ResearchLEAP

Journal of International Business Research and Marketing
Volume x, Issue x, year
journal homepage: www.researchleap.com

Designing Autonomous Decision Loops for Cybersecurity, Banking, and Healthcare in Kenya and Africa: A Governance-First Conceptual Framework

[1]Stanley Mwangi Chege, [2]Mary Wainaina

[1] Department of Information and Computer Science, School of Science, Catholic University of Eastern Africa, Nairobi, Kenya

2021 Research Leap/Inovatus Services Ltd. All rights reserved.

DOI:
URL:

Keywords: *Autonomous decision loops, AI governance, cybersecurity, banking, healthcare, Africa, Kenya, decision intelligence*

ABSTRACT

African organizations are operating in increasingly complex and high-velocity digital environments characterized by mobile-first service delivery, persistent cyber threats, skills shortages, and rising regulatory expectations. Traditional human-centered decision-making models struggle to respond effectively at machine speed, particularly in critical sectors such as cybersecurity, banking, and healthcare. This paper proposes a governance-first conceptual framework for **Autonomous Decision Loops (ADLs)**—closed-loop systems that sense, decide, act, learn, and operate under continuous oversight. Grounded in decision-cycle theory, decision intelligence, high-reliability organizing, and contemporary AI governance standards, the framework explains how ADLs can reduce response latency, embed compliance, and enhance operational resilience in Kenya and across Africa. The study develops testable propositions and discusses implications for managers, regulators, and policymakers seeking to balance autonomy with accountability in high-risk digital ecosystems.

1. Introduction

Digital transformation across Kenya and the wider African region has accelerated rapidly over the past decade, driven by mobile financial services, digital health initiatives, and cloud-based enterprise systems. While this transformation has expanded access and efficiency, it has also intensified exposure to cyber threats, financial fraud, and systemic operational risks (Serianu, 2025). Decision windows in these environments are increasingly measured in seconds rather than hours or days, placing pressure on organizations that continue to rely on manual escalation and periodic governance processes. In intense digital environment, technological innovation is crucial for competitivness and sustainability (Maxamadumarovich et al., 2012).

In cybersecurity operations, security operations centres (SOCs) face high alert volumes and persistent adversaries operating at machine speed. In banking and fintech ecosystems, particularly mobile-money-dominated markets, fraud losses can occur instantaneously if detection and interdiction are delayed (World Bank, 2017). In healthcare, system downtime and cyber incidents can directly affect patient safety and continuity of care (Health-ISAC, 2025). These conditions expose the limitations of traditional, human-centric decision-making models.

This paper argues that **Autonomous Decision Loops (ADLs)** offer a viable strategic response. Rather than automating isolated tasks, ADLs delegate bounded decision authority to machines operating within clearly defined governance constraints. By embedding policy, risk appetite, and compliance requirements directly into decision logic, ADLs enable organizations to act at machine speed while preserving accountability. The purpose of this study is to develop a **governance-first conceptual framework** for ADLs and to apply it to cybersecurity, banking, and healthcare contexts in Kenya and Africa.

2. Literature review

2.1 Decision cycles and autonomy

The concept of decision cycles has its roots in the Observe–Orient–Decide–Act (OODA) loop, originally developed to explain competitive advantage in dynamic environments. Contemporary scholarship highlights that accelerating decision cycles can confer strategic advantage, but also introduces risks when orientation and decision stages are increasingly shaped by algorithmic systems (Johnson, 2022). Automating decision loops without appropriate oversight may amplify errors, bias, or unintended consequences at scale.

2.2 Decision intelligence and engineered decision systems

Decision Intelligence (DI) extends traditional analytics by treating decisions as explicit, designable assets rather than by-products of analysis. DI emphasizes modeling decision logic, measuring outcomes, and continuously improving decision quality through feedback (Gartner, n.d.). This perspective aligns closely with ADLs, which operationalize DI principles by linking sensing, decision-making, execution, and learning within a closed loop. Adoption of AI systems provide data management for informed decision making and governance (Obrenovic et al., 2026).

2.3 High-reliability organizing and resilience

High-reliability organization (HRO) theory examines how organizations operate safely in complex, high-risk environments. Core principles include preoccupation with failure, sensitivity to operations, and commitment to resilience. These principles suggest that autonomy must be carefully bounded and supported by mechanisms for rapid detection and containment of failure. ADLs designed without HRO considerations risk becoming brittle rather than resilient.

2.4 Automation in cybersecurity, banking, and healthcare

In cybersecurity, security orchestration, automation, and response (SOAR) technologies are increasingly recognized as necessary to manage alert volumes and reduce response times. Empirical and conceptual studies indicate that automation improves operational effectiveness when integrated with skilled human oversight rather than replacing it entirely (Ismail, 2025).

In banking, the literature on fraud detection demonstrates that static rules and post-hoc reviews are insufficient in environments characterized by rapidly evolving fraud typologies. Adaptive, real-time detection mechanisms are required to mitigate losses effectively (Preciado Martínez et al., 2025). Kenyan and regional studies further emphasize the unique challenges posed by mobile-first financial ecosystems (World Bank, 2017).

In healthcare, industry threat intelligence reports document a persistent rise in ransomware and availability-focused attacks, underscoring the need for resilient, automated response capabilities that prioritize patient safety and continuity of care (Health-ISAC, 2025).

2.5 Governance and regulatory context in Kenya

Kenya's Data Protection Act (2019) establishes obligations for safeguarding personal data, including requirements for appropriate security controls and accountability. In financial services, regulatory frameworks emphasize consumer protection, AML/CFT compliance, and operational resilience. These regulatory expectations reinforce the need for decision systems that are not only fast, but also auditable and explainable. The NIST Artificial Intelligence Risk Management Framework (AI RMF) further provides guidance on integrating governance across the AI lifecycle, emphasizing that governance should function as a cross-cutting control plane (NIST, 2023).

Figure 1: ADLs for Africa's Critical Industries

3. Conceptual Framework: A Governance-First ADL

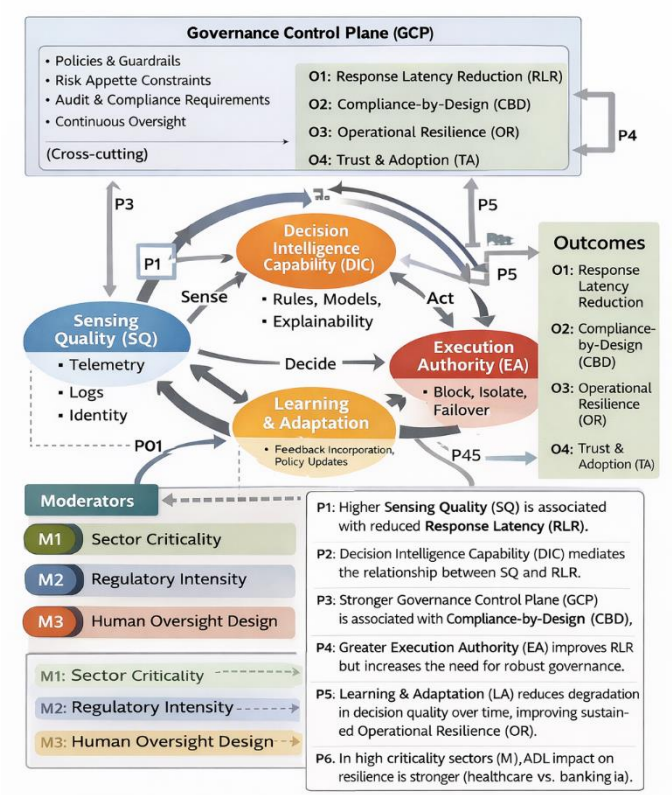

Figure 1: Conceptual framework for governance-first ADLs in Kenya/Africa

Model

This study proposes a **Governance-First Autonomous Decision Loop (GF-ADL)** framework composed of five core constructs: sensing quality, decision intelligence capability, execution authority, learning and adaptation, and a governance control plane.

Recent Empirical Evidence on Autonomous Systems

Radanliev and De Roure (2022) show that self-optimising and self-adaptive AI can strengthen healthcare cybersecurity by enabling continuous monitoring and autonomous response to evolving threats. Their findings support the use of closed-loop decision systems in complex healthcare environments where static controls are insufficient.

Kalejaiye (2022) demonstrates that reinforcement learning–driven cyber defense frameworks enable autonomous risk prediction and adaptive threat response without reliance on predefined rules. This approach aligns with decision loop architectures that improve defensive effectiveness through continuous learning.

Koh (2025) highlights the role of AI-based cybersecurity and fraud analytics in securing integrated healthcare and cloud banking ecosystems. The study underscores the necessity of autonomous decision mechanisms to manage high-velocity data flows and cross-domain risk.

Wahed et al. (2025) argue that AI-driven autonomous defense systems are essential for protecting telemedicine platforms against real-time cyber threats. Their work emphasizes the value of machine-speed decision and response capabilities in distributed healthcare environments.

Burrell (2024) examines the complexity of healthcare cybersecurity risk management and identifies limitations in traditional governance and control models. The study supports the need for adaptive, system-level decision frameworks capable of responding dynamically to emerging risks.

Taiwo et al. (2021) propose human-centered privacy protection frameworks that emphasize accountability and transparency in financial and health analytics platforms. Their findings reinforce the importance of integrating human oversight into autonomous decision systems to preserve trust and regulatory compliance.

3.1 Core constructs

Sensing Quality (SQ) refers to the completeness, timeliness, and integrity of data collected from operational environments, such as security telemetry, transaction logs, or system availability metrics. High sensing quality is a prerequisite for reliable autonomous decisions.

Decision Intelligence Capability (DIC) encompasses the models, rules, and reasoning mechanisms used to evaluate options and select actions. This includes explainability and the ability to assess outcomes against intended objectives (Gartner, n.d.).

Execution Authority (EA) defines the scope of actions that an ADL is permitted to perform autonomously, such as isolating a system, blocking a transaction, or triggering failover procedures.

Learning and Adaptation (LA) capture the mechanisms through which the system incorporates feedback, detects drift, and updates decision logic over time to maintain effectiveness in dynamic environments.

Governance Control Plane (GCP) represents the policies, risk thresholds, approval mechanisms, audit trails, and accountability structures that constrain and guide the entire loop. Consistent with the NIST AI RMF, governance is treated as a cross-cutting function rather than a post-hoc review activity (NIST, 2023).

3.2 Outcomes and moderators

The framework links these constructs to four primary outcomes: response latency reduction, compliance-by-design, operational resilience, and stakeholder trust. Sector criticality, regulatory intensity, and human oversight design are proposed as moderators influencing the strength and direction of these relationships

4. Application to Key Sectors in Kenya and Africa

4.1 Cybersecurity

In cybersecurity, ADLs enable autonomous detection and response by integrating sensing from endpoints, networks, and

identities with decision logic that prioritizes threats based on business impact. Execution authority may include isolating compromised assets or terminating malicious sessions. Learning mechanisms reduce false positives over time, while governance ensures that actions are auditable and aligned with organizational risk appetite. Such designs address the skills shortages and alert fatigue documented in African SOC environments (Serianu, 2025).

4.2 Banking and fintech

In banking and fintech, particularly mobile-money ecosystems, ADLs support real-time fraud interdiction. Continuous sensing of transactions and behavioral signals feeds adaptive decision models that can block or step-up authentication before funds are lost. Governance mechanisms embed AML/CFT and consumer protection requirements directly into decision logic, enabling continuous compliance rather than retrospective review (World Bank, 2017; Preciado Martínez et al., 2025).

4.3 Healthcare

In healthcare, ADLs prioritize system availability and patient safety. Sensing focuses on system integrity and access anomalies, while decision logic incorporates clinical criticality. Autonomous actions may include isolating affected systems and triggering disaster recovery. Governance mechanisms ensure alignment with data protection obligations and allow for human override in safety-critical scenarios (Health-ISAC, 2025).

5. Research Propositions

Based on the framework, the following propositions are advanced for empirical testing:

P1: Higher sensing quality is positively associated with response latency reduction.
P2: Decision intelligence capability mediates the relationship between sensing quality and response latency reduction.
P3: A stronger governance control plane is positively associated with compliance-by-design outcomes.
P4: Greater execution authority improves response latency but increases the need for robust governance mechanisms.
P5: Learning and adaptation reduce degradation in decision quality over time, improving sustained resilience.
P6: The impact of ADLs on operational resilience is stronger in healthcare than in banking or general cybersecurity contexts.

6. Discussion

The governance-first ADL framework contributes to the literature by integrating decision-cycle theory, decision intelligence, and AI governance into a unified model tailored to African contexts. For practitioners, the framework emphasizes that autonomy should be calibrated rather than maximized. The need for governance in all digital environments can add to the strain, while interventions can curtail negative outcomes for users (Abueva et al., 2025). For regulators and policymakers, it highlights the importance of encouraging designs that embed compliance and accountability within autonomous systems.

7. Conclusion

As Kenyan and African organizations confront machine-speed risks in critical sectors, the delegation of bounded decision authority to autonomous systems becomes a strategic necessity. This paper has proposed a governance-first conceptual framework for ADLs and demonstrated its relevance to cybersecurity, banking, and healthcare. By embedding governance into the core of autonomous decision-making, organizations can achieve speed, resilience, and accountability simultaneously. Future research should empirically test the proposed relationships and explore cross-country variations in regulatory and institutional contexts.

Literature

- BAbueva, N., Buzelo, A., Wu, Y., Turniyazova, Z., Karakushev, D., & Obrenovic, B. (2025). Digital technologies and student mental health: Risks of social media and the promise of virtual reality and autonomous sensory meridian response interventions. *Psychology Research and Behavior Management*, 2179-2191.
- Burrell, D. N. (2024). Understanding healthcare cybersecurity risk management complexity. *Land Forces Academy Review*, *29*(1), 38-49.
- Gartner, Inc. (n.d.). *Decision intelligence*. https://www.gartner.com/en/information-technology/glossary/decision-intelligence
- Health-ISAC. (2025). *2025 health sector cyber threat landscape*. https://health-isac.org
- Ismail, I. (2025). Toward robust security orchestration and automated response. *Information, 16*(5), 365.
- Johnson, J. (2022). Automating the OODA loop in the age of intelligent machines. *Journal of Strategic Studies*. https://doi.org/10.1080/14702436.2022.2102486
- Kalejaiye, A. N. (2022). Reinforcement learning-driven cyber defense frameworks: Autonomous decision-making for dynamic risk prediction and adaptive threat response strategies. *International Journal of Engineering Technology Research & Management (IJETRM)*, *6*(12), 92-111.
- Kenya Law. (2019). *Data Protection Act, No. 24 of 2019*. https://new.kenyalaw.org
- Koh, C. W. H. B. (2025). AI-Based Cybersecurity and Fraud Analytics for Healthcare Data Integration in Cloud Banking Ecosystems. *International Journal of Engineering & Extended Technologies Research (IJEETR), 7*(6), 11021-11028.
- Maxamadumarovich, U. A., Obrenovic, B., & Amonboyev, M. (2012). Understanding the innovation concept. *Journal on Innovation and Sustainability* RISUS, 3(3), 19-26.
- NIST. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). https://nvlpubs.nist.gov
- Obrenovic, B., Asa, A. R., & Oblakovic, G. (2026).

The use of ChatGPT in the workplace: a bibliometric analysis of integration and influence trends. *AI & SOCIETY*, 41(1), 655-668.

- Preciado Martínez, P. M., et al. (2025). Comparative analysis of machine learning models for banking fraud detection. *Cogent Engineering, 12*(1).
- Radanliev, P., & De Roure, D. (2022). Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptative artificial intelligence (part 2). *Health and Technology*, *12*(5), 923-929.
- Serianu. (2025). *Africa cybersecurity report – Kenya*. https://www.serianu.com
- Taiwo, A. E., Omolayo, O., Aduloju, T. D., Okare, B. P., Oyasiji, O., & Okesiji, A. (2021). Human-centered privacy protection frameworks for cyber governance in financial and health analytics platforms. *International Journal of Multidisciplinary Research and Growth Evaluation*, *2*(3), 659-668.
- Wahed, M. A., Wahed, S. A., & Alzoubi, A. E. (2025). AI-Driven Cybersecurity for Telemedicine: Enhancing Protection Through Autonomous Defense Systems. In *AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense* (pp. 375-406). IGI Global Scientific Publishing.
- World Bank. (2017). *Fraud in mobile financial services*. https://documents.worldbank.org