Self-Service Failure Recovery and Autonomous Operational Remediation in Multi-Tenant Financial Systems: A Conceptual Framework

Emmanuel Chukwuma Okeke[1], Ifeanyichukwu Okwesa[2], Uchechi Unamma[3*], Serif Oyindamola Oyesiji[4], Oluranti Ogundapo[5], Olabode Michael Soneye[6]
[1] Arcesium, New York, NY, USA
[2] Barclays [Location for Barclays to be confirmed]
[3] Peace House, Park City, Utah, USA
[4] Harrisburg University of Science and Technology,
Harrisburg, PA, USA ORCID: https://orcid.org/0009-0000-1203-8063
[5] Google, USA
[6] EQ Bank, Toronto, ON, Canada
* Corresponding author: Uchechi Unamma,
uchechiunamma@gmail.com

https://doi.org/DOI: 10.56201/rjpst.vol.8.no8.2025.pg142.181

Abstract
Multi-tenant financial platforms, including core banking as a service, payment processors, embedded finance providers and wealth management back offices, concentrate the operations of many regulated institutions onto shared infrastructure. When such platforms fail, the cost is measured not only in downtime but in misposted balances, duplicated payments, breached settlement windows and regulatory exposure for every tenant at once. Two operational paradigms have matured in parallel to address this: autonomous remediation, in which the platform detects and corrects faults without human intervention, and self-service recovery, in which tenants are given the tools to diagnose and resolve incidents affecting their own scope. Yet the literature treats these largely in isolation, and neither is well theorised for environments where financial integrity, tenant isolation and supervisory accountability are binding constraints. Using a conceptual research design grounded in an integrative synthesis of 252 sources, including 227 applied seed publications screened from a consolidated corpus of 1,056 peer works, this paper proposes SAFER-FS (Self-service and Autonomous Failure Engineering for Resilient Financial Systems), a seven-layer conceptual framework that integrates containment, tenant-aware observation, diagnosis, policy-governed autonomy, integrity-preserving execution, self-service recovery and evidentiary assurance into a single closed control loop. The framework introduces a graduated autonomy scale (A0 to A5), a risk-weighted remediation admission function, a set of financial integrity invariants that every remediation must preserve, and an explicit mapping to the operational resilience obligations that have taken effect, most notably the European Union Digital Operational Resilience Act and the United Kingdom operational resilience regime. The paper discusses the theoretical, practical and regulatory implications of the model, acknowledges its

limitations, and concludes with six testable propositions, an evaluation metric set and a future research agenda.

Keywords: *self-healing systems; autonomous remediation; self-service recovery; multi-tenancy; financial technology; operational resilience; DORA; AIOps; site reliability engineering*

1. Introduction

Financial services have moved decisively onto shared, cloud-hosted platforms. A single payments or ledger provider may now serve hundreds of banks, credit unions, brokerages and fintech firms, each a separate tenant with its own customers, configuration, risk appetite and regulator. This concentration delivers economies of scale, but it also concentrates failure. A schema migration that stalls, a third-party card network that times out, or a malformed batch file from one tenant can degrade service for all tenants simultaneously, and the consequences propagate into customer balances, liquidity positions and statutory reporting. Operational practice has responded along two lines. The first is **autonomous operational remediation**: platforms increasingly detect anomalies and execute corrective actions automatically, restarting unhealthy components, shedding load, failing over to secondary regions, or replaying failed messages. This lineage runs from the autonomic computing vision of self-managing systems (Kephart & Chess, 2003) through site reliability engineering (Beyer et al., 2016) to contemporary AIOps, which applies machine learning to incident detection, localisation and mitigation (Dang et al., 2019; Notaro et al., 2021). The second is **self-service failure recovery**: rather than routing every incident through the provider's support queue, platforms expose recovery capabilities directly to tenants, for example letting an operations analyst at a client bank requeue a failed payment batch, reverse a duplicate posting within defined limits, or rotate a compromised credential without waiting for provider staff. Both paradigms promise shorter recovery times and lower operating cost. Both, however, carry distinctive hazards in financial settings. An autonomous action that is safe in a stateless web service, such as retrying a request, can be catastrophic in a ledger if the original request actually succeeded, producing a double debit. A self-service capability that lets one tenant replay messages can, if poorly scoped, expose or corrupt another tenant's data. And in both cases, supervisors now expect firms to evidence who decided what, on what basis, and with what effect. The year 2025 marks an inflection point for this problem. The EU Digital Operational Resilience Act (Regulation (EU) 2022/2554, hereafter DORA) became applicable on 17 January 2025, imposing harmonised requirements on ICT risk management, incident management, resilience testing and oversight of critical ICT third-party providers. In the United Kingdom, the transitional period of the operational resilience framework set by the Prudential Regulation Authority and Financial Conduct Authority ended on 31 March 2025, by which date firms were required to remain within impact tolerances for their important business services. These regimes reframe recovery from an engineering concern into a supervisory obligation, and they do so precisely as autonomous tooling is becoming capable enough to act without humans in the loop. This paper addresses the resulting gap. Its research question is: *how should multi-tenant financial platforms combine autonomous remediation and tenant self-service recovery so that recovery is fast, financial integrity and tenant isolation are preserved, and accountability is demonstrable to supervisors?* The contribution is conceptual. The paper (i) characterises the failure and recovery problem specific to multi-tenant financial systems, (ii) proposes the SAFER-FS framework with its constituent layers, autonomy scale, admission function and integrity invariants, (iii) maps the framework to 2025 regulatory obligations, and (iv)

derives propositions and metrics for empirical testing. The remainder of the paper is organised as follows. Section 2 describes the research method. Section 3 presents the results and discussion, comprising the literature synthesis, the conceptual model, a discussion of the model, its theoretical, practical and regulatory implications, its limitations and a future research agenda. Section 4 concludes.

2. Research Method

This study adopts a conceptual research design. Conceptual papers contribute by integrating existing knowledge into new theoretical structures rather than by collecting primary data, and their rigour rests on transparent choices about which literatures are drawn upon and how they are combined (MacInnis, 2011; Jaakkola, 2020). Following Jaakkola's (2020) typology, the paper is primarily a *model* paper: it builds a framework that identifies constructs, specifies their relationships and derives testable propositions. It also borrows from design science, in that the framework is an artefact intended to guide the construction of real systems and should be judged by its utility as well as its coherence (Hevner et al., 2004).

The evidence base comprises two streams. The **foundational stream** consists of widely cited works in autonomic and self-adaptive computing, recovery-oriented computing, site reliability engineering, AIOps, multi-tenant architecture, transaction processing and human-automation interaction, together with the primary regulatory instruments and supervisory statements that define operational resilience obligations in 2025. These were identified through the author's knowledge of the field and backward citation tracing.

The **seed stream** was drawn from a consolidated, deduplicated reference list of 1,056 peer publications organised into 68 subject areas. Selection followed an integrative review logic (Torraco, 2005; Snyder, 2019) and proceeded in three steps:

- **Subject-area screening.** Subject areas were retained where they plausibly informed at least one framework concern: automation and AI operations, cloud and service management, incident response and security, continuous validation, identity and data protection, payments and banking operations, fraud analytics, auditing and controls, governance and regulation, and decision support. Areas such as agriculture, clinical care, livestock science and pedagogy were excluded.
- **Title and abstract screening.** Within retained areas, each entry was judged as *related* (directly addressing a framework concern in a financial or enterprise technology setting) or *semi-related* (addressing an analogous concern in an adjacent sector, such as health-sector cyber governance or critical infrastructure). Entries with neither connection were excluded.
- **Temporal criterion.** Because the paper is situated in 2025, only works published in or before 2025 were retained. Works dated later, including manuscripts in preparation, were excluded. This process yielded 227 seed publications, which together with the foundational and methodological sources give a reference base of 252 works.

Retained works were coded thematically against the concerns listed above, producing eleven themes. Each theme was then mapped to the framework layer or governance mechanism it informs. Model development was abductive and iterative: candidate constructs were proposed from the foundational literature, tested against the seed themes for coverage and consistency, and refined where the seed literature revealed a missing concern, such as autonomy budgets or symmetry of control. Two illustrative scenarios were used to probe the model's internal logic, and propositions were derived where the model implies a relationship that can be observed empirically. The

methodology is summarised as: literature identification, screening, thematic coding, layer mapping, abductive model construction, scenario probing and proposition derivation.

3. Results and Discussion

This section reports the results of the integrative review and model development and discusses their significance. It first presents the literature synthesis and the conceptual model, then discusses the model and sets out its implications, limitations and a future research agenda.

This section synthesises the two literature streams identified in Section 2: the foundational scholarship on autonomic computing, reliability engineering, multi-tenancy, transactional integrity and regulation, and the applied seed corpus on enterprise operations, security, payments and financial controls. It closes by distilling the gaps that motivate the conceptual model.

Kephart and Chess (2003) articulated the autonomic computing agenda around four self-properties: self-configuration, self-optimisation, self-healing and self-protection. Its operational core is the MAPE-K loop, in which a manager Monitors a managed element, Analyses symptoms, plans adaptations and Executes them, all informed by shared Knowledge. Subsequent surveys catalogued self-healing techniques and their limitations (Ghosh et al., 2007; Huebscher & McCann, 2008; Psaier & Dustdar, 2011), and the broader field of self-adaptive systems has since formalised feedback loops, uncertainty handling and assurance (Weyns, 2020). A recurring finding is that self-healing works best when the space of faults and safe responses is well characterised, and that assurance of autonomous behaviour, rather than its technical feasibility, is the binding constraint. Parallel work on recovery-oriented computing argued that fast, cheap recovery is often more valuable than fault avoidance. Crash-only software (Candea & Fox, 2003) and microreboots (Candea et al., 2004) demonstrated that components designed to be safely restarted at any time make automated recovery tractable. These ideas underpin modern container orchestration, but they assume that state is externalised and that restart is idempotent, assumptions that hold only partially for financial workloads. Site reliability engineering operationalised reliability through service level indicators and objectives, error budgets, blameless post-incident review and the elimination of repetitive manual work, termed toil (Beyer et al., 2016). Chaos engineering extended this by deliberately injecting faults in production to verify that recovery mechanisms work (Basiri et al., 2016). Stability patterns such as circuit breakers, bulkheads and timeouts became standard vocabulary (Nygard, 2018). AIOps research has since targeted the incident lifecycle with learned models for anomaly detection, root cause localisation and automated mitigation recommendation, while documenting persistent challenges around data quality, interpretability and trust in automated actions (Dang et al., 2019; Notaro et al., 2021). The rapid adoption of large language model agents for operations from 2023 onwards has sharpened these concerns, since such agents can propose and execute novel actions that are not drawn from a fixed runbook.

Multi-tenant software as a service shares application instances and data stores across customers to reduce cost, introducing concerns of performance isolation, configurability, data segregation and fault isolation (Bezemer & Zaidman, 2010; Krebs et al., 2012). Isolation models range from fully shared schemas to dedicated stacks per tenant, with cell-based architectures, in which tenants are partitioned into independent replicas of the full stack, emerging as a pragmatic compromise that bounds blast radius. The recovery literature for multi-tenant systems is comparatively thin, and almost none of it addresses the case where tenants are themselves regulated entities with their own recovery obligations.

Financial systems impose correctness requirements absent from many web services. Double-entry ledgers must balance; payments must be executed at most once and accounted exactly once; external settlement files must reconcile. Distributed transaction patterns such as sagas, in which a long-running operation is decomposed into steps each paired with a compensating action (Garcia-Molina & Salem, 1987), and idempotency keys that make retries safe (Helland, 2012), are the main tools for reconciling availability with integrity. Remediation that ignores these patterns converts an availability incident into an integrity incident, which is typically far more costly to resolve.

Supervisors have converged on operational resilience as an outcome to be evidenced rather than a set of controls to be listed. The Basel Committee on Banking Supervision (2021) principles call on banks to identify critical operations, set tolerances for disruption, and test their ability to remain within them, including when operations depend on third parties. DORA translates this into binding EU law with articles on ICT risk management (Art. 5 to 16, including response and recovery in Art. 11 and backup and restoration in Art. 12), incident management, classification and reporting (Art. 17 to 23), digital operational resilience testing (Art. 24 to 27) and ICT third-party risk (Art. 28 to 44). The UK regime (PRA, 2021) requires firms to map important business services, set impact tolerances and demonstrate by March 2025 that they can stay within them in severe but plausible scenarios. For multi-tenant platform providers, these obligations arrive twice: directly where the provider is itself regulated, and indirectly through contractual flow-down from tenants who must evidence control over their outsourced services.

The foundational literature reviewed above is complemented by a large and fast-growing body of applied research, much of it published between 2019 and 2025, on enterprise operations, cybersecurity, payments and financial controls. Although few of these studies address multi-tenant financial recovery directly, together they supply components, evidence and design lessons that SAFER-FS integrates. They are grouped here by the framework concern they inform.

Work on AI-driven security operations shows how detection and response can be automated end to end, from deep learning based autonomous threat mitigation in software systems (Odejobi et al., 2025) to continuously learning cyber-physical prevention in legacy SCADA (Amadi, 2025) and AI-based posture management that tracks NIST Cybersecurity Framework adherence in real time (Amadi et al., 2025a). Security orchestration and automation models report faster detection and response when playbooks are codified (Adegbite et al., 2024b; Dosunmu & Ogundele, 2025c), and the move from periodic audit to continuous control is argued to be as much an organisational readiness problem as a technical one (Adebayo, Amadi, et al., 2025). Human-in-the-loop research cautions that the benefits of automation depend on well-designed human oversight and evidence validation (Elebe & Anunagba, 2025; Ladapo, Dosunmu, et al., 2022; Ladapo, Jooda, et al., 2024), a point reinforced by work casting the business analyst as a broker of responsible automation (Alieme et al., 2025b). Studies of large language model governance highlight release gating through model-based judges (Nwakamma et al., 2024a), new attack surfaces in agentic workflows such as prompt injection and tool poisoning (Nwakamma et al., 2024b) and context-aware data curation for fine-tuning (Oyesiji et al., 2024); related work applies physics-informed detection and digital twins to ransomware defence (Ojukwu et al., 2023) while work on bias and spoofing countermeasures in biometric systems shows how adversarial inputs can mislead automated judgement (Adeniyi et al., 2025). These findings motivate the separation of proposal (Layer 3) from authorisation (Layer 4) in SAFER-FS.

Elastic capacity is the first line of autonomous remediation. Predictive scaling with machine learning (Ahmed et al., 2020), constraint-based network resource allocation (Ahmed et al., 2019),

energy-aware virtual machine placement (Ahmed & Odejobi, 2018b), rightsizing with long-horizon usage forecasting (Upreti & Oteri, 2023) and database optimisation complexity (Odejobi et al., 2019) all inform the capacity actions that SAFER-FS catalogues at A4. Multi-tenant performance under high concurrency has been evaluated empirically (Odejobi & Ahmed, 2018b), and integrated frameworks for scaling B2B SaaS across multiple clouds (Ukadike, 2024) and for secure enterprise messaging architectures (Ahmed & Odejobi, 2018a) address the shared-infrastructure economics that the framework inherits. Portable cloud-to-edge runtimes (Ojukwu et al., 2025) and malware classification for cloud-native microservices (Idika et al., 2021) extend the analysis to heterogeneous estates. Configuration drift is a recurrent incident cause, motivating continuous misconfiguration monitoring (Aliliele et al., 2023a), infrastructure-as-code governance (Mbonu et al., 2020b), resilient cloud network design (Upreti & Oteri, 2025) and AI-based predictive maintenance for e-commerce platforms (Mayo et al., 2021).

The IT service management literature documents both the benefits and the implementation challenges of structured service practice (Ladapo, Dosunmu, et al., 2023b), with platform studies describing orchestration of incident and change workflows (Ladapo, Jooda, et al., 2023a; Oteri et al., 2025). Integrated network and security operation centres (Ladapo, Dosunmu, et al., 2024) and change management analytics (Oteri & Chibwaye, 2025) bear directly on the handoff between automated and human response. Maturity models for standardising support across distributed offices (Anyanwu, 2019), balancing remote and on-site support (Anyanwu, 2020), KPI-driven service delivery optimisation (Edivri & Oteri, 2024) and first-contact resolution competency (Wikiri, 2021) ground the self-service plane empirically, since that plane is in effect a first-contact resolution channel operated by the tenant; skill transfer from IT operations to digital ventures has also been examined (Anyanwu, 2022). Governance models for change, incident and problem management in mission-critical estates (Olagunju et al., 2023), operational reliability and service assurance frameworks for large user populations (Olagunju et al., 2025), predictive early-warning analytics for technology estates (Okwesa et al., 2024), predictive capacity planning across multi-stakeholder portfolios (Edivri & Oteri, 2022; Olagunju et al., 2022) and performance optimisation for high-demand rollouts (Olagunju et al., 2024; Oteri & Edivri, 2024) together describe the reliability programme within which autonomous remediation sits. Studies of IT decoupling after mergers (Fadero et al., 2025) and of cloud migration (Ladapo et al., 2025; Ladapo, Jooda, et al., 2022) show that recovery capability is often weakest during transitions, which SAFER-FS addresses by lowering autonomy ceilings during change windows.

Automated log analytics coupled to SIEM platforms (Mbonu, Iwuanyanwu, et al., 2019) and rapid containment through incident response and digital forensics (Dosunmu & Ogundele, 2021; Ogbole et al., 2025) are the closest security analogues of automated remediation. Insider threat classification (Akeju et al., 2018), security audit and enterprise risk assessment (Dosunmu & Ogundele, 2019), intrusion detection and prevention (Dosunmu & Ogundele, 2020), threat intelligence integration (Dosunmu & Ogundele, 2022), threat actor analysis (Dosunmu & Ogundele, 2023), intrusion detection with feature-selected machine learning (Ajagbe et al., 2025), mitigation of NTP amplification DDoS attacks (Jimoh & Ahmed, 2024), directory service attack signatures and management (Ladapo et al., 2019; Ladapo, Dosunmu, et al., 2023a) and surveys of threat evolution (Okoruwa et al., 2024) inform the security-driven failure class in Table 1. Critical infrastructure research offers mature thinking on safety-constrained automation. Systematic reviews cover ICS and SCADA threat detection with SIEM and network detection tools (Adegbite et al., 2023), machine learning for industrial control threat detection (Adebayo, Adegbite, et al.,

2023), comparative deep learning for SCADA anomaly detection (Amadi et al., 2025b) and the cyber-physical attack surface of legacy SCADA (Amadi et al., 2025c). Adversarial machine learning threat modelling (Adebayo et al., 2022), NERC CIP compliance (Adegbite et al., 2020), IT and OT convergence architectures (Adegbite et al., 2022), zero trust for operational technology (Ahmed et al., 2021), vulnerability governance from exposure mapping to remediation (Adegbite et al., 2024a), cyber risk quantification (Adegbite et al., 2025), adaptive protection in digital substations (Shittu et al., 2024), blockchain-assisted SCADA data exchange (Shittu et al., 2022) and IoT security for smart transportation infrastructure (Jimoh, Abolle-Okoyeagu, et al., 2023) complete this body of work. Its central lesson, that automation in safety-critical systems must be bounded by physical invariants, transfers directly to the financial invariants of Layer 5.

Continuous validation is the testing counterpart of autonomous remediation. Breach and attack simulation (Dosunmu & Ogundele, 2024a), enterprise-scale continuous security validation (Dosunmu & Ogundele, 2024c), threat-informed measurement of control effectiveness (Dosunmu & Ogundele, 2024d), adversary simulation design (Dosunmu & Ogundele, 2025a), risk-based assurance and data availability (Fadayomi et al., 2019), board-level cyber defence performance measurement (Dosunmu & Ogundele, 2025b) and cyber risk quantification for investment prioritisation (Dosunmu & Ogundele, 2024b) parallel the chaos engineering tradition and support resilience testing obligations. AI-assisted software testing (Borah et al., 2022) and secure regression control (Mbonu et al., 2021b), CI/CD and version control governance (Badmus et al., 2018; Badmus et al., 2020; Badmus et al., 2022a) and platform governance in regulated environments (Badmus et al., 2019b) describe release controls that reduce change-induced failures. Data-driven lifecycle performance management for digital transformation (Adelanwa et al., 2023a), multi-site benchmarking methodologies (Anene et al., 2023) and simulation-based process optimisation (Tonoyan et al., 2022b) show how change programmes can be staged and measured so that continuity is preserved.

Tenant confinement depends on identity and data governance. Relevant work examines identity and access management in hybrid and multi-cloud environments (Mbonu et al., 2020), cloud identity governance at large scale (Mbonu et al., 2022b), federated identity models (Oshoba et al., 2019), identity-centric zero trust (Ogbole et al., 2021), privacy-centric security engineering (Okoruwa et al., 2020), privacy-driven access control policies (Ladapo, Jooda, et al., 2023b), offline assessment of directory services (Ladapo et al., 2018) and role-based security for sensitive CRM data (Badmus et al., 2024); attribute-based encryption for access control (Shittu & Nabil, 2023) illustrates cryptographic enforcement of scoped access. Data protection impact assessment in multi-cloud financial infrastructure (Mbonu et al., 2022a), cross-jurisdiction data protection and cloud implementation (Mbonu, Aliliele, et al., 2019), data sensitivity classification with regulatory traceability (Aliliele et al., 2024a), lakehouse governance for data loss prevention (Aliliele et al., 2025b), legal and ethical risk modelling in data protection (Mbonu et al., 2018) and privacy-preserving architectures for regulated analytics (Atakpa & Abolaji, 2022) inform the transparency constraints placed on the self-service plane.

Payment infrastructure research bears directly on the in-doubt transaction problem. Interoperability and standardisation models for distributed-ledger cross-border payments (Adesuyi, Akomolafe, et al., 2023; Akomolafe et al., 2025b), resilience and continuity of global payment infrastructure under geopolitical risk (Adesuyi et al., 2025b), scalable blockchain payment gateways (Akomolafe et al., 2024a), collaborative governance for payment data sharing (Akomolafe et al., 2025a), regulatory adaptation in payment product redesign (Olaogun et al.,

2023), AI risk scoring for trade payments (Adesuyi et al., 2024), remittance liquidity optimisation (Akomolafe et al., 2023), smart contract automation and dispute resolution for supplier payments (Akomolafe et al., 2022; Akomolafe et al., 2024b) and the macroeconomic effects of blockchain payments in emerging economies (Olaogun et al., 2025) all bear on how remediation interacts with external rails. On banking operations, end-to-end monitoring controls for correspondent banking (Okafor, Farounbi, et al., 2024), high-throughput digital collections platforms (Osuji et al., 2021), fintech transformation of transaction banking (Okafor et al., 2021), digital banking and financial inclusion in Sub-Saharan Africa (Agboada et al., 2022), customer data platforms in emerging-market banking (Ukadike, 2022), business continuity and disaster recovery lessons from COVID-19 (Fadero et al., 2020) and harmonised risk governance and technology infrastructure (Okafor, Osuji, et al., 2024) describe the settings in which platform tenants operate. Treasury architecture for cash and FX risk control (Dada et al., 2021a), post-pandemic resilience collaboration between banks and capital markets (Isiekwu et al., 2025), credit decisioning governance (Uzondu et al., 2020), relationship banking performance (Ezeako et al., 2019) and CRM adoption in financial services (Okoli et al., 2025) complete the picture of tenant-side business context.

Fraud analytics shares the detection problem with remediation, but against an adversary. Reviews of machine learning for banking fraud (Atakpa & Abetoh, 2022), AML predictive analytics (Atakpa, 2021), anomaly detection in financial time series (Atakpa & Fobellah, 2023), real-time adaptive fraud risk scoring (Fadayomi et al., 2024), AI fraud detection in UK digital payments (Bello, Oguntola, et al., 2025), synthetic identity detection (Elebe et al., 2023), cyber-enabled fraud forensics (Ekechi et al., 2022), investment risk monitoring in SME fintech (Eboh & Aliliele, 2025b), SME financial governance and accountability (Eboh et al., 2025), analyst decision support for financial crime investigation (Okoruwa et al., 2025), integrated cybersecurity and AML governance (Fadayomi et al., 2021), regulatory technology for fraud reporting (Bello, Elebe, et al., 2025), cybersecurity compliance frameworks for financial institutions (Bello et al., 2024), fraud ecosystems for international payment channels (Adesuyi et al., 2025a), predictive fraud detection in public systems (Adelanwa et al., 2023b), AI-assisted compliance monitoring in high-volume transactions (Ominyi et al., 2024a) and forensic analytics for fraud detection (Mbonu et al., 2021) supply models for distinguishing genuine faults from malicious activity, a distinction the diagnosis layer must make before selecting a remediation.

The assurance plane draws on continuous auditing research, including AI-assisted continuous auditing of technology risk (Aliliele et al., 2025a), automation of IT general controls and SOX audit (Mbonu et al., 2022), auditing AI-powered financial systems (Fobellah, 2025b), cross-border SOX frameworks (Agu et al., 2023a), technology-enabled internal audit quality (Akomolafe & Agu, 2018), risk-based internal control in banking and insurance (Akomolafe & Agu, 2019a), data-driven risk evaluation in emerging markets (Akomolafe & Agu, 2019b), integrated governance for financial resilience (Akomolafe & Agu, 2019c), risk-based auditing (Akomolafe et al., 2023a), compliance risk quantification (Akomolafe et al., 2023b), data-driven compliance analytics (Akomolafe et al., 2025), capital adequacy frameworks (Mensah et al., 2019), analytics-driven audit quality (Ozowara, Adebayo, et al., 2025), data-driven tax compliance in banking (Bola-Sadipe et al., 2022), predictive payroll and receivables audit (Okoli et al., 2022) data-driven procurement risk management (Bello et al., 2023), cognitive biases in audit and risk judgement (Fobellah, 2025a) and the compliance burdens that financial regulation imposes (Fobellah, 2025c). Blockchain-based tamper-proof regulatory recordkeeping (Anichukwueze et al., 2021), blockchain-assisted KYC and AML (Bello, Oduro, et al., 2025) and blockchain audit trails for

cloud configuration management (Oshoba et al., 2020) directly inform the design of the append-only remediation ledger.

Governance and regulatory research supplies the accountability layer. API governance and risk prioritisation in financial institutions (Aliliele et al., 2023b), risk-based business intelligence architecture for fintech platforms (Mbonu et al., 2021a), cybersecurity governance frameworks (Jimoh, Ahmed, et al., 2023), cyber risk maturity under national insurance and data protection regulation (Fadero et al., 2021) and IT risk embedded in digital transformation (Mbonu et al., 2020a) address governance of shared technical platforms. Algorithmic accountability and model risk management in financial services (Ominyi & Anichukwueze, 2023), responsible AI governance for automated decision systems (Ominyi & Anichukwueze, 2024), algorithmic accountability and trade secret protection (Annan, 2024), automated decision-making and anti-discrimination compliance (Annan, 2025a), readiness for the EU Artificial Intelligence Act (Ominyi et al., 2024b), multi-agent AI quality control for regulated documents (Ominyi et al., 2025a), legal privilege in enterprise LLM deployment (Ominyi et al., 2025c) and machine learning governance in insurance underwriting (Oluwo et al., 2024) bear on governing learned diagnostic components. Cross-border privacy governance (Annan, 2022), harmonisation of GDPR, NDPR and US privacy regimes (Ominyi & Anichukwueze, 2022a), cybersecurity compliance as competitive advantage (Annan, 2025b), post-merger compliance integration in multi-jurisdictional banking (Ominyi, 2020), AML and anti-bribery regimes (Ominyi & Anichukwueze, 2021), real-time compliance pipelines (Uchechi et al., 2022), automated governance in multi-country networks (Uchechi, Ominyi, Anichukwueze, et al., 2025), standardisation of compliance controls (Uchechi et al., 2023) and NLP detection of regulatory liabilities in contracts (Uchechi, Ominyi, Uzougbo, et al., 2025), standardised contract review workflows (Uchechi et al., 2021), cross-functional legal education as risk mitigation (Anichukwueze et al., 2022), privacy by design in corporate restructuring (Ominyi, 2021), regulatory clearance for cross-border financial mergers (Ominyi & Anichukwueze, 2020) and ethics and compliance training (Anichukwueze et al., 2020) support the contractual and supervisory mapping presented later in this section. Semi-related health-sector studies offer useful parallels on zero trust cost-effectiveness (Adebayo, Anunagba, et al., 2025), blockchain cross-border data exchange (Kumuyi et al., 2023), privacy-focused digital identity for financial inclusion (Kumuyi et al., 2024b), cybersecurity investment and financial performance (Ozowara et al., 2022), ransomware economics and financial resilience (Ozowara, Anunagba, et al., 2025), cyber risk pricing and insurance (Adebayo, Adepoju, et al., 2023), information governance and data verification (Peteranaba et al., 2022) and AI payment fraud detection (Atakpa et al., 2024).

Decision-support and enterprise analytics research informs how remediation evidence reaches executives and tenants. Real-time KPI tracking (Tonoyan et al., 2024b), executive dashboards (Walawalkar et al., 2025), data-driven executive decision systems (Lawal & Oduleye, 2019b), behavioural financial analytics (Lawal & Oduleye, 2023b), measurement of the strategic impact of financial analysis (Oduleye & Medon, 2023b), predictive budgeting (Adesuyi et al., 2022), automated financial consolidation (Bola-Sadipe et al., 2023), compliance-oriented financial reporting (Medon & Oduleye, 2022), CRM-based forecasting in lending (Dada et al., 2021b), analytics-driven decision-making in banking (Oluwo et al., 2025), data-led cost governance (Adesuyi, Kalu, et al., 2023), predictive vendor risk assessment (Tonoyan et al., 2024a), integrated data management for forecasting (Agu et al., 2023b), predictive financial risk assessment (Agu et al., 2025), AI decision support for operations and resource planning (Adelanwa et al., 2024a) and

performance intelligence for large public services (Adelanwa et al., 2024b) are relevant to the evaluation metrics proposed for future research. Requirements engineering for AI-enabled automation (Alieme et al., 2024; Alieme et al., 2025a), governance of AI-assisted CRM workflows (Badmus et al., 2025), integration and ETL patterns in multi-cloud CRM architectures (Badmus et al., 2019a; Badmus et al., 2022b), and human factors research on security awareness, BYOD risk, password practice and records confidentiality (Onche & Ogbonna, 2022; Onche et al., 2020; Onche et al., 2023; Onche et al., 2024) round out the socio-technical considerations.

Three gaps follow from this review. First, autonomous remediation research rarely models financial integrity as a first-class constraint on action selection. Second, self-service recovery is widely practised but almost untheorised; it appears in product documentation rather than scholarship. Third, no framework integrates provider autonomy and tenant agency within a single governance model aligned to current supervisory expectations. SAFER-FS is proposed to address all three. Building on the synthesis, this section develops the conceptual model. It first characterises the failure problem the model must address, then presents the SAFER-FS framework and its seven layers, its governance and regulatory alignment, two illustrative scenarios and the propositions the model implies. Recovery design must begin from the failures it addresses. Table 1 proposes a taxonomy of failure classes in multi-tenant financial systems along two dimensions that matter most for remediation design: the *scope* of impact (single tenant, tenant cohort, or platform-wide) and the *integrity exposure* (whether the failure can corrupt financial state, or only delays it).

Table 1. Failure taxonomy for multi-tenant financial systems

Failure class	**Typical examples**	**Usual scope**	**Integrity exposure**	**Dominant recovery owner**
Capacity and resource	Noisy neighbour, connection pool exhaustion, queue backlog	Cohort to platform	Low (delay)	Provider, autonomous
Component and infrastructure	Node loss, zone outage, database failover	Cell to platform	Low to medium	Provider, autonomous
Change-induced	Faulty deployment, schema migration, feature flag error	Cohort to platform	Medium to high	Provider, supervised
Dependency and third party	Card scheme timeout, payment rail outage, KYC vendor failure	Cohort to platform	Medium (in-doubt transactions)	Shared
Tenant configuration	Wrong fee schedule, expired certificate, misrouted webhook	Single tenant	Medium	Tenant, self-service

Failure class	Typical examples	Usual scope	Integrity exposure	Dominant recovery owner
Tenant data and input	Malformed batch file, duplicate submission, bad reference data	Single tenant	High	Tenant, self-service with guardrails
Integrity and logic	Unbalanced ledger, double posting, reconciliation break	Any	High	Joint, human-approved
Security-driven	Credential compromise, abusive API traffic	Single tenant to platform	High	Shared, security-led

Four properties distinguish this problem space from generic cloud recovery.

- **Asymmetric cost of wrong action.** In stateless services a mistaken restart costs seconds.

In financial processing, a mistaken replay can create liabilities that require customer contact, regulatory notification and manual unwinding. The penalty for wrong action frequently exceeds the penalty for delay.

- **In-doubt states.** Timeouts to external rails leave transactions whose outcome is unknown. Safe remediation must resolve the in-doubt state, through status enquiry or reconciliation, before retrying.
- **Divided knowledge.** The provider sees infrastructure and platform telemetry; the tenant understands business context, such as whether a payroll batch is time-critical or whether a spike reflects fraud. Neither party alone has sufficient information for many recovery decisions.
- **Layered accountability.** The tenant remains accountable to its regulator for outcomes even where the provider performs the recovery, so the tenant needs both visibility and, in some cases, a decision right over actions affecting its customers.

SAFER-FS organises recovery capability into seven layers bound together by a closed control loop (Figure 1). The lower layers provide the conditions under which autonomous action is safe; the middle layers decide and act; the upper layers extend agency to tenants and produce the evidence that supervisors and tenants require. The layers map onto the MAPE-K loop: tenant-aware observation implements Monitor, diagnosis and planning implement Analyse, the policy engine governs Plan, and integrity-preserving execution implements Execute, with the evidence plane serving as durable Knowledge.

Figure 1. The SAFER-FS layered framework



Figure 1. SAFER-FS layers and their relation to the MAPE-K control loop

Autonomy is only as safe as the blast radius of its mistakes. Layer 1 therefore establishes structural limits on failure propagation: cell-based partitioning of tenants, bulkheaded resource pools, per-tenant rate limits and quotas, circuit breakers on shared dependencies, and tenant-scoped feature flags that allow a change to be withdrawn from one tenant without affecting others. Containment converts many platform-wide failures into cohort or single-tenant failures, which in turn widens the range of actions that can be automated or delegated to tenants. The design principle is *containing first, then repair*, consistent with resilient cloud network design and zero trust segmentation in critical systems (Ahmed et al., 2021; Ogbole et al., 2021; Upreti & Oteri, 2025).

Conventional monitoring aggregates across tenants and so hides precisely the failures that matter most to individual clients. Layer 2 requires that service level indicators be computed per tenant and per important business service, and that observation extend beyond technical signals to **financial invariants**: ledger balance checks, posting-to-payment ratios, unmatched settlement items, and the age distribution of in-doubt transactions. A spike in failed card authorisations for one tenant, invisible in platform averages, is a first-class signal. Observation outputs are attributed to tenants and to the business services defined in each tenant's resilience mapping, so that detection speaks the same language as impact tolerances. Automated log analytics, predictive early warning and financial time-series anomaly detection provide practical building blocks for this layer (Mbonu, Iwuanyanwu, et al., 2019; Okwesa et al., 2024; Atakpa & Fobellah, 2023).

Layer 3 localises faults and generates candidate remediations. It combines deterministic rules for known failure signatures with statistical or learned models for anomaly correlation and root-cause

ranking, and, increasingly, language model agents that reason over logs, traces and runbooks. Crucially, the layer's outputs are *proposals*, each annotated with the affected tenants, the expected effect, the confidence of diagnosis, the reversibility of the action, and the integrity invariants it touches. Separating proposal from authorisation allows sophisticated, even opaque, diagnostic models to be used while keeping the authority to act within a transparent policy layer.

Layer 4 decides whether a proposed action may proceed, at what autonomy level, and with whose approval. Two constructs are central: a graduated autonomy scale and a risk-weighted admission function.

Graduated autonomy. Drawing on the levels-of-automation tradition in human factors (Parasuraman et al., 2000), SAFER-FS defines six autonomy levels for remediation actions (Table 2). Every action type in the platform's catalogue is assigned a maximum level, and the effective level for a given incident may be lowered dynamically by context, for example during month-end close or when diagnostic confidence is low.

Table 2. SAFER-FS remediation autonomy scale

Level	Name	Behaviour	Typical financial examples
A0	Manual	System detects only; humans diagnose and act	Ledger correction journals, regulatory reporting fixes
A1	Advisory	System proposes ranked actions with evidence; humans select and execute	Unwinding a double posting
A2	Approved execution	System prepares an executable plan; a human (provider or tenant) approves	Bulk replay of a payment file; tenant-wide config rollback
A3	Supervised autonomy	System executes and notifies; a human may veto within a window	Failover of a read replica; requeue of idempotent messages
A4	Bounded autonomy	System executes within pre-approved budgets; reports afterwards	Pod restarts, load shedding, circuit breaking, autoscaling
A5	Full autonomy	System executes any catalogued action without per-incident oversight	Reserved; not recommended where integrity exposure exists

Risk-weighted admission. For each candidate action *a* in incident context *x*, the policy engine computes a remediation risk score:

$$R(a, x) = I(a) \times B(a, x) \times (1 - C(x)) \times (1 - V(a)) \times W(x)$$

where $I(a)$ is the integrity exposure of the action (0 for purely infrastructural actions, approaching 1 for actions that write financial state), $B(a, x)$ is the normalised blast radius in tenants and transaction value, $C(x)$ is diagnostic confidence, $V(a)$ is reversibility (1 for an instantly reversible action, 0 for an irreversible one), and $W(x)$ is a temporal criticality weight that rises near settlement cut-offs and reporting deadlines. The action is admitted at the highest autonomy level whose risk threshold θ_k exceeds $R(a, x)$, subject to the action's catalogue ceiling. In addition, an **autonomy budget** analogous to an error budget limits the cumulative blast radius of autonomous actions within a rolling window; once exhausted, further actions drop to A2 until a human reset the budget. This prevents runaway remediation loops, a known failure mode in which automated responses amplify an incident, and reflects calls for human oversight and model risk management in automated financial decision systems (Ladapo, Dosunmu, et al., 2022; Ominyi & Anichukwueze, 2023; Ominyi & Anichukwueze, 2024).

The engine also enforces separation of duties. Actions that alter financial state require four-eyes approval, and approvals from the tenant side are required when an action affects that tenant's customers beyond a materiality threshold set in the service agreement.

Layer 5 ensures that whatever is executed, by machine or tenant, cannot violate the platform's financial correctness. Every executable remediation must satisfy five integrity invariants:

- **INV-1 Conservation.** No remediation may create or destroy value; every ledger effect is a balanced double entry.
- **INV-2 At-most-once external effect.** No remediation may cause an external payment instruction to be executed more than once; retries carry idempotency keys and in-doubt items are resolved by status enquiry before replay.
- **INV-3 Tenant confinement.** No remediation initiated for one tenant may read or modify another tenant's data or capacity beyond pre-agreed shared-resource limits.
- **INV-4 Compensability.** Every multi-step remediation is structured as a saga with defined compensating steps, or is explicitly classified as irreversible and capped at A2 or below.
- **INV-5 Reconciliation closure.** A remediation is not complete until post-action reconciliation confirms that internal records agree with external counterparties and that affected invariants hold.

Execution therefore proceeds through a pre-flight check (simulate effects against invariants, ideally on a shadow copy of state), a guarded commit, and a post-flight reconciliation gate. Failure at the gate triggers automatic compensation and escalation, mirroring end-to-end monitoring controls used in correspondent banking operations (Okafor, Farounbi, et al., 2024).

Layer 6 exposes recovery capability to tenants. Its rationale is both economic and epistemic: tenants hold business context the provider lacks, and many incidents, especially those in the tenant configuration and tenant input classes of Table 1, are faster to resolve by the party who caused them. The plane comprises four elements.

- **Transparency.** A tenant-scoped incident view showing detected anomalies, provider actions taken or proposed, affected business services and current position against impact tolerances.
- **Guided runbooks.** Parameterised, pre-validated recovery procedures, such as requeue failed webhooks, re-submit a corrected batch, roll back my configuration change, or rotate credentials, which pass through the same Layer 4 and Layer 5 controls as autonomous actions.
- **Scoped decision rights.** Tenants can approve, veto or defer provider actions that affect their

customers, within the bounds of the service agreement, and can set their own context weights, for example marking a payroll run as time-critical.

- **Escalation with context.** When a self-service path is insufficient, escalation to provider staff carries the full diagnostic and action history, eliminating the re-triage that dominates conventional support handoffs and reflecting evidence on first-contact resolution and support standardisation (Wikiri, 2021; Anyanwu, 2019; Ladapo, Jooda, et al., 2023a).

The key design principle is **symmetry of control**: a tenant-initiated action and a machine-initiated action are evaluated by the same admission function and invariants. Self-service thus extends, rather than bypasses, the guardrail system, and the platform's safety case does not depend on the competence of any individual tenant operator.

Layer 7 records every detection, proposal, admission decision, approval, execution and reconciliation outcome in an append-only, tamper-evident remediation ledger, attributed to the human or machine actor and to the policy version in force. This ledger serves three purposes: it provides the audit trail that supervisors expect when examining incident handling; it produces tenant-specific incident reports that tenants can pass to their own regulators, including the content needed for major incident classification and reporting under DORA; and it supplies the training and calibration data that allow the platform to raise or lower autonomy ceilings over time based on observed outcomes. Tamper-evident recordkeeping and continuous auditing research support this design (Anichukwueze et al., 2021; Aliliele et al., 2025a; Uchechi et al., 2022). Post-incident learning, in the blameless tradition of SRE, closes the loop by updating runbooks, thresholds and catalogue ceilings. SAFER-FS is designed so that its artefacts double as compliance evidence. Table 3 maps framework components to the principal 2025 obligations. The mapping is indicative rather than legal advice, and firms should validate it against their own supervisory context; related compliance frameworks for financial institutions and business continuity studies offer complementary guidance (Bello et al., 2024; Okafor, Osuji, et al., 2024; Fadero et al., 2020).

Table 3. Indicative mapping of SAFER-FS to 2025 operational resilience obligations

Obligation	**Source**	**SAFER-FS components**
Protection, prevention and containment	DORA Art. 9	L1 containment, L4 guardrails
Detection of anomalous activity	DORA Art. 10	L2 tenant-aware observation
Response and recovery plans; backup and restoration	DORA Art. 11 to 12	L3 to L6 runbooks, L5 compensation and reconciliation
Incident management, classification and reporting	DORA Art. 17 to 19	L2 attribution, L7 remediation ledger and tenant reports
Resilience testing	DORA Art. 24 to 26	Chaos experiments against L1 to L5; autonomy budget drills

Obligation	Source	SAFER-FS components
Third-party risk and exit planning	DORA Art. 28 to 30	L6 transparency and decision rights; L7 evidence for tenants
Important business services and impact tolerances	PRA/FCA regime, effective March 2025	L2 per-service indicators; W(x) weighting; tolerance tracking in L6
Critical operations and tolerance for disruption	BCBS (2021) principles	Whole framework; L7 learning loop

Three governance mechanisms complement the mapping. First, an **autonomy register** lists every catalogued action, its integrity exposure, reversibility, ceiling level and approving authority, and is reviewed by the provider's risk function and made visible to tenants. Second, **autonomy promotion** follows an evidence-based path: an action may move up one level only after a defined number of executions at the lower level without integrity breach or reversal, mirroring how error budgets govern release velocity. Third, **model risk management** applies to learned diagnostic and planning components, with the explicit separation of proposal (L3) from authorisation (L4) allowing opaque models to be used without delegating authority to them.

The first illustrative scenario concerns a payment rail timeout with in-doubt transactions. A domestic instant payment rail begins timing out for a subset of requests. Layer 1 circuit breakers trip for the affected connector, preventing thread exhaustion from spreading to other cells. Layer 2 detects a rising count of in-doubt payments for 14 tenants and attributes them to the rail. Layer 3 proposes two actions: retry all timed-out payments, and run status enquiries before selective retry. The policy engine scores blind retry as high risk, since its integrity exposure is high and it is not reversible once funds move, and rejects it outright under INV-2. Status enquiry is low risk and is admitted at A4. Enquiries confirm that 60 per cent of in-doubt payments in fact settled; these are marked complete. The remainder are proposed for retry at A3 with a veto window. Two tenants, whose payroll batches are flagged time-critical, see the proposal in their Layer 6 view and approve immediately; others allow the window to elapse. Post-flight reconciliation confirms closure. The Layer 7 ledger generates a per-tenant report with timelines and counts suitable for each tenant's incident classification process.

The second scenario concerns a duplicate batch submission by a tenant. A credit union tenant accidentally uploads the same direct debit file twice. Platform-level duplicate detection catches exact duplicates, but this file was regenerated with new identifiers. Layer 2 observes an anomalous doubling of collection volume against that tenant's baseline and raises a tenant-scoped alert. Because the failure is confined to one tenant and originates in its input, the framework routes it to the tenant's self-service plane rather than to provider operations. The tenant's operator selects the guided runbook for withdrawing a batch, which shows that the second file has not yet been submitted to the clearing system. The withdrawal is a reversible, single-tenant action and is admitted at A2 with the tenant's own four-eyes approval. Had the file already been submitted, the runbook would instead have constructed a saga of recall requests and compensating ledger entries, capped at A1, with provider involvement. Resolution takes minutes rather than the hours typical of a support ticket, and no provider engineer is paged.

The framework yields the following propositions, each stated to permit empirical testing through multi-case studies, platform telemetry analysis or controlled fault-injection experiments.

- **P1.** Platforms that gate autonomous remediation through explicit financial integrity invariants will exhibit fewer remediation-induced integrity incidents than platforms that gate only on technical health checks, without a material increase in mean time to recovery for availability incidents.
- **P2.** The proportion of incidents that can be safely automated is positively associated with the strength of containment (Layer 1), because containment reduces blast radius and therefore remediation risk.
- **P3.** For failures in the tenant configuration and tenant input classes, guided self-service recovery will reduce time to recovery relative to provider-mediated support, and this effect will be moderated by runbook coverage and tenant operator training.
- **P4.** Symmetry of control, in which tenant-initiated and machine-initiated actions share the same admission controls, will be associated with higher tenant trust and greater willingness of tenants to accept higher provider autonomy levels.
- **P5.** Autonomy budgets will reduce the frequency and severity of runaway remediation loops relative to unbounded automation.
- **P6.** Platforms that maintain an evidentiary remediation ledger will reduce the effort and elapsed time required for tenants to complete regulatory incident reporting.

SAFER-FS reframes the question of how much to automate. Rather than a single organisational choice, autonomy becomes a property of each action in each context, computed from integrity exposure, blast radius, confidence, reversibility and timing, and constrained by budgets and evidence. This allows aggressive automation of low-risk infrastructural actions to coexist with conservative human oversight of actions that write financial state. The framework also reframes self-service: tenants become participants in the control loop rather than recipients of support, and the platform's guardrails protect both the tenant and its neighbours from operator error.

The model also clarifies how the applied literature fits together. Work on security orchestration and continuous control (Dosunmu & Ogundele, 2025c; Adebayo, Amadi, et al., 2025) supplies execution mechanics but rarely addresses financial correctness; payment and banking operations research (Okafor, Farounbi, et al., 2024; Osuji et al., 2021) captures correctness concerns but seldom considers autonomy; and continuous auditing and governance research (Aliliele et al., 2025a; Ominyi & Anichukwueze, 2023; Uchechi et al., 2022) supplies accountability without engineering detail. SAFER-FS positions these as complementary layers of one system, which is its principal integrative contribution. Several tensions remain. Exposing diagnostic detail to tenants can leak information about shared infrastructure or other tenants, so transparency must itself be tenant-confined. Veto windows add latency that may breach tolerances in fast-moving incidents, and calibrating them is non-trivial. The admission function's parameters are judgemental, and their calibration will require operational data that few platforms currently collect in the needed form. The rise of language model operations agents creates particular difficulty: such agents can generate actions outside the catalogue, and the framework's response, which is to admit only catalogued actions above A1 and to treat novel proposals as advisory, may forgo real benefits. Finally, regulatory expectations continue to develop, with technical standards under DORA and supervisory practice in 2025 and beyond likely to refine what counts as adequate evidence.

For autonomic and self-adaptive systems theory, the model adds financial integrity invariants as first-class constraints on the planning and execution stages of the MAPE-K loop, extending safety-

constrained adaptation from physical to financial domains in the way critical infrastructure research has done for cyber-physical systems (Adegbite et al., 2024a; Ahmed et al., 2021). For the human-automation literature, it treats the level of automation as a dynamic, per-action property governed by risk and budgets rather than a fixed system attribute (Parasuraman et al., 2000; Ladapo, Dosunmu, et al., 2022). For multi-tenancy research, it introduces the tenant as an active participant in recovery and proposes symmetry of control as a design principle that has not previously been articulated. For platform providers, the framework offers a sequencing logic: invest first in containment and tenant-aware observation, then build the integrity-preserving execution layer, and only then extend autonomy and self-service, since each later layer depends on the safety properties of the earlier ones. An autonomy registers and autonomy budgets give engineering and risk teams a shared vocabulary for deciding what to automate (Olagunju et al., 2023; Olagunju et al., 2025). For tenant institutions, the self-service plane and remediation ledger convert outsourced recovery from an opaque dependency into an observable and partly controllable process, supporting their own oversight of third-party risk (Okafor, Osuji, et al., 2024; Fadero et al., 2020). For security and operations teams, the separation of proposal from authorisation allows AI and language model tools to be adopted for diagnosis without delegating authority to them (Nwakamma et al., 2024b; Nwakamma et al., 2024a). For supervisors, the framework suggests that evidence of recovery capability can be produced as a by-product of operation rather than assembled after the fact, which may reduce reporting burden while improving its quality (Uchechi et al., 2022; Anichukwueze et al., 2021). It also highlights a supervisory blind spot: where autonomous remediation acts on behalf of many regulated tenants at once, accountability for machine decisions should be explicitly allocated in contracts and in incident reporting templates. Policymakers developing guidance on AI in financial services may find the graduated autonomy scale a useful basis for proportionate expectations, consistent with model risk management and responsible AI governance approaches (Ominyi & Anichukwueze, 2023; Ominyi & Anichukwueze, 2024; Ominyi et al., 2024b).

As a conceptual paper, this work has not been validated empirically. The propositions and metrics are offered as a basis for such validation, and the scenarios are illustrative rather than drawn from specific firms. The framework is also oriented toward platforms with mature engineering practices; smaller providers may need to adopt it incrementally, beginning with containment, tenant-aware observation and the evidence ledger before introducing higher autonomy levels.

The literature base also carries limitations. The seed corpus was drawn from a single consolidated list and screened by title and subject area, so relevant work outside that list, and nuances visible only in full texts, may have been missed. Many seed studies are themselves conceptual, which strengthens the framework's coverage of concerns but not its empirical grounding. Finally, the regulatory mapping reflects the European and United Kingdom regimes in force in 2025 and may not transfer directly to other jurisdictions, such as those covered by emerging-market data protection and insurance regulation (Fadero et al., 2021; Ominyi & Anichukwueze, 2022a).

Future research should test the six propositions using three complementary designs. Multi-case studies of platform providers and their tenants can examine how autonomy decisions are made and governed in practice. Analysis of incident and remediation telemetry can estimate the effects predicted in P1, P2, P3 and P5. Controlled fault-injection experiments, building on chaos engineering and breach and attack simulation (Basiri et al., 2016; Dosunmu & Ogundele, 2024a; Dosunmu & Ogundele, 2024c), can compare remediation strategies under identical failure conditions.

Testing the propositions requires measures that capture integrity and accountability as well as speed. Table 4 proposes a metric set organised by framework objective.

Table 4. Proposed SAFER-FS evaluation metrics

Objective	Metric	Definition
Speed	Tenant-weighted MTTR	Mean time to recovery weighted by affected tenants and transaction value
Speed	Tolerance adherence rate	Share of incidents resolved within each tenant's impact tolerance
Integrity	Remediation-induced integrity incidents	Count of integrity breaches caused by a remediation action, per 1,000 actions
Integrity	Reconciliation closure time	Time from action to confirmed reconciliation closure (INV-5)
Isolation	Cross-tenant impact ratio	Tenants affected by an action relative to tenants in the action's intended scope
Autonomy	Safe automation coverage	Share of incidents resolved at A3 or above without reversal
Autonomy	Reversal rate	Share of autonomous actions subsequently compensated or vetoed
Self-service	Self-service resolution rate	Share of tenant-scoped incidents resolved without provider staff
Assurance	Evidence completeness	Share of actions with complete actor, policy and outcome records
Assurance	Reporting lead time	Time for a tenant to assemble a regulator-ready incident report

Beyond testing, several directions merit attention: calibration methods for the admission function using historical incident data (Okwesa et al., 2024; Fadayomi et al., 2024); safe incorporation of language model agents that propose actions outside a fixed catalogue (Nwakamma et al., 2024b; Oyesiji et al., 2024); privacy-preserving transparency for tenants on shared infrastructure (Atakpa & Abolaji, 2022; Okoruwa et al., 2020); extension of the framework to distributed-ledger and cross-border payment infrastructures (Adesuyi, Akomolafe, et al., 2023; Adesuyi et al., 2025b); and comparative study of how supervisors in different jurisdictions evaluate evidence of autonomous recovery (Ominyi & Anichukwueze, 2021; Ominyi, 2020).

4. Conclusion

Multi-tenant financial platforms face a recovery problem that neither classic self-healing research nor generic cloud operations practice fully addresses. Failures are shared, but accountability is distributed; speed matters, but wrong action costs more than delay; and from 2025, supervisors in Europe and the United Kingdom expect recovery capability to be demonstrated, not merely asserted. SAFER-FS responds by integrating autonomous remediation and tenant self-service within one governed control loop, anchored by containment, financial integrity invariants, graduated and budgeted autonomy, symmetric control for human and machine actors, and an evidentiary ledger. The framework offers practitioners a structure for designing and governing recovery capability, and offers researchers a set of propositions and metrics for testing whether the promise of autonomous, self-service recovery can be realised without compromising the integrity on which financial systems depend.

RJPST

References

Adebayo, A., Adegbite, M. P., & Ahmed, M. O. (2022). Adversarial machine learning in critical infrastructure: A conceptual framework for threat modeling AI enabled OT systems. World Journal of Innovation and Modern Technology, 6(1), 184-234. https://doi.org/10.56201/wjimt.v6.no1.2022.pg184.234

Adebayo, A., Adegbite, M. P., & Ahmed, M. O. (2023). 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, 9(3), 287-340. https://doi.org/10.56201/ijcsmt.v9.no3.2023.pg287.340

Adebayo, A., Adepoju, P. A., & Ozowara, D. E. (2023). Conceptual model for cyber risk pricing and insurance structuring in health technology platforms. Gyanshauryam, International Scientific Refereed Research Journal, 6(6).

Adebayo, A., Amadi, C., & Ijagbemi, A. O. (2025). 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, 11(8), 88-134. https://doi.org/10.56201/ijcsmt.vol.11.no8.2025.pg88.134

Adebayo, A., Anunagba, C. O., & Ozowara, D. E. (2025). A review of zero trust security models and cost effectiveness in healthcare infrastructure. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2269-2283. https://doi.org/10.62225/2583049X.2025.5.6.6051

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2020). 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, 6(3), 103-146. https://doi.org/10.56201/ijemt.vol.6.no3.2020.pg103.146

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2022). 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, 8(2), 81-132. https://doi.org/10.56201/ijcsmt.v8.no2.2022.pg81.132

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2023). 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, 7(2), 121-182. https://doi.org/10.56201/wjimt.v7.no2.2023.pg121.182

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2024a). A vulnerability governance architecture for power and utilities corporations: From exposure mapping to remediation verification. World Journal of Innovation and Modern Technology, 8(6), 185-246. https://doi.org/10.56201/wjimt.v8.no6.2024.pg185.246

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2024b). 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, 10(11), 197-256. https://doi.org/10.56201/ijemt.v10.no11.2024.pg197.256

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2025). A cyber risk quantification and governance architecture for critical infrastructure: From posture measurement to executive reporting. International Journal of Computer Science and Mathematical Theory, 11(12), 232-293. https://doi.org/10.56201/ijcsmt.vol.11.no12.2025.pg232.293

Adelanwa, A., Basnet, A., & Anene, U. N. (2023a). Data driven digital transformation models for lifecycle performance management in infrastructure delivery. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2646-2662. https://doi.org/10.62225/2583049X.2023.3.6.5968

Adelanwa, A., Basnet, A., & Anene, U. N. (2023b). Predictive analytics models for financial risk detection and fraud prevention in public systems. International Journal of Advanced Multidisciplinary Research and Studies, 3(6). https://doi.org/10.62225/2583049X.2023.3.6.5969

Adelanwa, A., Basnet, A., & Anene, U. N. (2024a). Advanced AI based decision support systems for healthcare operations and resource planning. Gyanshauryam, International Scientific Refereed Research Journal, 7(1), 244-276. http://doi.org/10.32628/GISRRJ

Adelanwa, A., Basnet, A., & Anene, U. N. (2024b). Performance intelligence models for optimization and outcome measurement in large scale public services. Shodhshauryam, International Scientific Refereed Research Journal, 6(1).

Adeniyi, A. I., Odejobi, O., & Taiwo, T. (2025). Countermeasures against bias and spoofing in modern facial recognition systems. World Journal of Advanced Research and Reviews, 25(1), 1914-1930.

Adesuyi, M. O., Akomolafe, O., Olaogun, B. O., Ndukwe, V. U., & Sakyi, J. K. (2023). Global interoperability model for distributed ledger-based cross-border payment systems. International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), 1291-1300. https://doi.org/10.54660/.IJMRGE.2023.4.6.1291-1300

Adesuyi, M. O., Akomolafe, O., Olaogun, B. O., Ndukwe, V. U., & Sakyi, J. K. (2024). AI-driven risk scoring model for global cross-border trade payment transactions. International Journal of Advanced Multidisciplinary Research and Studies, 4(1), 1569-1581. https://doi.org/10.62225/2583049X.2024.4.1.5281

Adesuyi, M. O., Akomolafe, O., Olaogun, B. O., Ndukwe, V. U., & Sakyi, J. K. (2025a). AI-enabled fraud detection ecosystem model for securing international payment channels. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 866-882. https://doi.org/10.62225/2583049X.2025.5.6.5284

Adesuyi, M. O., Akomolafe, O., Olaogun, B. O., Ndukwe, V. U., & Sakyi, J. K. (2025b). Resilience and continuity model for global payment infrastructure under geopolitical risks. International Journal of Multidisciplinary Research and Growth Evaluation, 6(4), 1467-1482. https://doi.org/10.54660/.IJMRGE.2025.6.4.1467-1482

Adesuyi, M. O., Kalu, A., & Walawalkar, G. (2023). Data-led cost governance in technology-intensive enterprises. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(3), 877-896. https://doi.org/10.32628/IJSRCSEIT

Adesuyi, M. O., Walawalkar, G., & Kalu, A. (2022). Predictive budgeting models using operational and market signals. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(5), 818-837. https://doi.org/10.32628/IJSRCSEIT

Agboada, P., Anene, U. N., Obukadata, V. O., & Ezeako, R. (2022). Financial inclusion and digital banking transformation in Sub-Saharan Africa: A review of advances and policy implications. International Journal of Management and Organizational Research, 1(1), 267-282. https://doi.org/10.54660/IJMOR.2022.1.1.267-282

Agu, M. U., Akomolafe, O., & Bello, A. (2023a). A comparative review of SOX compliance frameworks in cross-border financial auditing. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2297-2306. https://doi.org/10.62225/2583049X.2023.3.6.5362

Agu, M. U., Akomolafe, O., & Bello, A. (2023b). A review of integrated data management systems for enhancing financial forecasting accuracy. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2335-2344.

Agu, M. U., Akomolafe, O., & Bello, A. (2025). Advances in predictive financial risk assessment using Python-based forecasting systems. International Journal of Computer Science and Mathematical Theory, 11(11), 131-148. https://doi.org/10.56201/ijcsmt.vol.11.no11.2025.pg131.148

Ahmed, K. S., & Odejobi, O. D. (2018a). Conceptual framework for scalable and secure cloud architectures for enterprise messaging. IRE Journals, 2(1), 1-15.

Ahmed, K. S., & Odejobi, O. D. (2018b). Resource allocation model for energy-efficient virtual machine placement in data centers. IRE Journals, 2(3), 1-10.

Ahmed, K. S., Odejobi, O. D., & Oshoba, T. O. (2019). Algorithmic model for constraint satisfaction in cloud network resource allocation. IRE Journals, 2(12), 516-532.

Ahmed, K. S., Odejobi, O. D., & Oshoba, T. O. (2020). Predictive model for cloud resource scaling using machine learning techniques. Journal of Frontiers in Multidisciplinary Research, 1(1), 173-183.

Ahmed, M. O., Adegbite, M. P., & Adebayo, A. (2021). 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, 7(1), 66-113. https://doi.org/10.56201/ijemt.vol.7.no1.2021.pg66.113

Ajagbe, S. A., Akindolani, A., Akande, T. O., Adeyanju, K. I., Aiyeniko, O., & Ajiboye, G. O. (2025). Intrusion detection system with feature selection on machine learning algorithm. In Proceedings of the 6th International Conference and Workshop on Engineering and Technology Research (ICWETR) LAUFET 2025 (pp. 24-39).

Akeju, B., Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., & Abolaji, T. O. (2018). Conceptual model for insider threat classification and risk modeling in complex digital systems. Iconic Research and Engineering Journals, 1(9), 476-492. https://doi.org/10.64388/IREV1I9-1713778

Akomolafe, O., & Agu, M. U. (2018). A conceptual model for enhancing internal audit quality through technology-enabled risk assessment frameworks. Iconic Research and Engineering Journals, 1(9), 458-475.

Akomolafe, O., & Agu, M. U. (2019a). A conceptual framework for developing risk-based internal control models in the insurance and banking sectors. Iconic Research and Engineering Journals, 2(8), 335-354.

Akomolafe, O., & Agu, M. U. (2019b). A review of data-driven risk evaluation models for emerging market financial institutions. Iconic Research and Engineering Journals, 3(6), 433-448.

Akomolafe, O., & Agu, M. U. (2019c). Advances in financial resilience through integrated governance and compliance strategies. Iconic Research and Engineering Journals, 2(10), 607-620.

Akomolafe, O., Agu, M. U., & Bello, A. (2023a). A conceptual model for implementing risk-based auditing in strategic financial management. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2274-2286. https://doi.org/10.62225/2583049X.2023.3.6.5359

Akomolafe, O., Agu, M. U., & Bello, A. (2023b). A quantitative conceptual model for assessing compliance risk in emerging economies. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2287-2296. https://doi.org/10.62225/2583049X.2023.3.6.5360

Akomolafe, O., Agu, M. U., & Bello, A. (2025). A conceptual model for advancing risk governance through data-driven compliance analytics in financial institutions. Journal of Accounting and Financial Management, 11(11), 211-228. https://doi.org/10.56201/jafm.vol.11.no11.2025.pg211.228

Akomolafe, O., Olaogun, B. O., Adesuyi, M. O., Ndukwe, V. U., & Sakyi, J. K. (2022). Smart contract automation model for supplier payment systems and performance benchmarking. International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), 827-836. https://doi.org/10.54660/.IJMRGE.2022.3.6.827-836

Akomolafe, O., Olaogun, B. O., Adesuyi, M. O., Ndukwe, V. U., & Sakyi, J. K. (2023). Predictive AI model for remittance liquidity optimization in international payment systems. International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), 1301-1311. https://doi.org/10.54660/.IJMRGE.2023.4.6.1301-1311

Akomolafe, O., Olaogun, B. O., Adesuyi, M. O., Ndukwe, V. U., & Sakyi, J. K. (2024a). Scalable blockchain payment gateway architecture model for enterprise-grade adoption. International Journal of Advanced Multidisciplinary Research and Studies, 4(1), 1552-1568. https://doi.org/10.62225/2583049X.2024.4.1.5280

Akomolafe, O., Olaogun, B. O., Adesuyi, M. O., Ndukwe, V. U., & Sakyi, J. K. (2024b). Smart contract-based dispute resolution model for international supplier payments. International Journal of Advanced Multidisciplinary Research and Studies, 4(1), 1582-1601. https://doi.org/10.62225/2583049X.2024.4.1.5282

Akomolafe, O., Olaogun, B. O., Adesuyi, M. O., Ndukwe, V. U., & Sakyi, J. K. (2025a). Collaborative governance framework for secure cross-border payment data sharing. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 849-865. https://doi.org/10.62225/2583049X.2025.5.6.5283

Akomolafe, O., Olaogun, B. O., Adesuyi, M. O., Ndukwe, V. U., & Sakyi, J. K. (2025b). Global standardization model for next-generation blockchain interoperability in payment systems. International Journal of Multidisciplinary Research and Growth Evaluation, 6(6), 820-834. https://doi.org/10.54660/.IJMRGE.2025.6.6.820-834

Alieme, J. I., Sule, A., & Obukadata, V. O. (2024). From ambiguity to AI-ready requirements: A business analysis framework for structuring business problems for intelligent process automation. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), 2088-2117. https://doi.org/10.54660/.IJMRGE.2024.5.6.2088-2117

Alieme, J. I., Sule, A., & Obukadata, V. O. (2025a). Requirements elicitation for AI-enabled process automation: A comparative review of Agile, Waterfall, and Hybrid implementation approaches. Gulf Journal of Computer Sciences, 1(4), 116-169.

Alieme, J. I., Sule, A., & Obukadata, V. O. (2025b). 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, 11(8), 299-355. https://doi.org/10.56201/ijebm.vol.11.no8.2025.pg299.355

Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2023a). 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, 9(10), 373-394. https://doi.org/10.32628/CSEIT2361071

Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2023b). A review of API governance and risk prioritization frameworks in modern financial institutions. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(10), 395-433. https://doi.org/10.32628/CSEIT2361072

Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2024a). A conceptual framework for enterprise data sensitivity classification and regulatory traceability mechanisms. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3103-3124. https://doi.org/10.62225/2583049X.2024.4.6.5991

Aliliele, C., Mbonu, I. S., Uzoka, E., & Iwuanyanwu, U. (2025a). A review of AI assisted continuous auditing systems in technology risk and cybersecurity oversight. Gyanshauryam, International Scientific Refereed Research Journal, 8(4), 210-250. https://doi.org/10.32628/GISRRJ258369

Aliliele, C., Mbonu, I. S., Uzoka, E., & Iwuanyanwu, U. (2025b). Advances in data lakehouse governance architectures for enterprise data loss prevention and compliance assurance. Shodhshauryam, International Scientific Refereed Research Journal, 8(4), 171-213. https://doi.org/10.32628/SHISRRJ258474

Amadi, C. (2025). An autonomous, continuously-learning framework for real-time cyber-physical threat prevention in legacy SCADA systems. World Journal of Innovation and Modern Technology, 9(8), 148-183. https://doi.org/10.56201/wjimt.v9.no8.2025.pg148.183

Amadi, C., Adebayo, A., & Ijagbemi, A. O. (2025a). 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, 9(8), 99-147. https://doi.org/10.56201/wjimt.v9.no8.2025.pg99.147

Amadi, C., Adebayo, A., & Ijagbemi, A. O. (2025b). 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, 11(8), 352-392. https://doi.org/10.56201/ijemt.vol.11.no8.2025.pg352.392

Amadi, C., Adebayo, A., & Ijagbemi, A. O. (2025c). 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, 11(8), 135-169. https://doi.org/10.56201/ijcsmt.vol.11.no8.2025.pg135.169

Anene, U. N., Ezeako, R., Alugwe, S., & Awulu, I. (2023). Benchmarking methodologies for multi-site operations networks: A review of advances in regression-based performance analysis. International Journal of Multidisciplinary Futuristic Development, 4(1), 142-158. https://doi.org/10.54660/IJMFD.2023.4.1.142-158

Anichukwueze, C. C., Ominyi, M., Uzougbo, N. S., & Jones, B. C. (2022). Cross-functional legal education as risk mitigation: Empirical analysis of contract error reduction in engineering

teams. International Journal of Engineering and Modern Technology, 8(5), 142-180. https://doi.org/10.56201/ijemt.v8.no5.2022.pg142.180

Anichukwueze, C. C., Osuji, V. C., & Oguntegbe, E. E. (2020). Designing ethics and compliance training frameworks to drive measurable cultural and behavioral change. International Journal of Multidisciplinary Research and Growth Evaluation, 1(3), 205-220.

Anichukwueze, C. C., Osuji, V. C., & Oguntegbe, E. E. (2021). Blockchain-based architectures for tamper-proof regulatory recordkeeping and real-time audit readiness. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 485-504.

Annan, A. O. (2022). Data privacy governance models for cross-border digital platforms. International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), 949-964.

Annan, A. O. (2024). Algorithmic accountability and trade secret protection in artificial intelligence. Shodhshauryam, International Scientific Refereed Research Journal, 7(5), 315-347.

Annan, A. O. (2025a). Automated decision-making and anti-discrimination compliance under U.S. law. International Journal of Advanced Multidisciplinary Research and Studies, 5(2), 2522-2540.

Annan, A. O. (2025b). Cybersecurity compliance as a source of competitive advantage in technology markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(5), 456-487.

Anyanwu, K. C. E. (2019). Developing a maturity model for standardizing IT support operations across geographically distributed multi-office organizations. Iconic Research and Engineering Journals, 3(5)., 580-598.

Anyanwu, K. C. E. (2020). Balancing cost and operational continuity in hybrid remote and on-site IT support for multi-branch SMEs. International Journal of Economics and Financial Management, 5(2), 132-148. https://doi.org/10.56201/ijefm.v5.no2.2020.pg132.148

Anyanwu, K. C. E. (2022). Bridging enterprise IT operations and digital entrepreneurship: A systematic review of skill transfer mechanisms and pathways. World Journal of Entrepreneurial Development Studies, 7(1), 114-134. https://doi.org/10.56201/wjeds.v7.no1.2022.pg114.134

Atakpa, M. I. (2021). 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, 7(2), 778-804. https://doi.org/10.32628/CSEIT2064813

Atakpa, M. I., & Abetoh, N. F. (2022). 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, 8(2), 771-801. https://doi.org/10.32628/CSEIT23906220

Atakpa, M. I., & Abolaji, T. O. (2022). 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, 8(3), 781-808. https://doi.org/10.32628/CSEIT22558

Atakpa, M. I., & Fobellah, A. N. (2023). 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, 9(2), 967-997. https://doi.org/10.32628/CSEIT2342441

Atakpa, M. I., Abetoh, N. F., & Akeju, B. (2024). Advances in artificial intelligence for healthcare payment fraud detection: A review of NHS applications. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(4), 1161-1194. https://doi.org/10.32628/CSEIT26123240

Badmus, O., Dosunmu, A. A., & Anunagba, C. O. (2025). 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, 2(1), 59-80.

Badmus, O., Dosunmu, A. A., & Ozowara, D. E. (2018). A systematic review of CI/CD pipeline strategies in Salesforce DevOps: Tools, practices, and deployment outcomes. Iconic Research and Engineering Journals, 2(6).

Badmus, O., Dosunmu, A. A., & Ozowara, D. E. (2019a). A conceptual model for ETL design and data integration in Salesforce-centric enterprise architectures. Iconic Research and Engineering Journals, 3(5).

Badmus, O., Dosunmu, A. A., & Ozowara, D. E. (2019b). A governance framework for Salesforce platform management in regulated healthcare environments. Iconic Research and Engineering Journals, 3(6).

Badmus, O., Dosunmu, A. A., Ozowara, D. E., & Anunagba, C. O. (2020). 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, 1(5), 1021-1031. https://doi.org/10.54660/.IJMRGE.2020.1.5.1021-1031

Badmus, O., Jooda, D., & Anunagba, C. O. (2024). A privacy-by-design framework for role-based security architecture in Salesforce environments handling sensitive personal data. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3244-3254. https://doi.org/10.62225/2583049X.2024.4.6.6243

Badmus, O., Jooda, D., Ozowara, D. E., & Anunagba, C. O. (2022a). A framework for Git-based version control and code review governance in Salesforce development teams. Shodhshauryam, International Scientific Refereed Research Journal, 5(2), 473-493.

Badmus, O., Jooda, D., Ozowara, D. E., & Anunagba, C. O. (2022b). A systematic review of MuleSoft ESB integration patterns in multi-cloud Salesforce architectures. Gyanshauryam, International Scientific Refereed Research Journal, 5(3), 462-481.

Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements.

Basiri, A., Behnam, N., de Rooij, R., Hochstein, L., Kosewski, L., Reynolds, J., & Rosenthal, C. (2016). Chaos engineering. *IEEE Software, 33*(3), 35 to 41.

Bello, A. A., Oduro, D. A., Manu, E. O., Bello, A. D., Leo, A. O., Ukatu, C. E., & Okika, N. (2025). Enhancing Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance using blockchain: A business analysis approach. Iconic Research and Engineering Journals, 8(9), 297-305.

Bello, A. D., Elebe, O., Hammed, N. I., Okoruwa, P. O., Fadayomi, O., & Omoegun, G. O. (2025). An advanced regulatory technology framework for improving financial transparency and fraud reporting accuracy. International Journal of Advanced Multidisciplinary Research and Studies, 5(6).

Bello, A. D., Elebe, O., Hammed, N. I., Omoegun, G. O., & Fadayomi, O. (2024). A cybersecurity risk management and regulatory compliance framework for financial institutions. Iconic Research and Engineering Journals. https://www.irejournals.com/paper-details/1713553

Bello, A. D., Oguntola, O. B., Ajibade, A. T., Akindolani, A., Ayoola, O., & Bello, A. M. (2025). AI-driven fraud detection in UK digital payment systems: Challenges and solutions. Iconic Research and Engineering Journals, 9(1), 1329-1343.

Bello, A., Akomolafe, O., & Agu, M. U. (2023). A conceptual framework for data-driven procurement risk management in multinational enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2307-2316. https://doi.org/10.62225/2583049X.2023.3.6.5363

Beyer, B., Jones, C., Petoff, J., & Murphy, N. R. (Eds.). (2016). *Site reliability engineering: How Google runs production systems*. O'Reilly Media.

Bezemer, C.-P., & Zaidman, A. (2010). Multi-tenant SaaS applications: Maintenance dream or nightmare? In *Proceedings of the Joint ERCIM Workshop on Software Evolution and International Workshop on Principles of Software Evolution* (pp. 88 to 92). ACM.

Bola-Sadipe, D., Aliliele, C., & Odihi, F. (2023). Conceptual model for automated financial consolidation and transparency in multinational corporations. Gyanshauryam, International Scientific Refereed Research Journal, 6(6), 414-455. https://doi.org/10.32628/GISRRJ236645

Bola-Sadipe, D., Eboh, E. E., & Odihi, F. (2022). Advances in data-driven tax compliance and financial reporting systems in banking institutions. Shodhshauryam, International Scientific Refereed Research Journal, 5(1), 366-403. https://doi.org/10.32628/SHISRRJ247137

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

Candea, G., & Fox, A. (2003). Crash-only software. In *Proceedings of the 9th Workshop on Hot Topics in Operating Systems (HotOS IX)*. USENIX.

Candea, G., Kawamoto, S., Fujiki, Y., Friedman, G., & Fox, A. (2004). Microreboot: A technique for cheap recovery. In *Proceedings of the 6th Symposium on Operating Systems Design and Implementation (OSDI)*. USENIX.

Dada, T., Isiekwu, C. P., & Oluwo, K. (2021a). Advances in multinational cash flow consolidation and FX risk control using tiered treasury architecture. Iconic Research and Engineering Journals, 4(11), 601-620. https://doi.org/10.64388/IREV4I11-1714351

Dada, T., Isiekwu, C. P., & Oluwo, K. (2021b). Designing CRM-based sales forecasting models for multichannel lending institutions. Iconic Research and Engineering Journals, 5(3), 451-466. https://doi.org/10.64388/IREV5I3-1714352

Dang, Y., Lin, Q., & Huang, P. (2019). AIOps: Real-world challenges and research innovations. In *Proceedings of the 41st International Conference on Software Engineering: Companion Proceedings* (pp. 4 to 5). IEEE/ACM.

Dosunmu, A. A., & Ogundele, P. O. (2019). Security audit and enterprise risk assessment frameworks for resilient information systems. Iconic Research and Engineering Journals, 3(5), 434-447. https://doi.org/10.64388/IREV3I5-1713225

Dosunmu, A. A., & Ogundele, P. O. (2020). Intrusion detection and prevention models for enhancing organizational cyber defense effectiveness. Iconic Research and Engineering Journals, 4(6), 310-324. https://doi.org/10.64388/IREV4I6-1713226

Dosunmu, A. A., & Ogundele, P. O. (2021). Incident response and digital forensics strategies for rapid cyber attack containment. Gyanshauryam, International Scientific Refereed Research Journal, 4(4), 239-258.

Dosunmu, A. A., & Ogundele, P. O. (2022). Threat intelligence integration frameworks supporting proactive enterprise cybersecurity decision making. Gyanshauryam, International Scientific Refereed Research Journal, 5(3), 397-416.

Dosunmu, A. A., & Ogundele, P. O. (2023). Cyber threat actor analysis models for strategic enterprise security planning. Shodhshauryam, International Scientific Refereed Research Journal, 6(5), 513-531.

Dosunmu, A. A., & Ogundele, P. O. (2024a). Breach and attack simulation frameworks for continuous validation of enterprise security controls. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(3), 1100-1119.

Dosunmu, A. A., & Ogundele, P. O. (2024b). Cyber risk quantification models for prioritizing enterprise security investment decisions. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), 1777-1785. https://doi.org/10.54660/.IJMRGE.2024.5.6.1777-1785

Dosunmu, A. A., & Ogundele, P. O. (2024c). Enterprise scale continuous security validation models for regulated digital infrastructures. International Journal of Scientific Research in Humanities and Social Sciences, 1(2), 929-945.

Dosunmu, A. A., & Ogundele, P. O. (2024d). Threat informed defence engineering models for measuring security control effectiveness at scale. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 2847-2858.

Dosunmu, A. A., & Ogundele, P. O. (2025a). Adversary simulation design frameworks for proactive cyber defense in complex environments. International Journal of Computer Science and Mathematical Theory, 11(12), 193-209. https://doi.org/10.56201/ijcsmt.vol.11.no12.2025.pg193.209

Dosunmu, A. A., & Ogundele, P. O. (2025b). Cyber defense performance measurement frameworks for executive and board level governance. Computer Science and IT Research Journal, 6(11), 895-913. https://doi.org/10.51594/csitrj.v6i11.2164

Dosunmu, A. A., & Ogundele, P. O. (2025c). Security orchestration and automation models for accelerating incident detection and response. Computer Science and IT Research Journal, 6(11), 878-894. https://doi.org/10.51594/csitrj.v6i11.2163

Eboh, E. E., & Aliliele, C. (2025b). 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, 11(2), 3969-4010. https://doi.org/10.32628/CSEIT25113398

Eboh, E. E., Aliliele, C., & Odihi, F. (2025). Advances in financial governance and accountability systems in small and medium enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2223-2245. https://doi.org/10.62225/2583049X.2025.5.6.6013

Edivri, J., & Oteri, O. (2022). 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, 8(4), 826-845.

Edivri, J., & Oteri, O. (2024). A conceptual KPI-driven decision and optimization framework for IT service delivery, portfolio performance, and adoption. Gyanshauryam, International Scientific Refereed Research Journal, 7(1), 167-187. https://doi.org/10.32628/GISRRJ246643

Ekechi, N. V., Anunagba, C. O., & Ozowara, D. E. (2022). Advances in financial forensics techniques for detecting cyber-enabled fraud in telemedicine services. Shodhshauryam, International Scientific Refereed Research Journal, 5(1), 428-450.

Elebe, O., & Anunagba, C. O. (2025). Responsible artificial intelligence in IT auditing through evidence validation, human oversight, and regulatory compliance. International Journal of Technology, Health and Sustainability, 1(2), 310-328.

Elebe, O., Hammed, N. I., Omoegun, G. O., Fadayomi, O., & Bello, A. D. (2023). An advanced machine learning model for detecting synthetic identity fraud in e-commerce platforms [Preprint]. ResearchGate.

European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). *Official Journal of the European Union, L 333*.

Ezeako, R., Okoli, I. E., Uzondu, C. S., & Ibeh, A. V. (2019). Relationship banking performance: A conceptual framework for portfolio growth and profitability acceleration. International Journal of Engineering Technology Research & Management, 3(11), 132-151.

Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., Okoruwa, P. O., & Akeju, B. (2019). Risk-based cybersecurity assurance and data availability: Limitations, advances and future research opportunities. Iconic Research and Engineering Journals, 2(12), 602-617. https://doi.org/10.64388/IREV2I12-1713779

Fadayomi, O., Bello, A. D., Elebe, O., Hammed, N. I., & Omoegun, G. O. (2021). An integrated cybersecurity and anti-money laundering governance framework for financial crime prevention [Preprint]. ResearchGate.

Fadayomi, O., Bello, A. D., Elebe, O., Hammed, N. I., & Omoegun, G. O. (2024). An adaptive fraud risk scoring model for real-time transaction monitoring at scale. IIARD International Journal of Banking and Finance Research, 10(10), 212-230.

Fadero, S., Jooda, D., Oyesiji, S. O., & Nwakamma, S. (2020). Business continuity and disaster recovery preparedness in African financial services: Lessons from the COVID-19 pandemic. Iconic Research and Engineering Journals, 3(9), 525-544. https://doi.org/10.64388/IREV3I9-1722620

Fadero, S., Jooda, D., Oyesiji, S. O., & Nwakamma, S. (2025). IT services decoupling after mergers, acquisitions, and ownership transitions: A framework for secure infrastructure separation. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2471-2485.

Fadero, S., Nwakamma, S., Jooda, D., & Oyesiji, S. O. (2021). Cyber risk management maturity in Nigeria's insurance sector: An assessment against the NAICOM and NDPR regulatory landscape. Iconic Research and Engineering Journals, 5(2), 401-420. https://doi.org/10.64388/IREV5I2-1722621

Fobellah, A. N. (2025a). 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, 16(2), 17-22. https://doi.org/10.30574/ijsra.2025.16.2.2273

Fobellah, A. N. (2025b). Navigating digital transformation: Auditing artificial intelligence-powered financial systems: A conceptual review. International Journal of Science and Research Archive, 16(2), 23-28. https://doi.org/10.30574/ijsra.2025.16.2.2274

Fobellah, A. N. (2025c). Unintended consequences of financial regulations: A study of corporate compliance burdens: A conceptual review. International Journal of Science and Research Archive, 16(2), 29-34. https://doi.org/10.30574/ijsra.2025.16.2.2275

Garcia-Molina, H., & Salem, K. (1987). Sagas. In *Proceedings of the 1987 ACM SIGMOD International Conference on Management of Data* (pp. 249 to 259). ACM.

Ghosh, D., Sharman, R., Rao, H. R., & Upadhyaya, S. (2007). Self-healing systems: Survey and synthesis. *Decision Support Systems*, *42*(4), 2164 to 2185.

Helland, P. (2012). Idempotence is not a medical condition. *Communications of the ACM, 55*(5), 56 to 65.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75 to 105.

Huebscher, M. C., & McCann, J. A. (2008). A survey of autonomic computing: Degrees, models, and applications. *ACM Computing Surveys*, *40*(3), Article 7.

Idika, C. N., Salami, E. O., Ijiga, O. M., & Enyejo, L. A. (2021). 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, 7(4).

Isiekwu, C. P., Oluwo, K., & Dada, T. (2025). 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, 5(6), 2104-2116.

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review, 10*(1 to 2), 18 to 26.

Jimoh, H. O., & Ahmed, M. O. (2024). Analyzing Network Time Protocol (NTP) based amplification DDoS attack and its mitigation techniques. Journal of Digital Innovations and Contemporary Research in Science, Engineering and Technology, 12(2), 17-24. https://doi.org/10.22624/AIMS/DIGITAL/V11N2P2x

Jimoh, H. O., Abolle-Okoyeagu, C. J., Ahmed, M. O., & Lawal, N. O. (2023). Advancing security in IoT-driven critical infrastructure: A focus on smart transportation system. American Journal of Engineering Research, 12(12), 33-46.

Jimoh, H. O., Ahmed, M. O., & Fagbade, M. O. (2023). The role of frameworks in cybersecurity governance. Journal of Behavioural Informatics, Digital Humanities and Development Research, 9(4), 7-16. https://doi.org/10.22624/AIMS/BHI/V9N4P2

Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. *Computer*, *36*(1), 41 to 50.

Krebs, R., Momm, C., & Kounev, S. (2012). Architectural concerns in multi-tenant SaaS applications. In *Proceedings of the 2nd International Conference on Cloud Computing and Services Science (CLOSER)* (pp. 426 to 431).

Kumuyi, O., Akeju, B., Uzoka, E., & Ozowara, D. E. (2023). Framework for blockchain-based cross-border data exchange and regulatory transparency. International Journal of Multidisciplinary Futuristic Development, 4(1), 99-113.

Kumuyi, O., Uzoka, E., Akeju, B., & Ozowara, D. E. (2024b). Framework for privacy-focused digital identity verification supporting financial inclusion in Africa. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3150-3162. https://doi.org/10.62225/2583049X.2024.4.6.6005

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2018). Lessons learned from offline assessment of security-critical systems: The case of Microsoft Active Directory. Iconic Research and Engineering Journals, 2(6), 277-299. https://doi.org/10.64388/IREV2I6-1717205

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2022). Human-in-the-loop machine learning: A state of the art. Journal of Frontiers in Multidisciplinary Research, 3(1), 656-669. https://doi.org/10.54660/.JFMR.2022.3.1.656-669

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2023a). Active Directory attacks steps, types, and signatures. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2863-2874. https://doi.org/10.62225/2583049X.2023.3.6.6204

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2023b). An IT service management literature review: Challenges, benefits, opportunities, and implementation practices. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2875-2889. https://doi.org/10.62225/2583049X.2023.3.6.6205

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2024). Integrated network and security operation center: A systematic analysis. International Journal of Multidisciplinary Futuristic Development, 5(1), 65-80. https://doi.org/10.54660/IJMFD.2024.5.1.65-80

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2025). 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, 6(6), 1361-1375. https://doi.org/10.54660/.IJMRGE.2025.6.6.1361-1375

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2019). Implementation of Active Directory for efficient management of enterprise networks. Iconic Research and Engineering Journals, 3(4), 608-627. https://doi.org/10.64388/IREV3I4-1717206

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2022). Navigating digital transformation: Best practices for cloud migration strategies in the enterprise. Journal of Frontiers in Multidisciplinary Research, 3(1), 643-655. https://doi.org/10.54660/.JFMR.2022.3.1.643-655

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2023a). A comprehensive survey on ServiceNow for IT service management. International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), 1532-1545. https://doi.org/10.54660/.IJMRGE.2023.4.6.1532-1545

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2023b). 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, 3(6), 2890-2904. https://doi.org/10.62225/2583049X.2023.3.6.6206

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2024). Keeping humans in the loop: Human-centered automated annotation with generative AI. International Journal of

Multidisciplinary Futuristic Development, 5(1), 81-95. https://doi.org/10.54660/IJMFD.2024.5.1.81-95

Lawal, O. A., & Oduleye, T. E. (2019b). Conceptualizing data driven executive decision systems for strategic financial planning. Iconic Research and Engineering Journals, 3(3).

Lawal, O. A., & Oduleye, T. E. (2023b). Behavioral financial analytics: A conceptual model for explaining enterprise performance. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2590-2604.

MacInnis, D. J. (2011). A framework for conceptual contributions in marketing. *Journal of Marketing, 75*(4), 136 to 154.

Mayo, W., Ogbole, J. I., Okoruwa, P. O., & Babatope, O. M. (2021). 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, 7(5), 416-440. https://doi.org/10.32628/IJSRCSEIT

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Oluoha, O. M. (2018). A conceptual framework for legal and ethical risk modeling in enterprise data protection governance systems. Iconic Research and Engineering Journals, 2(2), 207-226. https://doi.org/10.64388/IREV2I2-1714911

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2020). A review of identity and access management integration strategies in hybrid and multi cloud environments. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 795-810. https://doi.org/10.54660/.IJMRGE.2020.1.5.795-810

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2021a). A conceptual framework for risk based business intelligence architecture in financial technology platforms. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 731-746. https://doi.org/10.54660/.IJMRGE.2021.2.6.731-746

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2021b). 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, 7(5), 468-496. https://doi.org/10.32628/CSEIT217565

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2022). A conceptual framework for AI enabled IT general controls and SOX audit automation processes. Gyanshauryam, International Scientific Refereed Research Journal, 5(5), 384-414. https://doi.org/10.32628/GISRRJ2256239

Mbonu, I. S., Aliliele, C., Uzoka, E., & Oluoha, O. M. (2019). A review of comparative data protection regulations and secure cloud implementation strategies across jurisdictions. Iconic Research and Engineering Journals, 2(9), 482-501. https://doi.org/10.64388/IREV2I9-1714912

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2020a). A conceptual framework for agile supply chain digital transformation with embedded IT risk and ISO compliance controls. Iconic Research and Engineering Journals, 3(11), 566-593. https://doi.org/10.64388/IREV3I11-1714916

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2020b). Advances in infrastructure as code governance for secure terraform based enterprise cloud deployments. International

Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 811-828. https://doi.org/10.54660/.IJMRGE.2020.1.5.811-828

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2021). A review of VoIP forensic analytics models for financial fraud detection and regulatory compliance monitoring. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 711-730. https://doi.org/10.54660/.IJMRGE.2021.2.6.711-730

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2022a). 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, 8(1), 589-623. https://doi.org/10.32628/CSEIT25442

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2022b). Advances in cloud identity and access governance optimization in large scale AWS enterprise environments. Shodhshauryam, International Scientific Refereed Research Journal, 5(3), 403-438. https://doi.org/10.32628/SHISRRJ225490

Mbonu, I. S., Iwuanyanwu, U., Uzoka, E., & Oluoha, O. M. (2019). Advances in enterprise log analytics and automated incident response architectures using Python and SIEM platforms. Iconic Research and Engineering Journals, 3(2), 1000-1019. https://doi.org/10.64388/IREV3I2-1714915

Medon, J. J., & Oduleye, T. E. (2022). A comprehensive financial reporting model for strengthening compliance and organizational accountability systems. International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), 768-777.

Mensah, K. O., Pedro, O., Kinyanjui, A., Okoli, I., & Agboada, P. (2019). A review of capital adequacy frameworks and risk weighted asset optimization in modern banking systems. Iconic Research and Engineering Journals, 3(6), 731-768. https://doi.org/10.64388/IREV3I6-1723267

Notaro, P., Cardoso, J., & Gerndt, M. (2021). A survey of AIOps methods for failure management. *ACM Transactions on Intelligent Systems and Technology, 12*(6), Article 81.

Nwakamma, S., Ojukwu, J., & Oyesiji, S. O. (2024a). LLM-as-a-judge for automated model governance: A review of methods, biases, and release-gating practices. World Journal of Innovation and Modern Technology, 8(6), 185-216. https://doi.org/10.56201/wjimt.v8.no6.2024.pg185.216

Nwakamma, S., Ojukwu, J., & Oyesiji, S. O. (2024b). Securing agentic AI enterprise workflows against prompt injection, tool poisoning, memory manipulation, and excessive agency threats. World Journal of Innovation and Modern Technology, 8(6), 217-248. https://doi.org/10.56201/wjimt.v8.no6.2024.pg217.248

Nygard, M. T. (2018). *Release it! Design and deploy production-ready software* (2nd ed.). Pragmatic Bookshelf.

Odejobi, O. D., & Ahmed, K. S. (2018b). Performance evaluation model for multi-tenant Microsoft 365 deployments under high concurrency. IRE Journals, 1(11), 92-107.

Odejobi, O. D., Hammed, N. I., & Ahmed, K. S. (2019). Approximation complexity model for cloud-based database optimization problems. IRE Journals, 2(9), 1-10.

Odejobi, O. D., Okonkwo, C. S., Ahiaeke Patrick, M. C., Okeke, O. T., & Mayo, W. (2025). AI-augmented secure software engineering: Leveraging deep learning for autonomous threat detection and mitigation. International Journal of Engineering and Modern Technology, 11(12), 101-121. https://doi.org/10.56201/ijemt.vol.11.no12.2025.pg101.121

Oduleye, T. E., & Medon, J. J. (2023b). A quantitative model for measuring the strategic impact of financial analysis on enterprise growth. International Journal of Advanced Multidisciplinary Research and Studies, 3(1), 1663-1672. https://doi.org/10.62225/2583049X.2023.3.1.5334

Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., & Akeju, B. (2021). Conceptual model for identity-centric zero trust architecture in enterprise security governance. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 393-415. https://doi.org/10.32628/IJSRCSEIT217562

Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., & Abolaji, T. O. (2025). Security analytics and digital forensics for enterprise risk management, advances and practical implications. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2017-2028.

Ojukwu, J., Oyesiji, S. O., & Nwakamma, S. (2023). 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, 9(5), 193-228. https://doi.org/10.56201/ijcsmt.v9.no5.2023.pg193.228

Ojukwu, J., Oyesiji, S. O., & Nwakamma, S. (2025). 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, 11(12), 232-263. https://doi.org/10.56201/ijcsmt.vol.11.no12.2025.pg232.263

Okafor, C. M., Farounbi, B. O., Adesanya, O. S., & Akinola, A. S. (2024). 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, 10(4), 1050-1071.

Okafor, C. M., Osuji, V. C., & Dako, O. F. (2021). 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, 2(6), 485-504.

Okafor, C. M., Osuji, V. C., & Dako, O. F. (2024). Harmonizing risk governance, technology infrastructure, and compliance frameworks for future-ready banking systems. International Journal of Scientific Research in Humanities and Social Sciences, 1(1), 316-337.

Okoli, I., Agboada, P., Kinyanjui, A., Akintobi, A., & Pedro, O. (2025). Enterprise CRM technology adoption and revenue growth analytics in financial services firms. International Journal of Science, Technology and Society, 9(1), 31-60.

Okoli, I., Kinyanjui, A., Mensah, K. O., Agboada, P., & Pedro, O. (2022). 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, 8(5), 851-889. https://doi.org/10.32628/CSEIT23902204

Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., & Akeju, B. (2024). Enterprise cybersecurity trends and threat evolution, advances and emerging research directions. Global Multidisciplinary Perspectives Journal, 1(6), 194-204. https://doi.org/10.54660/GMPJ.2024.1.6.194-204

Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., Ogbole, J. I., & Abolaji, T. O. (2020). 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, 7(5), 371-389.

Okoruwa, P. O., Fadayomi, O., Bello, A. D., Elebe, O., Hammed, N. I., & Omoegun, G. O. (2025). An artificial intelligence-driven financial crime investigation framework for analyst decision support. International Journal of Multidisciplinary Research and Growth Evaluation, 6(6).

Okwesa, I. J., Ashore-Onisemo, F., Oyesiji, S. O., & Abdulmalik, A. U. (2024). Predictive risk analytics for early-warning systems in enterprise technology estates. Shodhshauryam, International Scientific Refereed Research Journal, 7(6), 327-386. https://doi.org/10.32628/SHISRRJ24797

Olagunju, E. O., Edivri, J., & Oteri, O. (2022). Predictive capacity planning and resource utilization forecasting models for multi program and multi stakeholder IT portfolios. Shodhshauryam, International Scientific Refereed Research Journal, 5(3), 336-356.

Olagunju, E. O., Edivri, J., & Oteri, O. (2023). A conceptual governance model for change, incident, and problem management in mission-critical enterprise IT environments. Gyanshauryam, International Scientific Refereed Research Journal, 6(6), 365-384.

Olagunju, E. O., Edivri, J., & Oteri, O. (2024). Applied performance optimization frameworks for managing high-demand enterprise technology programs and system rollouts. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3059-3070. https://doi.org/10.62225/2583049X.2024.4.6.5915

Olagunju, E. O., Oteri, O., & Edivri, J. (2025). An operational reliability and service assurance framework for enterprise IT systems supporting large user populations. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2117-2128. https://doi.org/10.62225/2583049X.2025.5.6.5916

Olaogun, B. O., Adesuyi, M. O., Akomolafe, O., Ndukwe, V. U., & Sakyi, J. K. (2023). Regulatory compliance adaptation model for cross-border payment product redesign. International Journal of Advanced Multidisciplinary Research and Studies, 3(1), 1651-1662. https://doi.org/10.62225/2583049X.2023.3.1.5279

Olaogun, B. O., Adesuyi, M. O., Akomolafe, O., Ndukwe, V. U., & Sakyi, J. K. (2025). Macroeconomic impact model for blockchain-enabled payment adoption in emerging economies. International Journal of Multidisciplinary Research and Growth Evaluation, 6(6), 835-853. https://doi.org/10.54660/.IJMRGE.2025.6.6.835-853

Oluwo, K., Bola-Sadipe, D., & Aliliele, C. (2025). Conceptual framework for data analytics driven financial decision making in banking sector organizations. Shodhshauryam, International Scientific Refereed Research Journal, 8(5), 259-302. https://doi.org/10.32628/SHISRRJ258529

Oluwo, K., Dada, T., & Isiekwu, C. P. (2024). Transforming insurance underwriting with machine learning: A review and application cases. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3008-3019.

Ominyi, M. (2020). Developing a conceptual framework for post-merger compliance integration in multi-jurisdictional banking transaction. IIARD International Journal of Banking and Finance Research, 6(3), 78-95. https://doi.org/10.56201/ijbfr.vol.6.no3.2020.pg78.95

Ominyi, M. (2021). Toward a conceptual framework for embedding privacy by design in corporate restructuring and transaction structuring. Journal of Accounting and Financial Management, 7(5), 152-173. https://doi.org/10.56201/jafm.vol.7.no5.2021.p152.173

Ominyi, M., & Anichukwueze, C. C. (2020). A review of regulatory clearance frameworks for cross-border mergers and acquisitions in African financial markets. Journal of Accounting

and Financial Management, 6(4), 73-99. https://doi.org/10.56201/jafm.vol.6.no4.2020.pg73.99

Ominyi, M., & Anichukwueze, C. C. (2021). A systematic review of anti-money laundering and anti-bribery compliance regimes across emerging and developed markets. International Journal of Economics and Financial Management, 6(2), 89-118. https://doi.org/10.56201/ijefm.v6.no2.2021.pg89.118

Ominyi, M., & Anichukwueze, C. C. (2022a). A conceptual framework for harmonizing data protection compliance across GDPR, NDPR, and United States privacy regimes. International Journal of Social Sciences and Management Research, 8(5), 148-174. https://doi.org/10.56201/ijssmr.v8.no5.2022.pg148.174

Ominyi, M., & Anichukwueze, C. C. (2023). A review of algorithmic accountability and model risk management approaches in financial services. Journal of Accounting and Financial Management, 9(12), 218-238. https://doi.org/10.56201/jafm.v9.no12.2023.pg218.238

Ominyi, M., & Anichukwueze, C. C. (2024). Conceptualizing responsible AI governance structures for automated decision systems in regulated industries. International Journal of Social Sciences and Management Research, 10(11), 403-430. https://doi.org/10.56201/ijssmr.v10.no11.2024.pg.403.430

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2024a). Developing a conceptual framework for AI-assisted compliance monitoring and anomaly detection in high-volume transaction environments. World Journal of Innovation and Modern Technology, 8(6), 204-228. https://doi.org/10.56201/wjimt.v8.no6.2024.pg204.228

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2024b). A systematic review of organizational readiness for the EU Artificial Intelligence Act in multinational enterprises. World Journal of Innovation and Modern Technology, 8(6), 185-203. https://doi.org/10.56201/wjimt.v8.no6.2024.pg185.203

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2025a). A conceptual framework for multi-agent AI quality control in the review of regulated documents. International Journal of Social Sciences and Management Research, 11(8), 534-557. https://doi.org/10.56201/ijssmr.vol.11no8.2025.pg534.557

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2025c). Reviewing legal privilege and confidentiality challenges in enterprise deployment of large language models. Journal of Law and Global Policy, 10(3), 150-176. https://doi.org/10.56201/jlgp.vol.10.no3.2025.pg150.176

Onche, V. O., & Ogbonna, C. S. (2022). Password practices, authentication behaviour, and data-protection compliance among secretarial professionals in higher education. International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), 1001-1015. https://doi.org/10.54660/.IJMRGE.2022.3.6.1001-1015

Onche, V. O., Adegbite, M. P., & Ogbonna, C. S. (2023). BYOD adoption and information-security risk in university administrative offices: Evidence from Nigerian federal universities. International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), 1549-1563. https://doi.org/10.54660/.IJMRGE.2023.4.6.1549-1563

Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2020). Information-security awareness and records confidentiality in Nigerian university registries: A behavioural assessment. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1032-1044. https://doi.org/10.54660/.IJMRGE.2020.1.5.1032-1044

Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2024). Effectiveness of cybersecurity awareness training on insider-threat behavior among university administrators: An integrative academic review. International Journal of Computer Science and Mathematical Theory, 10(2), 117-144. https://doi.org/10.56201/ijcsmt.v10.no2.2024.pg117.144

Oshoba, T. O., Hammed, N. I., & Odejobi, O. D. (2019). Secure identity and access management model for distributed and federated systems. IRE Journals, 3(4), 550-567.

Oshoba, T. O., Hammed, N. I., & Odejobi, O. D. (2020). Blockchain-enabled compliance and audit trail model for cloud configuration management. Journal of Frontiers in Multidisciplinary Research, 1(1), 193-201.

Osuji, V. C., Okafor, C. M., & Dako, O. F. (2021). Engineering high-throughput digital collections platforms for multibillion-dollar payment ecosystems. Shodhshauryam, International Scientific Refereed Research Journal, 4(4), 315-335.

Oteri, O., & Chibwaye, I. P. (2025). Advances and conceptual models in enterprise level change management analytics for large scale organizational system transitions. Gyanshauryam, International Scientific Refereed Research Journal, 8(5), 177-211.

Oteri, O., & Edivri, J. (2024). Applied performance optimization frameworks for managing high-demand enterprise technology programs and system rollouts. Gyanshauryam, International Scientific Refereed Research Journal, 7(1), 188-210.

Oteri, O., Olagunju, E. O., & Edivri, J. (2025). Conceptual models for cloud-based IT service management architecture and orchestration using ServiceNow platforms. Shodhshauryam, International Scientific Refereed Research Journal, 8(6), 185-203.

Oyesiji, S. O., Nwakamma, S., & Ojukwu, J. (2024). A conceptual framework for context-aware data curation in fine-tuning pipelines. International Journal of Engineering and Modern Technology, 10(11), 197-228. https://doi.org/10.56201/ijemt.v10.no11.2024.pg197.228

Ozowara, D. E., Adebayo, A., & Anunagba, C. O. (2022). A systematic review of cybersecurity investments and their impact on healthcare financial performance. Shodhshauryam, International Scientific Refereed Research Journal, 5(1), 404-427.

Ozowara, D. E., Adebayo, A., & Anunagba, C. O. (2025). Advanced conceptual model for strengthening audit quality using data analytics across financial institutions. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2246-2268. https://doi.org/10.62225/2583049X.2025.5.6.6050

Ozowara, D. E., Anunagba, C. O., & Adepoju, P. A. (2025). A review of ransomware economics and financial resilience strategies in hospital networks. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2284-2298. https://doi.org/10.62225/2583049X.2025.5.6.6052

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics, Part A, 30*(3), 286 to 297.

Peteranaba, S. F., Osinem, H. E., Eribenne, F., & Soyege, O. S. (2022). 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, 6(1), 60-84.

Prudential Regulation Authority. (2021). *PS6/21 Operational resilience: Impact tolerances for important business services*. Bank of England.

Psaier, H., & Dustdar, S. (2011). A survey on self-healing systems: Approaches and systems. *Computing*, *91*(1), 43 to 73.

Shittu, H., & Nabil, M. (2023). Smart supply chain management with attribute-based encryption access control. In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 198-204). IEEE. https://doi.org/10.1109/CCWC57344.2023.10099268

Shittu, H., Olagunju, F., & Shittu, M. A. (2024). Cyber physical resilience in digital substations: IoT enabled adaptive protection for secure DER integration. International Journal of Science, Architecture, Technology and Environment, 1(3), 81-99. https://doi.org/10.63680/ijsate032532.08

Shittu, M. A., Adeniji, I. O., Shittu, H., & Opara, I. S. (2022). Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems. Iconic Research and Engineering Journals, 6(3), 359-379. https://doi.org/10.64388/IREV6I3-1714041

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333 to 339.

Tonoyan, A., Dada, O., & Ayivi-Donkor, S. S. (2022b). Algorithmic process optimization and cost reduction: A review of simulation modeling and financial impact assessment. Journal of Accounting and Financial Management, 8(8), 139-169. https://doi.org/10.56201/jafm.vol.8.no8.2022.p139.169

Tonoyan, A., Dada, O., & Ayivi-Donkor, S. S. (2024a). Advances in supply chain resilience: Predictive models for vendor risk assessment and procurement cost optimization. International Journal of Social Sciences and Management Research, 10(11), 525-551. https://doi.org/10.56201/ijssmr.v10.no11.2024.pg.525.551

Tonoyan, A., Dada, O., & Ayivi-Donkor, S. S. (2024b). Real-time KPI tracking systems: A review of automated performance monitoring and data-driven decision making. World Journal of Innovation and Modern Technology, 8(6), 247-281. https://doi.org/10.56201/wjimt.v8.no6.2024.pg247.281

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, *4*(3), 356 to 367.

Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2021). Standardizing contract review workflows in enterprise legal operations: A systematic review. International Journal of Multidisciplinary Evolutionary Research, 2(2), 148-166. https://doi.org/10.54660/IJMER.2021.2.2.148-166

Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2022). Real-time compliance pipelines: A review of automated risk monitoring and enterprise data governance. International Journal of Multidisciplinary Futuristic Development, 3(2), 66-94. https://doi.org/10.54660/IJMFD.2022.3.2.66-94

Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2023). Advances in standardizing un-standardized compliance controls for high-volume non-traditional distribution networks. International Journal of Advanced Multidisciplinary Research and Studies, 3(6). https://doi.org/10.62225/2583049X.2023.3.6.6838

Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2025). Advances in automated governance: Mitigating operational and systemic risks in multi-country delivery networks. Gulf Journal of Advance Business Research, 3(12), 1626-1669. https://doi.org/10.51594/gjabr.v3i12.219

Uchechi, N., Ominyi, M., Uzougbo, N. S., & Jones, B. C. (2025). Advances in NLP-driven analytics for automated detection of regulatory liabilities in high-volume contracts. Research Journal of Pure Science and Technology, 8(8), 142-212. https://doi.org/10.56201/rjpst.vol.8.no8.2025.pg142.212

Ukadike, C. A. (2022). Advances in customer data platforms for emerging-market banking: Architecture, adoption, and customer trust. IIARD International Journal of Banking and Finance Research, 8(4), 67-87. https://doi.org/10.56201/ijbfr.v8.no4.2022.pg.67.87

Ukadike, C. A. (2024). Scaling B2B SaaS ventures: An integrated framework for multi-cloud optimization, distributed agile delivery, and investment readiness. World Journal of Finance and Investment Research, 8(5), 196-217. https://doi.org/10.56201/wjfir.v8.no5.2024.pg196.217

Upreti, M., & Oteri, O. (2023). Analytical model for optimizing cloud resource allocation through rightsizing and long-term usage forecasting. Gyanshauryam, International Scientific Refereed Research Journal, 6(1), 400-424.

Upreti, M., & Oteri, O. (2025). Security design model for resilient network architectures in large scale cloud computing platforms. Shodhshauryam, International Scientific Refereed Research Journal, 8(5), 84-104.

Uzondu, C. S., Ibeh, A. V., Alugwe, S., & Awulu, I. (2020). Corporate credit portfolio growth in emerging markets: A review of advances in credit decisioning and governance. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1279-1294. https://doi.org/10.54660/.IJMRGE.2020.1.5.1279-1294

Walawalkar, G., Adesuyi, M. O., Kalu, A., & Oduleye, T. E. (2025). Executive financial dashboards for real-time strategic oversight. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2042-2054.

Weyns, D. (2020). *An introduction to self-adaptive systems: A contemporary software engineering perspective*. Wiley.

Wikiri, M. (2021). Improving first-contact resolution in enterprise technology support: A workforce competency and service-quality framework. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 1212-1225. https://doi.org/10.54660/.IJMRGE.2021.2.6.1212-1225