monitoring systems. Journal of Scientific Research and Reports. 2025;31(11):163-182. doi:10.9734/jsrr/2025/v31i113658
29. Akomolafe O, Agu MU. A conceptual model for enhancing internal audit quality through technology-enabled risk assessment frameworks. Iconic Research and Engineering Journals. 2018;1(9):458-475.
30. Akomolafe O, Agu MU. A conceptual framework for developing risk-based internal control models in the insurance and banking sectors. Iconic Research and Engineering Journals. 2019;2(8):335-354.
31. Akomolafe O, Agu MU. A review of data-driven risk evaluation models for emerging market financial institutions. Iconic Research and Engineering Journals. 2019;3(6):433-448.
32. Akomolafe O, Agu MU. Advances in financial resilience through integrated governance and compliance strategies. Iconic Research and Engineering Journals. 2019;2(10):607-620.
33. Akomolafe O, Agu MU, Bello A. A conceptual model for implementing risk-based auditing in strategic financial management. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(6):2274-2286. doi:10.62225/2583049X.2023.3.6.5359
34. Akomolafe O, Agu MU, Bello A. A quantitative conceptual model for assessing compliance risk in emerging economies. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(6):2287-2296. doi:10.62225/2583049X.2023.3.6.5360
35. Akomolafe O, Agu MU, Bello A. A conceptual model for advancing risk governance through data-driven compliance analytics in financial institutions. Journal of Accounting and Financial Management. 2025;11(11):211-228. doi:10.56201/jafm.vol.11.no11.2025.pg211.228
36. Akomolafe O, Olaogun BO, Adesuyi MO, Ndukwe VU, Sakyi JK. Smart contract automation model for supplier payment systems and performance benchmarking. International Journal of Multidisciplinary Research and Growth Evaluation. 2022;3(6):827-836. doi:10.54660/.IJMRGE.2022.3.6.827-836
37. Akomolafe O, Olaogun BO, Adesuyi MO, Ndukwe VU, Sakyi JK. Predictive AI model for remittance liquidity optimization in international payment systems. International Journal of Multidisciplinary Research and Growth Evaluation. 2023;4(6):1301-1311. doi:10.54660/.IJMRGE.2023.4.6.1301-1311
38. Akomolafe O, Olaogun BO, Adesuyi MO, Ndukwe VU, Sakyi JK. Scalable blockchain payment gateway architecture model for enterprise-grade adoption. International Journal of Advanced Multidisciplinary Research and Studies. 2024;4(1):1552-1568. doi:10.62225/2583049X.2024.4.1.5280
39. Akomolafe O, Olaogun BO, Adesuyi MO, Ndukwe VU, Sakyi JK. Smart contract-based dispute resolution model for international supplier payments. International Journal of Advanced Multidisciplinary Research and Studies. 2024;4(1):1582-1601. doi:10.62225/2583049X.2024.4.1.5282
40. Akomolafe O, Olaogun BO, Adesuyi MO, Ndukwe VU, Sakyi JK. Collaborative governance framework for secure cross-border payment data sharing. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):849-865. doi:10.62225/2583049X.2025.5.6.5283
41. Akomolafe O, Olaogun BO, Adesuyi MO, Ndukwe VU, Sakyi JK. Global standardization model for next-generation blockchain interoperability in payment systems. International Journal of Multidisciplinary Research and Growth Evaluation. 2025;6(6):820-834. doi:10.54660/.IJMRGE.2025.6.6.820-834
42. Alieme JI, Sule A, Obukadata VO. The business analyst as an AI-transformation broker: A framework for stakeholder alignment, responsible automation, and value realization in small and medium-sized enterprises. International Journal of Economics and Business Management. 2025;11(8):299-355. doi:10.56201/ijebm.vol.11.no8.2025.pg299.355
43. Aliliele C, Mbonu IS, Iwuanyanwu U. A conceptual framework for continuous cloud misconfiguration monitoring and enterprise risk mitigation strategies.

International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023;9(10):373-394. doi:10.32628/CSEIT2361071
44. Aliliele C, Mbonu IS, Iwuanyanwu U. A conceptual framework for enterprise data sensitivity classification and regulatory traceability mechanisms. International Journal of Advanced Multidisciplinary Research and Studies. 2024;4(6):3103-3124. doi:10.62225/2583049X.2024.4.6.5991
45. Aliliele C, Mbonu IS, Iwuanyanwu U. Advances in HIPAA compliant data architecture and secure analytics frameworks for community healthcare organizations. Shodhshauryam, International Scientific Refereed Research Journal. 2024;7(2):277-324. doi:10.32628/SHISRRJ2472163
46. Aliliele C, Mbonu IS, Uzoka E, Iwuanyanwu U. A review of AI assisted continuous auditing systems in technology risk and cybersecurity oversight. Gyanshauryam, International Scientific Refereed Research Journal. 2025;8(4):210-250. doi:10.32628/GISRRJ258369
47. Aliliele C, Mbonu IS, Uzoka E, Iwuanyanwu U. Advances in data lakehouse governance architectures for enterprise data loss prevention and compliance assurance. Shodhshauryam, International Scientific Refereed Research Journal. 2025;8(4):171-213. doi:10.32628/SHISRRJ258474
48. Amadi C. An autonomous, continuously-learning framework for real-time cyber-physical threat prevention in legacy SCADA systems. World Journal of Innovation and Modern Technology. 2025;9(8):148-183. doi:10.56201/wjimt.v9.no8.2025.pg148.183
49. Amadi C, Adebayo A, Ijagbemi AO. AI-based security posture management as an enabling layer for real-time NIST Cybersecurity Framework adherence: A theory-grounded conceptual framework. World Journal of Innovation and Modern Technology. 2025;9(8):99-147. doi:10.56201/wjimt.v9.no8.2025.pg99.147
50. Amadi C, Adebayo A, Ijagbemi AO. Deep learning architectures for anomaly detection in SCADA networks: A comparative analysis of LSTM, CNN, and hybrid LSTM-autoencoder models. International Journal of Engineering and Modern Technology. 2025;11(8):352-392. doi:10.56201/ijemt.vol.11.no8.2025.pg352.392
51. Amadi C, Adebayo A, Ijagbemi AO. The cyber-physical attack surface of legacy SCADA networks: A systematic review of vulnerabilities, threats, and detection gaps in critical infrastructure. International Journal of Computer Science and Mathematical Theory. 2025;11(8):135-169. doi:10.56201/ijcsmt.vol.11.no8.2025.pg135.169
52. Aneke OB, Sydney E, Adesemoye AC. Data integrity and governance in regulated life sciences operations: A review of failures, controls, and remediation strategies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023;9(10):538-568.
53. Anichukwueze CC, Osuji VC, Oguntegbe EE. Designing ethics and compliance training frameworks to drive measurable cultural and behavioral change. International Journal of Multidisciplinary Research and Growth Evaluation. 2020;1(3):205-220.
54. Anichukwueze CC, Osuji VC, Oguntegbe EE. Blockchain-based architectures for tamper-proof regulatory recordkeeping and real-time audit readiness. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(6):485-504.
55. Annan AO. Data privacy governance models for cross-border digital platforms. International Journal of Multidisciplinary Research and Growth Evaluation. 2022;3(6):949-964.
56. Annan AO. Cybersecurity compliance as a source of competitive advantage in technology markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2025;11(5):456-487.
57. Anyanwu KCE. Developing a maturity model for standardizing IT support operations across geographically distributed multi-office organizations. Iconic Research and Engineering Journals. 2019;3(5):580-598.
58. Anyanwu KCE. Bridging enterprise IT operations and digital entrepreneurship: A systematic review of skill transfer mechanisms and pathways. World Journal of Entrepreneurial Development Studies. 2022;7(1):114-134. doi:10.56201/wjeds.v7.no1.2022.pg114.134
59. Apache Software Foundation. Apache Kafka 4.0.0 release announcement. 2025. Available from: https://kafka.apache.org/blog/2025/03/18/apache-kafka-4.0.0-release-announcement/
60. Apache Software Foundation. Apache Kafka 4.1.0 release announcement. 2025. Available from: https://kafka.apache.org/blog/2025/09/04/apache-kafka-4.1.0-release-announcement/
61. Asibor E, Isong DE. Risk-based process engineering framework for strengthening reliability across complex natural gas infrastructure systems. Iconic Research and Engineering Journals. 2019;3(2):1020-1060. doi:10.64388/IREV3I2-1723153
62. Asiedu W, Quainoo R, Asiedu A. A conceptual framework for characterizing fundamental energy, reliability, and latency trade-offs in green communication paradigms for next-generation IoT. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2447-2453. doi:10.62225/2583049X.2025.5.6.6479
63. Atakpa MI. A review of predictive analytics models for anti-money laundering detection in commercial banking systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021;7(2):778-804. doi:10.32628/CSEIT2064813
64. Atakpa MI, Abetoh NF. A systematic review of machine learning advances in financial fraud detection for banking systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022;8(2):771-801. doi:10.32628/CSEIT23906220
65. Atakpa MI, Abolaji TO. A privacy-preserving data architecture model for regulated industry analytics under GDPR and HIPAA compliance. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022;8(3):781-808. doi:10.32628/CSEIT22558
66. Atakpa MI, Fobellah AN. Anomaly detection in financial time-series data: A conceptual model for healthcare and banking applications. International Journal of Scientific Research in Computer Science,

Engineering and Information Technology. 2023;9(2):967-997. doi:10.32628/CSEIT2342441
67. AutoMQ. Apache Kafka 4.0: Features and changes. 2025. Available from: https://www.automq.com/blog/apache-kafka-40-features-amp-changes
68. Badmus O, Dosunmu AA, Anunagba CO. A governance framework for AI-assisted CRM workflows: Agentforce deployment, risk management, and organizational readiness in enterprise Salesforce environments. International Journal of Scientific Research in Humanities and Social Sciences. 2025;2(1):59-80.
69. Badmus O, Dosunmu AA, Ozowara DE. A systematic review of CI/CD pipeline strategies in Salesforce DevOps: Tools, practices, and deployment outcomes. Iconic Research and Engineering Journals. 2018;2(6).
70. Badmus O, Dosunmu AA, Ozowara DE. A conceptual model for ETL design and data integration in Salesforce-centric enterprise architectures. Iconic Research and Engineering Journals. 2019;3(5).
71. Badmus O, Dosunmu AA, Ozowara DE. A governance framework for Salesforce platform management in regulated healthcare environments. Iconic Research and Engineering Journals. 2019;3(6).
72. Badmus O, Dosunmu AA, Ozowara DE, Anunagba CO. A comparative framework for Salesforce DevOps tooling: Evaluating Copado, Flosum, and Salesforce DX across enterprise deployment contexts. International Journal of Multidisciplinary Research and Growth Evaluation. 2020;1(5):1021-1031. doi:10.54660/.IJMRGE.2020.1.5.1021-1031
73. Badmus O, Jooda D, Ozowara DE, Anunagba CO. A systematic review of MuleSoft ESB integration patterns in multi-cloud Salesforce architectures. Gyanshauryam, International Scientific Refereed Research Journal. 2022;5(3):462-481.
74. Bello AA, Oduro DA, Manu EO, Bello AD, Leo AO, Ukatu CE, et al. Enhancing Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance using blockchain: A business analysis approach. Iconic Research and Engineering Journals. 2025;8(9):297-305.
75. Bello AD, Elebe O, Hammed NI, Okoruwa PO, Fadayomi O, Omoegun GO. An advanced regulatory technology framework for improving financial transparency and fraud reporting accuracy. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6).
76. Bello AD, Elebe O, Hammed NI, Omoegun GO, Fadayomi O. A cybersecurity risk management and regulatory compliance framework for financial institutions. Iconic Research and Engineering Journals; 2024. Available from: https://www.irejournals.com/paper-details/1713553
77. Bello AD, Oguntola OB, Ajibade AT, Akindolani A, Ayoola O, Bello AM. AI-driven fraud detection in UK digital payment systems: Challenges and solutions. Iconic Research and Engineering Journals. 2025;9(1):1329-1343.
78. Bello A, Akomolafe O, Agu MU. A conceptual framework for data-driven procurement risk management in multinational enterprises. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(6):2307-2316. doi:10.62225/2583049X.2023.3.6.5363
79. Beyer B, Jones C, Petoff J, Murphy NR, editors. Site reliability engineering: How Google runs production systems. O'Reilly Media; 2016.
80. Bindplane. KubeCon Europe 2025: OpenTelemetry recap from London. 2025. Available from: https://bindplane.com/blog/kubecon-europe-2025-opentelemetry-recap-from-london
81. Bola-Sadipe D, Aliliele C, Eboh EE. Conceptual model for strategic accounting systems strengthening financial transparency and regulatory compliance. IRE Journals. 2019;3(6):535-564. doi:10.64388/IREV3I6-1715327
82. Bola-Sadipe D, Eboh EE, Odihi F. Advances in data-driven tax compliance and financial reporting systems in banking institutions. Shodhshauryam, International Scientific Refereed Research Journal. 2022;5(1):366-403. doi:10.32628/SHISRRJ247137
83. Borah, S., Aliliele, K. C., Rakshit, S., & Vajjhala, N. R. (2022). Applications of artificial intelligence in software testing. In P. K. Mallick et al. (Eds.), Cognitive informatics and soft computing (Lecture Notes in Networks and Systems, Vol. 375, pp. 727-736). Springer. https://doi.org/10.1007/978-981-16-8763-1_60
84. Burke A, Price T. Navigating the DORA ICT incident reporting obligations. LexBlog; 2025. Available from: https://www.lexblog.com/?p=3096288
85. Central Bank of Ireland. Reporting major ICT-related incidents and significant cyber threats under DORA. 2025. Available from: https://centralbank.ie/regulation/digital-operational-resilience-act-dora/reporting-major-ict-related-incidents-and-significant-cyber-threats
86. Dada T, Isiekwu CP, Oluwo K. Advances in multinational cash flow consolidation and FX risk control using tiered treasury architecture. Iconic Research and Engineering Journals. 2021;4(11):601-620. doi:10.64388/IREV4I11-1714351
87. Datadog. Datadog LLM Observability natively supports OpenTelemetry GenAI semantic conventions. 2025. Available from: https://datadoghq.com/blog/llm-otel-semantic-convention/
88. Datadog. Datadog launches Bits AI SRE agent to resolve incidents faster [Press release]. 2025. Available from: https://investors.datadoghq.com/news-releases/news-release-details/datadog-launches-bits-ai-sre-agent-resolve-incidents-faster
89. Dosunmu AA, Ogundele PO. Security audit and enterprise risk assessment frameworks for resilient information systems. Iconic Research and Engineering Journals. 2019;3(5):434-447. doi:10.64388/IREV3I5-1713225
90. Dosunmu AA, Ogundele PO. Incident response and digital forensics strategies for rapid cyber attack containment. Gyanshauryam, International Scientific Refereed Research Journal. 2021;4(4):239-258.
91. Dosunmu AA, Ogundele PO. Threat intelligence integration frameworks supporting proactive enterprise cybersecurity decision making. Gyanshauryam, International Scientific Refereed Research Journal. 2022;5(3):397-416.
92. Dosunmu AA, Ogundele PO. Cyber threat actor analysis models for strategic enterprise security planning. Shodhshauryam, International Scientific Refereed Research Journal. 2023;6(5):513-531.

93. Dosunmu AA, Ogundele PO. Breach and attack simulation frameworks for continuous validation of enterprise security controls. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024;10(3):1100-1119.
94. Dosunmu AA, Ogundele PO. Cyber risk quantification models for prioritizing enterprise security investment decisions. International Journal of Multidisciplinary Research and Growth Evaluation. 2024;5(6):1777-1785. doi:10.54660/.IJMRGE.2024.5.6.1777-1785
95. Dosunmu AA, Ogundele PO. Enterprise scale continuous security validation models for regulated digital infrastructures. International Journal of Scientific Research in Humanities and Social Sciences. 2024;1(2):929-945.
96. Dosunmu AA, Ogundele PO. Threat informed defence engineering models for measuring security control effectiveness at scale. International Journal of Advanced Multidisciplinary Research and Studies. 2024;4(6):2847-2858.
97. Dosunmu AA, Ogundele PO. Cyber defense performance measurement frameworks for executive and board level governance. Computer Science and IT Research Journal. 2025;6(11):895-913. doi:10.51594/csitrj.v6i11.2164
98. Dosunmu AA, Ogundele PO. Security orchestration and automation models for accelerating incident detection and response. Computer Science and IT Research Journal. 2025;6(11):878-894. doi:10.51594/csitrj.v6i11.2163
99. Dynatrace. OpenTelemetry trends: Catching up with OpenTelemetry in 2025. 2025. Available from: https://www.dynatrace.com/news/blog/opentelemetry-trends-2025/
100. Eboh EE, Aliliele C. Portfolio risk optimization models for venture capital investment strategy and fraud exposure analysis. Iconic Research and Engineering Journals. 2023;7(4):759-792. doi:10.64388/IREV7I4-1715305
101. Eboh EE, Aliliele C. AI-driven data analytics framework for risk assessment and detection of venture capital and private equity investment fraud in U.S. capital markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024;10(6):2624-2665. doi:10.32628/CSEIT2410787
102. Eboh EE, Aliliele C. Advanced financial due diligence models for preventing venture capital investment fraud and strengthening investor protection. Shodhshauryam, International Scientific Refereed Research Journal. 2025;8(5):153-197. doi:10.32628/SHISRRJ258526
103. Eboh EE, Aliliele C. Predictive analytics systems for investment risk monitoring in SME FinTech companies and cross-border capital markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2025;11(2):3969-4010. doi:10.32628/CSEIT25113398
104. Eboh EE, Aliliele C, Odihi F. Advances in financial governance and accountability systems in small and medium enterprises. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2223-2245. doi:10.62225/2583049X.2025.5.6.6013
105. Edivri J, Oteri O. Predictive capacity planning and resource utilization forecasting models for multi-program and multi-stakeholder IT portfolios. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022;8(4):826-845.
106. Edivri J, Oteri O. A conceptual KPI-driven decision and optimization framework for IT service delivery, portfolio performance, and adoption. Gyanshauryam, International Scientific Refereed Research Journal. 2024;7(1):167-187. doi:10.32628/GISRRJ246643
107. Ekechi NV, Anunagba CO, Ozowara DE. Advances in financial forensics techniques for detecting cyber-enabled fraud in telemedicine services. Shodhshauryam, International Scientific Refereed Research Journal. 2022;5(1):428-450.
108. Elebe O, Anunagba CO. Responsible artificial intelligence in IT auditing through evidence validation, human oversight, and regulatory compliance. International Journal of Technology, Health and Sustainability. 2025;1(2):310-328.
109. Elebe O, Hammed NI, Omoegun GO, Fadayomi O, Bello AD. An advanced machine learning model for detecting synthetic identity fraud in e-commerce platforms [Preprint]. ResearchGate; 2023.
110. Ezeako R, Okoli IE, Uzondu CS, Ibeh AV. Relationship banking performance: A conceptual framework for portfolio growth and profitability acceleration. International Journal of Engineering Technology Research & Management. 2019;3(11):132-151.
111. Fadayomi O, Abolaji TO, Edivri J, Ogbole JI, Okoruwa PO, Akeju B. Risk-based cybersecurity assurance and data availability: Limitations, advances and future research opportunities. Iconic Research and Engineering Journals. 2019;2(12):602-617. doi:10.64388/IREV2I12-1713779
112. Fadayomi O, Bello AD, Elebe O, Hammed NI, Omoegun GO. An adaptive fraud risk scoring model for real-time transaction monitoring at scale. IIARD International Journal of Banking and Finance Research. 2024;10(10):212-230.
113. Fadero S, Jooda D, Oyesiji SO, Nwakamma S. IT services decoupling after mergers, acquisitions, and ownership transitions: A framework for secure infrastructure separation. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2471-2485.
114. Fadero S, Nwakamma S, Jooda D, Oyesiji SO. Cyber risk management maturity in Nigeria's insurance sector: An assessment against the NAICOM and NDPR regulatory landscape. Iconic Research and Engineering Journals. 2021;5(2):401-420. doi:10.64388/IREV5I2-1722621
115. Financial Conduct Authority. Operational resilience: Insights and observations for firms. [date unknown]. Available from: https://www.fca.org.uk/firms/operational-resilience/insights-observations
116. Fobellah AN. Cognitive biases in financial decision-making: Implications for audit and risk management in large corporations: A conceptual review. International Journal of Science and Research Archive. 2025;16(2):17-22. doi:10.30574/ijsra.2025.16.2.2273
117. Fobellah AN. Navigating digital transformation: Auditing artificial intelligence-powered financial systems: A conceptual review. International Journal of

Science and Research Archive. 2025;16(2):23-28. doi:10.30574/ijsra.2025.16.2.2274
118. Folderit. DORA compliance: What changed on 17 January 2025. 2025. Available from: https://www.folderit.com/?p=59558
119. Gideon EN, Adaramola TS, Fadero S. Reliability engineering and failure analysis in complex engineering systems. Iconic Research and Engineering Journals. 2019;2(11):703-727. doi:10.64388/IREV2I11-1722490
120. Grafana Labs. OpenTelemetry and Grafana Labs: What's new and what's next in 2025. 2025. Available from: https://grafana.com/blog/2025/01/07/opentelemetry-and-grafana-labs-whats-new-and-whats-next-in-2025
121. Grafana Labs. Introducing OpenTelemetry eBPF Instrumentation: Why we donated Grafana Beyla to OpenTelemetry. 2025. Available from: https://grafana.com/blog/2025/05/07/opentelemetry-ebpf-instrumentation-beyla-donation/
122. Grafana Labs. Database observability: How OpenTelemetry semantic conventions improve consistency across signals. 2025. Available from: https://grafana.com/blog/2025/06/06/database-observability-how-opentelemetry-semantic-conventions-improve-consistency-across-signals
123. Idika CN, Salami EO, Ijiga OM, Enyejo LA. Deep learning driven malware classification for cloud-native microservices in edge computing architectures. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021;7(4).
124. Ilodigwe L, Adesemoye AC. The data backbone of health system transformation: A governance and architecture framework for interoperability, data quality, and advanced analytics at national scale. International Journal of Health and Pharmaceutical Research. 2021;6(2):52-76. doi:10.56201/ijhpr.vol.6.no2.2021.pg52.76
125. Isiekwu CP, Oluwo K, Dada T. A post-pandemic strategic collaboration model for banks and capital markets: Addressing resilience, recovery, and growth challenges. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2104-2116.
126. Jimoh HO, Abolle-Okoyeagu CJ, Ahmed MO, Lawal NO. Advancing security in IoT-driven critical infrastructure: A focus on smart transportation system. American Journal of Engineering Research. 2023;12(12):33-46.
127. Jimoh HO, Ahmed MO, Fagbade MO. The role of frameworks in cybersecurity governance. Journal of Behavioural Informatics, Digital Humanities and Development Research. 2023;9(4):7-16. doi:10.22624/AIMS/BHI/V9N4P2
128. Komi NM, Adamolekun A. Interpretable machine learning for early failure prediction in distributed renewable energy assets. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(6):1015-1038. doi:10.54660/.IJMRGE.2021.2.6.1015-1038
129. Ladapo OO, Dosunmu AA, Jooda D, Abolaji TO. Lessons learned from offline assessment of security-critical systems: The case of Microsoft Active Directory. Iconic Research and Engineering Journals. 2018;2(6):277-299. doi:10.64388/IREV2I6-1717205
130. Ladapo OO, Dosunmu AA, Jooda D, Abolaji TO. Integrated network and security operation center: A systematic analysis. International Journal of Multidisciplinary Futuristic Development. 2024;5(1):65-80. doi:10.54660/IJMFD.2024.5.1.65-80
131. Ladapo OO, Dosunmu AA, Jooda D, Abolaji TO. Migration of applications and information systems to cloud computing infrastructure: Lessons from a South African retail bank. International Journal of Multidisciplinary Research and Growth Evaluation. 2025;6(6):1361-1375. doi:10.54660/.IJMRGE.2025.6.6.1361-1375
132. Ladapo OO, Jooda D, Dosunmu AA, Abolaji TO. Implementation of Active Directory for efficient management of enterprise networks. Iconic Research and Engineering Journals. 2019;3(4):608-627. doi:10.64388/IREV3I4-1717206
133. Ladapo OO, Jooda D, Dosunmu AA, Abolaji TO. Navigating digital transformation: Best practices for cloud migration strategies in the enterprise. Journal of Frontiers in Multidisciplinary Research. 2022;3(1):643-655. doi:10.54660/.JFMR.2022.3.1.643-655
134. Ladapo OO, Jooda D, Dosunmu AA, Abolaji TO. Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(6):2890-2904. doi:10.62225/2583049X.2023.3.6.6206
135. Lawal OA, Oduleye TE. A conceptual model for financial analytics driven enterprise value creation in technology firms. Iconic Research and Engineering Journals. 2018;2(2).
136. Lawal OA, Oduleye TE. A review and conceptual framework for tax governance and cross-border compliance analytics. Iconic Research and Engineering Journals. 2018;2(5).
137. Lawal OA, Oduleye TE. Conceptualizing data driven executive decision systems for strategic financial planning. Iconic Research and Engineering Journals. 2019;3(3).
138. Lawal OA, Oduleye TE. A conceptual decision model for capital allocation using financial analytics. Gyanshauryam, International Scientific Refereed Research Journal. 2021;4(2):269-295.
139. Lawal OA, Oduleye TE. Aligning financial planning analytics with corporate strategy: A conceptual integration model. Shodhshauryam, International Scientific Refereed Research Journal. 2021;4(3):319-346.
140. Lawal OA, Oduleye TE. Behavioral financial analytics: A conceptual model for explaining enterprise performance. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(6):2590-2604.
141. Mayo W, Ogbole JI, Okoruwa PO, Babatope OM. Designing an AI-predictive maintenance model for e-commerce systems using machine learning and cloud analytics. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021;7(5):416-440. doi:10.32628/IJSRCSEIT
142. Mbonu IS, Aliliele C, Iwuanyanwu U, Oluoha OM. A conceptual framework for legal and ethical risk

modeling in enterprise data protection governance systems. Iconic Research and Engineering Journals. 2018;2(2):207-226. doi:10.64388/IREV2I2-1714911
143. Mbonu IS, Aliliele C, Iwuanyanwu U, Uzoka E. A review of identity and access management integration strategies in hybrid and multi cloud environments. International Journal of Multidisciplinary Research and Growth Evaluation. 2020;1(5):795-810. doi:10.54660/.IJMRGE.2020.1.5.795-810
144. Mbonu IS, Aliliele C, Iwuanyanwu U, Uzoka E. A conceptual framework for risk based business intelligence architecture in financial technology platforms. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(6):731-746. doi:10.54660/.IJMRGE.2021.2.6.731-746
145. Mbonu IS, Aliliele C, Iwuanyanwu U, Uzoka E. Advances in artificial intelligence techniques for secure software testing and automated regression control mechanisms. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021;7(5):468-496. doi:10.32628/CSEIT217565
146. Mbonu IS, Aliliele C, Iwuanyanwu U, Uzoka E. A conceptual framework for AI enabled IT general controls and SOX audit automation processes. Gyanshauryam, International Scientific Refereed Research Journal. 2022;5(5):384-414. doi:10.32628/GISRRJ2256239
147. Mbonu IS, Aliliele C, Uzoka E, Oluoha OM. A review of comparative data protection regulations and secure cloud implementation strategies across jurisdictions. Iconic Research and Engineering Journals. 2019;2(9):482-501. doi:10.64388/IREV2I9-1714912
148. Mbonu IS, Iwuanyanwu U, Aliliele C, Uzoka E. A conceptual framework for agile supply chain digital transformation with embedded IT risk and ISO compliance controls. Iconic Research and Engineering Journals. 2020;3(11):566-593. doi:10.64388/IREV3I11-1714916
149. Mbonu IS, Iwuanyanwu U, Aliliele C, Uzoka E. Advances in infrastructure as code governance for secure terraform based enterprise cloud deployments. International Journal of Multidisciplinary Research and Growth Evaluation. 2020;1(5):811-828. doi:10.54660/.IJMRGE.2020.1.5.811-828
150. Mbonu IS, Iwuanyanwu U, Aliliele C, Uzoka E. A review of VoIP forensic analytics models for financial fraud detection and regulatory compliance monitoring. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(6):711-730. doi:10.54660/.IJMRGE.2021.2.6.711-730
151. Mbonu IS, Iwuanyanwu U, Aliliele C, Uzoka E. A review of data protection impact assessment models in multi cloud financial infrastructure systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022;8(1):589-623. doi:10.32628/CSEIT25442
152. Mbonu IS, Iwuanyanwu U, Aliliele C, Uzoka E. Advances in cloud identity and access governance optimization in large scale AWS enterprise environments. Shodhshauryam, International Scientific Refereed Research Journal. 2022;5(3):403-438. doi:10.32628/SHISRRJ225490
153. Mbonu IS, Iwuanyanwu U, Uzoka E, Oluoha OM. Advances in enterprise log analytics and automated incident response architectures using Python and SIEM platforms. Iconic Research and Engineering Journals. 2019;3(2):1000-1019. doi:10.64388/IREV3I2-1714915
154. Medon JJ, Oduleye TE. A comprehensive financial reporting model for strengthening compliance and organizational accountability systems. International Journal of Multidisciplinary Research and Growth Evaluation. 2022;3(6):768-777.
155. Medon JJ, Oduleye TE. An integrated predictive analytics model for enhancing strategic financial forecasting and decision accuracy. Gyanshauryam, International Scientific Refereed Research Journal. 2024;7(3):258-279. doi:10.32628/GISRRJ247322
156. Mensah KO, Pedro O, Kinyanjui A, Okoli I, Agboada P. A review of capital adequacy frameworks and risk weighted asset optimization in modern banking systems. Iconic Research and Engineering Journals. 2019;3(6):731-768. doi:10.64388/IREV3I6-1723267
157. Nwakamma S, Ojukwu J, Oyesiji SO. Securing agentic AI enterprise workflows against prompt injection, tool poisoning, memory manipulation, and excessive agency threats. World Journal of Innovation and Modern Technology. 2024;8(6):217-248. doi:10.56201/wjimt.v8.no6.2024.pg217.248
158. Observe, Inc. Observe introduces AI SRE and o11y.ai agents, accelerating developer productivity while cutting enterprise observability costs [Press release]. 2025. Available from: https://www.observeinc.com/news-pr/observe-introduces-ai-sre-and-o11y-ai-agents-accelerating-developer-productivity-while-cutting-enterprise-observability-costs
159. Odejobi OD, Hammed NI, Ahmed KS. Approximation complexity model for cloud-based database optimization problems. IRE Journals. 2019;2(9):1-10.
160. Odejobi OD, Okonkwo CS, Ahiaeke Patrick MC, Okeke OT, Mayo W. AI-augmented secure software engineering: Leveraging deep learning for autonomous threat detection and mitigation. International Journal of Engineering and Modern Technology. 2025;11(12):101-121. doi:10.56201/ijemt.vol.11.no12.2025.pg101.121
161. Oduleye TE, Medon JJ. A data-driven cost management model for improving strategic financial planning and performance evaluation. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(6):524-537.
162. Oduleye TE, Medon JJ. A quantitative model for measuring the strategic impact of financial analysis on enterprise growth. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(1):1663-1672. doi:10.62225/2583049X.2023.3.1.5334
163. Ogbole JI, Okoruwa PO, Babatope OM, Oyewole T. Developing an integrated data visualization model for continuous business performance monitoring and optimization. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021;7(5):441-467. doi:10.32628/IJSRCSEIT
164. Ogbole JI, Okoruwa PO, Fadayomi O, Abolaji TO, Edivri J, Akeju B. Conceptual model for identity-centric zero trust architecture in enterprise security governance. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021;7(5):393-415. doi:10.32628/IJSRCSEIT217562

165. Ogbole JI, Okoruwa PO, Fadayomi O, Akeju B, Edivri J, Abolaji TO. Security analytics and digital forensics for enterprise risk management, advances and practical implications. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2017-2028.
166. Ogundairo KM, Ayivi-Donkor SS. Telemetry-driven value realization: Infusing economic evaluation algorithms directly into enterprise data pipelines. International Journal of Economics and Financial Management. 2023;8(8):195-232. doi:10.56201/ijefm.v8.no8.2023.pg195.232
167. Ojukwu J, Oyesiji SO, Nwakamma S. Cyber-physical ransomware defense in operational technology using physics-informed detection, digital twins, network telemetry, and resilient recovery. International Journal of Computer Science and Mathematical Theory. 2023;9(5):193-228. doi:10.56201/ijcsmt.v9.no5.2023.pg193.228
168. Ojukwu J, Oyesiji SO, Nwakamma S. WebAssembly component model and WASI for portable cloud-to-edge software: Language interoperability, security, performance, and container comparisons. International Journal of Computer Science and Mathematical Theory. 2025;11(12):232-263. doi:10.56201/ijcsmt.vol.11.no12.2025.pg232.263
169. Okafor CM, Farounbi BO, Adesanya OS, Akinola AS. Controls for cross-border payments operations: Correspondent banking risk reduction via end-to-end monitoring. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024;10(4):1050-1071.
170. Okafor CM, Osuji VC, Dako OF. Fintech-enabled transformation of transaction banking and digital lending as a catalyst for SME growth and financial inclusion. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(6):485-504.
171. Okafor CM, Osuji VC, Dako OF. Harmonizing risk governance, technology infrastructure, and compliance frameworks for future-ready banking systems. International Journal of Scientific Research in Humanities and Social Sciences. 2024;1(1):316-337.
172. Okoli I, Agboada P, Kinyanjui A, Akintobi A, Pedro O. Enterprise CRM technology adoption and revenue growth analytics in financial services firms. International Journal of Science, Technology and Society. 2025;9(1):31-60.
173. Okoli I, Kinyanjui A, Mensah KO, Agboada P, Pedro O. Data-driven auditing in payroll and receivables: Predictive models for enhancing accuracy in financial statement validation. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022;8(5):851-889. doi:10.32628/CSEIT23902204
174. Okoruwa PO, Fadayomi O, Abolaji TO, Edivri J, Ogbole JI, Akeju B. Enterprise cybersecurity trends and threat evolution, advances and emerging research directions. Global Multidisciplinary Perspectives Journal. 2024;1(6):194-204. doi:10.54660/GMPJ.2024.1.6.194-204
175. Okoruwa PO, Fadayomi O, Akeju B, Edivri J, Ogbole JI, Abolaji TO. Conceptual model for privacy-centric security engineering in digital and cloud computing systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2020;7(5):371-389.
176. Okwesa IJ, Ashore-Onisemo F, Oyesiji SO, Abdulmalik AU. Predictive risk analytics for early-warning systems in enterprise technology estates. Shodhshauryam, International Scientific Refereed Research Journal. 2024;7(6):327-386. doi:10.32628/SHISRRJ24797
177. Olagunju EO, Edivri J, Oteri O. A conceptual governance model for change, incident, and problem management in mission-critical enterprise IT environments. Gyanshauryam, International Scientific Refereed Research Journal. 2023;6(6):365-384.
178. Olagunju EO, Edivri J, Oteri O. Applied performance optimization frameworks for managing high-demand enterprise technology programs and system rollouts. International Journal of Advanced Multidisciplinary Research and Studies. 2024;4(6):3059-3070. doi:10.62225/2583049X.2024.4.6.5915
179. Olagunju EO, Oteri O, Edivri J. An operational reliability and service assurance framework for enterprise IT systems supporting large user populations. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2117-2128. doi:10.62225/2583049X.2025.5.6.5916
180. Olaogun BO, Adesuyi MO, Akomolafe O, Ndukwe VU, Sakyi JK. Regulatory compliance adaptation model for cross-border payment product redesign. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(1):1651-1662. doi:10.62225/2583049X.2023.3.1.5279
181. Olaogun BO, Adesuyi MO, Akomolafe O, Ndukwe VU, Sakyi JK. Macroeconomic impact model for blockchain-enabled payment adoption in emerging economies. International Journal of Multidisciplinary Research and Growth Evaluation. 2025;6(6):835-853. doi:10.54660/.IJMRGE.2025.6.6.835-853
182. Oluwo K, Bola-Sadipe D, Aliliele C. Conceptual framework for data analytics driven financial decision making in banking sector organizations. Shodhshauryam, International Scientific Refereed Research Journal. 2025;8(5):259-302. doi:10.32628/SHISRRJ258529
183. Ominyi M. Developing a conceptual framework for post-merger compliance integration in multi-jurisdictional banking transaction. IIARD International Journal of Banking and Finance Research. 2020;6(3):78-95. doi:10.56201/ijbfr.vol.6.no3.2020.pg78.95
184. Ominyi M. Toward a conceptual framework for embedding privacy by design in corporate restructuring and transaction structuring. Journal of Accounting and Financial Management. 2021;7(5):152-173. doi:10.56201/jafm.vol.7.no5.2021.p152.173
185. Ominyi M, Anichukwueze CC. A review of regulatory clearance frameworks for cross-border mergers and acquisitions in African financial markets. Journal of Accounting and Financial Management. 2020;6(4):73-99. doi:10.56201/jafm.vol.6.no4.2020.pg73.99
186. Ominyi M, Anichukwueze CC. A systematic review of anti-money laundering and anti-bribery compliance regimes across emerging and developed markets. International Journal of Economics and Financial Management. 2021;6(2):89-118. doi:10.56201/ijefm.v6.no2.2021.pg89.118

187. Ominyi M, Anichukwueze CC. A review of algorithmic accountability and model risk management approaches in financial services. Journal of Accounting and Financial Management. 2023;9(12):218-238. doi:10.56201/jafm.v9.no12.2023.pg218.238
188. Ominyi M, Anichukwueze CC. Conceptualizing responsible AI governance structures for automated decision systems in regulated industries. International Journal of Social Sciences and Management Research. 2024;10(11):403-430. doi:10.56201/ijssmr.v10.no11.2024.pg.403.430
189. Ominyi M, Anichukwueze CC, Uzougbo NS. Developing a conceptual framework for AI-assisted compliance monitoring and anomaly detection in high-volume transaction environments. World Journal of Innovation and Modern Technology. 2024;8(6):204-228. doi:10.56201/wjimt.v8.no6.2024.pg204.228
190. Ominyi M, Anichukwueze CC, Uzougbo NS. A systematic review of organizational readiness for the EU Artificial Intelligence Act in multinational enterprises. World Journal of Innovation and Modern Technology. 2024;8(6):185-203. doi:10.56201/wjimt.v8.no6.2024.pg185.203
191. Ominyi M, Anichukwueze CC, Uzougbo NS. A conceptual framework for multi-agent AI quality control in the review of regulated documents. International Journal of Social Sciences and Management Research. 2025;11(8):534-557. doi:10.56201/ijssmr.vol.11no8.2025.pg534.557
192. Onche VO, Ogbonna CS, Adegbite MP. Effectiveness of cybersecurity awareness training on insider-threat behavior among university administrators: An integrative academic review. International Journal of Computer Science and Mathematical Theory. 2024;10(2):117-144. doi:10.56201/ijcsmt.v10.no2.2024.pg117.144
193. Oshoba TO, Hammed NI, Odejobi OD. Secure identity and access management model for distributed and federated systems. IRE Journals. 2019;3(4):550-567.
194. Oshoba TO, Hammed NI, Odejobi OD. Blockchain-enabled compliance and audit trail model for cloud configuration management. Journal of Frontiers in Multidisciplinary Research. 2020;1(1):193-201.
195. Osuji VC, Okafor CM, Dako OF. Engineering high-throughput digital collections platforms for multibillion-dollar payment ecosystems. Shodhshauryam, International Scientific Refereed Research Journal. 2021;4(4):315-335.
196. Oteri O, Chibwaye IP. Advances and conceptual models in enterprise level change management analytics for large scale organizational system transitions. Gyanshauryam, International Scientific Refereed Research Journal. 2025;8(5):177-211.
197. Oteri O, Olagunju EO, Edivri J. An operational reliability engineering framework for sustained high availability in 5G core networks serving millions. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2129-2147.
198. Oteri O, Olagunju EO, Edivri J. Conceptual models for cloud-based IT service management architecture and orchestration using ServiceNow platforms. Shodhshauryam, International Scientific Refereed Research Journal. 2025;8(6):185-203.
199. Oyesiji SO, Nwakamma S, Ojukwu J. A conceptual framework for context-aware data curation in fine-tuning pipelines. International Journal of Engineering and Modern Technology. 2024;10(11):197-228. doi:10.56201/ijemt.v10.no11.2024.pg197.228
200. Ozowara DE, Adebayo A, Anunagba CO. A systematic review of cybersecurity investments and their impact on healthcare financial performance. Shodhshauryam, International Scientific Refereed Research Journal. 2022;5(1):404-427.
201. Ozowara DE, Adebayo A, Anunagba CO. Advanced conceptual model for strengthening audit quality using data analytics across financial institutions. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2246-2268. doi:10.62225/2583049X.2025.5.6.6050
202. Ozowara DE, Anunagba CO, Adepoju PA. A review of ransomware economics and financial resilience strategies in hospital networks. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2284-2298. doi:10.62225/2583049X.2025.5.6.6052
203. Payment Expert. AWS outage: What we know so far. 2025. Available from: https://paymentexpert.com/2025/10/20/live-aws-outage-what-we-know-so-far/
204. Peteranaba SF, Osinem HE, Eribenne F, Soyege OS. Health information governance and regulatory compliance: Comparative frameworks for data verification, risk screening, and confidentiality in health and financial systems. International Journal of Science, Technology & Society. 2022;6(1):60-84.
205. Reddy H. Anatomy of a cloud collapse: A technical deep dive on the AWS outage of October 2025. DEV Community; 2025. Available from: https://dev.to/harshith_reddy_dev/anatomy-of-a-cloud-collapse-a-technical-deep-dive-on-the-aws-outage-of-october-2025-2mj4
206. Robinson D. Major AWS outage across US-East region breaks half the internet. The Register; 2025. Available from: https://www.theregister.com/2025/10/20/amazon_aws_outage/
207. Rukh S, Seyi-Lande OB, Oziri ST. An integrated framework for AI and predictive analytics in supply chain management. International Journal of Scientific Research in Humanities and Social Sciences. 2024;1(1):451-491.
208. Shittu H, Shittu MA. AI powered digital twins for predictive maintenance and operational optimization of renewable energy systems. International Journal of Science, Architecture, Technology and Environment. 2024;1:151-163. doi:10.63680/ijsate0324085.011
209. Shittu H, Olagunju F, Shittu MA. Cyber physical resilience in digital substations: IoT enabled adaptive protection for secure DER integration. International Journal of Science, Architecture, Technology and Environment. 2024;1(3):81-99. doi:10.63680/ijsate032532.08
210. Shittu MA, Adeniji IO, Shittu H, Opara IS. Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems. Iconic Research and Engineering Journals. 2022;6(3):359-379. doi:10.64388/IREV6I3-1714041

211. Shittu MA, Shittu HA, Adeleke OJ, Adedokun OJ. Digital twin modeling for real time monitoring and fault detection in smart substations. International Journal of Industrial Engineering Research and Development. 2023;14(2):25-44. doi:10.34218/IJIERD_14_02_003
212. Sidley Austin LLP. (2025, January 7). UK operational resilience rules: Are you ready for 31 March 2025? https://www.sidley.com/en/insights/newsupdates/2025/01/uk-operational-resilience-rules-are-you-ready-for-31-march-2025
213. Tonoyan A, Dada O, Ayivi-Donkor SS. Conceptual model for predictive cost optimization: Machine learning applications in business transformation analysis. International Journal of Economics and Business Management. 2022;8(6):68-102. doi:10.56201/ijebm.v8.no6.2022.pg68.102
214. Tonoyan A, Dada O, Ayivi-Donkor SS. Advances in supply chain resilience: Predictive models for vendor risk assessment and procurement cost optimization. International Journal of Social Sciences and Management Research. 2024;10(11):525-551. doi:10.56201/ijssmr.v10.no11.2024.pg.525.551
215. Tonoyan A, Dada O, Ayivi-Donkor SS. Real-time KPI tracking systems: A review of automated performance monitoring and data-driven decision making. World Journal of Innovation and Modern Technology. 2024;8(6):247-281. doi:10.56201/wjimt.v8.no6.2024.pg247.281
216. Uchechi N, Ominyi M, Anichukwueze CC, Jones BC. Real-time compliance pipelines: A review of automated risk monitoring and enterprise data governance. International Journal of Multidisciplinary Futuristic Development. 2022;3(2):66-94. doi:10.54660/IJMFD.2022.3.2.66-94
217. Uchechi N, Ominyi M, Anichukwueze CC, Jones BC. Advances in standardizing un-standardized compliance controls for high-volume non-traditional distribution networks. International Journal of Advanced Multidisciplinary Research and Studies. 2023;3(6). doi:10.62225/2583049X.2023.3.6.6838
218. Uchechi N, Ominyi M, Anichukwueze CC, Jones BC. Advances in automated governance: Mitigating operational and systemic risks in multi-country delivery networks. Gulf Journal of Advance Business Research. 2025;3(12):1626-1669. doi:10.51594/gjabr.v3i12.219
219. Ukadike CA. Advances in customer data platforms for emerging-market banking: Architecture, adoption, and customer trust. IIARD International Journal of Banking and Finance Research. 2022;8(4):67-87. doi:10.56201/ijbfr.v8.no4.2022.pg.67.87
220. Ukadike CA. Scaling B2B SaaS ventures: An integrated framework for multi-cloud optimization, distributed agile delivery, and investment readiness. World Journal of Finance and Investment Research. 2024;8(5):196-217. doi:10.56201/wjfir.v8.no5.2024.pg196.217
221. Ukadike CA, Ibeh AV. Advances in predictive customer journey analytics for cross-sell and upsell in financial services. Journal of Accounting and Financial Management. 2023;9(12):218-237. doi:10.56201/jafm.v9.no12.2023.pg218.237
222. Upreti M, Oteri O. Analytical model for optimizing cloud resource allocation through rightsizing and long-term usage forecasting. Gyanshauryam, International Scientific Refereed Research Journal. 2023;6(1):400-424.
223. Upreti M, Oteri O. Security design model for resilient network architectures in large scale cloud computing platforms. Shodhshauryam, International Scientific Refereed Research Journal. 2025;8(5):84-104.
224. USENIX. SREcon25 Europe/Middle East/Africa call for participation. 2025. Available from: https://www.usenix.org/node/306466
225. Walawalkar G, Adesuyi MO, Kalu A, Oduleye TE. Executive financial dashboards for real-time strategic oversight. International Journal of Advanced Multidisciplinary Research and Studies. 2025;5(6):2042-2054.
226. Walkers Global. Navigating DORA: Key compliance steps from 17 January 2025. 2025. Available from: https://www.walkersglobal.com/en/Insights/2025/01/Navigating-DORA-Key-compliance-steps-from-17-January-2025
227. Wikiri M. Improving first-contact resolution in enterprise technology support: A workforce competency and service-quality framework. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(6):1212-1225. doi:10.54660/.IJMRGE.2021.2.6.1212-1225

How to Cite This Article
Ibe PN, Okeke EC, Okwesa I, Ogundapo O, Soneye OM, Mensah KO, et al. Advances in service reliability engineering and observability for distributed financial data processing platforms. Int J Future Eng Innov. 2025;2(6):74-95. doi:10.54660/IJFEI.2025.2.6.74-95.

Creative Commons (CC) License
This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms