Association des Banques Centrales Africaines

Association of African Central Banks

CONTINENTAL SEMINAR ON THE THEME

"Cyber Risks and Innovative Financial Technologies:

Challenges and Policy Responses"

Organized by: Bank Al-Maghrib

(Rabat, Morocco, July 21 – 23, 2025)

REPORT

1. INTRODUCTION

In line with the decision made during the Assembly of Governors held in Mauritius on September 4, 2024, the 2025 Continental Seminar of the Association of African Central Banks (AACB) was hosted by Bank Al-Maghrib. The Seminar was held in Rabat, Morocco, from July 21 – 23, 2025, under the theme *"Cyber Risks and Innovative Financial Technologies: Challenges and Policy Responses".* Eighty-five delegates from member Central Banks and representatives of regional and international institutions attended the Seminar. The list of participants is attached in the appendix of this report.

2. OPENING CEREMONY

The opening ceremony was chaired by Mr. Abdellatif JOUAHRI, Honourable Governor of Bank Al-Maghrib.

In his introductory remarks, Dr. Djoulassi Kokou OLOUFADE, AACB Executive Secretary, speaking on behalf of the AACB Chairperson, Dr. Rama Krishna SITHANEN, G.C.S.K., Honourable Governor of Bank of Mauritius, expressed his sincere gratitude to Bank Al-Maghrib for having agreed to host the 2025 Continental Seminar and for the exceptional efforts made in organizing the event. He extended his profound appreciation to the Head of State and Commander of the Faithful, His Majesty King Mohammed VI, may God assist him, as well as to the Government and people of Morocco for the outstanding arrangements made to ensure a pleasant stay. He also thanked the experts for their generous acceptance to share their insights on the topics under discussion during the Seminar. Furthermore, he congratulated the participants for their strong turnout, which reflects their firm commitment to contributing to the monetary and financial integration process in Africa.

In addition, the Executive Secretary underscored that the AACB continues to pursue its objectives by promoting the exchange of ideas and experiences related to monetary, financial, banking, and economic issues in Africa. The annual Continental Seminar stands as a key platform for achieving these goals. The theme of the 2025 Seminar, which focuses on cyber risks and innovative financial technologies, aligns with the ongoing digital transformation of African financial systems, characterized by the rise of mobile services, Artificial Intelligence (AI), digital payment platforms, and cloud computing. Africa is distinguished by its dynamic and inclusive innovation, illustrated by the rapid growth in mobile money transactions.

However, this increasing digitalization is accompanied by heightened exposure to cyber risks, threatening financial stability, data protection, and user confidence. The Executive Secretary emphasized the scale of cyber threats identified by the World Bank and INTERPOL, particularly the rise in ransomware attacks and tech-enabled fraud targeting Central Banks, public services, and private enterprises alike. Against this backdrop, the Seminar aims to explore the opportunities that technology offers to enhance financial inclusion, while identifying vulnerabilities and sharing regulatory best practices.

To conclude his statement, the Executive Secretary expressed confidence in the quality of the discussions and the relevance of the recommendations to be submitted to the Honourable

Governors during the upcoming AACB Annual Meetings in Yaoundé, scheduled for November 2025.

In his opening address, Mr. Abdellatif JOUAHRI, Honourable Governor of Bank Al-Maghrib, welcomed all participants and wished them a pleasant stay in Rabat, the capital of the Kingdom of Morocco. He expressed gratitude to the AACB for accepting Bank Al-Maghrib's proposal to host such an important event in Morocco and announced that the Seminar had gathered participants from African Central Banks as well as regional and international partner institutions.

He highlighted that the 2025 theme, "Cyber Risks and Innovative Financial Technologies: Strategic Challenges and Responses", is highly relevant and timely, given the wave of digital innovations in recent years that are profoundly transforming African countries and opening up unprecedented opportunities for the financial services sector. He noted that it is the responsibility of Central Banks to foster innovation to meet both their own operational needs and those of the private financial sector, while remaining vigilant to associated risks and strengthening their capacity to mitigate threats to the stability of the monetary and financial system.

According to the Governor, digital strategies, particularly in areas such as cybersecurity for cross-border digital payments and anti-money laundering/combating the financing of terrorism (AML/CFT), require regional cooperation led by the AACB to share best practices and regulatory frameworks. FinTech is a key driver of development, particularly in emerging economies, revolutionizing finance by expanding product offerings, improving services, lowering costs, and redefining the customer experience.

The Honourable Governor further noted that mobile money, instant transfers, peer-to-peer payments, and FinTech solutions have enabled remarkable performance in several African countries. New credit models based on alternative data are emerging, facilitating access to finance for small businesses and individuals. African banks must adapt by forging partnerships with FinTech firms to counter the growing influence of "Big Tech" players in lending, driven by Artificial Intelligence.

He cited a 2024 McKinsey report, which forecasts a fivefold increase in revenues from African FinTech by 2028, although this growth remains concentrated in 11 key markets. FinTechs, however, face multiple challenges, including fragile profitability, limited access to financing, talent shortages, weak governance, and inadequate regulatory frameworks. The expansion of large global tech platforms (in payments, crypto-assets, and stablecoins), often operating outside regulatory oversight, threatens national payment systems and deepens market fragmentation.

These developments, according to the Governor, underscore the enhanced role of Central Banks in regulating payment systems and reinforcing their resilience. The Pan-African Payment and Settlement System (PAPSS), recently joined by Bank Al-Maghrib, is crucial for promoting innovation, efficiency, and autonomy across the continent. Authorities must also regulate crypto-assets and stablecoins, which pose risks of money laundering and disintermediation.

He stressed that the rapid pace of digital transformation increases Central Banks' exposure to cyber risks, making cyber resilience a core pillar of financial stability. Moreover, the growing

incidence of attacks, such as phishing and digital payment fraud, necessitates continuous strengthening of cybersecurity measures. In 2024, the average cost of a cyberattack on an African financial institution exceeded USD 2.5 million, with Africa being identified by INTERPOL as particularly vulnerable to such threats.

In conclusion, the Honourable Governor of Bank Al-Maghrib underscored the growing global cyber threats and the pressing need to strengthen cyber resilience through enhanced cooperation, especially at the continental level. He highlighted the role of the AACB's Cybersecurity Working Group, as well as Morocco's national efforts to establish a robust regulatory framework. He called for a concerted African approach, harmonized regulations, and the establishment of excellence centers to collectively address digital challenges. He concluded by reiterating his support for the AACB's mission and expressing his gratitude to the experts mobilized for the Seminar.

3. STRUCTURE OF THE SEMINAR

The Seminar was structured into two plenary sessions and breakout sessions. In the first plenary session, resource persons presented three sub-themes, while the second session focused on experience sharing by Central Bank representatives. The break-out sessions focused on three other sub-themes, with feedback on conclusions and recommendations.

3.1. Plenary Session 1: Presentation of the sub-themes

The session was chaired by Mr. Wilner Junior Boussougou, Head of the Financial Operations and Banking Activities Systems Administration Department, Banque des Etats de l'Afrique Centrale (BEAC). Mr. Soulaimane Lahrech, Founder of Talaty FinTech; Mr. Mohamed Tazi, Director of Information Systems Security, Attijariwafa Bank Group, and Ms. Najwa Benmadani, Director of Investigations and Financial Intelligence, National Financial Intelligence Authority (ANRF), presented the following sub-themes, respectively:

- Leveraging Big Data Analytics and Artificial Intelligence for Cross-border and Intercontinental Trade;
- Challenges of Innovative Financial Technologies in the Face of Growing Cyber Risks and Financial Inclusion Strategies;
- Cross-Border Digital Transactions, Cybersecurity, and Measures to Mitigate Money Laundering and Terrorism Financing (ML/FT).

a) Leveraging Big Data Analytics and Artificial Intelligence for Cross-border and Intercontinental Trade

In his presentation, Mr. Lahrech shared a comprehensive reflection with participants on the profound transformations reshaping cross-border trade, in light of advances in Artificial Intelligence (AI) and Big Data analytics. These technologies have moved beyond experimental stages; they are now actively redefining practices in logistics, compliance, trade finance, risk assessment, and transaction processing. For both public institutions and private operators, they offer powerful levers for enhancing efficiency, responsiveness, and transparency in a context where trade flows are increasingly fast-paced, complex, and exposed to heightened risks.

Continuing his remarks, the Speaker emphasized the need to lay a solid technological foundation for this transformation. Advanced AI systems are now capable of learning from experience, detecting subtle patterns, and making near-autonomous decisions. Big Data, in turn, enables the real-time processing of massive volumes of heterogeneous data, far beyond human capabilities or traditional tools. Mr. Lahrech also introduced more advanced concepts, such as generative AI, which can create novel content and insights, and agentic AI, which powers autonomous systems capable of acting independently in complex environments. General Artificial Intelligence (AGI), though still theoretical, holds the potential to disrupt all sectors of the economy.

However, Mr. Lahrech underlined that these concepts are far from abstract. They already have tangible applications, some of which are deployed at scale. For example, predictive analytics platforms can now forecast port congestion by combining maritime signals, satellite imagery, and Internet of Things (IoT) sensors. Such solutions help anticipate logistics bottlenecks and provide Central Banks with early signals on trade flows, well ahead of official data releases, offering strategic advantages in managing foreign exchange policies and reserves.

A flagship example cited by the Speaker was the Japanese customs system, which has used an automated inspection platform powered by X-ray imaging and machine learning for several years. This system identifies illicit goods in real-time while enhancing the fluidity of legitimate trade. It also enhances the quality of trade statistics and contributes to curbing illicit currency outflows, a challenge well-known to many African monetary authorities.

In the context of intra-African trade, the Jetstream Africa platform illustrates the potential of AI in trade finance. Connecting thousands of SMEs and freight forwarders across 14 countries, it automates document processing, anticipates cash flow needs, and facilitates multi-currency disbursements. This solution not only accelerates trade transactions but also provides Central Banks with valuable insights into currency demand and the risks of under-invoicing.

The regulatory compliance domain is also undergoing a profound shift thanks to agentic AI. These intelligent agents continuously monitor sanction lists, ownership structures, and transactions, including those on blockchain networks, to generate accurate alerts with significantly reduced false positives. A live demonstration of an "Agentic Crisis Room" showcased how such systems can support real-time responses to major disruptions in global trade, while ensuring decision traceability for regulators. At a time when value chains are being reconfigured, regulatory requirements are tightening, and competitiveness is critical, integrating AI and Big Data into trade systems is no longer a technical option; it is a strategic imperative. The key question is not whether to embrace these technologies, but rather how to accelerate their implementation in the service of African economies.

Discussions explored the growing role of AI and Big Data in transforming cross-border operations, particularly in areas such as trade, customs compliance, logistics, and payments. Several use cases were highlighted: autonomous X-ray inspection, currency flow surveillance, automated compliance monitoring, and advanced detection of financial risks. These technologies, already deployed in certain contexts, enable faster and more targeted interventions by Central Banks, particularly in anticipating inflationary shocks or guiding foreign exchange market policies.

Participants emphasized the strategic importance of developing sovereign data infrastructures to ensure local processing capabilities, while also recognizing the value of regional cooperation through federated and securitized systems. A key challenge identified was the quality and harmonization of data across countries and financial institutions, a prerequisite for the effective development of AI systems. Speakers also stressed the rise of explainable AI algorithms, which reconcile analytical power with decision-making transparency. The development of hybrid models integrating behavioral, fiscal, and political indicators was highlighted as a means to improve inflation forecasting.

Finally, several questions addressed governance, cybersecurity, the explainability of AI-driven decisions, and the adaptability of these innovations in countries with limited technical capacity. The example of Morocco, where startups specializing in cyber threat detection and an innovation hub have been launched, illustrates the proactive approach of certain Central Banks. The core idea remains that AI should not only be regulated but also fostered by encouraging local initiatives, sharing best practices, and anticipating emerging risks within increasingly interconnected financial ecosystems.

b) Challenges of Innovative Financial Technologies in the Face of Growing Cyber Risks and Financial Inclusion Strategies

The second sub-theme, presented by Mr. Tazi, focused on the challenges posed by innovative Financial Technologies (FinTechs) amid escalating cybercrime risks and the rapidly advancing financial inclusion across the African continent.

Mr. Tazi emphasized that African FinTechs play a critical role in fostering economic sovereignty and integrating unbanked populations. A notable example is the collaboration between Bank Al-Maghrib and local startups, which illustrates how the agility of FinTech firms, combined with the legitimacy of formal banking institutions, has significantly improved financial inclusion rates. This momentum has been further accelerated by the rise of mobile money, which now accounts for more than half of global mobile accounts, with a particularly strong footprint in Africa.

In this context of digital expansion, cybersecurity emerges as a strategic priority. Mr. Tazi drew attention to the sharp increase in cyberattacks across the continent, with weekly incidents in Africa up by 23 percent since 2023. He highlighted that 80 percent of African banks have experienced at least one cyberattack, with an average financial impact of USD 2.5 million. Threats are becoming increasingly sophisticated, ranging from ransomware and fraudulent transfers to phishing campaigns and deepfakes. The growing use of Artificial Intelligence by cybercriminals exacerbates the vulnerabilities of existing systems, particularly in environments characterized by service digitization, cloud adoption, and interconnection with external service providers.

To address this growing threat, Mr. Tazi outlined the pillars of a comprehensive cyber resilience framework tailored to African realities. Key measures include the adoption of Zero Trust architectures, the integration of security-by-design principles, enhanced oversight of third-party partners, the deployment of Security Operations Centers (SOCs), and continuous cybersecurity training for staff. He also cited Morocco's Law N° 05-20 on cybersecurity, enacted in 2020, as a modern legal framework particularly relevant to critical sectors such as banking, telecommunications, and insurance.

In conclusion, Mr. Tazi called for strengthened continental governance in cybersecurity. Through the "Casablanca Call," he advocated for coordination among African Central Banks, arguing that only a collective response can effectively address systemic threats. He illustrated this point with

a powerful metaphor: "The ant that travels alone moves quickly, but the colony crosses the desert." This image underscores the significance of solidarity, resource pooling, and knowledge sharing in fostering a secure, resilient, and inclusive African financial ecosystem.

The discussions shed light on the rapid pace of digital transformation and financial innovation in Africa, with a particular emphasis on the development of FinTech solutions. Participants highlighted significant progress in digital payments, financial inclusion, and the establishment of enabling regulatory frameworks. Several structural initiatives, such as regulatory sandboxes, fast-track licensing for FinTechs, and support mechanisms, demonstrate the commitment of African monetary authorities to foster a dynamic, inclusive, and resilient ecosystem. Key regional players such as Hightech Payment Systems (HPS) were cited as foundational to this evolution.

Moreover, there was a broad consensus on the critical importance of cybersecurity in the face of increasing digital risks. African Central Banks were urged to strengthen the resilience of financial systems by implementing harmonized regulatory frameworks, ensuring personal data protection, enabling electronic signatures, and adopting international best practices. Calls were made for collective action through the establishment of national and regional Computer Emergency Response Teams (CERTs), real-time sharing of threat intelligence, and the development of reinforced continental cybersecurity governance. Three core recommendations emerged: information sharing, regulatory harmonization, and capacity-building in cybersecurity.

Lastly, the discussions highlighted the need for effective and proactive governance, both within Central Banks and financial institutions operating across multiple jurisdictions. This governance must incorporate cybersecurity at the highest levels, ensure regulatory compliance, and enforce robust risk management for third-party service providers. The strategic importance of digital sovereignty and local data hosting was also emphasized, especially in light of the absence of major African Big Tech companies. The session concluded with a strong call for continental cooperation, institutional solidarity, and the integration of technology into a secure, inclusive, and sustainable African financial system.

c) Cross-Border Digital Transactions, Cybersecurity, and Measures to Mitigate Money Laundering and Terrorism Financing (ML/FT)

In her presentation, Mrs. Najwa Benmadani provided an in-depth analysis of the challenges associated with financial crime in the digital age.

She began by recalling the guiding principles of the Financial Action Task Force (FATF), the intergovernmental body responsible for setting global AML/CFT standards. She specifically highlighted the FATF's 40 Recommendations, which serve as the international normative framework, along with the mutual evaluation process used to assess national compliance. She also presented the role of the Middle East and North Africa Financial Action Task Force (MENAFATF), of which Morocco is a founding member and recent chair.

Mrs. Benmadani then addressed the specific risks emerging from the growth of cross-border digital transactions. While such transactions enhance the speed and efficiency of fund transfers and boost international trade, they also introduce new vulnerabilities, anonymity, opacity, rapid execution, and multiple intermediaries. These features are often exploited by criminal networks and terrorist organizations for money laundering and illicit financing purposes. In this context, FATF Recommendations 15 and 16 are particularly relevant, setting out specific obligations for countries and financial institutions: oversight of virtual assets (cryptocurrencies), traceability of transactions, mandatory identification of counterparties, and implementation of the "Travel

Rule," which requires the transmission of sender and beneficiary information for transfers above a defined threshold.

The second part of her presentation focused on the National Financial Intelligence Authority (ANRF), Morocco's Financial Intelligence Unit (FIU), established by Law 43-05. As an independent administrative authority reporting directly to the Head of Government, the ANRF coordinates the national AML/CFT framework. It operates through several specialized divisions (legal, investigations, cooperation, IT, compliance, etc.), and its governing council includes key national stakeholders (ministries, regulators, judicial authorities, Bank Al-Maghrib, the Foreign Exchange Office, and others). The ANRF serves as the central node of the system, both for preventive measures (awareness, inter-agency coordination) and enforcement (financial analysis, judicial referrals, international cooperation).

On an operational level, Mrs. Benmadani described the ANRF's investigative techniques for detecting money laundering schemes. These rely on tactical financial analysis to identify atypical transactions relative to customer profiles, such as inconsistent flows, structured deposits, or the use of nominees. This is complemented by strategic analysis focused on identifying systemic patterns and typologies, such as smurfing (the deliberate fragmentation of transactions to stay below reporting thresholds) or trade-based money laundering (TBML), often observed in import-export flows. The ANRF utilizes advanced tools, such as goAML, an integrated, secure data processing and messaging system developed by the United Nations Office on Drugs and Crime (UNODC).

Ms. Benmadani emphasized the importance of information sources. In addition to Suspicious Transaction Reports (STRs) from obligated entities, the ANRF leverages reports from public agencies, data from foreign authorities (via 24 bilateral cooperation agreements/MOUs), exchanges through the Egmont Group (comprising 177 Financial Intelligence Units (FIUs) worldwide), and Open-Source Intelligence (OSINT) from public databases, social media, and commercial platforms.

The presentation concluded with two practical case studies illustrating the ANRF's operational capacity. The first case involved detecting of an attempted terrorist financing operation using virtual assets, which provided an opportunity to coordinate efforts among all national stakeholders involved in AML/CFT in Morocco. The second case revealed a cross-border money laundering scheme. These examples highlighted the critical role of data cross-referencing, transactional pattern reconstruction, and fund traceability in supporting judicial prosecutions. Ms. Benmadani ended her presentation by calling for enhanced cooperation among financial institutions, public authorities, and international partners to respond effectively to the evolving threats posed by digital financial flows.

The subsequent discussions highlighted the significant challenges faced by African Central Banks amid the rapid digitalization of financial services, particularly in cross-border transactions. This evolution raises critical issues regarding technical compliance and the effectiveness of AML/CFT regimes. The case of Zimbabwe was presented as an example of efforts to build a coherent institutional framework through collaboration between the Central Bank, the financial intelligence unit, and payment system regulators. Implementation of the Travel Rule, improved

data collection and processing systems, and comprehensive risk assessments were identified as key steps toward addressing the financial threats associated with cryptocurrencies and emerging digital tools.

Participants also emphasized the importance of regional coordination and regulatory harmonization, particularly within Regional Economic Communities (RECs) such as the Southern African Development Community (SADC), where regulatory discrepancies between countries (e.g., South Africa and its neighbors) create exploitable gaps. In this regard, mechanisms for cooperation, knowledge sharing, and mutual technical assistance are essential. Morocco's initiative of regularly hosting African delegations to share its AML/CFT compliance experience was recognized as a best practice, with suggestions to formalize and expand such efforts through a continental directory of available expertise.

Ultimately, the discussions emphasized that combating cybercrime and protecting personal data are fundamental pillars of financial sector resilience. Regulators were urged to strengthen the security of mobile applications, enforce FinTech compliance, and raise consumer awareness about digital risks. Regulatory sandboxes were proposed as a lever for promoting responsible innovation. A key proposal emerged: the creation of a continental coordination mechanism linking regulatory sandboxes with financial intelligence units to bolster collective responses to transnational digital and financial threats.

3.2 Plenary session 2: Experiences of AACB Central Banks

Four AACB Central Banks shared their experiences regarding the main theme of the Seminar.

3.2.1 Central Bank of Egypt (CBE)

With a median age of approximately 24 years, Egypt boasts a youthful and digitally inclined demographic, primed for rapid technology adoption. Coupled with nationwide efforts to enhance financial inclusion, particularly for the unbanked and underserved, this youth-driven momentum is fueling a transformative shift in Egypt's financial ecosystem.

The National Payments Council (NPC), established in 2017, introduced the Less-Cash Transformation Framework to lead Egypt's transition toward a digital economy. FinTech & Innovation, and Cybersecurity are both important enablers of this framework. Financial technology also plays a key enabling role in the Financial Inclusion Framework launched in 2022.

In 2019, the Central Bank of Egypt (CBE) launched its FinTech & Innovation Strategy, aligning with Egypt's Vision 2030 and the evolving market needs and aspirations. Egypt aims to position itself as a leading FinTech hub in the Arab region and Africa, fostering innovation, talent, and next-generation financial services.

The CBE initiatives are supported by a robust legal framework that mandates digital payments for government transactions and lays out the legislative basis for digital transformation in the financial and banking sectors. It also promotes the use of modern technologies in any of the fields providing financial, banking, or regulatory services.

To strengthen regulatory coordination, the FinTech and Innovation Committee was established in July 2019, bringing together all relevant regulators to ensure effective oversight and support for the growing FinTech industry.

The Regulatory Sandbox, launched in July 2019, provides a controlled environment where FinTech startups and innovators can live-test solutions under the Central Bank's supervision, but without exposing the wider financial system to risk.

One of the key innovations currently under study is digital lending via behavioral scoring, which leverages data from mobile usage and utility payments to enable nano-loans. This approach aims at advancing financial inclusion, particularly for Egypt's unbanked population.

The Central Bank of Egypt (CBE) has developed comprehensive cybersecurity strategic and operational cybersecurity objectives aimed at addressing challenges in a reliable and consistent manner. These objectives support the execution of organizational policies and initiatives under an integrated strategic plan. They also contribute to enhancing national competencies capable of effectively mitigating and responding to cyber threats while leveraging their threat intelligence hub.

The Cybersecurity Readiness Oversight Central Department, within the Cybersecurity Sector of CBE, has spearheaded efforts to unify cybersecurity controls across Egypt's Financial and Banking Sector. Key achievements include:

- Development of the first sectoral regulatory cybersecurity framework: EG-FinCSF.
- Integration of international best practices and standards into CBE regulations and circulars.
- Support for financial institutions in aligning cybersecurity initiatives with business objectives and emerging technological innovations.
- Establishment of a mechanism for independent benchmarking of cybersecurity readiness for all entities licensed under CBE's supervision.

The CBE Cybersecurity Sector launched the Readiness & Risk Oversight Program, enabling both self-assessments and independent assessments of institutions' cybersecurity compliance. This program focuses on:

- Monitoring the maturity, risks, capability, resilience, and readiness of banks, financial institutions, and FinTech companies.
- Validating compliance with the EG-FinCSF.
- Enhancing cybersecurity strategies through preemptive risk identification.
- Fostering continuous improvement and sustainable compliance practices across the sector.

The Central Bank of Egypt has established the EG-FinCIRT (Egyptian Financial Sector Computer Incident Response Team), responsible for incident handling and emergency response across banks and FinTech entities. Key functions include:

- Early detection and mitigation of cybersecurity incidents.
- Deployment of advanced security monitoring and unconventional detection technologies.
- Analysis of digital evidence and identification of cybersecurity vulnerabilities.
- Execution of malware analysis and reverse engineering procedures to strengthen sector-wide cyber resilience.
- Enhance the technical competencies of financial sector personnel through professional awareness initiatives and specialized training and awareness programs, delivered either by qualified experts in collaboration with international entities specializing in cybersecurity.

This model serves as a benchmark for other central banks seeking to foster innovation while proactively addressing rapidly evolving Cyber risks.

3.2.2 Central Bank of Kenya (CBK)

The Central Bank of Kenya plays a leading role in transforming the country's financial sector, characterized by rapid digitalization and the accelerated adoption of financial technologies. This presentation highlights the evolution of Kenya's banking landscape, the rise of FinTech innovations, and the growing cybersecurity-related risks.

Kenya's formal banking system comprises regulated financial institutions, including commercial banks, microfinance institutions, and payment service providers. The country has emerged as a leading continental innovator in FinTech. The revolution in digital financial services is driven by significant advances in mobile money, digital lending, and instant payments. Flagship platforms such as M-Pesa have not only enhanced customer experience but also significantly advanced financial inclusion by reaching previously underserved populations. This development is supported by a hybrid ecosystem combining tech companies, telecom operators, and a regulatory environment conducive to innovation.

While FinTech innovations bring gains in efficiency, accessibility, and speed, they also introduce new operational and security vulnerabilities. The sector faces challenges such as cyberattacks, data protection breaches, and increasing reliance on third-party technology providers, particularly cloud platforms. These risks necessitate the development of tailored risk management strategies and the continuous improvement of cybersecurity frameworks. Common attack vectors include phishing, malware, SIM-swap fraud, and ransomware. These threats target both institutional infrastructures and end-users, underscoring the need for a holistic and integrated defense mechanism.

To address these risks, Kenya has adopted a proactive legal and regulatory framework. The Computer Misuse and Cybercrimes Act, adopted in 2018, serves as the legislative foundation for prosecuting digital offenses. In parallel, the CBK has issued sector-specific regulations and guidelines that define minimum compliance standards and strengthen detection and response capabilities to security incidents. The CBK employs a risk-based supervisory approach, focusing on resilience, proactive threat management, and regulatory compliance. It conducts regular assessments, mandates incident reporting, and maintains ongoing dialogue with stakeholders to ensure regulatory practices remain aligned with emerging technologies. This flexible approach enables CBK to strike a balance between innovation and security.

A survey on the implementation of CBK's 2017 Cybersecurity Guidelines reveals uneven practice among financial structures. While significant progress has been made in governance and internal controls, gaps remain in incident management, employee training, and oversight of third-party risk. These findings highlight the need to enhance capacity across all levels.

The CBK is committed to sustainably strengthening Kenya's financial sector's cybersecurity posture through a mix of short and long-term initiatives. Priorities include updating the regulatory framework, promoting sectoral cooperation, developing awareness and training programs, and enhancing real-time threat monitoring and response tools. The overarching objective is to ensure that innovation is matched by resilience within a secure and trusted financial ecosystem.

3.2.3 Banque Centrale du Congo (BCC)

The Central Bank of Congo presented its institutional experience in managing cyber threats within a rapidly digitizing financial ecosystem. As both regulator and catalyst, the BCC is committed to preserving the stability of the national financial system, which comprises over 112

credit institutions, including 15 commercial banks and 183 non-bank financial entities, among which are four electronic money issuers and several FinTech aggregators. This vigilance is critical to preventing systemic malfunctions that could trigger cascading effects.

For the BCC, digital transformation, while promoting financial inclusion and payment modernization, also exposes the sector to increased cyber risks, including attacks targeting payment platforms, prepaid cards, mobile services, cloud environments, and emerging FinTech solutions. Acknowledging the interconnected nature of the sector, the Bank advocates for a collective and collaborative approach, recognizing that no single institution can effectively address these threats in isolation. The BCC's response strategy thus relies on mobilizing all stakeholders, supported by a progressive supervisory framework encompassing regulation, risk monitoring, coordination, information sharing, and capacity building.

As a strategic institution, the BCC applies the same stringent requirements imposed on sector actors. During cyber incidents, it adopts a proactive stance by intervening immediately to assist affected institutions, providing personalized follow-up on incident resolution, and conducting a post-incident evaluation. This process facilitates the securitized sharing of experiences across the sector to disseminate best practices. Moreover, the BCC is currently drawing up a national payment systems strategy for 2025-2030, including a cybersecurity component.

3.2.4 South African Reserve Bank (SARB)

South Africa has a developed banking and financial sector, with widely accessible digital payment services and a high level of financial inclusion. Under its Vision 2025, improvements have been made to the national payment system, notably the launch of a fast payment system (PayShap) in March 2023 and the introduction of contactless payments and QR codes. However, despite increasing digitization, cash remains dominant ("cash is king"), and digital payment adoption remains limited among low-income households. To address this, the SARB launched its Digital Payments Roadmap (Project Stimela), aiming to expand access to the national payment system, offer innovative low-cost solutions, and modernize payment infrastructure.

The country faces a rising incidence of fraud, as reported by the Southern African Fraud Prevention Service (SAFPS), particularly in account takeover, document forgery, and identity theft, the latter showing the fastest growth. To strengthen the fight against these risks, SARB relies on several specialized entities, notably the Prudential Authority (prudent regulation, cyber risk, and AML/CFT), the National Payment Systems Department (domestic payments), the Financial Surveillance Department (exchange controls and cross-border payments), the Financial Stability Department (systemic risk management including cyber risks), the FinTech Division (innovation), and the Cybersecurity and Information Security Unit (CISU) (cyber risk management).

The SARB's CISU collaborates closely with the South African financial sector, as well as at regional (e.g., SADC) and international (e.g., Bank for International Settlements - BIS) levels, to enhance resilience against cyber threats. It notably chairs a Cyber Resilience Subcommittee and is working to establish a dedicated sector-specific Computer Security Incident Response Team (CSIRT). Furthermore, the two components of the SARB's Payment Ecosystem Modernization Programme (PEM) were highlighted: component 4 (interoperability, fraud

prevention, and regulatory harmonization) and component 1 (Foundational Enablers, including a Digital Financial Identity – DFID). The DFID is being developed in partnership with the government.

Finally, SARB is actively engaged in FinTech innovation, for instance, through its partnership with the BIS Innovation Hub. Under the G20 Presidency, it launched TechSprint 2025, focused on digital identity, credit data portability, and fraud mitigation. SARB is also a founding member of the Intergovernmental FinTech Working Group (IFWG), which seeks to obtain regulatory clarity of various financial sector innovations through its regulatory sandbox.

Following the experience-sharing sessions, discussions focused on how African Central Banks, particularly those of Egypt, Kenya, the Democratic Republic of Congo, and South Africa, are adapting their policies and infrastructure to oversee financial innovation while ensuring consumer protection. Instruments such as regulatory sandboxes, behavioral scoring frameworks, third-party integration initiatives (including FinTechs, microfinance institutions, and mobile network operators), and data protection regulations were highlighted as key mechanisms to regulate emerging actors within the financial ecosystem. The Egyptian case was particularly illustrative, showcasing a dynamic regulatory framework and stakeholder engagement mechanisms designed to enhance the compliance of FinTech entities across successive cohorts.

Participants emphasized the growing complexity and cross-border nature of cyber threats, underscoring the need for coordinated and multi-layered responses to address these threats effectively. Examples included the implementation of 24/7 security operation centers, regular cyber incident simulations (also known as cyber drills), "security by design" policies, and the establishment of integrated controls across all layers of the information system. Continuous professional training and public awareness, particularly in rural areas, were also recognized as essential pillars for strengthening systemic resilience.

A key point of discussion was the cooperation between national and international financial institutions and regulatory authorities. Central Banks have acknowledged the critical importance of effective coordination, both internally (across cybersecurity, regulatory, and supervisory units) and externally (with data protection authorities, telecommunications regulators, and judicial entities), as well as with global partners such as the BIS, G20, and peer Central Banks. Memoranda of Understanding (MoUs) were cited as crucial tools for formalizing and institutionalizing these collaborations. The example of the DRC's establishment of a national FinCERT illustrated the commitment to a coordinated national response framework.

Finally, Speakers stressed the need for regulatory frameworks that are risk-based, flexible, and responsive to the rapid pace of technological change. Policies should be embedded within a clear, inclusive, and evolving national strategy. Particular attention was drawn to unregulated or informal institutions, which are often responsible for abusive practices. In this context, transparency, accountability, and financial literacy are priorities for fostering a secure and inclusive digital financial ecosystem across Africa. The challenge for Central Banks is to balance digital sovereignty, regional interoperability, and effective inclusion, while safeguarding trust and stability in the financial system, which remains a central challenge. Strengthening networks of expertise and sharing best practices could lay the groundwork for meaningful continental and international cooperation in financial cybersecurity.

4. GROUP SESSIONS

Delegates deliberated on three topics in the breakout sessions.

Group I: "Adoption of Central Bank Digital Currencies (CBDCs) in Africa: Challenges and Opportunities"

I. Background

The adoption of Central Bank Digital Currencies (CBDCs) is gaining momentum across Africa, as countries explore innovative solutions to enhance financial inclusion, improve payment systems, and strengthen monetary sovereignty. Driven by the rapid digital transformation of economies and the rising demand for secure, cost-effective, and accessible financial services, several African Central Banks are actively researching or piloting CBDCs. However, the path to implementation is complex and presents a unique set of challenges, including infrastructure constraints, cybersecurity risks, regulatory uncertainties, and public trust. At the same time, CBDCs offer significant opportunities to bridge financial gaps, modernize monetary policy tools, and foster greater economic resilience.

Currently, globally, the underlisted statistics highlight the deployment of CBDC at different stages:

- 134 countries (covering over 98 percent of global GDP) are exploring CBDCs;
- 39 countries are in the advanced stages (pilot and launch);
- 11 countries have fully launched a CBDC;
- 53 countries are in the development or pilot phase;
- Only 2 countries have abandoned their CBDC projects after piloting.

Africa-Specific CBDC Deployment Statistics (as of 2025)

Country	Status	CBDC Type	Key Focus Area
Nigeria	Launched	Retail	Financial inclusion and cost of cash.
Ghana	Pilot	Hybrid	Offline use and mobile money integration.
South Africa	Pilot (Wholesale)	Wholesale	Interbank settlement (Project Khokha).
Namibia	Feasibility Study	To be determined	Payment efficiency.
Rwanda	Research	To be determined	CBDC design and impact analysis.
Kenya	Monitoring Developments	To be determined	Monitoring developments – following issuance of discussion paper on CBDCs and report on public comments on the discussion paper.
WAEMU (BCEAO)	Research	To be determined	Exploring a regional CBDC.
SADC Region	Exploratory	Mixed	Potential for cross-border pilot.

Survey Highlights from Bank for International Settlements (BIS) survey (Focus on Africa in 2024/2025):

- 80 percent of African Central Banks are actively exploring or planning CBDCs;
- 63 percent cite interoperability with mobile money as a key design goal;
- Over 70 percent expressed concern about potential impacts on commercial bank intermediation;
- Less than 40 percent have an adequate legal framework in place to issue a CBDC today.

THE ARCHITECTURE

While designing and implementing CBDCs, a set of key decisions needs to evaluated at different stages, relating to technology and access, privacy, and the distribution model. CBDCs also require the creation of payment infrastructure to cover everything from the database on which CBDCs are recorded to the applications and point of sale devices that are used to initiate payments. The key considerations for building the CBDC solution and the platform have been evaluated in detail.

Central Banks must decide whether to adopt a token-based or account-based approach.

Token-based:

In the case of a token-based CBDC, distribution of the currency will involve the transfer of an object of value from one wallet to another. Token-based CBDCs ensure that the transaction is approved by the originator and beneficiary through the use of public-private key pairs and digital signatures. Thus, the system provides a high level of privacy but makes it more difficult to trace money laundering and fraudulent transactions. Further, customers need to remember their access keys, or they will lose access to funds.

Account-based:

In account-based CBDC, the distribution of currency will involve a transfer from one account to another. The model would ensure that the transaction is approved by the originator and beneficiary based on the verification of user identities. In issuing such accounts, Central Banks would have to ensure the existence of a digital account for every user.

While both access technologies have their advantages and disadvantages, the token-based approach is generally preferred by regulators for cross-border transactions, where both entities only need wallets to facilitate transactions. The token-based approach also facilitates financial inclusion goals, as only an internet connection is required for both users to complete the payment. Also, the token-based approach provides a high degree of anonymity for users. On the other hand, an account-

based approach allows regulators to monitor transactions more closely and have a relatively higher degree of involvement in the end-to-end payment process.

The Direct vs Indirect Approach:

	Mechanism	**Control**	**Examples**
Direct CBDC	The Central Bank acts as the direct provider of the digital currency to the public, potentially through a digital wallet or other payment system.	The Central Bank maintains a high degree of control over the CBDC, including its issuance, distribution, and management.	This could involve the Central Bank creating accounts directly for citizens or using a token-based system where individuals hold the digital currency in a wallet.
Indirect CBDC	The Central Bank issues the CBDC to commercial banks or other financial institutions, who then manage the distribution and access for their customers.	The Central Bank's control is less direct, as it relies on the intermediary institutions to manage the public-facing aspects of the CBDC.	This could involve the Central Bank providing digital currency to commercial banks who then offer it to their customers through their existing banking infrastructure.

This section highlights the evolving landscape of CBDC adoption in Africa, highlighting the key opportunities and challenges shaping this digital monetary future, with countries having different objectives.

II. Opportunities:

1. Safety since it is backed by the monetary authority;
2. Ease of access/financial inclusion - as it provides a pathway for those excluded from traditional banking to access financial services. This is especially relevant in developing countries or remote areas where access to traditional banking infrastructure is limited;
3. Fast payment processes - potentially reducing transaction times and costs compared to existing systems, including those for cross-border payments;
4. Reduce the reliance on intermediaries, which can lower transaction fees and potentially improve the speed of payment;

5. Interoperability - with other payment platforms and providing speed of alternative means of payment;

6. Technological innovation - e.g., programmability with other payment platforms that require digital payments for customers to make payments;

7. Reduce Risks - CBDCs could, by design, mitigate certain risks, notably counterparty risks, as CBDCs represent a claim on the Central Bank and, therefore, the safest medium of payment;

8. Lower cost for Central Banks – CBDCs would reduce the costs of issuing cash by Central Banks since the introduction of CBDC would mean less circulation of cash;

9. Flexibility for customers - ease of switching between CBDCs and other alternative finance platforms like fiat money for customers.

III. Challenges:

1. Limited Digital Infrastructure: Many African countries face gaps in digital infrastructure that constrain CBDC adoption. In rural areas, internet access is unreliable, and the electricity supply is inconsistent. The high cost of smartphones and compatible devices further limits accessibility, particularly among low-income populations;

2. Financial and Digital Literacy: Low levels of financial and digital literacy across the continent hinder public understanding and uptake of CBDCs. Many citizens are unfamiliar with digital financial services, and past experiences with financial fraud or system instability have fostered mistrust in digital platforms;

3. Cybersecurity and Fraud Risks: CBDC systems are vulnerable to cybersecurity threats, including hacking, phishing, and fraud. Many African countries lack the infrastructure and skilled personnel needed to secure digital financial platforms, increasing the risk of data breaches and financial losses, particularly for less tech-savvy users;

4. Central Bank Capacity and Governance: The successful rollout of CBDCs demands significant technical and institutional capacity. Some African Central Banks may lack the expertise and resources to design, implement, and manage digital currencies. Regulatory alignment with existing financial and mobile money laws adds further complexity;

5. Disintermediation of Commercial Banks: If users hold digital currency directly with the Central Bank, it may reduce deposits in commercial banks. This could constrain banks' lending ability and affect liquidity, potentially disrupting traditional banking roles and prompting resistance from the banking sector. The monetary policy transmission mechanism might be challenging;

6. Interoperability with Existing Systems: In many African countries, mobile money services (e.g., M-Pesa in Kenya) are already well-integrated. Ensuring that CBDCs can operate seamlessly within these existing digital ecosystems, across mobile money, card networks, and banking platforms, is both technically and institutionally complex;

7. Privacy and Surveillance Concerns: Public skepticism regarding government surveillance may hinder CBDC adoption. In the absence of clear and enforceable data protection laws, citizens may fear their financial transactions could be monitored or misused, reducing trust in the system;

8. Cost of Implementation: Designing and maintaining a secure and scalable CBDC infrastructure requires substantial investment. Some African countries may lack the resources to fund CBDC initiatives without relying on external donors or international financial institutions;

9. Cross-border Payment Complexity: CBDCs could improve cross-border trade, but this requires harmonized frameworks, interoperability between national systems, and coordination among Central Banks. Limited regional cooperation and infrastructure disparities currently make such integration difficult;

10. Currency Convertibility Challenges: Some African currencies may not freely be convertible, which complicates cross-border CBDC use. Without mechanisms to support currency conversion, CBDCs may struggle to facilitate regional or international transactions effectively;

11. Know Your Customer (KYC) and Identity Verification: Effective KYC protocols are essential for preventing illicit financial activity. However, a large portion of Africa's population lacks formal identification, making it difficult to onboard users without excluding vulnerable groups, especially in remote and underserved communities;

12. Stability of Financial Systems: If not carefully managed, CBDCs could introduce instability in the financial system. A large-scale shift of deposits from commercial banks to CBDCs may weaken banks' ability to lend, increase systemic liquidity risks, and disrupt traditional financial intermediation;

13. Public Engagement and Coordination: CBDCs implementation requires coordinated efforts across government agencies, regulators, financial institutions, telecom operators, and end users. Lack of inclusive stakeholder engagement or unclear communication strategies can result in poor design choices and low adoption.

IV. Recommendations

To support the effective adoption of Central Bank Digital Currencies (CBDCs) in Africa, a multi-pronged strategies are proposed:

1. Countries should prioritize strengthening digital and financial infrastructure. Expanding internet connectivity, improving electricity reliability, and ensuring access to affordable digital devices, particularly in rural and underserved areas, will be fundamental to broad CBDC accessibility. This can be achieved through targeted investments and public-private partnerships;

2. Enhancing financial and digital literacy is crucial to building user confidence and promoting informed usage. Public education campaigns should be launched to raise awareness about how CBDCs work, their benefits, and how they complement other digital payment tools. Special focus should be placed on reaching marginalized groups such as women, the elderly, and the underserved, and addressing concerns related to surveillance, fraud, and data misuse. A deliberate public awareness campaign should accompany the development of CBDCs to prevent misunderstanding and low usage by the public;

3. Governments and Central Banks must establish robust legal and regulatory frameworks. These should clarify the legal tender status of CBDCs, align with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulations, ensure strong data protection measures, and provide for cross-border interoperability. Regulatory coherence across

Central Banks, financial institutions, and telecom regulators will be key to managing CBDCs effectively. To ensure CBDCs coexist with prevailing financial systems, it is necessary that all relevant stakeholders are part of the policy design process;

4. Cybersecurity and data protection must be made a top priority and robust. CBDCs should be developed with advanced security features to guard against hacking, identity theft, and system failures. This requires investment in secure digital infrastructure, capacity building for Central Bank IT teams, and the adoption of internationally recognized standards for cybersecurity and privacy. Further, as CBDCs evolve, African Central Banks must prioritize the ongoing enhancement of supervisory and risk management frameworks to ensure the safety, soundness, and integrity of the digital financial ecosystem;

   Traditional oversight mechanisms may not fully capture the complexities, real-time nature, and technological risks associated with digital currencies. Therefore, supervisory frameworks must be modernized to reflect the operational, cyber, and systemic risks introduced by CBDCs. Central Banks should adopt real-time monitoring tools, data analytics, and artificial intelligence (AI)-based systems to improve early warning capabilities, fraud detection, and anomaly tracking within CBDC transactions. These tools are essential for identifying emerging threats, ensuring compliance with anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations, and maintaining public confidence;

5. CBDCs should be designed to integrate seamlessly with existing financial systems, including mobile money platforms, banking infrastructure, and regional payment systems. Promoting interoperability will help avoid market disruption, encourage user adoption, and enable CBDCs to support cross-border transactions, particularly within regional economic blocs;

6. Countries should adopt a phased, inclusive, and collaborative approach to CBDCs implementation. This involves beginning with pilot programs or regulatory sandboxes to test models in real-world conditions, engaging stakeholders from the public and private sectors early in the process, and allowing for continuous feedback and adaptation. Such an approach ensures that CBDCs are tailored to local contexts, responsive to public concerns, and more likely to achieve their intended financial and policy goals;

7. In the context of a monetary union, there should be clear coordination among all countries involved to limit cross-border disruption, including but not limited to trade and capital flight.

Group II: "Policies and Regulatory Frameworks for Emerging Financial Technology (FinTech) Solutions"

I. Background

The rapid growth of financial technology (FinTech) is reshaping the global financial system, offering both opportunities and challenges, especially for Emerging Markets and Developing Economies (EMDEs). In Africa, FinTech innovations are driving increased financial inclusion, accelerating the digitization of payments, credit, insurance, and enabling other services. The COVID-19 pandemic significantly catalyzed this transformation, pushing more users and institutions toward digital financial solutions where traditional infrastructure was limited.

However, the pace of innovation also presents regulatory and supervisory challenges. FinTech actors ranging, from e-money issuers enabled by telecoms, payment aggregators, and digital lenders to insure-techs and AI-driven platforms, often fall outside traditional regulatory

perimeters. As such, many jurisdictions are grappling with how to appropriately classify these new actors, understand their risk profiles, and assess their systemic impact.

A sound regulatory and policy framework must begin with a clear understanding of the FinTech landscape, including its actors, risks, and gaps. This requires tailoring supervision through proportional approaches that balance innovation and risk mitigation. The rise of AI-driven financial models further complicates oversight, requiring flexible, forward-looking policies. Regulatory tools such as sandboxes have emerged to support innovation, but questions remain on their effectiveness and scalability.

This session provided an opportunity for Central Banks to exchange experiences, explore how to foster innovation while preserving financial stability, and discuss whether the existing regulatory framework originally designed for brick-and-mortar institutions is fit for purpose in the era of digital finance.

II. Key Issues

The key issues that were discussed are as follows:

1. Definitional Clarity and Scope: Participants agreed that current definitions of FinTech, such as the one from the Financial Stability Board[1], are too generic. While we use this definition for the purpose of this report, there is a need to refine the definition to fit the context of the country. The objective should be to identify the value-add of FinTech and tailor regulations accordingly. And the definition should consider both Fintech and Fintech-enabled financial solutions.
2. Proportional Regulation and Risk-Based Approaches: Regulators emphasized the importance of proportionality in regulation, moving from a sector-based to an activity-based approach. Technologies should be seen as enablers, with supervision focused on the nature of financial activities (e.g., credit issuance), regardless of the provider. This distinction is critical to ensure that innovative actors are regulated appropriately without stifling development.
3. Consumer Protection and Financial Education: Strong concerns were raised about consumer vulnerability. Participants stressed the importance of financial education, and more importantly, awareness, as well as, clear disclosure and safeguarding consumers from fraud and predatory practices.
4. Supervisory Capacity and Collaboration: The fast-evolving FinTech space demands enhanced supervisory capabilities, particularly in IT auditing and cyber risk.
5. Data Protection and Systemic Risks: Growing concerns were shared over data misuse and its potential to disrupt business continuity, financial stability, and even social order.
6. Regulatory Innovation Tools: Countries are adopting various tools, such as regulatory sandboxes, to test and learn before regulating.
7. Infrastructure and Architecture Awareness: Understanding the underlying technology architecture, both functional and non-functional, was seen as essential for effective supervision. Regulators must understand how data flows and systems interact to tailor meaningful policies.
8. Need for Cross-Sector Coordination: The involvement of telecoms and other non-traditional players (especially in payments and digital channels) raises questions about regulatory perimeters. There's a need to clarify responsibilities and strengthen cooperation across sectors.

[1] FinTech encompasses new financial digital products and services enabled by new technologies and policies.

III. Recommendations

In light of the diverse discussions and experiences shared by participating Central Banks and financial sector players, several key recommendations emerged to guide the development of effective policies and regulations.

1. Adopt Principle-Based Policies and Regulations: Tailor global standards like Basel and PFMIs to local contexts rather than applying a one-size-fits-all approach.
2. Consider introducing Open Finance Frameworks: Ensure existing data protection laws are considered, and regulators in charge are consulted in the process.
3. Consider developing FinTech Strategies in alignment with national or regional strategies and establishing a FinTech functionary. This may involve conducting diagnostic assessments to ensure there is a need and these are not covered in other strategies or functions.
4. Simplify Licensing & Promote Passporting: Create streamlined licensing processes and explore bilateral or regional license recognition.
5. For Central Banks that don't have regulatory sandboxes in place, explore the possibility of introducing Regulatory Sandboxes to encourage innovation testing in controlled environments.
6. Update Legal Frameworks to Reflect Emerging Models: Laws should be revised to recognize and regulate alternative finance (like crowdfunding and P2P lending) and digital-only banks, ensuring clarity on licensing, governance, and consumer protection while enabling innovation within a supervised framework.
7. Consider the collaboration of regulators on hybrid FinTech products through new or revised laws or guidelines. For example, working with the Capital Market Authority for crowdfunding is beneficial.
8. Enhance Consumer Protection: Prioritize consumer awareness, financial education, effective complaint mechanisms, and responsible product design.
9. Support Innovation Ecosystems for Small FinTechs: Invest in incubation and acceleration programs and create platforms for ongoing innovation dialogue.
10. Broaden Engagement: Collaborate with commercial banks, telecoms, and other actors to ensure inclusive and balanced FinTech development and a good understanding of the risks from the players.
11. Regulators should both adopt and oversee the responsible use of AI in the financial sector by deploying Artificial Intelligence and Machine Learning (AI/ML) tools for supervisory purposes such as detecting fraud, money laundering (ML), and terrorist financing (TF), while also establishing regulatory guidance to govern how licensed entities use AI, including standards for explainability, bias mitigation, and accountability in decision-making algorithms.
12. Countries should adopt a national cloud sovereignty strategy to ensure secure management of financial sector data, maintain regulatory oversight and business continuity, and progressively reduce dependence on foreign or third-party cloud providers.

Group III: "Cross-Border Collaboration on Cyberattack Intelligence and Response"

I. Introduction

As Africa is being more digitalized, cyber risk has become integral to doing business and is therefore a perpetual part of the risk landscape. The speed and scale with which an incident could emerge and escalate are different from other operational and business risks. They require a good understanding of the threat landscape and a strong ability to detect and respond to emerging threats.

Advances in technology might introduce new risks while also exacerbating existing risks. The use of generative artificial intelligence has increased the velocity with which impersonation attacks may be executed. The interconnectivity of global systems and the reliance on third parties were, for instance, evidenced in the CrowdStrike incident, where a failed operational process brought global systems to a standstill. Recent developments, including ransomware targeting financial institutions, sophisticated SIM-swap frauds, supply-chain attacks, and the weaponization of open-source intelligence (OSINT), have demonstrated the limitations of isolated national responses.

Using the NIST Cybersecurity Framework as a guide, governance and protection remain crucial. However, the ability to detect, respond, and recover has become the focus. In other words, in a world where it is not if but when you are attacked, resilience is key. The sharing of threat intelligence and having an incident response capability, such as a Cyber Security Incident Response Team (CSIRT), has become imperative.

The rise in cyber threats facing Africa's financial systems has underscored the urgency for coordinated regional action. The session focused on the need to enhance cross-border collaboration in cyberattack intelligence sharing and incident response, especially in the context of increasing digitalization, mobile money adoption, and interconnectivity of financial services across Africa. With most African countries at different stages of cybersecurity maturity, participants agreed that a harmonized and cooperative approach is essential to protecting regional financial stability and consumer trust.

II. Key Issues:

- There is a lack of cross-border cyber resilience, threat intelligence sharing, and incident response frameworks to enable cross-border cooperation. An example of what is missing is the shared adoption of the European Central Bank's Cyber Resilience Oversight Expectations (CROE), which aims to strengthen the resilience of payment systems. Different data classification, incident reporting thresholds, and legal frameworks across borders hinder timely information exchange.

- Cybersecurity capabilities are fragmented across jurisdictions. While some Central Banks have established Security Operations Centers (SOCs) and CSIRTs, others lack basic threat detection infrastructure. Different Central Banks may be at different maturity levels.

- Some jurisdictions may lack cybersecurity-related laws that enable threat sharing and incident response across borders, while at the same time, there might be concerns over contravening data protection legislation.

- There is a lack of threat intelligence, cyber incident sharing, and forensic labs platforms across African borders.

III. Challenges:

- Some jurisdictions may lack a clear mandate to deal with the incident response and threat sharing element of cybersecurity from an operational and industry perspective.

- There is poor alignment and integration of different stakeholders. For instance, unregulated entities may pose risks to the regulated financial sector, but are not legally required to participate in threat intelligence sharing and/or incident response structures.

- There is inadequate cybersecurity knowledge, skills, capabilities, and resources in some jurisdictions. This includes threat intelligence sharing, incident response, and digital forensics. In addition, where such are available, it may prove difficult to retain the relevant staff members.

- Reliance on third parties for cybersecurity could provide an additional challenge, with such entities potentially being unwilling to share information and participate in incident response.

- Management reporting on cybersecurity proves challenging, particularly knowing which metrics to report on that would signify both the risks faced as well as the effectiveness of defensive measures.

- In order to obtain their buy-in and ensure informed decision-making, the board and senior management may require cybersecurity training and awareness.

- Threat analysis is a laborious task, which requires sifting through a lot of data, increasing the risk of missing crucial indicators of an incident. Jurisdictions may not be using automation effectively to assist them in threat and anomaly detection.

IV. Recommendations

- Cross-border cyber resilience, threat intelligence sharing and incident response frameworks to support cross-border cyber collaboration

    - The AACB Cybersecurity Sub-working Group should consider the establishment of three frameworks for AACB member countries, namely on cyber-resilience, threat intelligence sharing, and incident response.

    - Cyber resilience: Member countries must work to align on cybersecurity and resilience frameworks, adopting global best practices, where possible, to support the harmonization of standards across borders.

- Threat intelligence: Consideration should be given to establishing a pan-African threat intelligence platform, once the relevant frameworks and standards are in place. This could be developed in collaboration with the African Union. Additionally, a framework for sharing data among AACB members must take into account compliance with relevant data protection legislation across all jurisdictions. Similarly, individual members must consider how their regulated entities are permitted to share data under their respective jurisdiction's legislative frameworks.

- Incident response: The incident response framework must clearly define the procedures for incident handling and reporting. The framework must support the development of incident response playbooks for different jurisdictions and align with members. The effectiveness of incident response playbooks should be tested through tabletop exercises and can also form part of other testing, or cyber range exercises. The organizational structure of these incident response structures must be considered, with a jurisdictional CSIRT, for instance, reporting into a regional CSIRT.

- The frameworks must clearly specify the relevant structures required, for instance, SOCs, CSIRTs, and Information Sharing and Analysis Centers (ISACs). Clear roles and responsibilities must be defined for each structure, ultimately to be established and enabled through domestic legislative frameworks. Consideration must be given to how the Central Bank structures participate within their respective jurisdictions and align with national cybersecurity information sharing and incident response structures. For instance, the Southern African Development Community (SADC), which has similar structures, may be informative and it should be consulted.

- Fragmented cybersecurity capabilities across jurisdictions and different maturity levels

  - As different jurisdictions are at different maturity levels, a roadmap must be established with the initial establishment of the relevant structures being a 'minimum viable product' with a clear roadmap to achieve the desired maturity levels over time.

  - Consideration should be given to enhancing capabilities and maturity by using global benchmarks, such as C2M2 (Cybersecurity Capability Maturity Model).

- Education, training, and awareness

  AACB member countries must have a clear plan to build human capacity surrounding threat intelligence and incident response structures. At the same time, the board and senior management must receive requisite cybersecurity and awareness training to ensure buy-in and informed decision-marking from their side. Financial institutions should ensure that they conduct regular awareness programs for employees, third parties, customers, and other relevant stakeholders

- Better use of technologies

  Consideration must also be given to leveraging emerging technologies, such as Artificial Intelligence, to aid in the automated and speedy detection of threats and incidents.

Done in Rabat, Marriott Conference Center, on July 23, 2025

LIST OF PARTICIPANTS

N°	Institution	Name	Position	Email
1	Attijariwafa Bank	Mr Mohamed Tazi	Director of Information Systems Security	moh.tazi@attijariwafa.com
2	Attijariwafa Bank	Mrs Fatima Zahra Essami	Staff	
3	Autorité Nationale du Renseignement Financier	Mrs. Najwa Benmadani	Director of the Investigations and Financial Intelligence Division	benmadani@anrf.gov.ma
4	Autorité Nationale du Renseignement Financier	Mr Badr Taiabi	Staff	taiabi@anrf.gov.ma
5	Autorité Nationale du Renseignement Financier	Mr Alae Laachoub	Staff	laachoub@anrf.gov.ma
6	Banco de Moçambique	Mr Jamal Luis Abacar Omar	Executive Director and Board Member	Micaela.Pascoal@bancomoc.mz
7	Banco de Moçambique	Mr Turay Filipe De Melo	Assistant Manager	turay.melo@bancomoc.mz
8	Banco Nacional de Angola	Mr Luis Vieira	Engineer	lvieira@bna.ao

N°	Institution	Name	Position	Email
9	Bank of Ghana	Mr Elhanan Owureku Asare	Director	elhanan.asare@bog.gov.gh
10	Bank of Mauritius	Mrs Kaajal Seebaluck-Beerbul	Senior Analyst	kaajal.beerbul@bom.mu
11	Bank of Sierra Leone	Mrs Adama Aduadjoe	IT EXAMINER	aaduadjoe@bsl.gov.sl
12	Bank of Sierra Leone	Mr Edmund Tamuke	Economic Adviser to the Governor	etamuke@bsl.gov.sl
13	Bank of Uganda	Mr Alfred Labu Kurong	Team Leader/Acting Deputy Director	akurong@bou.or.ug
14	Bank of Zambia	Mr Musonda Mathew Mbalazi	Assistant Manager Payment Systems Fintech and Research	mmbalazi@boz.zm
15	Bank of Zambia	Mr Daniel Chibesakunda	Acting Assistant Director - IT Security	dchibesakunda@boz.zm
16	Banque Centrale de la République de Guinée	Mr Kerfalla Sylla	Directeur Adjoint des Systèmes et Moyens de Paiement	kerfalla.sylla@bcrg-guinee.org
17	Banque Centrale de Tunisie	Mr Riadh Mejri	Directeur du Développement et de la Surveillance des Systèmes et des moyens de Paiement	riadh.mejri@bct.gov.tn

N°	Institution	Name	Position	Email
18	Banque Centrale de Tunisie	Mr Aymen Rejeb	Head of IT Networks Department	aymen.rejeb@bct.gov.tn
19	Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO)	Miss Fatou Ndiaye	IT RISK ANALYST	fndiaye@bceao.int
20	Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO)	Mr Hidja Serge Eric Bama	Adjoint au Directeur des Systèmes d'Information	hsebama@bceao.int
21	Banque Centrale du Congo	Mr Willy Luboa Ngovo	Directeur	luboa@bcc.cd
22	Banque Centrale du Congo	Mr Jimmy Mpongo	Acting IT Director	mpongo@bcc.cd
23	Banque des Etats de l'Afrique Centrale (BEAC)	Mr Wilner Junior Boussougou	Chef de Service en Charge des Opérations Financières et Activités Bancaires	boussougou@beac.int
24	Banque des Etats de l'Afrique Centrale (BEAC)	Mr Mankololo Yebas Pierre Ariel Roger	Chef de Service SMP	arielmankololo@gmail.com

N°	Institution	Name	Position	Email
25	Central Bank of Egypt	Mrs Mary Safwat Hanna	Head of Fintech Enablement Office	mary.safwat@cbe.org.eg
26	Central Bank of Egypt	Dr. Mohamed Elsheshtawy	Head of Readiness & Risk Oversight	mohamed.shishtawy@cbe.org.eg
27	Central Bank of Eswatini	Mr Sipho Skosana	Deputy Director Research, BOP and International Economics	Siphos@centralbank.org.sz
28	Central Bank of Kenya	Mr James Yogo	Deputy Director – Cyber Security	yogojo@centralbank.go.ke
29	Central Bank of Kenya	Mr Mike Ombuna	Information Systems Auditor	OmbunaMG@centralbank.go.ke
30	Central Bank of Lesotho	Mr Bafokeng Martin Noosi	Director of Other Financial Institutions Supervision	bnoosi@centralbank.org.ls
31	Central Bank of Liberia	Mr Collins W. Teah Jr.	Senior Technical Advisor	cwteah@cbl.org.lr
32	Central Bank of Liberia	Mr Bouleigh D. Cooper	Deputy Director	bdcooper@cbl.org.lr
33	Central Bank of Libya	Dr. Salem Jebriel	Director of Information Security Department	salsewi@cbl.gov.ly
34	Central Bank of Nigeria	Mr Amarachukwu Nelson Nwosu	Economist/Researcher	annwosu@cbn.gov.ng

N°	Institution	Name	Position	Email
35	Central Bank of Nigeria	Mr Waiyeola Itanola Ajakaiye	Assistant Director	wajakaiye@cbn.gov.ng
36	Central Bank of Nigeria	Miss Nafisat Gaffar Olajide	Cybersecurity Operations	ngolajide@cbn.gov.ng
37	Central Bank of Seychelles	Mr Yanick Sauzier	Senior Systems Administrator	yanick.sauzier@cbs.sc
38	Central Bank of Seychelles	Miss Tisha Constance	Financial Surveillance Analyst	tisha.constance@cbs.sc
39	COMESA Clearing House	Mr Brighton Dube	Payments and Transition Officer	bdube@comesach.org
40	COMESA Monetary Institute	Dr. Thomas Bwire	Deputy Director	tbwire@comesa.int
41	COMESA Monetary Institute	Dr. Lucas Njoroge	Director	LNJOROGE@COMESA.INT
42	Commission de l'UEMOA	Mr Kouakou Hyppolite Konan	Chef de la Division du Suivi de la Politique Monétaire	khkonan@uemoa.int
43	East Africa Community (EAC)	Mr Julius Kilonzi Mutemi	Payment Systems Expert	jmutemi@eachq.org

N°	Institution	Name	Position	Email
44	Federal Reserve Bank of New York (FRBNY)	Mrs Susmitha Thomas	Associate Director	susmitha.thomas@ny.frb.org
45	IOX Labs 34 Ventures Talaty	Mr Soulaimane Lahrech	Founder of Talaty	soulaimane@talatypay.com
46	National Bank of Rwanda	Mr Songa Chris Musonera	Ag. Manager, Offsite surveillance, Payment Systems	csonga@bnr.rw
47	National Bank of Rwanda	Mr Olivier Mugwaneza	Manager, Financial Sector Policy	omugwaneza@bnr.rw
48	Reserve Bank of Malawi	Dr. Wytone Jombo	Principal Economist	jombowytone@gmail.com
49	Reserve Bank of Zimbabwe	Mrs Julia Njobo	Chief - Digital Financial Services & Licensing	jnjobo@rbz.co.zw
50	South African Reserve Bank	Mr Gerhard Van Deventer	Financial Sector Cybersecurity Consultant	gerhard.vandeventer@resbank.co.za
51	United Nations Economic Commission for Africa (UNECA)	Dr. Adam Elhiraika	Director	elhiraika@un.org
52	West African Monetary Agency (WAMA)	Mr Boima S. Kamara	Director General	bskamara@amao-wama.org

N°	Institution	Name	Position	Email
53	West African Monetary Institute (WAMI)	Dr. Sikiru Abdulsalam	Director	saabdulsalam@wami-amao.org
54	World Bank	Mr Mazen Bouri	Lead Financial Sector Specialist	mbouri@worldbank.org
55	Bank Al-Maghrib	Mr Abdouahed Rhiat	Head - Cooperation & Institutional Relations Division	a.rhiat@bkam.ma
56	Bank Al-Maghrib	Miss Ghita Faddi	Deputy Head - Cooperation & Institutional Relations Division	g.faddi@bkam.ma
57	Bank Al-Maghrib	Mr Mohamed Ait Ali	Head of the Protocol and Events Unit	m.aitali@bkam.ma
58	Bank Al-Maghrib	Miss Rabab Akaaboune	Officer in charge of Protocol and Events	r.akaaboune@bkam.ma
59	Bank Al-Maghrib	Mr Zakaria Hasnaoui	Officer in charge of Protocol and Events	z.hasnaoui@bkam.ma
60	Bank Al-Maghrib	Mr. Youssef Maazouzi	Foreign Organization Relations Officer	y.maazouzi@bkam.ma
61	Bank Al-Maghrib	Mr Chihab Saadi	Lab Innovation Department	c.saadi@bkam.ma

N°	Institution	Name	Position	Email
62	Bank Al-Maghrib	Mr Nabil Badr	Deputy Head – Banking Supervision Department	n.badr@bkam.ma
63	Bank Al-Maghrib	Mrs Ilham Zainane	Deputy Head – Banking Supervision Department	i.zainane@bkam.ma
64	Bank Al-Maghrib	Mrs Asmaa Hajar Essaid	Responsable du Service Statistiques Monétaires	as.essaid@bkam.ma
65	Bank Al-Maghrib	Mrs. Hiba Afailal	Ingénieur Etudes et Développement	h.afailal@bkam.ma
66	Bank Al-Maghrib	Mrs Dounia Tahri	Adjoint du Responsable de la Direction Statistiques et Gestion des Données	d.tahiri@bkam.ma
67	Bank Al-Maghrib	Mr Yassine El Bada	Ingénieur Data	y.elbada@bkam.ma
68	Bank Al-Maghrib	Mr Lhoussaine Derouich	Responsable du Département Régulation de la Finance Digitale	l.derouich@bkam.ma
69	Bank Al-Maghrib	Mr Nour Dine Hajjami	Responsable de la Direction Système d'Information	n.hajjami@bkam.ma
70	Bank Al-Maghrib	Mr Nassim El Hayani	Expert en Cybersecurité	n.elhayani@bkam.ma
71	Bank Al-Maghrib	Mr Yassine Abane	Responsable du Département Sécurité de l'Information	y.abane@bkam.ma

N°	Institution	Name	Position	Email
72	Bank Al-Maghrib	Mr Halim Jadi	Responsable de la Direction Risques, Conformité et Cybersécurité	h.jadi@bkam.ma
73	Bank Al-Maghrib	Mrs Siham Halim	Spécialiste Réglementation SMP Senior	s.halim@bkam.ma
74	Bank Al-Maghrib	Mme Sana Ghafour	Responsable du Service Gestion des Fraudes et Risques Technologiques	s.ghaffour@bkam.ma
75	Bank Al-Maghrib	Mr Mohamed Bazzi El Idrissi	Adjoint du Responsable du Département Stratégie, Transformation	m.bazzi@bkam.ma
76	Bank Al-Maghrib	Mme Sarah Belkasmi	Responsable du Département Communication	s.belkasmi@bkam.ma
77	Bank Al-Maghrib	Chahrazade El Alaoui	Spécialiste Inclusion Financière Senior	c.elalaoui@bkam.ma
78	Bank Al-Maghrib	Mrs Sara Zitouni	Chef de Projet Innovation	s.zitouni@bkam.ma
79	Bank Al-Maghrib	Mr Ilias Dekkoun	Chargé d'organisation	i.dekkoun@bkam.ma
80	AACB Secretariat	Dr. Djoulassi Kokou Oloufade	AACB Executive Secretary	dkoloufade@bceao.int
81	AACB Secretariat	Mr Thierno Mountaga Mbow	Accountant	tmbow@bceao.int
82	AACB Secretariat	Mr Konan Yao Arthur Koffi	Website Manager	kyakoffi@bceao.int

N°	Institution	Name	Position	Email
83	AACB Secretariat	Mr Abdourahimoune Amadou Abdoul Aziz	Research Officer	aamadouabdoulaziz@bceao.int
84	AACB Secretariat	Mr Wend-Panga Justin Ouedraogo	Research Officer	jwpouedraogo@bceao.int
85	AACB Secretariat	Mrs Confort Freda Ansayi Akouvi Djamie Amessoudji	Assistant	cfaadeamessoudji@bceao.int