ZECITI CISO BRIEFING | 2027

Six priorities for cyber leaders in African finance and government.

A sourced briefing for attendees of The Cyber Accountability Forum, Abuja, 12 March 2027. What regulators and threat reports are signalling, and the questions to take to your board.

Hosted by ZECITI. Executive judgment. Technical depth.

01 Treat AI agents as identities you must govern

Fewer than half of CISOs are confident they can identify every AI agent in their environment (47%), centrally control what agents can access (46%) or authorize what each agent may do (45%). A separate summary of the same survey reports that 81% of security leaders worry about excessive AI access.

Source: Okta, Global CISO Insights 2026 (survey of about 300 security executives); SC Media summary.

ZECITI view: give every agent an owner, a scope and an audit trail before the next deployment, and add agents to the same access reviews as people.

02 Evidence alignment with the CBN framework, not intent

The Central Bank of Nigeria issued its Risk-Based Cybersecurity Framework and Guidelines for deposit money banks and payment service banks on 31 May 2024 as minimum requirements. On 30 March 2026 it introduced a mandatory Cybersecurity Self-Assessment Tool for regulated financial institutions, with implementation roadmaps reported due by 10 June 2026.

Sources: CBN framework letter (2024); Digital Policy Alert (30 March 2026); Vanguard; Channels TV.

ZECITI view: a self-assessment is only as strong as the evidence behind each answer. Keep decision records, exceptions and test results where a supervisor can follow them.

03 Instant payments now carry explicit security baselines

A CBN circular dated 12 March 2026 set minimum baseline security requirements for instant payment systems, including liveness checks and device limits, with a compliance date reported as 1 July 2026.

Source: TechCabal reporting on the 12 March 2026 CBN circular.

ZECITI view: fraud controls and cyber controls are converging. Assign one accountable owner across both.

04 Exposure follows the value

Technology, the public sector and financial services together account for 44% of observed cyber threat activity across Africa. INTERPOL's African Cyberthreat Assessment Report 2026 identifies AI as an accelerant of cybercrime. A West Africa threat report by Esentry found more than NGN 1 billion in fraudulent transactions slipped past conventional security tools in the first half of 2026.

Sources: Mastercard Africa Cybersecurity Whitepaper (2026); INTERPOL (June 2026), via Help Net Security; Esentry via Legit.ng.

ZECITI view: test controls against the abuse of legitimate access and credentials, not only against external intrusion.

05 Prepare for national expectations

In February 2026 the Federal Government said it planned a national cybersecurity framework, expected to be implemented later that year, that would require organisations to meet minimum cybersecurity spending thresholds. The UNODC 2025 Nigeria Cybercrime Assessment estimated losses of NGN 1.1 trillion across banks, telecoms and government agencies between 2017 and 2023.

Source: Nairametrics, 10 February 2026. Status of the framework should be checked against current official publications.

ZECITI view: build a cost-and-outcome view of cyber spend now, so you can show what it buys.

06 Design for the talent gap

Africa has approximately 200,000 unfilled cybersecurity positions, a 23% workforce gap. EY's Africa Cybersecurity Threat Outlook 2026 describes 12 trends in which identity compromise, operational disruption and leadership decision-making reshape resilience.

Sources: Mastercard (2026); EY Africa Cybersecurity Threat Outlook 2026 (May 2026).

ZECITI view: hiring alone will not close the gap. Reduce the number of decisions that need a specialist, and document the ones that do.

FOR YOUR NEXT BOARD OR AUDIT COMMITTEE

Eight questions to take back.

- Which AI agents and automations act in our environment today, who owns each one, and what can each one access?
- Can we show a supervisor the evidence behind every answer in our CBN self-assessment, and who signed it off?
- Which cyber and fraud controls overlap, and who is accountable for the combined outcome?
- What would we need to prove about instant-payment security controls in the next 30 days?
- Where are our approved exceptions to policy, who accepted the risk, and when do they expire?
- Which third parties hold legitimate access to our systems, and how would we know if it was misused?
- What does our cyber spend buy, in outcomes the board can read?
- If a regulator, a customer or the press asked who is accountable for cyber risk, would the answer be the same in every part of the organisation?

SOURCES

Okta, Global CISO Insights 2026: okta.com/newsroom/articles/global-ciso-insights-2026/

SC Media, Loss of control: the AI agent governance crisis: scworld.com/resource/loss-of-control-the-ai-agent-governance-crisis

Central Bank of Nigeria, Risk-Based Cybersecurity Framework and Guidelines for DMBs and PSBs (2024): cbn.gov.ng

Digital Policy Alert, CBN directive on the Cybersecurity Self-Assessment Tool (30 March 2026): digitalpolicyalert.org

Vanguard Nigeria and Channels TV reporting on CBN cybersecurity timelines (2026): vanguardngr.com, channelstv.com

TechCabal, CBN mandates liveness checks and device limits to fight digital banking fraud: techcabal.com

Mastercard, Africa Cybersecurity Whitepaper: mastercard.com/mea/en/business/cybersecurity-fraud-prevention/africa-cybersecurity-whitepaper.html

INTERPOL, African Cyberthreat Assessment Report 2026 (June 2026), and Help Net Security coverage (5 August 2026)

Legit.ng, Esentry West Africa threat landscape report (2026)

Nairametrics, FG to launch cybersecurity framework (10 February 2026)

EY, Africa Cybersecurity Threat Outlook 2026 (May 2026): ey.com

This briefing is compiled from public sources as of 23 November 2026 and is general information, not legal or regulatory advice. Figures are quoted as published by each source; please check the original before relying on them. "ZECITI view" notes are ZECITI's own perspective.

ZECITI Technologies sp. z o.o. | zecititech.com | advisory@zecititech.com