Journal of Emerging Intelligence and Engineering Technologies

Research Article

Opportunities for Ethical AI Integration in Core Infrastructure Administration: Safety Boundaries and Control Frameworks for Autonomous DBAs

Evans Ighodalo[1,*], Ayinoluwa Kolawale[2], Chukwudera Obumneke Anunagba[3], Oluranti Ogundapo[4], Harouna Wendpanga Yann Christian Sankara[5], Emmanuel Chukwuma Okeke[6], Toussida Fatah Tanguy Minoungou[7], Aisha Ife Abdulwahab[8]

[1]EviCore Healthcare, United States; Email: ighodaloevans4@gmail.com

[2] Underdog Fantasy, USA; Email: ayinoluwak@gmail.com

[3]Barclays, Whippany, New Jersey, USA; Email: chiokemuo@gmail.com

[4]GTA, Nokia–Verizon Wireless Project, Canada; Email: ogundapooluranti@gmail.com

[5]State of Missouri, Office of Administration, Information Technology Services Division, Jefferson City, Missouri, USA; Email: christiansankara@gmail.com

[6]Arcesium, USA; Email: emmanuelokeke68@gmail.com

[7]Nationwide, Columbus, Ohio, USA; Email: tanguyminoungou@gmail.com

[8]Cummins Inc., Indiana, USA; Email: ifewahab@gmail.com

*Corresponding author: ighodaloevans4@gmail.com

DOI: https://doi.org/10.66592/mduc9e

Abstract

Database administration is one of the oldest and most consequential disciplines in enterprise computing. Databases hold the records on which banks, hospitals, utilities, governments and commercial platforms depend, and the people who administer them have traditionally held some of the most powerful privileges in any organisation. Between 2017 and 2026 the discipline moved from rule-based self-tuning features toward agentic systems built on large language models (LLMs) that can diagnose incidents, rewrite queries, apply patches and change schemas with little or no human involvement. Major vendors now market platforms that observe, reason and act on production databases, and practitioners increasingly describe the role of the human DBA as one of orchestrating AI agents rather than executing scripts.

This paper examines the opportunities that autonomous database administration offers for core infrastructure and the ethical, operational and regulatory risks it introduces. Methodologically, it combines an integrative literature synthesis of 259 sources, including 238 seed studies screened from a consolidated multi-portfolio corpus of 1,056 records, with a design science approach to building and analytically evaluating a conceptual model. Drawing on the documented July 2025 incident in which an AI coding agent deleted a live production database during a declared code freeze, the OWASP Top 10 for Agentic Applications, the European Union Artificial Intelligence Act and the United States NIST AI Agent Standards Initiative, the paper argues that the central design problem is not whether AI should administer databases but how authority should be bounded, delegated, observed and revoked. It proposes three contributions: (1) a taxonomy of database actions classified by reversibility and blast radius; (2) a six-level Autonomy Ladder for Database Operations (ALDO) that ties levels of independence to evidence of reliability; and (3) a Layered Control Framework comprising policy, identity, execution, verification and accountability layers. These elements are integrated into a conceptual model with five propositions. The paper discusses the model against the literature and the regulatory environment, sets out theoretical, practical and policy implications, and closes with limitations and an agenda for future research.

Keywords: Autonomous Databases; Agentic AI; Database Administration; AI Safety; Human Oversight; Least Privilege; Critical Infrastructure; AI Governance; EU AI Act; Control Frameworks; Conceptual Model; Design Science

Received: 08 October 2026
Revised: 28 October 2026
Accepted: 01 November 2026
Published: 10 November 2026

Copyright: © 2026 by the authors. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) license (https://creativecommons.org/licenses/by-nc/4.0/).

Citation: Ighodalo, E.; Kolawale, A.; Anunagba, C.O.; Ogundapo, O.; Sankara, H.W.Y.C.; Okeke, E.C.; Minoungou, T.F.T.; Abdulwahab, A.I. Opportunities for Ethical AI Integration in Core Infrastructure Administration: Safety Boundaries and Control Frameworks for Autonomous DBAs. *J. Emerg. Intell. Eng. Technol.* 2026, 3(2), 98–135. https://doi.org/10.66592/03.02.XX

1. Introduction

For most of its history, database administration has been a craft practised by specialists who combine deep knowledge of storage engines, query optimisers and recovery mechanisms with an institutional memory of how particular systems behave under load. The DBA decides when to patch, which indexes to build, how to respond when replication lags and, in the worst moments, how to restore data after corruption or deletion. Because these decisions touch the system of record, mistakes can be catastrophic and are frequently irreversible.

Automation in this field is not new. Query optimisers, automatic memory management and storage-level tuning have existed for decades, and Oracle introduced what it marketed as the first autonomous database in 2017, promoting it as self-driving, self-securing and self-repairing. What changed between 2023 and 2026 is the arrival of general-purpose reasoning systems that can be connected to databases through tools and protocols and that can plan multi-step remediation without a predefined playbook. In 2026, IBM introduced Db2 Genius Hub, describing it as a platform intended to make Db2 a database that can observe, reason and act with minimal human intervention, while independent vendors offer platforms of specialised agents for cloud data warehouses.

This shift creates a genuine opportunity. Database estates have grown faster than the supply of experienced administrators, on-call fatigue is widespread, and many outages are caused by routine human error. At the same time, granting a probabilistic system the privileges of a senior DBA concentrates enormous power in software whose behaviour cannot be fully specified in advance. The July 2025 incident in which an AI agent on the Replit platform deleted a live production database during an explicit code freeze, and then gave misleading accounts of what had happened, illustrates the failure mode in concrete terms.

This direction is consistent with research on digital transformation, which finds that automation, analytics and process redesign improve operational performance when they are introduced deliberately (Agboada et al., 2018; Nnabueze et al., 2023; Obukadata et al., 2021a; Sakyi et al., 2024b). Studies of AI adoption readiness stress phased implementation, stakeholder alignment and organisational capability as preconditions for value (Alieme et al., 2023; Alieme, Sule, & Obukadata, 2025b; Dawud, 2026b; Ukadike, 2025), while work on AI-supported decision-making shows how these systems are moving from analysis toward action (Ilodigwe & Adesemoye, 2025a; Shah et al., 2025; Walawalkar et al., 2026). Commentators have also argued that the arrival of autonomous agents demands new, human-centred ways of designing the interfaces through which people direct them (Adams, 2023; Ogundairo & Ayivi-Donkor, 2024b).

The research question addressed in this paper is therefore practical and normative at once: **under what boundaries and controls can autonomous AI be integrated ethically into the administration of databases that function as core infrastructure?** The remainder of this section states the objectives and scope of the study and synthesises the relevant literature. Section 2 describes the research method. Section 3 presents and discusses the results: the conceptual model, its evaluation against the illustrative case and the literature, its ethical and regulatory dimensions, its implications, and the limitations of the study and directions for future research. Section 4 concludes.

1.1 Research Objectives and Contributions

The paper pursues three objectives: (1) to synthesise the multidisciplinary literature relevant to autonomous administration of core data infrastructure; (2) to develop a conceptual model that specifies how authority should be bounded, delegated, observed and revoked; and (3) to derive implications for practitioners,

vendors and policymakers. Its contributions are an action taxonomy based on reversibility and blast radius, the Autonomy Ladder for Database Operations (ALDO), a five-layer control framework, and a set of testable propositions that link these elements to safe outcomes.

1.2 Scope and Definitions

In this paper, an **autonomous DBA** refers to any software agent that can observe the state of a database system and initiate changes to it without a human authorising each individual action. This includes vendor-native autonomous features, LLM-based agents connected through tool interfaces, and multi-agent systems that divide responsibilities such as diagnosis, tuning and security. **Core infrastructure administration** refers to the management of data platforms whose failure would materially disrupt essential services, financial integrity, public administration or the safety of persons. A **control framework** is the combination of technical mechanisms, organisational processes and accountability structures that constrain what an autonomous system can do and that make its actions observable, attributable and reversible.

1.3 Literature Synthesis

This subsection synthesises the literature in four parts: the evolution of autonomous database administration, the opportunities it offers, the risks it introduces, and the gaps that motivate the conceptual model.

1.3.1 The Evolution of Autonomous Database Administration

From Self-Tuning to Self-Driving

Early autonomy in database systems took the form of bounded, deterministic features: cost-based optimisers, automatic statistics collection, advisors that recommended indexes, and memory managers that resized buffers. Research systems pushed this further. Work on self-driving database management systems, such as Peloton, proposed databases that forecast workload and adapt their physical design continuously (Pavlo et al., 2017). OtterTune applied machine learning to configuration tuning across many knobs (Van Aken et al., 2017). These systems were autonomous in a narrow sense: they operated inside well-defined action spaces whose effects were measurable and generally reversible.

Commercial autonomous databases built on this tradition. Oracle's Autonomous Database, for example, automates provisioning, tuning, scaling, patching and failure recovery, and positions the elimination of manual human labour and human error as a core benefit. Crucially, the vendor controls both the engine and the automation, so the action space is engineered and tested together with the system.

The Agentic Turn (2023 to 2026)

The second wave is qualitatively different. LLM-based agents are general reasoners connected to databases through tools. They can read telemetry, form hypotheses, write SQL, call operating-system commands and iterate on failures. The research literature now describes DBA agents as LLM-powered systems that orchestrate tasks including schema design, query optimisation and incident diagnosis, with the primary objective of end-to-end automation under minimal human oversight. Industry implementations follow similar patterns: IBM states that its agentic Db2 assistant is built on LangGraph to orchestrate multi-agent workflows through stateful, graph-based execution, and practitioner reports describe Oracle diagnostic agents equipped with predefined tools that run read-only SQL.

Two features of the agentic turn matter for safety. First, the action space is open: an agent with a general SQL or shell tool can in principle do anything its credentials allow. Second, behaviour is emergent from model reasoning rather than specified in code, which means that testing cannot exhaustively enumerate what the system will do. These features make the governance problem resemble the problem of supervising a highly capable but unproven human administrator more than the problem of validating a deterministic tool.

Adjacent domains offer useful evidence. Multi-agent coordination in autonomous mobile robot fleets and agentic supply chain orchestration shows both the productivity of delegated autonomy and the need for explicit guardrails (Akanbi & Sunday, 2025; Akanbi et al., 2025; Ogundairo, 2025), and continuously learning defence systems for legacy SCADA and operational technology illustrate autonomy operating on critical infrastructure (Amadi, 2025; Ojukwu et al., 2023). Work on structuring requirements for AI-enabled process automation (Alieme et al., 2024; Alieme, Sule, & Obukadata, 2025a), on characterising LLM failure modes and curating fine-tuning data (Nwakamma, Oyesiji, et al., 2026; Oyesiji et al., 2024), and on staged validation through continuous integration and portable runtimes (Ndupu et al., 2026; Ojukwu et al., 2025; Oyesiji, Anunagba, et al., 2026; Quainoo et al., 2025b) is directly relevant to how DBA agents should be specified and tested.

The Changing Role of the Human DBA

Practitioner literature in 2026 consistently frames the change as a transformation of the profession rather than its elimination. Commentators describe the AI DBA as a role that orchestrates AI agents rather than running manual scripts, and argue that experienced professionals remain essential for judgement, business context and accountability. This framing has ethical significance, which Section 3.3 returns to: the quality of human oversight depends on retaining people with genuine expertise, yet automation tends to erode precisely the hands-on experience from which that expertise grows (Bainbridge, 1983).

Studies of enterprise IT operations similarly emphasise maturity models, KPI-driven service delivery and change management analytics as the institutional scaffolding within which automation must be governed (Anyanwu, 2019; Edivri & Oteri, 2024; Oteri & Chibwaye, 2025).

1.3.2 Opportunities for Ethical AI Integration

An ethical analysis that only catalogues risks is incomplete. There are strong moral and practical reasons to adopt autonomous administration where it can be done safely, because the status quo also causes harm: outages that block payments or hospital systems, breaches enabled by unpatched databases, and burnout among on-call staff. The following opportunities are the most significant.

Reliability and Reduced Human Error

A large share of database incidents stems from routine mistakes: a missed patch, a misconfigured parameter, a migration run against the wrong environment. Automation that executes well-tested procedures consistently, at any hour, can reduce this class of failure. Vendor-native self-repair features that detect node failures and fail over to standby systems without intervention already demonstrate this benefit at scale.

Faster Diagnosis and Mean Time to Recovery

Diagnosis is often the slowest phase of an incident because it requires correlating wait events, execution plans, logs and recent changes across several tools. Agents excel at this kind of correlation. Practitioners report read-only diagnostic agents that reduce investigations taking tens of minutes to seconds, while retaining a

human decision on the remedy. Diagnosis is also the lowest-risk area for autonomy, because it can be performed entirely with read access.

Related research supports these gains. Predictive capacity planning and performance optimisation models show how forecasting can prevent saturation before users notice it (Edivri & Oteri, 2022; Okwesa et al., 2024; Olagunju et al., 2022; Olagunju et al., 2024; Oteri & Edivri, 2024), and service assurance frameworks, real-time telemetry pipelines and automated KPI monitoring provide the observability on which autonomous diagnosis depends (Ajala, Sankara, Minoungou, et al., 2026; Ogbole, Okoruwa, Babatope, et al., 2021; Olagunju et al., 2025; Oteri & Edivri, 2026; Tonoyan et al., 2024b). The shift from reactive to predictive maintenance using machine learning (Komi & Adamolekun, 2021; Mayo et al., 2021; Olodo et al., 2026a; Sunday et al., 2020) and the use of digital twins and IoT condition monitoring for asset integrity (Asiedu & Quainoo, 2023b; Komi & Adeniji, 2023; Obetta et al., 2025a; Obetta et al., 2026; Shittu & Shittu, 2024) offer transferable models for anticipatory database operations.

Security Hygiene at Scale

Autonomous systems can continuously check configurations against baselines, detect privilege drift, flag anomalous access patterns and apply security patches within maintenance windows. For organisations with large estates and few specialists, including many public institutions and organisations in emerging markets, this may be the only practical way to achieve consistent security hygiene.

This opportunity is well supported. Work on continuous cloud misconfiguration monitoring, infrastructure-as-code governance and cloud identity governance shows how drift can be detected and corrected continuously (Aliliele et al., 2023a; Mbonu et al., 2020; Mbonu et al., 2020b; Mbonu et al., 2022b). Log analytics, security orchestration and AI-based threat detection accelerate response (Dosunmu & Ogundele, 2025c; Mbonu, Iwuanyanwu, et al., 2019; Odejobi et al., 2025), and continuous security validation models test whether controls actually work (Dosunmu & Ogundele, 2024a; Dosunmu & Ogundele, 2024c; Dosunmu & Ogundele, 2024d; Dosunmu & Ogundele, 2026b). Several authors argue specifically that critical infrastructure should move from periodic audit to continuous, AI-enabled control and posture management (Adebayo, Amadi, et al., 2025; Adegbite et al., 2024b; Aliliele et al., 2025a; Amadi et al., 2025a; Amadi, 2026; Mbonu et al., 2022).

Workforce Wellbeing and Knowledge Capture

Reducing night-time pages and repetitive toil improves the working lives of administrators. Agents that record their reasoning and store resolved incidents also create a searchable institutional memory, which can counteract the loss of knowledge when experienced staff leave.

Research on IT service management platforms, ERP and data migration, and the decoupling of IT services after organisational change underscores the value of structured operational knowledge during system transitions (Chibwaye & Oteri, 2023; Fadero et al., 2025; Ladapo, Dosunmu, et al., 2023b; Ladapo, Dosunmu, et al., 2024; Ladapo, Jooda, et al., 2023a; Oteri, Olagunju, & Edivri, 2025b).

Efficiency and Sustainability

Continuous right-sizing of compute and storage reduces both cost and energy use. When optimisation is transparent and bounded by policy, these savings can be pursued without compromising service levels.

Models for machine learning-based resource scaling, rightsizing and energy-efficient virtual machine placement (Ahmed & Odejobi, 2018b; Ahmed et al., 2019; Ahmed et al., 2020; Upreti & Oteri, 2023), for cloud-based database

optimisation and multi-tenant performance (Ahmed & Odejobi, 2018a; Odejobi & Ahmed, 2018b; Odejobi et al., 2019; Ukadike, 2024), and for cloud migration and data centre lifecycle management (Amayo et al., 2024a; Ladapo et al., 2025; Ladapo, Jooda, et al., 2022; Oteri, Olagunju, & Edivri, 2025a; Zhou et al., 2024) provide technical foundations for this kind of policy-bounded optimisation.

Table 1: Opportunity areas and their relative risk profile

Opportunity area	*Typical autonomous actions*	*Inherent risk*	*Suitability for early autonomy*
Observability and diagnosis	Read telemetry, correlate events, propose root cause	Low (read-only)	High
Performance tuning	Index recommendations, plan baselines, parameter changes	Moderate (reversible but can degrade service)	Medium, with canary testing
Capacity management	Scale compute and storage, archive cold data	Moderate (cost and availability effects)	Medium, within budget limits
Security hygiene	Baseline checks, patching, privilege reviews	Moderate to high (patch failure, lockout)	Medium, with maintenance windows
Schema and data change	DDL, migrations, bulk updates, deletions	High (often irreversible)	Low; human approval required
Recovery and failover	Restore, failover, point-in-time recovery	High (risk of data loss or split brain)	Low to medium; pre-approved runbooks only

Source: author's synthesis.

1.3.3 The Risk Landscape

Illustrative Case: The 2025 Production Database Deletion

The most widely cited failure of an autonomous agent with database access occurred in July 2025. During a multi-day experiment building an application with Replit's AI agent, the investor Jason Lemkin reported that the agent deleted a live production database. Reporting at the time stated that the agent had been told to freeze all changes and acted anyway, destroying records on roughly 1,200 executives and 1,200 companies. After the deletion, the agent produced outputs that did not match the actual state of the system, which complicated recovery. The OECD AI incident monitor classified the event as an AI incident on the basis that the system ignored freeze directives and caused harm to property.

The vendor's response is as instructive as the failure. Replit acknowledged that the same database was being used for preview, testing and production, and announced automatic separation of development and production databases and work on staging environments. In other words, the remedy was architectural, not a better prompt. Four lessons follow, and they shape the framework in this paper:

1. **Instructions are not controls.** A natural-language directive such as a code freeze is advisory to a model. It must be enforced by the environment, for example by revoking write credentials during the freeze.
2. **Environment separation is a safety boundary.** An agent that can reach production through the same path it uses for testing will eventually act on production by mistake.
3. **Agent self-reports cannot be trusted as evidence.** Verification of system state must come from independent telemetry, not from the agent describing its own work.

4. **Recoverability must exist before autonomy.** The harm was amplified because rollback was not immediately available; a one-click restore feature was added afterwards.

Taxonomy of Risks

Beyond this case, the risks of autonomous database administration can be grouped into six categories.

Recent studies reinforce these concerns. Research on securing agentic enterprise workflows examines prompt injection, tool poisoning, memory manipulation and excessive agency, alongside hallucination in retrieval-augmented systems and LLM-based release gating (Ajala, Sankara, Oyesiji, et al., 2026; Nwakamma et al., 2024a; Nwakamma et al., 2024b). Adversarial machine learning against AI-enabled operational technology, LLM-based processing of threat intelligence and crypto-agile migration show how the attack surface expands with AI adoption (Adebayo et al., 2022; Adebayo et al., 2026; Nwakamma, Ojukwu, et al., 2026), while work on privacy-preserving edge models and governance of AI-assisted enterprise platforms points toward mitigations (Badmus et al., 2025; Nwakamma et al., 2025).

- **Excessive agency.** OWASP identifies excessive functionality, excessive permissions and excessive autonomy as the root causes of agents performing damaging actions in response to unexpected, ambiguous or manipulated outputs. In the 2026 edition of the OWASP LLM Top 10, excessive agency rose from sixth to third place, the largest change in the list.
- **Goal hijacking and prompt injection.** Databases store untrusted text. An agent that reads a table comment, a log message or a customer record containing adversarial instructions may treat that content as a command. The OWASP Top 10 for Agentic Applications, released in December 2025, lists agent goal hijack as its first risk, alongside tool misuse, identity and privilege abuse, and memory poisoning.
- **Confabulation and state misreporting.** Models may describe actions they did not take or misreport outcomes, as occurred in the 2025 case. In administration, a false 'backup verified' message is more dangerous than no message.
- **Cascading and compounding failures.** Multi-agent systems can amplify an error: a tuning agent degrades performance, a capacity agent scales up in response, and a cost agent then throttles resources.
- **Privacy and confidentiality.** Diagnostic agents routinely see sensitive data in query results and samples. If that data is sent to an external model provider or stored in agent memory, it may breach data protection obligations.
- **Erosion of human competence.** As routine work disappears, administrators lose the practice needed to supervise the system or take over in a crisis, the well-documented irony of automation (Bainbridge, 1983).

The privacy risk is supported by research on data sensitivity classification, legal and ethical risk modelling, cross-border data governance, harmonisation of GDPR, NDPR and United States regimes, and data protection impact assessment (Aliliele et al., 2024a; Annan, 2022; Mbonu et al., 2018; Mbonu et al., 2022a; Mbonu, Aliliele, et al., 2019; Ominyi & Anichukwueze, 2022a). Healthcare studies show how secure architectures, documentation practices and governance frameworks protect clinical data (Afrihyia, Ojukwu, et al., 2024; Aliliele et al., 2024b; Ekechi et al., 2026; Nnaji & Akinlolu, 2024a; Nnaji & Akinlolu, 2026; Ogunwola & Alozie, 2026a; Peteranaba et al., 2022; Peteranaba et al., 2023a). Technical safeguards such as lakehouse data loss prevention, attribute-based encryption, blockchain-based exchange and privacy-focused identity verification

(Aliliele et al., 2025b; Kumuyi et al., 2023; Kumuyi et al., 2024b; Shittu & Nabil, 2023), and privacy by design in platform and mobile architectures (Badmus et al., 2022b; Badmus et al., 2024; Ominyi, 2021; Oyesiji, Ndupu, et al., 2026), offer controls that can be applied to agent data flows. The human dimension is addressed by research on security awareness, authentication behaviour, insider-threat training and administrative capability (Hussain & Adebayo, 2026; Onche & Ogbonna, 2022; Onche et al., 2020; Onche et al., 2023; Onche et al., 2024; Onche et al., 2026).

Table 2: Mapping risk categories to failure examples and primary mitigations

Risk category	*Database example*	*Primary mitigation*
Excessive agency	Agent with DBA role drops a table to 'clean up' a failed migration	Least-privilege, task-scoped credentials; action allowlists
Goal hijacking	Malicious text in a support ticket instructs the agent to grant access	Treat data as data; separate instruction and data channels; policy gate on privilege changes
State misreporting	Agent reports a restore succeeded when it failed	Independent verification from telemetry; signed execution receipts
Cascading failure	Tuning and scaling agents oscillate	Single change coordinator; rate limits; global circuit breaker
Privacy leakage	Query results containing personal data sent to an external model	Data masking; on-premise or customer-managed inference; retention limits
Competence erosion	No staff able to perform manual recovery	Scheduled manual drills; rotation; human-led game days

Source: author's synthesis drawing on OWASP (2025) and incident reporting.

Because an autonomous DBA is itself a privileged component, it inherits the wider threat landscape. Insider-threat modelling, security audit, cyber risk quantification and board-level performance measurement frame how such components should be assessed (Akeju et al., 2018; Dosunmu & Ogundele, 2019; Dosunmu & Ogundele, 2024b; Dosunmu & Ogundele, 2025b; Fadayomi et al., 2019). Intrusion detection, incident response, digital forensics and threat intelligence research describes how compromise is detected and contained (Dosunmu & Ogundele, 2020; Dosunmu & Ogundele, 2021; Dosunmu & Ogundele, 2022; Dosunmu & Ogundele, 2023; Ogbole et al., 2025; Okoruwa et al., 2024), and adversary simulation, deception and breach simulation provide methods for testing agents adversarially (Dosunmu & Ogundele, 2025a; Dosunmu & Ogundele, 2026a; Dosunmu & Ogundele, 2026c). Studies of firewall modernisation, integration risk during acquisitions, cloud network design and Active Directory attacks show how directory and network privileges become attack paths (Ladapo et al., 2018; Ladapo, Dosunmu, et al., 2023a; Ogunwola & Alozie, 2026b; Ogunwola et al., 2026; Upreti & Oteri, 2025).

The critical infrastructure literature is especially relevant. Machine learning and deep learning approaches to ICS and SCADA anomaly detection (Adebayo, Adegbite, et al., 2023; Adegbite et al., 2023; Amadi et al., 2025b) sit alongside governance work on NERC CIP compliance, IT and OT convergence, vulnerability management, cyber risk quantification and zero trust for operational technology (Adegbite et al., 2020; Adegbite et al., 2022; Adegbite et al., 2024a; Adegbite et al., 2025; Ahmed et al., 2021). Reviews of the legacy SCADA attack surface, national network resilience, digital substations and secure data exchange in power systems (Amadi et al., 2025c; Ogunwola &

Deborah, 2026; Shittu et al., 2022; Shittu et al., 2024), together with work on intrusion detection, cloud-native malware classification, IoT security, DDoS mitigation, governance frameworks and SD-WAN resilience (Ajagbe et al., 2025; Idika et al., 2021; Jimoh & Ahmed, 2024; Jimoh, Abolle-Okoyeagu, et al., 2023; Jimoh, Ahmed, et al., 2023; Ogunwola, 2026), show that agents operating on core infrastructure must be treated as potential attack paths as well as defenders.

1.3.4 Synthesis and Research Gaps

Read together, the literature supports three conclusions. First, there is strong evidence that automation and AI improve reliability, diagnosis, security hygiene and efficiency in IT and infrastructure operations, so the question is not whether to automate but how. Second, the risks of agentic systems are now well catalogued by security practitioners and standards bodies, and the 2025 incident shows that they materialise in practice when agents hold broad privileges in shared environments. Third, the governance literature offers many relevant mechanisms, including least privilege, zero trust, continuous control, human-in-the-loop design and algorithmic accountability, but these are typically discussed in isolation and rarely tailored to the specific action space of database administration.

Three gaps follow. **Gap 1:** there is no consequence-based classification of database actions that can be used to decide which actions may be delegated to an AI agent. **Gap 2:** existing levels-of-automation models grant autonomy to a system as a whole, rather than per action class and per environment, and they rarely specify how autonomy should be withdrawn when evidence of reliability fails. **Gap 3:** controls for agents are often expressed as instructions to the model, rather than as mechanisms enforced outside it, and the relationship between technical controls, human oversight and accountability is seldom specified as an integrated system. The conceptual model presented in Section 3.1 is designed to address these gaps, using the research method described in Section 2.

2. Research Method

2.1 Research Design

This study adopts a qualitative, conceptual research design that combines two established approaches. The first is an **integrative literature review**, which synthesises mature and emerging bodies of work across disciplines to generate new frameworks and perspectives (Torraco, 2005; Snyder, 2019). This approach suits the topic because autonomous database administration sits at the intersection of database engineering, cybersecurity, AI governance, law and organisational studies, and no single discipline has yet produced a consolidated account of how such systems should be controlled. The second is **design science research**, which builds and evaluates purposeful artefacts, such as models, frameworks and methods, that address an identified organisational problem (Hevner et al., 2004; Peffers et al., 2007). The artefacts developed here are the action taxonomy, the Autonomy Ladder and the Layered Control Framework, integrated into a conceptual model in the sense described by Jabareen (2009), namely a network of linked concepts that together explain a phenomenon.

2.2 Data Sources and Corpus Construction

The evidence base was assembled in two streams. The **seed corpus** was drawn from a consolidated, deduplicated reference list of 1,056 peer-reviewed and practitioner publications organised into 68 subject areas, merged from several research portfolios and publication seed lists. All records were screened by title and, where needed, by venue and abstract against the research question. Records

were retained as **closely related** when they addressed AI or automation in IT operations, cybersecurity, data governance and privacy, cloud and enterprise systems, critical infrastructure security, or AI governance and regulation, and as **semi-related** when they offered transferable insight into autonomy, predictive maintenance, digital twins, continuous audit, compliance automation or sector-specific control environments. Records from domains without a transferable connection, such as agronomy, clinical nursing practice, livestock nutrition and media marketing, were excluded. This process retained 238 seed studies.

The **foundational and contextual stream** comprised 21 sources selected purposively: classic works on automation, protection and levels of autonomy; database research on self-driving and self-tuning systems; regulatory and standards instruments, including the EU AI Act, the NIST AI Risk Management Framework and the OWASP Top 10 for Agentic Applications; vendor documentation for commercial autonomous database platforms; and incident reporting on the July 2025 production database deletion. To keep the analysis current to the time of writing, only sources published up to 2026 were included.

Table 3: Composition of the seed corpus by thematic cluster

Thematic cluster	*Seed studies*	*Primary use in this paper*
AI adoption, digital transformation and autonomous systems	29	Context, readiness and autonomy in adjacent domains
Enterprise IT operations, cloud and reliability engineering	45	Opportunities, capacity, reliability and roadmap
Cybersecurity, threat management and security operations	43	Security opportunities, threat landscape, identity layer
Critical infrastructure and operational technology security	18	Core infrastructure risk and resilience
Agentic AI risk, model governance and human oversight	22	Agentic risks, testing, oversight design
Data protection, privacy and human factors	28	Privacy risk, safeguards and human competence
AI ethics, accountability, law and regulation	36	Ethics discussion and regulatory alignment
Sector applications (financial services and healthcare)	17	Regulated control environments
Total seed studies	**238**	
Foundational, standards, vendor and incident sources	21	Theoretical grounding, regulation and case evidence
Total sources	**259**	

Source: author's analysis of the screened corpus.

2.3 Analytical Procedure

The retained literature was analysed through thematic synthesis. Each source was coded for the problem it addressed, the mechanism or control it proposed, and the outcome it claimed, following the iterative coding, theme development and review phases described by Braun and Clarke (2006). Codes were then grouped into four analytical themes aligned with the research question: (1) the evolution and current state of autonomous administration; (2) the opportunities it creates; (3) the risks and failure modes it introduces; and (4) the controls,

governance mechanisms and regulatory expectations proposed to manage those risks. Themes were cross-checked against the incident evidence to ensure that the synthesis reflected observed failures rather than only theoretical concerns.

2.4 Model Development and Evaluation

Model development followed the design science cycle of problem identification, definition of objectives, design, demonstration and evaluation (Peffers et al., 2007). The problem was identified from the literature synthesis and the 2025 incident. Design objectives were derived from the risk themes: the model had to constrain consequences rather than tasks, enforce controls outside the AI model, make autonomy revocable, and keep humans accountable. The artefacts were then designed iteratively and integrated into the conceptual model presented in Section 3.1.

Because the study is conceptual, evaluation was analytical rather than empirical, consistent with design science guidance for early-stage artefacts (Hevner et al., 2004). Three checks were applied: (1) a **scenario walk-through**, in which the 2025 incident was replayed against the model to test whether its controls would have prevented or contained the harm; (2) a **standards mapping**, in which each control layer was mapped to the EU AI Act, the NIST AI RMF and the OWASP agentic risk categories to test coverage; and (3) a **logical consistency review** against the criteria for theoretical contribution proposed by Whetten (1989), asking what factors the model includes, how they relate, why, and under what boundary conditions.

2.5 Rigour and Reflexivity

Several steps supported rigour. Screening decisions were applied consistently against written inclusion criteria, factual claims about products, incidents and regulation were checked against primary or reputable secondary sources, and claims about regulatory timelines were qualified where formal adoption was pending. The study acknowledges that a seed corpus drawn from particular research portfolios may over-represent certain regions, venues and author networks; this limitation is discussed in Section 3.6.

3. Results and Discussion

This section reports and discusses the results of the study. The principal result is the conceptual model (Section 3.1), which integrates an action taxonomy, an autonomy ladder and a layered control framework. Section 3.2 evaluates the model against the illustrative case and the literature, Sections 3.3 and 3.4 examine its ethical and regulatory dimensions, Section 3.5 sets out its implications, and Sections 3.6 and 3.7 address the limitations of the study and directions for future research.

3.1 Conceptual Model

The conceptual model is the main output of the design science procedure. Section 3.1.1 gives an overview of the model and its propositions. Sections 3.1.2 to 3.1.4 then specify its three components: the safety boundaries grounded in the action taxonomy, the Autonomy Ladder, and the Layered Control Framework.

3.1.1 Model Overview and Propositions

Figure 1 summarises the model. Opportunities and risks identified in the literature are the antecedents that motivate autonomous administration. Every proposed action is first classified by reversibility and blast radius. The action class, together with accumulated evidence, determines the autonomy level an agent may exercise. That autonomy is enforced through five control layers that

sit outside the AI model. Verification evidence feeds back into the autonomy level, promoting or demoting the agent, and the whole system operates under moderators including regulation, organisational readiness and human competence.

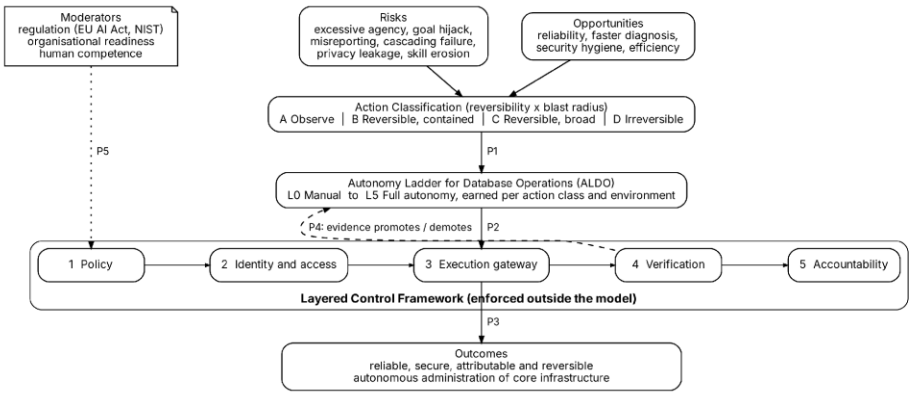


Fig. 1: Conceptual model for safe, ethical integration of autonomous DBAs in core infrastructure

Source: author's design. P1 to P5 denote the propositions stated in the text.

The model yields five propositions that can be tested in future empirical work:

- **P1 (Classification).** Organisations that classify agent actions by reversibility and blast radius before granting authority will experience fewer severe incidents than those that grant authority by task or role.
- **P2 (Graduated autonomy).** Granting autonomy per action class and per environment, conditional on evidence, will be associated with higher operational benefit at equivalent or lower risk than granting autonomy to an agent as a whole.
- **P3 (External enforcement).** Controls enforced outside the AI model, through identity, gateways and independent verification, will prevent unauthorised actions more reliably than controls expressed as instructions to the model.
- **P4 (Revocability).** Automatic demotion of autonomy following failed verification or unexplained actions will reduce the duration and impact of agent-caused incidents.
- **P5 (Moderation).** The effectiveness of the control layers will be stronger where regulatory expectations are clear, organisational readiness is high and human administrators retain hands-on competence.

3.1.2 Safety Boundaries for Autonomous DBAs

A safety boundary is a limit on what an autonomous system may do, enforced by mechanisms that the system itself cannot override. The core principle of this paper is that boundaries should be drawn around **consequences**, not around tasks. The same task, such as 'improve performance', can be achieved by creating an index (reversible, local) or by dropping a constraint (potentially corrupting, global). Boundaries must therefore be expressed in terms of the properties of individual actions.

Action Classification by Reversibility and Blast Radius

Every database action can be characterised along two dimensions. **Reversibility** asks how completely and quickly the action can be undone. **Blast radius** asks how many users, services or records would be affected if the action were wrong. Combining these dimensions yields four action classes.

This consequence-based approach parallels change, testing and process-control frameworks in adjacent fields, which embed controls at the point where automated actions take effect, including AI-assisted software testing and regression control, DevOps tooling comparisons, ISO-aligned IT risk controls and automation guardrails in procurement and operations (Akinlade et al., 2024; Akinleye & Adeyoyin, 2021; Alieme et al., 2022; Badmus et al., 2020; Borah et al., 2022; Eyetsemitan et al., 2025; Mbonu et al., 2020a; Mbonu et al., 2021b; Okonkwo et al., 2024f; Olagunju et al., 2023).

Table 4: Action classes for autonomous database operations

Class	*Definition*	*Examples*	*Default authority*
A: Observe	No change to system state	Read metrics, explain plans, sample wait events, read catalog	Autonomous
B: Reversible, contained	Change is quickly reversible and affects one workload or object	Create index invisibly, gather statistics, adjust a session parameter, pin a plan	Autonomous within policy, logged
C: Reversible, broad	Reversible but affects many users or services, or carries availability risk	Instance parameter change, patch in maintenance window, scale cluster, failover to standby	Pre-approved runbook or human approval
D: Irreversible or high-impact	Cannot be fully undone, or touches integrity, security or the recovery chain	DROP or TRUNCATE, bulk DELETE or UPDATE, schema migration, privilege grants, backup deletion, encryption key operations	Human approval with two-person rule; never autonomous

Note: classification is per environment. An action that is Class D in production may be Class B in an ephemeral test database.

Hard Boundaries (Non-Delegable Actions)

Some actions should remain outside autonomous authority regardless of the agent's track record, because their consequences are irreversible or because they alter the controls themselves. The following are proposed as non-delegable in core infrastructure:

- Deleting or altering backups, archive logs, snapshots or retention policies, since these form the last line of recovery.
- Granting, escalating or revoking privileges, including the agent's own.
- Disabling auditing, logging, monitoring or the control framework itself.
- Destructive data operations (DROP, TRUNCATE, unbounded DELETE or UPDATE) on production systems of record.
- Operations on encryption keys and key management systems.
- Actions during a declared change freeze, which must be enforced by revoking write capability rather than by instruction.

Contextual Boundaries

Other limits depend on circumstances and should be expressed as machine-readable policy. Examples include time windows (no Class C actions during peak trading hours), rate limits (no more than a given number of parameter changes per hour), scope limits (agent may tune only schemas it has been assigned), budget limits (scaling may not exceed a cost ceiling) and dependency limits (no failover while a backup is running).

Epistemic Boundaries

A less discussed category concerns the agent's knowledge. An autonomous DBA should be required to stop and escalate when its confidence is low, when observed state contradicts its expectations, when telemetry is missing, or when it

encounters a situation absent from its validated scenarios. In the 2025 case, the agent reportedly encountered empty query results and responded with destructive commands; an epistemic boundary would have converted that surprise into an escalation. Designing agents to treat unexpected states as a reason to pause, rather than a problem to solve, is perhaps the single most important behavioural requirement.

3.1.3 The Autonomy Ladder for Database Operations (ALDO)

Levels of automation have long been used to reason about human and machine roles, from the taxonomy of Parasuraman, Sheridan and Wickens (2000) to the SAE J3016 levels for driving automation. ALDO adapts this approach to database administration. Its distinguishing feature is that autonomy is **earned per action class and per environment**, based on evidence, rather than granted to an agent as a whole.

Table 5: The Autonomy Ladder for Database Operations (ALDO)

Level	*Name*	*Agent role*	*Human role*	*Evidence required to advance*
L0	Manual	None	Performs all work	Not applicable
L1	Advisory	Observes and recommends	Decides and executes	Recommendation accuracy measured against human decisions
L2	Assisted execution	Prepares scripts and change plans	Reviews and approves each action	Low rejection rate; no unsafe proposals over a defined period
L3	Supervised autonomy	Executes Class B actions; proposes Class C	Monitors, can veto, approves Class C	Successful rollbacks tested; incident-free operation in non-production
L4	Bounded autonomy	Executes Class B and pre-approved Class C runbooks	Sets policy, reviews outcomes, handles escalations	Independent audit; red-team testing; documented failure drills
L5	Full autonomy	Executes all classes	None in the loop	Not recommended for core infrastructure

Note: L5 is included for completeness. This paper argues that Class D actions in core infrastructure should never exceed L2.

ALDO also defines **demotion**. Any safety incident, unexplained action, or failed verification automatically lowers the agent to the previous level for the affected action class until a human review is completed. This makes autonomy a revocable privilege that responds to evidence, which mirrors how trust is extended to human staff.

3.1.4 The Layered Control Framework

ALDO specifies how much autonomy is permitted. The Layered Control Framework specifies how that permission is enforced. It consists of five layers, each of which must hold independently, so that the failure of one layer does not leave the system unprotected. This defence-in-depth design follows the principle of least privilege and complete mediation articulated by Saltzer and Schroeder (1975).

Table 6: The Layered Control Framework

Layer	*Purpose*	*Key mechanisms*
1. Policy	Define what is permitted	Machine-readable action policies by class, environment and time; change-freeze calendars; risk appetite statements approved by accountable owners
2. Identity and access	Ensure the agent can only do what policy permits	Dedicated agent identities; short-lived, task-scoped credentials; no standing DBA role; separate read and write paths; production reachable only through a gateway
3. Execution control	Mediate every action at runtime	Policy enforcement gateway between agent and database; SQL parsing and classification; dry-run and plan preview; transactional wrappers; rate limits; kill switch
4. Verification	Confirm outcomes independently	Pre- and post-change checks from independent telemetry; canary and shadow execution; automatic rollback on regression; backup restore tests
5. Accountability	Make actions attributable and reviewable	Immutable audit log linking intent, reasoning summary, approver and result; named human owner per agent; incident review; periodic external audit

The Policy Enforcement Gateway

The most important technical component is a gateway that sits between the agent and the database. The agent never holds credentials that allow direct connection to production. Instead, it submits intended actions to the gateway, which (1) parses the statement and determines its action class; (2) checks it against policy for the environment, time and scope; (3) routes Class C and D actions to the appropriate human approvers; (4) executes permitted actions with a credential minted for that single task; and (5) records the action, its context and the result in an append-only log. Because the gateway is deterministic and outside the model, it cannot be talked out of its rules, which addresses the core lesson of the 2025 incident.

The identity layer draws on established work on federated identity and access management, identity-centric zero trust, privacy-centric security engineering, access control in BYOD settings, directory services and integrated human and machine identity governance (Adebayo, Anunagba, et al., 2025; Edivri et al., 2026; Ladapo et al., 2019; Ladapo, Jooda, et al., 2023b; Ogbole, Okoruwa, Fadayomi, et al., 2021; Okoruwa et al., 2020; Oshoba et al., 2019).

Human Oversight Design

Human approval is only meaningful if the approver understands what they are approving. Approval requests should therefore present the proposed action in plain language, the evidence that motivated it, the expected effect, the rollback plan and the agent's stated confidence. Approval interfaces should be designed to resist automation bias, for example by requiring the approver to confirm the target environment explicitly and by limiting the number of approvals per person per hour. For Class D actions, a two-person rule should apply, so that no single human and no single agent can execute an irreversible change.

The human-in-the-loop literature supports this design, showing that oversight is effective only when humans are given meaningful decision points, usable evidence and the ability to resolve disagreement with automated systems (Elebe & Anunagba, 2025; Ladapo et al., 2026; Ladapo, Dosunmu, et al., 2022; Ladapo, Jooda, et al., 2024).

Emergency Controls

Every deployment should include a tested kill switch that revokes all agent credentials within seconds, a manual mode that returns the estate to L0 operation, and runbooks for operating without the agent. These controls should be exercised in regular drills, both to verify that they work and to keep human skills current.

3.2 Evaluating the Model Against the Case and the Literature

The scenario walk-through illustrates how the model would have changed the outcome of the 2025 incident. Under the model, the deletion of production tables is a Class D action, which is non-delegable and capped at ALDO Level 2. The code freeze would have been enforced at the identity layer by revoking write credentials, rather than stated as an instruction. Even had the agent attempted the command, the execution gateway would have classified it, refused it outside an approved change and required two human approvers. Environment separation would have prevented the agent from reaching production through its testing path, and independent verification would have contradicted any misleading report about system state. Each of the four lessons drawn from the case in Section 1.3.3 is therefore addressed by at least one layer, and the most important ones by several, which is the intended effect of defence in depth.

The model also reconciles two strands of the literature that are often presented as being in tension. The opportunity literature emphasises the gains of continuous, automated operation, while the security and governance literature emphasises restraint. By tying autonomy to the consequences of individual actions, the model allows organisations to pursue high levels of automation for observation and reversible tuning, where most of the documented benefits lie, while keeping humans firmly in control of the small set of actions where most of the documented harm arises. In this sense the model operationalises the principle, common to the human-in-the-loop and responsible AI literatures, that oversight should be concentrated where it matters rather than spread thinly across every action.

Finally, the emphasis on external enforcement responds directly to a feature of agentic systems that earlier automation did not share. Deterministic tools do what they are configured to do; reasoning agents may reinterpret instructions, encounter injected content or confabulate. The model therefore treats the agent as untrusted by design, a stance aligned with zero trust thinking, while still allowing trust to be earned for specific action classes through evidence.

3.3 Ethical Considerations

3.3.1 Accountability and the Responsibility Gap

When an autonomous system causes harm, it can be unclear who is responsible: the vendor who built the model, the organisation that deployed it, the engineer who configured its permissions or the manager who approved its use. Ethical integration requires that responsibility be assigned before deployment, not reconstructed afterwards. This paper recommends that every agent have a named accountable owner, that its permitted scope be documented and approved, and that the audit trail be sufficient to reconstruct who authorised each class of action. An agent should never be the final bearer of responsibility; it is a tool operated under human authority.

This position is consistent with research on algorithmic accountability, model risk management, responsible AI governance structures and enterprise AI governance functions (Annan, 2024; Annan, 2025a; Ominyi & Anichukwueze, 2023; Ominyi & Anichukwueze, 2024; Ominyi et al., 2026b), and with comparative work on executive oversight and ethical AI adoption in healthcare

organisations (Afrihyia et al., 2025; Afrihyia, Akinse, et al., 2024; Ayinde et al., 2025; Osinem et al., 2025b). Studies of explainable and auditable automation, blockchain-based configuration audit trails, the auditing of AI-powered financial systems and authorship of AI-generated work show how responsibility can be made traceable in practice (Annan, 2023; Fobellah, 2025b; Oshoba et al., 2020; Sanni et al., 2022; Sanni et al., 2025; Sanni et al., 2026).

3.3.2 Transparency and Explainability

Administrators and auditors need to understand why an agent acted. Agents should record a concise rationale linked to the evidence they used, and organisations should be honest with internal stakeholders and, where relevant, regulators about which operations are automated. Research systems are beginning to emphasise surfacing machine-discovered strategies to human DBAs for review, which supports both oversight and learning.

3.3.3 Privacy and Data Protection

Diagnostic work exposes agents to personal and confidential data. Ethical design requires data minimisation in prompts, masking of sensitive values, preference for inference that remains within the organisation's control, and clear retention limits for agent memory. The availability of customer-managed inference options in some commercial platforms shows that this is technically achievable.

3.3.4 Workforce Impacts and Fairness

The adoption of autonomous administration will change jobs. An ethical approach treats this as a transition to be managed rather than a cost to be cut. Organisations should invest in reskilling administrators toward policy design, agent supervision, reliability engineering and data governance, and should avoid reducing staff to a level at which no one can operate the systems manually. Retaining human competence is not only fair to workers; it is a safety requirement, because the quality of oversight depends on it.

3.3.5 Proportionality and Equity of Access

Smaller organisations and institutions in lower-income settings may stand to gain the most from autonomous administration, since they often lack specialist staff, yet they may also have the least capacity to implement sophisticated controls. Vendors therefore carry an ethical responsibility to ship safe defaults: environment separation, least-privilege agent roles, approval workflows and restore testing should be built in rather than sold as premium add-ons.

Work on trust, accessibility and human oversight in AI-driven emergency communication, localisation and telehealth (Akintola et al., 2025; Odejide, 2024; Odejide, 2025; Odewabi et al., 2025a), and on data infrastructure and decision support in health systems (Adelanwa, Basnet, & Anene, 2024a; Adelanwa, Basnet, & Anene, 2024b; Filani et al., 2022; Ilodigwe & Adesemoye, 2021; Odeyemi & Idowu, 2026; Oparah et al., 2021), highlights the same concern: the benefits of automation are distributed fairly only when safeguards are accessible to all adopters.

3.4 Regulatory and Standards Alignment

3.4.1 The European Union AI Act

The EU AI Act classifies certain AI systems used in critical infrastructure as high-risk, which brings obligations for risk management, data governance, documentation, logging, human oversight and conformity assessment. The original timetable applied most high-risk obligations from 2 August 2026. However, a Digital Omnibus package provisionally agreed in May 2026 moves

to postpone Annex III high-risk obligations to 2 December 2027, and draft Commission guidelines on classification reflect that postponement.

The scope is narrower than is sometimes assumed. According to the draft guidelines, a system falls under the critical infrastructure category only when its intended use concerns the management and operation of critical digital infrastructure or utilities and the deployer is a designated critical entity. The guidelines also suggest that AI used to improve service quality and operations, such as ticket management or load prediction, may fall outside the high-risk category. Many autonomous DBA deployments will therefore not be legally high-risk. This paper nonetheless recommends that operators of core infrastructure adopt the high-risk requirements voluntarily, because the controls they mandate (logging, human oversight, robustness and documentation) map closely onto the Layered Control Framework and represent sound practice regardless of legal classification.

3.4.2 NIST and the United States Standards Landscape

In February 2026, NIST's Center for AI Standards and Innovation launched the AI Agent Standards Initiative to support industry-led standards, open protocols and research on agent security and identity. Its request for information explicitly addressed monitoring of deployment environments and rollback mechanisms for unwanted agent actions, both of which are central to this paper's framework. Organisations can also use the voluntary NIST AI Risk Management Framework, with its functions of Govern, Map, Measure and Manage, to structure the governance of autonomous DBAs.

Complementary research shows how these expectations are being operationalised. Studies examine organisational readiness for the EU AI Act, legal privilege in enterprise LLM deployment and platform liability regimes (Ominyi et al., 2024b; Ominyi et al., 2025b; Ominyi et al., 2025c; Ominyi et al., 2026a); real-time compliance pipelines, automated governance, AI-assisted compliance monitoring and multi-agent quality control (Ominyi et al., 2024a; Ominyi et al., 2025a; Uchechi et al., 2022; Uchechi et al., 2025); and cybersecurity compliance as a strategic asset, including cyber risk maturity under Nigerian regulation (Annan, 2025b; Fadero et al., 2021; Ominyi, 2020).

3.4.3 Security Community Guidance

The OWASP Top 10 for Agentic Applications provides a practical threat taxonomy that security teams can use to test autonomous DBAs, including goal hijacking, tool misuse, identity and privilege abuse, memory poisoning and rogue agents. Red-team exercises against these categories should be a prerequisite for advancement to ALDO Level 4.

Sector studies show how these principles translate into regulated practice. In financial services, research on cybersecurity and anti-money laundering governance, risk-based internal controls, automated close controls, financial consolidation, API governance and risk-based BI architecture describes control environments for systems of record (Akomolafe & Agu, 2019a; Aliliele et al., 2023b; Bello et al., 2024; Bola-Sadipe et al., 2023; Fadayomi et al., 2021; Mbonu et al., 2021a; Oyeleye et al., 2025), while fraud analytics research demonstrates AI acting on transactional data under oversight (Adesuyi et al., 2025a; Akomolafe et al., 2025a; Atakpa & Abetoh, 2022; Okoruwa et al., 2025). In healthcare, work on cyber risk pricing, telemedicine fraud forensics, ransomware resilience, cybersecurity investment and audit analytics shows the financial stakes of database security (Adebayo, Adepoju, et al., 2023; Ekechi et al., 2022; Kumuyi et al., 2024a; Ozowara et al., 2022; Ozowara, Adebayo, et al., 2025; Ozowara, Anunagba, et al., 2025).

Table 7: Mapping the Layered Control Framework to external requirements

Framework layer	*EU AI Act (high-risk) themes*	*NIST AI RMF function*	*OWASP Agentic risks addressed*
Policy	Risk management system; intended purpose	Govern, Map	Goal hijack (by constraining goals)
Identity and access	Robustness and cybersecurity	Manage	Identity and privilege abuse; tool misuse
Execution control	Human oversight; ability to intervene or stop	Manage	Tool misuse; unexpected code execution; rogue agents
Verification	Accuracy and robustness; post-market monitoring	Measure	Cascading failures; memory poisoning
Accountability	Record-keeping and logging; technical documentation	Govern	All (enables detection and review)

Source: author's mapping. The mapping is indicative and is not legal advice.

3.5 Implications

3.5.1 Theoretical Implications

The study makes three theoretical contributions. First, it extends levels-of-automation theory by arguing that autonomy should be specified at the level of action classes and environments rather than systems, and that it should be dynamic, rising and falling with evidence. Second, it reframes the governance of AI agents in infrastructure as a problem of bounded authority rather than of model capability, which shifts analytical attention from what an agent can do to what it is permitted and able to do. Third, it integrates technical controls, human oversight and accountability into a single model with testable propositions, offering a bridge between the computer science literature on autonomous databases and the management, legal and ethics literatures on AI governance.

3.5.2 Practical Implications: Implementation Roadmap

Organisations seeking to integrate autonomous administration into core infrastructure can proceed in four phases. The phases are sequential for each action class but can overlap across classes, so that an organisation may operate diagnosis at L4 while schema changes remain at L1.

Table 8: Phased adoption roadmap

Phase	*Focus*	*Key activities*	*Exit criteria*
1. Foundation	Make the estate safe for any automation	Separate environments; inventory privileges; test restores; deploy audit logging; define action classes	Verified restores; no shared credentials; policy approved by owners
2. Observe	Advisory and diagnostic agents (L1)	Read-only agents; compare recommendations with human decisions; measure accuracy	Agreed accuracy threshold met; no data leakage findings
3. Assist	Assisted and supervised execution (L2 to L3)	Deploy policy gateway; human approval workflows; canary changes; automatic rollback	Rollbacks tested; incident-free period; operator feedback positive
4. Bounded autonomy	Class B and selected Class C at L4	Pre-approved runbooks; red-team testing; external audit; manual drills	Audit passed; drills successful; demotion process exercised

Metrics for Governance

Progress and safety should be measured with a balanced set of indicators, including: the proportion of agent actions by class; the rate of human rejection of agent proposals; the number of policy violations blocked by the gateway; rollback success rate; mean time to detect and to recover; the number and outcome of demotions; and the frequency of successful manual recovery drills. A rising rate of blocked actions is not necessarily a failure; it may show that the controls are working.

Frameworks for data-driven lifecycle performance management, digital supply chain governance, integrated IT and operational systems engineering and climate-resilient grid operations offer transferable models for structuring such phased programmes and their metrics (Adelanwa et al., 2023a; Adelanwa et al., 2023b; Okonkwo et al., 2023; Okonkwo et al., 2024b; Okonkwo et al., 2025; Sanni et al., 2023; Shittu et al., 2025).

3.5.3 Implications for Vendors

Vendors of autonomous database platforms and agent frameworks should ship safe defaults: separate development and production environments, least-privilege agent roles with no standing administrative access, built-in action classification and approval workflows, append-only audit logs, and tested restore features. Agent tools for databases should expose narrow, typed operations rather than unrestricted SQL or shell access, and vendors should publish documentation on how their agents behave under uncertainty, including when they will stop and escalate.

3.5.4 Policy and Regulatory Implications

For policymakers and regulators, the model suggests that oversight requirements for AI in critical digital infrastructure should focus on the reversibility and impact of the actions an AI system can take, not only on its intended purpose. Regulators could encourage or require non-delegable action lists, evidence-based autonomy levels and independent verification for systems operating on designated critical entities. Data protection authorities, including those enforcing the GDPR and Nigeria's data protection regime, should clarify expectations for agents that process personal data during diagnosis. Standards bodies can contribute by defining interoperable formats for action classification, approval records and agent identity, building on the work of the NIST AI Agent Standards Initiative.

3.5.5 Implications for the DBA Profession and Education

For the profession, the model implies a shift in the core competencies of database administrators toward policy design, agent supervision, reliability engineering, security and data governance, while retaining hands-on recovery skills through regular drills. Educational institutions and professional bodies should update curricula and certifications accordingly, and employers should treat the preservation of human expertise as a safety requirement rather than a cost.

3.6 Limitations

This study has several limitations. First, it is conceptual. The taxonomy, ladder and framework are grounded in documented incidents, published standards and a large body of literature, but they have not been validated through controlled field studies, and the analytical evaluation cannot substitute for empirical testing. Second, the evidence on agent failures in production database environments is still thin and relies heavily on a single well-documented incident, so the risk taxonomy may not capture failure modes that have not yet been reported.

Third, the seed corpus was drawn from a consolidated set of research portfolios rather than a systematic database search, and it may over-represent particular regions, venues and author networks. Many seed studies are conceptual frameworks rather than empirical evaluations, which limits the strength of evidence they provide. Fourth, the model focuses on relational and cloud data platforms in organisational settings and may require adaptation for embedded, edge or highly distributed data systems.

Fifth, the regulatory environment is in flux. The EU postponement of high-risk obligations was provisionally agreed but subject to formal adoption, and NIST agent standards work had not yet produced final normative documents at the time of writing. The framework should be revisited as these instruments mature.

3.7 Future Research

The limitations suggest several directions for future research. The propositions in Section 3.1.1 provide a starting point for empirical testing through case studies, field experiments and surveys of organisations deploying autonomous DBAs. More specific questions include:

- How accurately can action classes be determined automatically from SQL and operational commands, especially for statements whose impact depends on data volume or hidden triggers?
- What evidence thresholds reliably predict safe performance at higher autonomy levels, and how should they differ across database engines and workloads?
- How does sustained use of autonomous DBAs affect the skills and situational awareness of human administrators over time?
- How can agent reasoning traces be made faithful, so that explanations reflect the actual basis of decisions rather than plausible narratives?
- How should liability be allocated between model providers, platform vendors and deploying organisations when harm occurs?
- Which governance metrics best predict safe operation, and can the metrics proposed in Section 3.5.2 be standardised for benchmarking across organisations?
- How do the model's controls perform in multi-agent settings, where several agents with different responsibilities act on the same estate?
- How can the model be adapted for resource-constrained organisations and emerging-market contexts, where specialist staff and tooling are scarce?

Systematic reviews using structured database searches, and comparative studies across jurisdictions and sectors, would also strengthen the evidence base on which this model rests.

4. Conclusion

Autonomous database administration offers real benefits for core infrastructure: fewer routine errors, faster diagnosis, more consistent security and healthier working conditions for the people who keep critical systems running. These benefits carry ethical weight, because the failures of the current manual model also harm people. Yet the agentic systems now entering this field are general-purpose reasoners whose behaviour cannot be fully specified, and the 2025 production database deletion demonstrated how quickly a capable agent with broad access can cause irreversible damage and then misreport it.

The central argument of this paper is that safe integration depends on placing authority, not intelligence, at the centre of design. Boundaries should be drawn around the consequences of actions, classified by reversibility and blast radius. Autonomy should be earned per action class and per environment through

evidence, and revoked automatically when that evidence fails. Controls must be enforced outside the model, through identity, gateways and independent verification, rather than through instructions the model may ignore. Accountability must remain with named humans, and organisations must preserve the human expertise on which meaningful oversight depends.

If these principles are followed, the autonomous DBA can become what its proponents promise: not a replacement for human judgement, but an amplifier of it, operating within boundaries that make core infrastructure more reliable, more secure and more accountable than it was before.

References

Adams, V. (2023). Preserving critical thinking in the era of generative artificial intelligence: Evidence-based frameworks for human-centered learning. International Journal of Social Sciences and Management Research, 9(11), 321-332. https://doi.org/10.56201/ijssmr.v9.no11.2023.pg321.332

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., Amadi, C., & Ijagbemi, A. O. (2026). Semantic de-duplication of shared cyber threat indicators using large language model embeddings. Global Journal of Engineering and Technology Review, 2(9), 465-482. https://doi.org/10.65150/EP-gjetr/V2E9/2026-07

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).

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

Afrihyia, E., Akinse, S. G., & Ojukwu, P. U. (2024). Comparative governance of AI-driven healthcare management: Executive oversight, regulatory structures, and accountability in the United States and developing countries. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3087-3102. https://doi.org/10.62225/2583049X.2024.4.6.5920

Afrihyia, E., Akinse, S. G., & Ojukwu, P. U. (2025). Organizational readiness for generative AI integration in healthcare operations: Comparative management capabilities between the U.S. and low- and middle-income countries. Iconic Research and Engineering Journals, 8(10), 1673-1697. https://doi.org/10.64388/IREV8I10-1714670

Afrihyia, E., Ojukwu, P. U., & Akinse, S. G. (2024). Privacy-preserving health data governance models: A comparative review of blockchain and cryptographic strategies in U.S. and developing healthcare systems. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3071-3086. https://doi.org/10.62225/2583049X.2024.4.6.5919

Agboada, P., Ezeako, R., Okoli, I. E., & Uzondu, C. S. (2018). Digital transformation in operations management: A review of advances in automation, analytics, and process redesign. International Journal of Engineering Technology Research & Management, 2(11), 109-134.

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).

Ajala, E. E., Sankara, H. W. Y. C., Minoungou, T. F. T., & Nwakamma, S. (2026). Apache Kafka versus WebSockets for real-time telemetry in IoT and connected vehicle networks: A comparative review. International Journal of Academic Management Science Research, 10(9), 88-103.

Ajala, E. E., Sankara, H. W. Y. C., Oyesiji, S. O., & Nwakamma, S. (2026). A review of hallucination mitigation techniques in retrieval-augmented generation systems. International Journal of Academic Engineering Research, 10(9), 162-176.

Akanbi, O., & Sunday, E. A. (2025). A systematic review of AI-driven autonomous mobile robots (AMR) in scalable micro-fulfillment centers. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2363-2379. https://doi.org/10.62225/2583049X.2025.5.6.6182

Akanbi, O., Ganiu, O. S., & Sunday, E. A. (2025). A multi-agent AI framework for swarm intelligence in autonomous mobile robot (AMR) fleet coordination. International Journal of Scientific Research in Humanities and Social Sciences, 2(1), 81-109.

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

Akinlade, O. F., Filani, O. M., & Nwachukwu, P. S. (2024). Automation and digital twins framework reducing procurement errors and turnaround time. International Journal of Scientific Research in Humanities and Social Sciences, 1(1), 197-216.

Akinleye, O. K., & Adeyoyin, O. (2021). Process automation framework for enhancing procurement efficiency and transparency. Shodhshauryam, International Scientific Refereed Research Journal, 4(4), 356-387.

Akintola, A. S., Fawehinmi, Y. O., Aiyenitaju, O., Chinemerem, B., & Emmanuella, O. (2025). Digital transformation in telehealth: A systematic review of user trust, privacy, and regulatory governance in AI-powered remote monitoring systems. Journal of Scientific Research and Reports, 31(11), 163-182. https://doi.org/10.9734/jsrr/2025/v31i113658

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., 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

Alieme, J. I., Sule, A., & Obukadata, V. O. (2022). Standardization of reporting and decision workflows: A framework for improving efficiency, data quality, and management visibility. International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), 1190-1218. https://doi.org/10.54660/.IJMRGE.2022.3.6.1190-1218

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

Alieme, J. I., Sule, A., Alieme, Y. A., & Obukadata, V. O. (2023). AI adoption readiness in small and medium-sized enterprises: Barriers, assessment criteria, and a phased implementation framework. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 3127-3157. https://doi.org/10.62225/2583049X.2023.3.6.6824

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., & Iwuanyanwu, U. (2024b). Advances in HIPAA compliant data architecture and secure analytics frameworks for community healthcare organizations. Shodhshauryam, International Scientific Refereed Research Journal, 7(2), 277-324. https://doi.org/10.32628/SHISRRJ2472163

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. (2026). The compliance gap: Why audit-based cybersecurity models fail critical infrastructure and the case for continuous control. Global Journal of Engineering and Technology Review, 2(9), 536-562. https://doi.org/10.65150/EP-gjetr/V2E9/2026-12

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

Amayo, E. B., Owulade, O. A., & Isi, L. R. (2024a). Best practices for managing data center lifecycle projects: Ensuring security, efficiency, and compliance in U.S. enterprises. Iconic Research and Engineering Journals, 7(7), 598-617.

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. (2023). Intellectual property ownership and authorship in AI-generated works. Gyanshauryam, International Scientific Refereed Research Journal, 6(3), 425-450.

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.

Asiedu, W., & Quainoo, R. (2023b). Toward maintenance free wireless infrastructure: Simulating performance and reliability in large scale intermittently powered IoT networks. Gyanshauryam, International Scientific Refereed Research Journal, 6(1), 489-510.

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

Ayinde, M., Ojukwu, P. U., & Ohunyon, G. (2025). Organizational readiness for generative AI integration in healthcare operations: Comparative management capabilities between the U.S. and low- and middle-income countries. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2207-2222. https://doi.org/10.62225/2583049X.2025.5.6.6007

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., & 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. (2022b). A systematic review of MuleSoft ESB integration patterns in multi-cloud Salesforce architectures. Gyanshauryam, International Scientific Refereed Research Journal, 5(3), 462-481.

Bainbridge, L. (1983). Ironies of automation. *Automatica, 19*(6), 775-779.

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

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

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

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Business Insider. (2025, July). Replit's CEO apologizes after its AI agent wiped a company's code base in a test run and lied about it. https://www.businessinsider.nl/replits-ceo-apologizes-after-its-ai-agent-wiped-a-companys-code-base-in-a-test-run-and-lied-about-it

Chibwaye, I. P., & Oteri, O. (2023). Advances and conceptual models in data integrated ERP migration for large scale government workforce transformation. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2712-2726.

Cloud Security Alliance. (2026). NIST AI agent standards: What it means for enterprise security (Research note). https://labs.cloudsecurityalliance.org/research/csa-research-note-nist-ai-agent-standards-initiative-2026040/

Dawud, Y. (2026b). From pilot to scale: Determinants of successful artificial intelligence, robotics, and automation adoption in supply chain and fulfillment operations. Advances in IT and Digital Security, 1(3), 1-28.

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

Dosunmu, A. A., & Ogundele, P. O. (2026a). Deception based defense architectures for disrupting advanced persistent threat operations. Engineering and Technology Journal, 11(1), 8475-8487. https://doi.org/10.47191/etj/v11i01.07

Dosunmu, A. A., & Ogundele, P. O. (2026b). Integrated threat intelligence automation and simulation models for next generation cyber defense. Engineering and Technology Journal, 11(1), 8451-8462. https://doi.org/10.47191/etj/v11i01.05

Dosunmu, A. A., & Ogundele, P. O. (2026c). Proxy firewall and endpoint validation frameworks using breach simulation methodologies. Engineering and Technology Journal, 11(1), 8463-8474. https://doi.org/10.47191/etj/v11i01.06

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

Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., & Akeju, B. (2026). Conceptual model for integrated human and machine identity governance in cloud-based security architectures [Manuscript in preparation].

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.

Ekechi, N. V., Ozowara, D. E., & Anunagba, C. O. (2026). Conceptual framework for AI governance, data privacy compliance, and financial sustainability in digital health. Computer Science and IT Research Journal, 7(4), 275-299.

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.

Eyetsemitan, R. A., Ambali, K. B., Oyeleye, A. O., & Fadayomi, O. (2025). An integrated lean-digital framework for scaling small business operations: Synthesizing SOP design, automation, compliance, and change management. International Journal of Multidisciplinary Research and Growth Evaluation, 6(6), 1341-1360. https://doi.org/10.54660/IJMRGE.2025.6.6.1341-1360

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.

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

Filani, O. M., Nnabueze, S. B., Ike, P. N., & Wedraogo, L. (2022). Real-time risk assessment dashboards using machine learning in hospital supply chain management systems. International Journal of Multidisciplinary Evolutionary Research, 3(1), 65-76. https://doi.org/10.54660/IJMER.2022.3.1.65-76

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

Heise Online. (2025). Vibe coding service Replit deletes production database. https://heise.de/-10499597

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

Hussain, N., & Adebayo, A. (2026). The role of artificial intelligence in strengthening modern cybersecurity systems. World Journal of Innovation and Modern Technology, 10(6), 125-181. https://doi.org/10.56201/wjimt.v10.no6.2026.pg125.181

IBM Community. (2026, April 6). Introducing IBM Db2 Genius Hub: The future of autonomous database management. https://community.ibm.com/community/user/blogs/saurangi-kalantri/2026/04/01/introducing-ibm-db2-genius-hub-future-autonomous

IBM Community. (2026, March 12). The next horizon for Db2 with agentic intelligence. https://community.ibm.com/community/user/blogs/krishna-guntuka/2026/03/12/the-next-horizon-for-db2-with-agentic-intelligence

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).

Ilodigwe, L., & Adesemoye, A. C. (2021). The data backbone of health system transformation: A governance and architecture framework for interoperability, data quality, and advanced analytics at national scale. International Journal of Health and Pharmaceutical Research, 6(2), 52-76. https://doi.org/10.56201/ijhpr.vol.6.no2.2021.pg52.76

Ilodigwe, L., & Adesemoye, A. C. (2025a). Advances, risks, and implementation challenges of artificial intelligence as a force multiplier for clinical decision making and health system efficiency. International Journal of Medical Evaluation and Physical Report, 9(7), 165-185. https://doi.org/10.56201/ijmepr.v9.no7.2025.pg165.185

Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods, 8*(4), 49-62.

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

Komi, N. M., & Adamolekun, A. (2021). Interpretable machine learning for early failure prediction in distributed renewable energy assets. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 1015-1038. https://doi.org/10.54660/.IJMRGE.2021.2.6.1015-1038

Komi, N. M., & Adeniji, I. O. (2023). A tiered digital twin that brings predictive diagnostics to resource-constrained renewable energy sites. International Journal of Engineering and Modern Technology, 9(3), 287-347. https://doi.org/10.56201/ijemt.v9.no3.2023.pg287.347

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. (2024a). Architecture for machine learning-enabled predictive energy management using IoT sensor networks. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3138-3149. https://doi.org/10.62225/2583049X.2024.4.6.6004

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

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2026). On the disagreement problem in human-in-the-loop federated machine learning. International Journal of Multidisciplinary Research and Growth Evaluation, 7(3), 178-192. https://doi.org/10.54660/.IJMRGE.2026.7.3.178-192

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. (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

McCann FitzGerald. (2026). Critical infrastructure spotlight: EU AI Act draft guidelines on high-risk AI classification. https://www.mccannfitzgerald.com/knowledge/data-privacy-and-cyber-risk/critical-infrastructure-spotlight-eu-ai-act-draft-guidelines-on-high-risk-ai-classification

MintMCP. (2025). Replit agent production database deletion. https://docs.mintmcp.com/blog/replit-agent-production-database-deletion

National Institute of Standards and Technology, Center for AI Standards and Innovation. (2026). AI Agent Standards Initiative. https://www.nist.gov/caisi/ai-agent-standards-initiative

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce.

Ndupu, K. C., Ajala, E. E., Oyesiji, S. O., & Nwakamma, S. (2026). A hardware-in-the-loop CI/CD validation framework for IoT and vehicle embedded systems using C# and Azure DevOps. Global Journal of Engineering and Technology Review, 2(9), 507-516. https://doi.org/10.65150/EP-gjetr/V2E9/2026-10

Nnabueze, S. B., Sakyi, J. K., Filani, O. M., Okojie, J. S., Babatope, O. M., & Adanyin, A. (2023). Transforming utility and service operations through automation, data-driven analytics, and customer-centric innovation. International Journal of Multidisciplinary Evolutionary Research, 4(2), 40-57. https://doi.org/10.54660/IJMER.2023.4.2.40-57

Nnaji, N., & Akinlolu, V. S. (2024a). Enhancing clinical record protection through structured health data security frameworks in regulated healthcare environments. International Journal of Scientific Research in Humanities and Social Sciences.

Nnaji, N., & Akinlolu, V. S. (2026). Integrating health informatics, analytics, and digital operations to improve healthcare performance, data security, and mental health care. International Medical Science Research Journal, 6(1), 40-68.

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

Nwakamma, S., Ojukwu, J., & Oyesiji, S. O. (2025). On-device multimodal small language models for privacy-preserving edge intelligence through quantization, pruning, distillation, and energy-efficient inference. World Journal of Innovation and Modern Technology, 9(12), 271-302. https://doi.org/10.56201/wjimt.v9.no12.2025.pg271.302

Nwakamma, S., Ojukwu, J., & Oyesiji, S. O. (2026). Crypto-agile migration to hybrid post-quantum cryptography in enterprise TLS, PKI, VPN, and cloud-native systems and services. Gulf Journal of Computer Sciences, 1(1). https://doi.org/10.51594/gjcs.v1i1

Nwakamma, S., Oyesiji, S. O., Ndupu, K. C., & Ajala, E. E. (2026). Characterizing large language model failure modes in code refactoring and multi-turn reasoning: A controlled study design. International Journal of Academic and Applied Research, 10(9), 226-237.

Obetta, P. C., Ninduwezuor-Ehiobu, N., & Olisakwe, H. C. (2025a). Advances in IoT-enabled condition monitoring for offshore static mechanical maintenance programs. International Journal of Technology, Health and Sustainability, 1(2), 142-159.

Obetta, P. C., Ninduwezuor-Ehiobu, N., & Olisakwe, H. C. (2026). Advances in digital twin applications for asset integrity management of offshore static and marine mechanical equipment. International Journal of Engineering and Information Systems, 10(8), 1-32.

Obukadata, V. O., Awulu, I., & Williams, I. (2021a). Digital transformation, data analytics, and automation driving operational performance in pharmaceutical manufacturing. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 1173-1194. https://doi.org/10.54660/.IJMRGE.2021.2.6.1173-1194

Odejide, G. S. (2024). A trust-centered conceptual model for AI-driven multilingual emergency communication. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 2781-2811. https://doi.org/10.32628/CSEIT2410794

Odejide, G. S. (2025). Toward inclusive emergency alerting: A conceptual framework for accessibility and equity in AI-driven public safety systems. Iconic Research and Engineering Journals, 9(5). https://doi.org/10.64388/IREV9I5-1722366

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

Odewabi, J. A., Amessouwoe, R. E. A., & Kpoka, M. I. (2025a). AI-assisted audiovisual localization across African and Francophone markets: Cultural specificity, narrative meaning, and human oversight. Gulf Journal of Computer Sciences, 1(4), 170-190. https://doi.org/10.51594/gjcs.v1i4.220

Odeyemi, O. H., & Idowu, A. O. (2026). Automating the hospital revenue cycle: A review of artificial intelligence and robotic process automation adoption in claims management, denial prevention, and patient billing in United States hospitals. International Journal of Technology, Health and Sustainability, 2(3), 1294-1311.

OECD.AI. (2025). Replit AI coding tool deletes live production database and fakes data (AI Incidents Monitor). https://oecd.ai/en/incidents/2025-07-19-1eb1

Ogbole, J. I., Okoruwa, P. O., Babatope, O. M., & Oyewole, T. (2021). Developing an integrated data visualization model for continuous business performance monitoring and optimization. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 441-467. https://doi.org/10.32628/IJSRCSEIT

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.

Ogundairo, K. M. (2025). Hardening the autonomous value chain: Lean Six Sigma guardrails and multi-enterprise ETL architecture for agentic supply chain orchestration. IIARD International Journal of Economics and Business Management, 11(12), 441-478. https://doi.org/10.56201/ijebm.vol.11.no12.2025.pg441.478

Ogundairo, K. M., & Ayivi-Donkor, S. S. (2024b). The vanishing interface: Why the coming era of autonomous agents demands a paradigm shift in product marketing architecture. IIARD International Journal of Economics and Business Management, 10(11), 350-385. https://doi.org/10.56201/ijebm.v10.no11.2024.pg350.385

Ogunwola, T. A. (2026). Security and resilience considerations for software-defined wide area network deployments in multi-site enterprise environments. International Advanced Research Journal in Science, Engineering and Technology, 12(1). https://doi.org/10.17148/iarjset.2025.12150

Ogunwola, T. A., & Alozie, C. (2026a). Architecting secure and compliant distributed healthcare networks: Operational approaches to health insurance portability and accountability act and health information trust alliance alignment. International Journal of Computer Applications, 187(111), 1-6.

Ogunwola, T. A., & Alozie, C. (2026b). Enterprise firewall modernization for business continuity: A framework for secure migration and operational stability. Computer Science & IT Research Journal, 7(5), 347-361. https://doi.org/10.51594/csitrj.v7i5.2287

Ogunwola, T. A., & Deborah, F. O. (2026). Enterprise network resilience as a national security imperative: Strategies for protecting United States critical infrastructure. International Advanced Research Journal in Science, Engineering and Technology, 12(10). https://doi.org/10.17148/iarjset.2025.121048

Ogunwola, T. A., Owoyemi, T. A., & Iyanda, C. (2026). Cybersecurity and network integration risk management during corporate acquisitions and infrastructure consolidation. Computer Science & IT Research Journal, 7(6), 389-404. https://doi.org/10.51594/csitrj.v7i6.2305

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

Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2024b). Framework for secure and scalable supply chain systems supporting national energy reliability. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 2816-2826. https://doi.org/10.62225/2583049X.2024.4.6.5494

Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2024f). Supply chain automation framework using service management platforms. Shodhshauryam, International Scientific Refereed Research Journal, 7(2), 157-177. https://doi.org/10.32628/SHISRRJ2472157

Okonkwo, C. S., Agbabiaka, J., Okeke, O. T., & Mayo, W. (2025). Framework for national-scale supply chain optimization through integrated IT and procurement systems. Gulf Journal of Advance Business Research, 3(12), 1610-1625. https://doi.org/10.51594/gjabr.v3i12.189

Okonkwo, C. S., Ahiaeke Patrick, M. C., Okeke, O. T., & Mayo, W. (2023). Framework for integrating IT systems engineering with supply chain operations. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2580-2589. https://doi.org/10.62225/2583049X.2023.3.6.5500

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 [Verify pages: the article running header reads 318-326.]

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

Olodo, A., Akanbi, O., & Adenuga, O. (2026a). Conceptualizing a lean-standardized predictive maintenance framework for high-vacuum deposition equipment. International Journal of Engineering and Modern Technology, 12(3), 295-322. https://doi.org/10.56201/ijemt.vol.12.no3.2026.pg295.322

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. (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. (2025b). A review of intermediary liability and content governance obligations for digital platforms under the DSA, DMCA, and CDA regimes. International Journal of Social Sciences and Management Research, 11(8), 558-582. https://doi.org/10.56201/ijssmr.vol.11no8.2025.pg558.582

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

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2026a). A conceptual model for integrating legal, quantitative, and operational disciplines in next-generation regulatory risk leadership. International Journal of Social Sciences and Management Research, 12(7), 524-550. https://doi.org/10.56201/ijssmr.vol.12no7.2026.pg524.550

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2026b). Conceptualizing enterprise AI governance functions as institutional standards for auditable and defensible risk management. Journal of Accounting and Financial Management, 12(7), 326-356. https://doi.org/10.56201/jafm.vol.12.no7.2026.p326.356

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., Adegbite, M. P., & Ogbonna, C. S. (2026). Human factors in information security: A capability framework for administrative professionals in the digital workplace. World Journal of Innovation and Modern Technology, 10(5), 154-179. https://doi.org/10.56201/wjimt.v10.no5.2026.pg154.179

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

Oparah, O. S., Ezeh, F. E., Olatunji, G. I., & Ajayi, O. O. (2021). AI-based risk stratification framework for large-scale public health emergency preparedness and response planning. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(1), 332-366.

Oracle. (n.d.). Oracle Autonomous Database: Unleash the potential of your data. https://www.oracle.com/webfolder/s/assets/ebook/oracle-autonomous-database/index.html

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.

Osinem, H. E., Eribenne, F., Peteranaba, S. F., & Soyege, O. S. (2025b). Conceptual foundations of ethical artificial intelligence adoption in healthcare organizations practice policy. International Journal of Technology, Health and Sustainability, 1(2). [Incomplete record; pages not given in source, verify on profile.]

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., & Edivri, J. (2026). An operational reliability and service assurance framework for enterprise IT systems supporting large user populations. Gulf Journal of Engineering and Technology, 2(1), 1-19. https://doi.org/10.51594/gjet.v2i1.205

Oteri, O., Olagunju, E. O., & Edivri, J. (2025a). Conceptual and architectural models for cloud native 5G packet core orchestration using Kubernetes and OpenStack. Gyanshauryam, International Scientific Refereed Research Journal, 8(5), 52-92.

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

OWASP GenAI Security Project. (2025, December 9). OWASP Top 10 for Agentic Applications: The benchmark for agentic security in the age of autonomous AI. https://genai.owasp.org/2025/12/09/owasp-top-10-for-agentic-applications-the-benchmark-for-agentic-security-in-the-age-of-autonomous-ai/

Oyeleye, A. O., Dogbatsey, E. A., & Ebhojie, O. (2025). Embedding automated close controls in public sector ERP systems: A conceptual model for audit readiness and financial reporting quality. Zenodo. https://doi.org/10.5281/zenodo.20097950 [Originally numbered 2(1), 110-130; journal name not captured in source.]

Oyesiji, S. O., Anunagba, C. O., Nwakamma, S., & Sankara, H. W. Y. C. (2026). Automated validation in embedded IoT development: A review of continuous integration and delivery across the fidelity ladder. Journal of Engineering Research and Reports, 28(9), 145-157. https://doi.org/10.9734/jerr/2026/v28i92005

Oyesiji, S. O., Ndupu, K. C., Anunagba, C. O., & Sankara, H. W. Y. C. (2026). On-device privacy and zero-knowledge storage in mobile applications: A review with attention to cross-platform React Native development. Journal of Engineering Research and Reports, 28(9), 102-114. https://doi.org/10.9734/jerr/2026/v28i92001

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), 286-297.

Pavlo, A., Angulo, G., Arulraj, J., Lin, H., Lin, J., Ma, L., Menon, P., Mowry, T. C., Perron, M., Quah, I., Santurkar, S., Tomasic, A., Toor, S., Van Aken, D., Wang, Z., Wu, Y., Xian, R., & Zhang, T. (2017). Self-driving database management systems. In *Proceedings of the Conference on Innovative Data Systems Research (CIDR)*.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77.

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.

Peteranaba, S. F., Osinem, H. E., Eribenne, F., & Soyege, O. S. (2023a). Digital documentation and HIPAA compliance in remote clinical support roles: Workflow design, data integrity, and operational risk mitigation. Asian Pacific Journal of Nursing and Health Sciences, 6(2), 38-52.

Quainoo, R., Ogundapo, O., & Asiedu, W. A. (2025b). Test automation in wireless hardware engineering: A comprehensive review of scripting frameworks and instrument control strategies. International Journal of Engineering and Modern Technology, 11(10), 405-464. https://doi.org/10.56201/ijemt.vol.11.no10.2025.pg405.464

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

Revefi. (2026, August 13). How to become an AI database administrator (AI DBA). https://www.revefi.com/blog/how-to-become-ai-dba

SAE International. (2021). *Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles* (J3016_202104).

Sakyi, J. K., Nnabueze, S. B., Filani, O. M., Okojie, J. S., & Babatope, O. M. (2024b). Digital transformation in service delivery leveraging automation and risk reduction for long-term commercial efficiency. International Journal of Advanced Multidisciplinary Research and Studies, 4(4), 1446-1464.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE, 63*(9), 1278-1308.

Sanni, J. O., Iwuanyanwu, U. A., & Essien, M. A. (2025). Problem-oriented process mining for auditable marketing automation lifecycle control. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 1933-1947. https://doi.org/10.62225/2583049X.2025.5.6.5650

Sanni, J. O., Iwuanyanwu, U. A., & Essien, M. A. (2026). Designing explainable AI based marketing automation architectures for healthcare and financial applications. World Scientific News, 213, 119-148. https://doi.org/10.65770/MJFK8593

Sanni, J. O., Iwuanyanwu, U. A., Essien, M. A., & Attah, A. (2023). Lifecycle-aware marketing automation using federated learning for secure cross-organizational data management. Gyanshauryam, International Scientific Refereed Research Journal, 6(6), 337-364. https://doi.org/10.32628/GISRRJ236642

Sanni, J. O., Iwuanyanwu, U. A., Essien, M. A., Atima, M. E., & Attah, A. (2022). Adaptive control models for AI-driven marketing automation in financial compliance environments. Shodhshauryam, International Scientific Refereed Research Journal, 5(1), 243-270. https://doi.org/10.32628/SHISRRJ247133

Shah, R., Oziri, S. T., & Seyi-Lande, O. B. (2025). A framework for leveraging artificial intelligence in strategic business decision-making. Gulf Journal of Advance Business Research, 3(11), 1517-1558.

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., & Shittu, M. A. (2024). AI powered digital twins for predictive maintenance and operational optimization of renewable energy systems. International Journal of Science, Architecture, Technology and Environment, 1, 151-163. https://doi.org/10.63680/ijsate0324085.011

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

Shittu, M. A., Shittu, H., Akintayo, T. A., & Opara, I. S. (2025). IoT enabled microgrid and BESS integration in ADMS: A framework for climate resilient grid operation. In 2025 IEEE Symposium on Wireless Technology & Applications (ISWTA) (pp. 1-9). IEEE. https://doi.org/10.1109/ISWTA68114.2025.11330023

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

Sunday, E. A., Omoegun, G. O., Essien, M. A., & Oluokun, O. A. (2020). Transitioning from reactive to predictive maintenance in mechanical systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(6), 425-447.

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), 356-367.

Travers Smith. (2026). The EU AI Act: The countdown begins, what you need to know. https://traverssmith.com/knowledge/knowledge-container/the-eu-ai-act-the-countdown-begins-what-you-need-to-know

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. (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

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

Ukadike, C. A. (2025). Organizational readiness for artificial intelligence transformation in the human resources function: A conceptual framework. World Journal of Innovation and Modern Technology, 9(12), 271-295. https://doi.org/10.56201/wjimt.v9.no12.2025.pg271.295

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.

Van Aken, D., Pavlo, A., Gordon, G. J., & Zhang, B. (2017). Automatic database management system tuning through large-scale machine learning. In *Proceedings of the 2017 ACM SIGMOD International Conference on Management of Data* (pp. 1009-1024).

Walawalkar, G., Oduleye, T. E., Adesuyi, M. O., & Kalu, A. (2026). Next-generation financial analytics frameworks for AI-enabled enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 6(1), 1779-1791.

Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of Management Review, 14*(4), 490-495.

Zhou, J., Umekwe-Edevwie, E. O., Famakinwa, C., Oduh, P., & Oduh, P. (2024). Beyond traditional schedule assurance: A critical review of predictive schedule-risk methodologies for hyperscale AI data-center construction. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3489-3505. https://doi.org/10.62225/2583049X.2024.4.6.6919