REGIONAL MAPPING REPORT ON CYBERSECURITY INFORMATION-SHARING AND PEER LEARNING INITIATIVE FOR DIGITAL FINANCIAL SERVICES IN AFRICA

SPECIAL REPORT

CONTENTS

ACKNOWLEDGMENTS

This special report is a product of the African Financial Inclusion Policy Initiative (AfPI) and Cybersecurity Information-Sharing and Peer Learning Initiative (CISPLI) Task Team members.

Contributors:

From the CISPLI Task Team: Members from Angola, Burundi, Egypt, Eswatini, Ghana, Guinea, Kenya, Liberia, Madagascar, Morocco, Mozambique, Namibia, Nigeria, Rwanda, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, Tanzania, The Gambia, Uganda, Zimbabwe.

From the AFI Management Unit: Ali Ghiyazuddin Mohammad (Head of Policy Management, Policy Programs & Implementation), Boni Jeremia Massawe (Policy Specialist, Africa Regional Office), Evelyne Kilonzo (Regional Manager, Africa Regional Office), and Ira Aprilianti (Senior Policy Analyst, Digital Financial Services).

We would like to thank AFI member institutions, partners and donors for generously contributing to development of this publication.

This report is funded by GIZ through support from Germany's Federal Ministry for Economic Cooperation and Development (BMZ).

EXECUTIVE SUMMARY

Digital Financial Services (DFS) continue to expand rapidly across Africa, enabling millions of individuals and businesses to access and use financial products through mobile money, fintech platforms, and instant payments.

While this supports financial inclusion, it also significantly heightens exposure to cyber risks. The region has experienced a notable increase in cyberattacks, with financial services frequently targeted. As shown by an Alliance for Financial Inclusion (AFI) regional survey covering 32 institutions across all subregions, the African DFS ecosystem faces uneven cybersecurity readiness, fragmented information-sharing practices, and growing cross-border exposure.

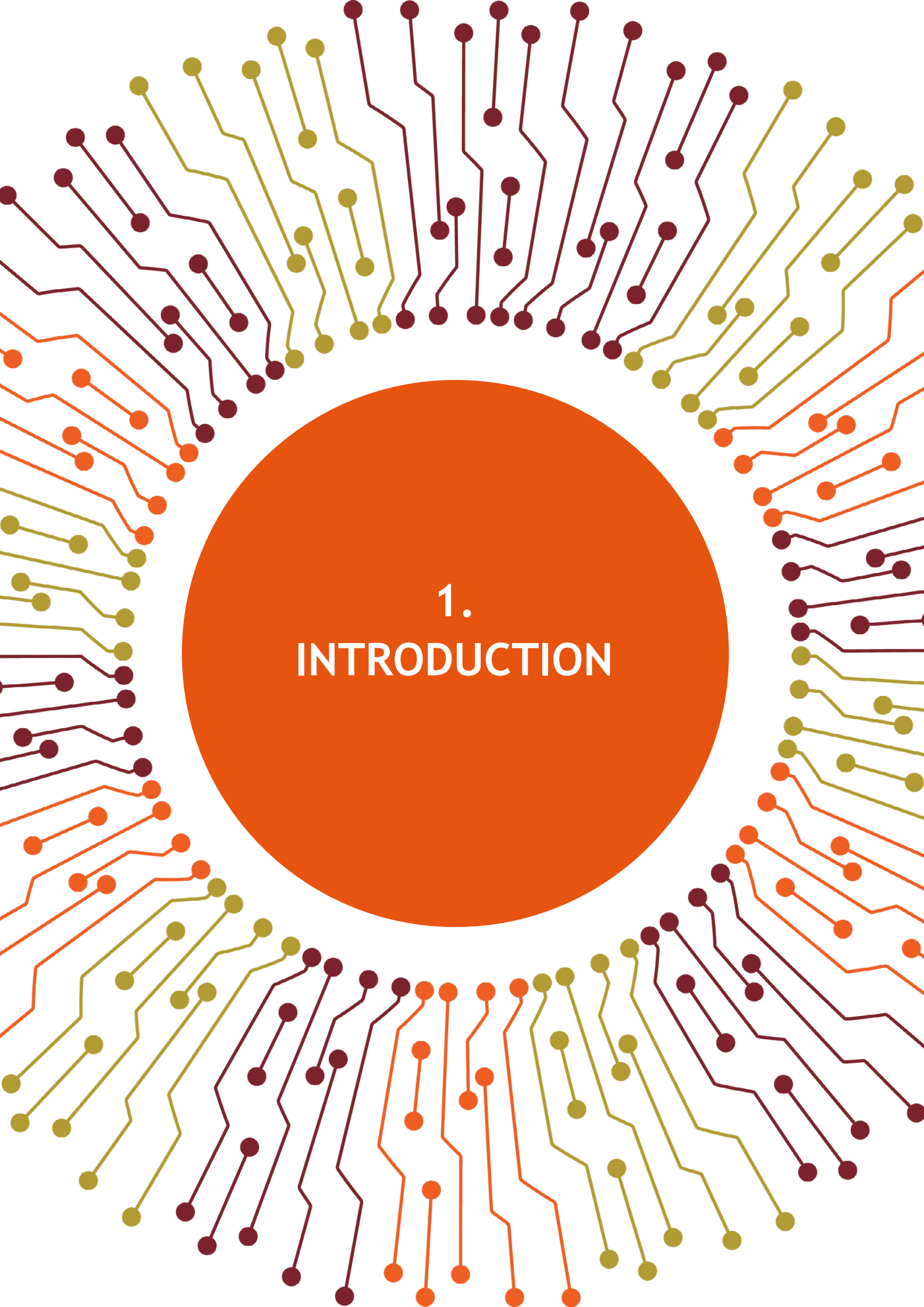
Most regulators oversee licensing of DFS providers, but few have clearly defined mandates for cybersecurity or data protection. Information sharing on cyber incidents remains predominantly ad hoc, relying heavily on emails, informal channels, and unstructured reporting formats. Advanced information-sharing mechanisms such as secure portals, Structured Threat Information Expression (STIX), Trusted Automated eXchange of Intelligence Information (TAXII) systems, or structured analytics, are still limited or under development. Incident trends reveal that social engineering, mobile money fraud, and malware dominate cyber threats, while under-reporting remains widespread due to gaps in detection, inconsistent obligations, and limited inter-agency coordination.

Despite these gaps, the survey highlights **strong willingness** among institutions to participate in a regional information-sharing and peer-learning mechanism. Over 78% of respondents favour a hybrid model, in which national entities retain ownership of sensitive data, while sharing anonymized insights with a regional hub. Institutions also expressed high demand for foundational enablers, including standard templates, legal gateways, safe-harbour provisions, anonymization tools, and practical cyber-incident playbooks.

Peer learning is recognized as a vital component of strengthening DFS cybersecurity, yet current practices remain uneven and largely dependent on sub-regional structures such as the Southern African Development Community (SADC), West African Economic and Monetary Union (WAEMU), and East African Community (EAC). Institutions identified capacity constraints, inadequate mutual trust, and lack of standardized approaches as major barriers limiting meaningful cross-border exchanges.

This Regional Mapping Report comprehensively assesses the current cybersecurity information-sharing and peer learning landscape across Africa's DFS ecosystem, identifies key technical, institutional, and legal gaps, and outlines high-priority enablers for strengthening regional cooperation. It offers clear and actionable recommendations for establishing a phased, practical, and inclusive regional information-sharing and peer-learning initiative, that aligns with African countries' diverse contexts and cybersecurity maturity levels. It outlines a governance framework that supports secure and effective regional collaboration. It also emphasizes the need for strong legal frameworks, practical tools for information exchange, multilingual support, trusted institutional partnerships, and targeted capacity building to strengthen cybersecurity capabilities.

RogerYebuah / Shutterstock



1. INTRODUCTION

1.1. BACKGROUND & RATIONALE

Across Africa, Digital Financial Services (DFS) and innovative finance solutions have expanded rapidly. Millions can now access financial services, such as payments, remittances, savings, credit and insurance, anytime and anywhere through mobile phones and fintech platforms. This expansion has been a major driver of financial inclusion, breaking down traditional barriers of cost, distance, and access, and enabling underserved populations, including rural communities, women, youth and informal workers, to participate in the formal economy.

Yet the growth of DFS also introduces new challenges related to cyber resilience and leads to increased cyber threats which pose significant risks to financial stability and inclusion. Vulnerabilities such as fraud, identity theft, and system breaches can erode trust, particularly among first-time users, and potentially reverse inclusion gains. Strengthening cybersecurity, DFS regulatory frameworks, and digital financial literacy, among other interventions, is therefore urgent to ensure that financial systems remain secure, resilient, and sustainable.

Cyber resilience, specifically, has been elevated as a core component of financial stability frameworks, and reflected in internationally agreed guidance such as the CPMI-IOSCO[1] *Guidance on Cyber Resilience for Financial Market Infrastructures*, which complements the Principles for Financial Market Infrastructures (PFMI) aimed at strengthening the safety and resilience of critical payment and settlement systems.

According to the 2025 INTERPOL Africa Cyberthreat Assessment Report, cybercrime is rapidly increasing across the continent, with many countries reporting that cyber-related offences now account for a substantial share of all reported crime, particularly in Western and Eastern Africa. Online scams, ransomware, business email compromise (BEC), and digital sextortion are frequently observed, illustrating the evolving and widespread nature of cyber risks in the region. Complementary analysis by the World Bank and the Carnegie Endowment for International Peace underscores the urgent need for robust cybersecurity measures to safeguard financial systems, and to ensure the continued trust and inclusion of users of DFS.

While individual countries and institutions have taken important steps to strengthen cybersecurity, cyber risks are inherently cross-border and systemic. No single authority or institution can address these challenges in isolation. Effective responses increasingly depend on timely information sharing, coordinated action, and the ability of policymakers and regulators to learn from each other's experiences, including successes, challenges, and lessons from cyber incidents.

In this context, the Cybersecurity Information Sharing and Peer Learning Initiative (CISPLI) has emerged as a critical enabler of cyber resilience. Information-sharing mechanisms allow authorities and market participants to exchange threat intelligence, incident information, and good practices, while peer learning supports capacity-building, informed policymaking, and convergence of approaches across jurisdictions.

Recognizing both the transformative role of DFS in advancing financial inclusion and economic empowerment in the African Region, and the growing importance of cyber resilience in safeguarding DFS ecosystems, high-level representatives of African financial sector policymakers and regulators, under the Alliance for Financial Inclusion (AFI), through the African Financial Inclusion Policy Initiative (AfPI), agreed to pursue a coordinated, Africa-led approach to strengthening cybersecurity. This includes the establishment of a dedicated cybersecurity task team expert to deliberate on modalities for regional cybersecurity information sharing and peer learning. This report represents a foundational step in these efforts, providing a clearer picture of existing practices, and setting the stage for deeper regional collaboration.

1.2. PURPOSE AND OBJECTIVES OF THE REPORT

As lead convener for the CISPLI flagship initiative, AFI presents this report as the first activity of the CISPLI Project. The report seeks to guide and support policymakers, regulators, and other stakeholders in understanding the current landscape, identifying key gaps and overlaps, and laying the groundwork for a coordinated and resilient regional approach. It works towards establishing a regional information sharing initiative, and strengthening peer learning, with the aim of enhancing the security, trust, and sustainability of DFS while advancing financial inclusion.

Specifically, the report aims to:

(A) Identify and map existing legal, policy, regulatory, and institutional frameworks that enable cybersecurity information sharing and peer learning for DFS at national, sub-regional, and regional levels.

(B) Assess gaps, overlaps, barriers, and emerging practices that affect the effectiveness of information-

[1] The Committee on Payments and Market Infrastructures (CPMI), and the International Organization of Securities Commissions (IOSCO).

sharing mechanisms, including considerations related to Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) alignment and cross-border data protection.

(C) Examine how existing local, and sub-regional mechanisms and initiatives can be leveraged to strengthen cyber resilience through peer learning, knowledge exchange, and coordinated responses.

(D) Offer recommendations on the design options for practical, phased, and inclusive approach to establishing or strengthening a regional cybersecurity information-sharing initiative for DFS that reflects Africa's diverse contexts and priorities.

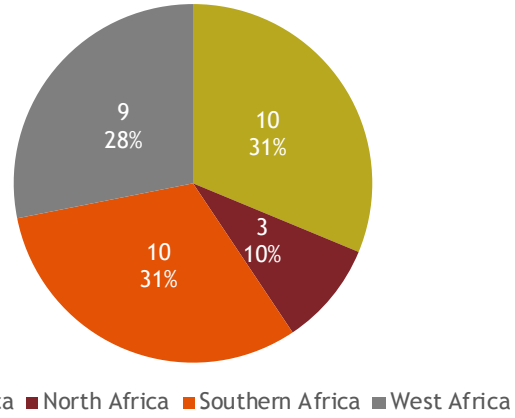
1.3. SCOPE, STAKEHOLDERS, AND LIMITATIONS

(A) Scope

This Regional Mapping report draws on a combination of desk-based research and stakeholder engagement conducted between October 2025 and February 2026, to assess cybersecurity information-sharing and peer-learning initiatives relevant to DFS across Africa. A key component of the study was a regional survey conducted among 32[2] AFI member institutions in Africa. Of the institutions that responded, 84 percent were central banks, while 16 percent represented other financial-sector policymakers and regulators ***(see Figure 1)***.

The report scope covers national, sub-regional, and regional mechanisms that facilitate the sharing of cybersecurity-related information, including threat intelligence, incident reporting, and coordinated response frameworks. The mapping focuses on institutional, legal, policy, and coordination dimensions rather than technical system testing.

FIGURE 1. RESPONDENTS PROFILES BY SUBREGION



Survey responses from 32 financial regulatory and supervisory institutions across Africa. East Africa, Southern Africa and West Africa each account for the largest share of respondents (9 respondents; 28 percent each), followed North Africa (3 respondents; 10 percent) and Central Africa (2 respondents; 6 percent) are also represented. This broad sub-regional distribution strengthens the relevance of the findings across diverse DFS market structures and regulatory environments.

Source: AFI Regional Survey; 2025

(B) Stakeholders

The study was informed by broad stakeholder engagement to ensure relevance, practicality, and regional alignment. Stakeholders engaged through these processes included financial regulators, DFS providers, cybersecurity and payment-system experts, academic institutions, AML/CFT specialists, and representatives from the private sector and international organizations. In addition, inputs were gathered through:

- Virtual Task Team meetings conducted during the initial phase of the study to discuss the current state of cybersecurity information sharing and peer learning, validate preliminary findings, and refine the scope of the assessment;
- A physical Task Team workshop, with representation from AFI member institutions across all African sub-regions, invited local stakeholders in Africa and invited partners and stakeholders[3];
- Virtual engagements, including Public-Private Dialogue (PPD) sessions and Developed Developing Dialogue (3D) with industry and technical stakeholders to capture operational perspectives and practical experiences in cybersecurity information sharing.

[2] Of the 32 countries represented, there was one regional Central Bank representing more than one country. Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) serves eight countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Côte d'Ivoire, Guinea-Bissau, Mali, Niger, Senegal, and Togo.

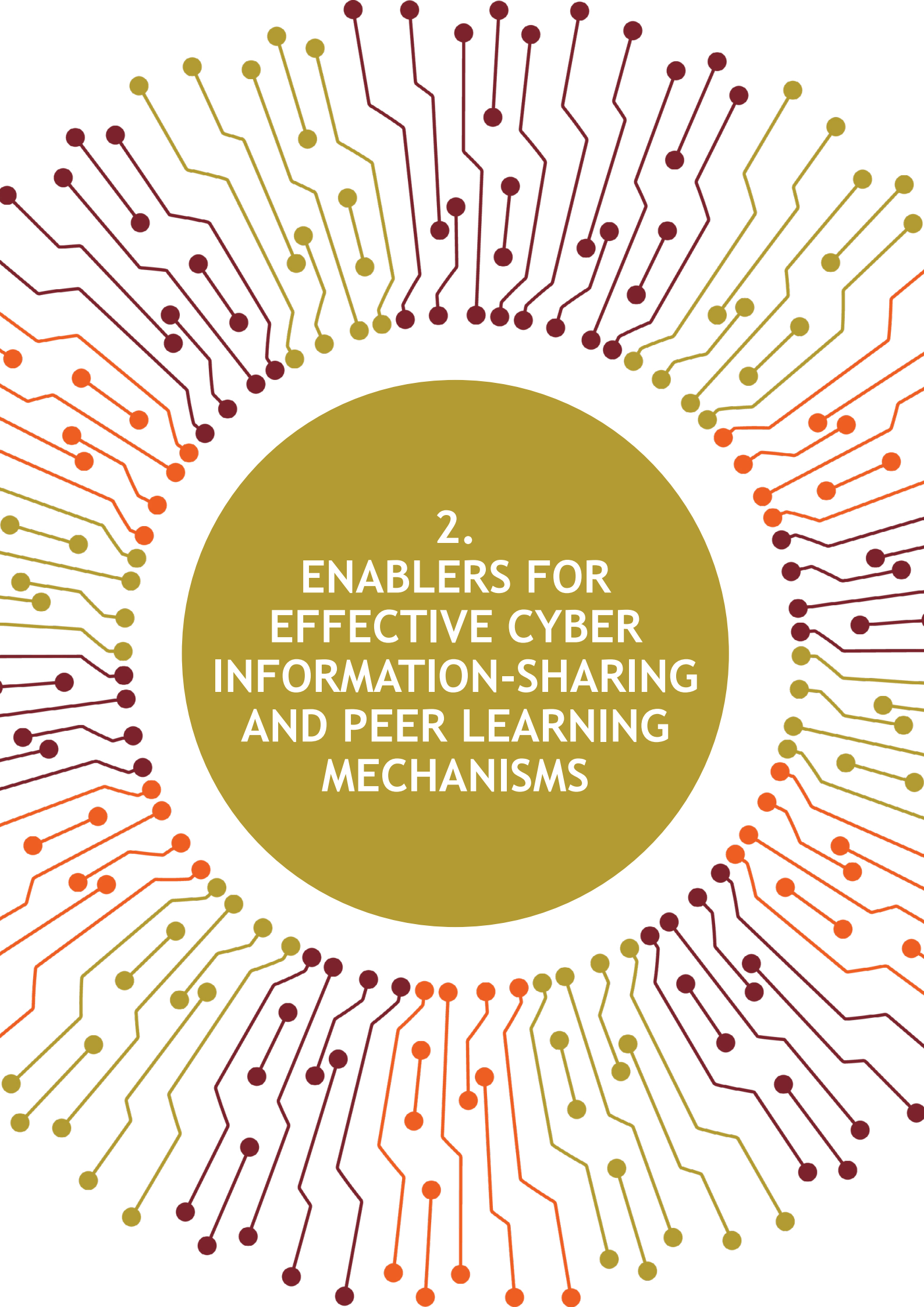
[3] Participating institutions included Africa Cybersecurity Resource Centre; Carnegie Mellon University Africa; National Institute of Information and Communication Technologies Mozambique; and Bank for International Settlements.

(C) Limitation of the study

This report is subject to several limitations. Variations in institutional readiness and internal approval processes affected the ability of some members to share detailed information within the study timeframe. Time constraints limited the depth of follow-up in certain areas, particularly for rapidly evolving or informal information-sharing arrangements.

Much of the analysis is based on survey responses, desk research, and structured stakeholder discussions, complemented by insights gathered during workshops and virtual engagements. Given the dynamic nature of cybersecurity frameworks and practices, the mapping represents a snapshot of the landscape **at the time of the study** and may not capture all recent developments or ongoing initiatives. In addition, some taskforce members were not present and therefore could not share insights into their relevant activities.

Furthermore, sub-regional analysis and graphical representations presented in the report should be interpreted in context. Differences observed across regions may reflect variations in the number and distribution of participating AFI member institutions, rather than actual differences in cybersecurity maturity or capacity. As such, these comparisons are intended to provide directional insights and highlight patterns, rather than to serve as a basis for direct benchmarking or ranking across regions.



2. ENABLERS FOR EFFECTIVE CYBER INFORMATION-SHARING AND PEER LEARNING MECHANISMS

In building a robust cybersecurity information-sharing and peer learning mechanism, especially in a region like Africa where cyber threats are growing rapidly, certain foundational elements must be in place to ensure effectiveness and sustainability.

Findings from stakeholder consultations, including virtual Public-Private Dialogues (PPD) and Developed-Developing Country Dialogues (3D), confirm that fragmented and ad-hoc approaches remain a key constraint across many jurisdictions.

Globally, studies consistently show that strong information-sharing mechanisms are built on a set of institutional, technical, legal, and human preconditions. Frameworks developed by organizations such as the United States National Institute of Standards and Technology (NIST), International Criminal Police Organization (INTERPOL), World Economic Forum (WEF), and various cybercrime task forces highlight that information sharing succeeds when it is *purpose-driven, trusted, resourced, and aligned with broader cybersecurity strategies*.

Below are the enablers for an effective cybersecurity information sharing and peer learning initiative:

2.1. CLEAR GOALS AND STRATEGIC ALIGNMENT

Information-sharing initiatives are most effective when they are explicitly linked to an organisation's or country's broader cybersecurity and risk-management strategy. Rather than sharing information for its own sake, successful mechanisms focus on why information is being shared: whether to improve incident response, detect emerging threats, protect critical infrastructure, or support law enforcement investigations. Global experience shows that when goals are unclear, information-sharing platforms often become underused, or overwhelmed with low-value data.

Insights from the PPD with GSMA indicate that, in the absence of clearly defined objectives, information-sharing initiatives tend to remain informal, reactive, and underutilized. Participants emphasized the importance of structuring mechanisms around defined operational workflows, including incident intake, triage, dissemination, coordinated response, and post-incident learning.

In the African context, it is important to align information-sharing objectives with national or institutional cybersecurity strategies, digital transformation agendas, and regional cooperation frameworks to ensure relevance and sustainability. Equally, these objectives complement financial inclusion goals by strengthening consumer confidence and trust in digital financial services, which are critical for sustained usage and adoption across diverse user groups. Several countries have implemented mandatory reporting and sectoral SOCs to complement voluntary sharing, ensuring critical threats are addressed collectively. For example, Mozambique is exploring mandatory incident reporting for financial systems, Kenya coordinates sectoral SOCs through a national apex SOC, and Ghana operates a central-bank-led sector SOC with real-time monitoring and forensic capabilities. These examples illustrate that national alignment, proportionate mandatory reporting, and trust-based frameworks are key enablers for sustainable cybersecurity information-sharing on the continent.

Similarly, discussions during the Mastercard PPD further demonstrated that clarity of purpose enables differentiation of information types (*tactical, strategic, and operational*), ensuring that shared information is actionable and aligned with stakeholder needs.

2.2. IDENTIFICATION OF INTERNAL THREAT INFORMATION SOURCES

Institutions should begin by assessing their internal threat landscape, identifying visibility gaps, and determining what information can be responsibly shared externally. This includes mapping internal data sources, capabilities, and limitations. Best practice also involves complementing internal data with external threat intelligence from CERTs, regional platforms, private-sector providers, and open-source channels.

The Mastercard PPD highlighted the risks of limited internal visibility, and single compromised API credentials at a merchant level propagating across multiple interconnected financial institutions. Institution-level awareness alone is insufficient in highly interconnected digital financial ecosystems. This is particularly relevant in resource-constrained environments, where collaboration serves as a force multiplier for cybersecurity capabilities.

2.3. DEFINE THE SCOPE OF INFORMATION SHARING ACTIVITIES

Effective information-sharing mechanisms operate within clearly defined boundaries. The scope of information sharing should reflect an organisation's capabilities, legal obligations, and risk tolerance. It is very important to have clarity on scope, as it helps

address common concerns related to data sensitivity, sovereignty, reputational risk, and misuse of shared information. International experience demonstrates that successful initiatives clearly specify:

- what types of information can be shared (e.g. indicators of compromise, tactics and techniques, trends, or strategic assessments);
- under what circumstances sharing is permitted (routine operations vs. incidents);
- with whom information may be shared (trusted peers, national authorities, regional bodies, or global partners).

PPD discussions with GSMA underscored the importance of adopting a phased approach, starting with a minimum viable scope, such as incident reporting and threat advisories, before expanding to more advanced coordination functions. Overly complex initial designs were identified as a barrier to early adoption and participation.

2.4. ESTABLISH INFORMATION SHARING RULES

Clear and enforceable rules are essential in enabling trust and participation. These typically include protocols for data classification, access control, usage limitations, and redistribution. Mechanisms such as the Traffic Light Protocol (TLP) are widely used to standardize handling of sensitive information.

Across all dialogue sessions, trust-related safeguards emerged as a primary enabler of participation. These include confidentiality arrangements, role-based access controls, non-punitive reporting frameworks, and clear data classification tiers.

Insights from the Banque de France and Deutsche Bundesbank highlighted that trust is reinforced through formal governance structures, secure communication platforms, and clear separation between information-sharing functions and enforcement actions. Without such safeguards, institutions may be reluctant to share timely and actionable information due to legal, reputational, or operational concerns.

2.5. PARTICIPATION IN TRUSTED SHARING COMMUNITIES

Institutions should identify and participate in sharing activities that complement their existing threat information capabilities. Evidence from the 3D Exchange illustrates how mature ecosystems operationalize this: the Paris Resilience Group (PRG), led by Banque de France, provides a structured public-private platform where institutions engage both in "*business-as-usual*" information exchange and "*coordinated crisis response*", supported by secure platforms and a central coordinating secretariat.

An institution may need to participate in multiple information sharing forums to meet its operational needs. Furthermore, institutions should consider public and private sharing communities, government repositories, commercial cyber threat information feeds, and open sources such as public websites, blogs, and data feeds. For African countries, strengthening regional and continental cooperation mechanisms is a critical enabler, particularly given the cross-border nature of cyber threats and cybercrime.

2.6. SUSTAINED CAPACITY AND ONGOING SUPPORT

Information-sharing initiatives require continuous investment and support. Technology alone is insufficient without skilled personnel, institutional backing, and access to expertise. Global experience highlights the importance of structured capacity-building approaches, including cyber-range simulations (e.g., CAPS exercises), Information Sharing and Analysis Centers (ISACs), and platforms such as the Malware Information Sharing Platform (MISP), which combine technical tools with trained communities of practice. These models demonstrate that effective information sharing depends not only on infrastructure but also on sustained investment in human capital, governance, and trusted networks.

The importance of operational readiness was strongly reinforced during the GSMA PPD, where participants identified joint tabletop exercises and cyber drills as critical mechanisms to test end-to-end workflows and improve coordination before real incidents occur. Similarly, the 3D Dialogue highlighted that mature systems such as the Paris Resilience Group conduct regular sector-wide exercises as part of business-as-usual preparedness.

In the Africa context, skills shortages and capacity gaps remain a significant challenge, as consistently highlighted during Task Team discussions and workshop sessions. Participants emphasized the limited availability of specialized cybersecurity professionals, uneven institutional capacity, and the need for continuous training and practical exposure, particularly in areas such as threat intelligence analysis, incident response coordination, and cyber risk assessment.

Practical initiatives including cyber-range exercises, secondments to more mature institutions, and peer-

learning exchanges were identified as effective ways to bridge these gaps. In addition, private-sector partners, such as Mastercard and Recorded Future, demonstrated how managed threat intelligence platforms can partially offset capacity constraints by providing validated, contextualized intelligence that institutions can act upon without requiring large in-house analytical teams.

Addressing capacity constraints through structured training programmes, regional collaboration, and partnerships with academic and technical institutions is therefore a critical enabler for strengthening cyber

Pingingz / Shutterstock

3. CURRENT STATE OF CYBERSECURITY AND DFS INFORMATION-SHARING IN AFRICA

This chapter presents an overview of the current state of cybersecurity and DFS-related information-sharing in Africa, drawing primarily on survey responses from AFI member institutions, complemented by targeted desktop research and various discussions between cybersecurity experts in Africa and globally.

The analysis examines how institutional mandates, regulatory frameworks, governance arrangements, and technical mechanisms shape the ability of authorities to prevent, detect, and respond to cyber incidents affecting DFS.

3.1. INSTITUTIONAL AND REGULATORY ENVIRONMENT

The institutional and regulatory environment plays a foundational role in shaping cybersecurity information-sharing in the DFS sector. Clear oversight mandates, well-defined regulatory responsibilities, and enabling legal frameworks are essential enablers for timely and trusted exchange of cyber threat intelligence, incident data, and risk information among authorities and market participants. Country experiences discussed during the workshop illustrate how institutional arrangements shape implementation.

South Africa and Nigeria reported ongoing efforts to strengthen sector-wide coordination mechanisms led by central banks, although progress has been constrained by resource limitations and institutional alignment challenges. In contrast, The Gambia is progressing through foundational and intermediate stages of cybersecurity maturity, with ongoing initiatives such as SOC operationalization, regulatory strengthening, and payment system security enhancements, though sector-wide coordination structures are still evolving. Meanwhile, Mozambique has introduced legislative measures to mandate cyber incident reporting, reflecting a shift toward more formalized oversight, and addressing challenges related to underreporting and limited trust in information-sharing processes.

3.1.1. Oversight models and responsible authorities

National experiences can also be situated within broader international and regional initiatives aimed at strengthening convergence in cybersecurity governance and cyber incident reporting. At the international level, the Financial Stability Board (FSB, 2023) Recommendations to Achieve Greater Convergence in Cyber Incident Reporting emphasize improving consistency, comparability, and cross-border coordination in financial sector cyber incident reporting frameworks. At regional level, the African Union Convention on Cyber Security and Personal Data Protection provides an overarching framework for strengthening cybersecurity governance, cybercrime prevention, and personal data protection across African Union member states.

In the context of cybersecurity information-sharing, oversight models influence which institutions are responsible for collecting cyber incident information, engaging with regulated entities, coordinating with national cybersecurity bodies, and participating in regional or international information-sharing mechanisms.

Overall, the findings indicate that cybersecurity oversight is often integrated into broader supervisory frameworks, rather than governed through dedicated or specialized regulatory structures. Further findings show that DFS oversight across Africa is primarily concentrated in licensing and supervisory functions, which are consistently exercised across all major DFS segments, including banks, non-bank payment service providers, mobile money operators, national switches, and cross-border remittance providers. Oversight of payment systems and AML/CFT obligations is also widely reported. In comparison, cybersecurity regulation and supervision are less uniformly assigned, with a smaller proportion of institutions indicating a clear mandate in this area. Responsibilities for data protection are reported even less frequently, reflecting the common practice of assigning these functions to separate authorities outside the financial regulatory perimeter, or sharing them across institutions (see Figure 2).

These oversight arrangements have direct implications for cybersecurity information-sharing initiatives in the DFS sector. Where cybersecurity mandates are not clearly articulated or are secondary to other supervisory responsibilities, institutional capacity to systematically collect, analyse, and share cyber-related information may be limited. This can result in fragmented reporting practices, inconsistent engagement with national or regional cybersecurity actors, and reduced participation in structured information-sharing arrangements. For a regional peer-learning and information-sharing initiative, this highlights the importance of supporting member institutions in strengthening cybersecurity supervisory roles, improving coordination with relevant authorities, and establishing clearer institutional ownership for DFS-related cyber risk management and information exchange.

FIGURE 2. OVERSIGHT MODELS AND RESPONSIBLE AUTHORITIES FOR CYBERSECURITY IN AFRICA.

Primary roles of the institution	Banks	Cross-border remittance providers	Microfinance / SACCOs on digital rails	Mobile money / MNO-led services	National switch/ instant payments	Non-bank PSPs / FinTechs	Others
Licensing and supervision of financial institutions	28	19	25	25	25	25	5
Oversight of payment systems, including licensing and supervision of payment service providers	26	19	23	25	25	24	3
AML/CFT oversight	23	16	23	22	22	22	2
Consumer protection	22	17	21	21	20	21	5
Cybersecurity regulation and supervision	**19**	**14**	**17**	**18**	**18**	**18**	**4**
Data Protection	10	9	9	11	10	10	2
Other	3	3	4	4	3	4	4

Source: AFI Regional Survey; 2025

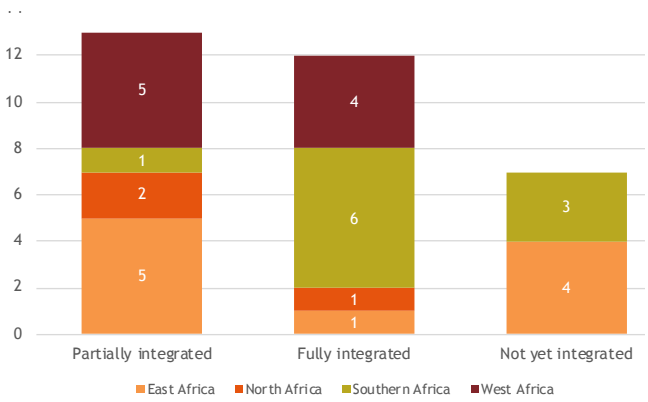
3.1.2. Cybersecurity and DFS regulatory integration

Our findings indicate that most respondent jurisdictions have adopted, or are in the process of developing, national cybersecurity strategies or policy frameworks, with strong representation across Southern, West, and East Africa (see Figures 3 and 4). These strategies are typically supported by cybercrime, computer misuse, and data protection legislation, and often include defined multi-year implementation horizons, commonly spanning five-year periods. Several respondents reported recently updated or newly adopted strategies, while others noted ongoing review processes. However, a number of jurisdictions remain at earlier stages, with strategies under development or not yet in place, suggesting uneven national preparedness. In parallel, survey responses show varying levels of integration of cybersecurity mandates into DFS regulatory and supervisory frameworks, ranging from fully integrated approaches to partial or emerging models.

Workshop discussions underscored that, while many countries have adopted national cybersecurity strategies, their operational integration into financial sector supervision remains uneven. For instance, Kenya has advanced integration through enforceable legal frameworks and mandatory reporting obligations, while Mozambique is aligning sector-specific cyber risk management guidelines with national strategies. Conversely, in jurisdictions such as Namibia, gaps in overarching cybersecurity or data protection legislation continue to limit the ability to operationalize cross-border information sharing, despite existing technical capabilities.

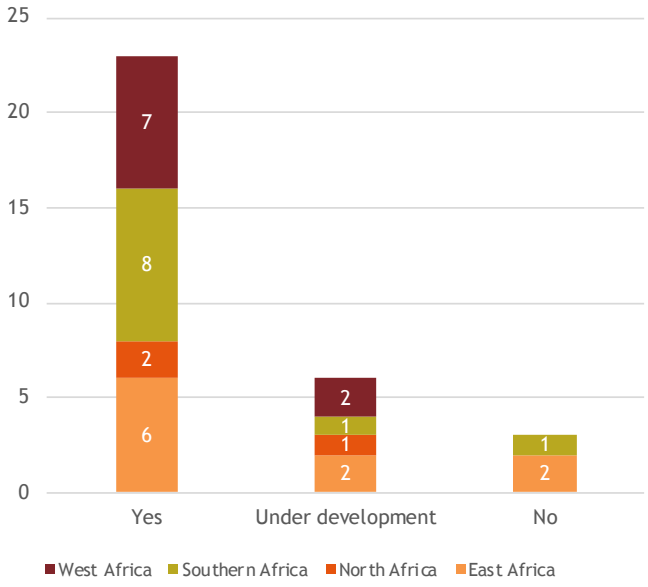
The findings have direct implications for the regional cybersecurity information-sharing and peer-learning initiative. Where national cybersecurity strategies are well established but only partially integrated into DFS oversight, financial authorities may lack clear supervisory tools or formalized channels to operationalize information sharing for DFS-related cyber incidents. Conversely, jurisdictions with limited or evolving national frameworks may face broader coordination challenges that affect the consistency and reliability of information exchange. These variations highlight the need for targeted peer learning to support deeper regulatory integration, promote alignment between national cybersecurity strategies and DFS supervision, and strengthen the institutional foundations required for effective, timely, and trusted cybersecurity information sharing across the region.

FIGURE 3. INTEGRATION OF CYBERSECURITY MANDATES IN FINANCIAL SECTOR REGULATION AND DFS SUPERVISION



Source: AFI Regional Survey; 2025

FIGURE 4. EXISTENCE OF A NATIONAL CYBERSECURITY STRATEGY OR POLICY FRAMEWORK



Source: AFI Regional Survey; 2025

3.1.3. Data protection, legal gateways, and safe-harbour status

Data protection frameworks, legal gateways for information exchange, and safe-harbour provisions are critical enablers of effective cybersecurity information sharing. These elements determine whether authorities and regulated entities can share cyber incident information in a timely and trusted manner, without undue legal or liability concerns. In the DFS context, where incidents may involve sensitive consumer data, proprietary information, and cross-border payment flows, clarity around confidentiality, liability protection, and permissible data-sharing practices is particularly important.

Our findings indicate that safe-harbour protections for cyber incident reporting remain limited and uneven across respondent jurisdictions. Only 19 percent of respondents reported the existence of safe-harbour provisions for financial institutions, while 6 percent indicated protections applicable to authorities only. A significant proportion (38 percent) reported that no such protections currently exist, and 34 percent indicated that safe-harbour frameworks are under development (see Figure 5). This suggests that, in many jurisdictions, both authorities and DFS providers may face legal uncertainty or potential liability when sharing cyber incident information, which can discourage timely reporting and limit the depth of information exchanged. With respect to data protection and privacy requirements, the survey reveals a similarly fragmented landscape. Mandatory data minimization or anonymization requirements for cross-institution or cross-border information-sharing were reported by 41 percent of respondents, while 31 percent described such practices as recommended but not legally required. At the same time, 25 percent of jurisdictions either reported no applicable legal requirements, or indicated that relevant laws are still under development (see Figure 6).

Insights from the workshop highlight how legal uncertainty continues to affect real-world practices. In several jurisdictions, participants noted that the absence of clear safe-harbour provisions and harmonized data protection laws discourages institutions from sharing sensitive incident information beyond national borders. For example, Namibia and Somalia emphasized that even where technical detection capabilities exist, the lack of explicit legal protections and data-classification protocols limits cross-border escalation. At the same time, emerging practices such as the use of anonymization and Traffic Light Protocol (TLP) classification are being explored in countries like Kenya, to enable safer and more structured information exchange.

These findings suggest that, while data protection considerations are increasingly embedded in legal frameworks, differences in legal maturity and interpretation may complicate cross-border cybersecurity information sharing. For a regional cybersecurity information-sharing and peer-learning initiative, this underscores the need to support members in clarifying legal gateways, promoting proportionate and risk-based data-sharing practices, and advancing policy dialogue on safe-harbour mechanisms that enable good-faith reporting while safeguarding confidentiality and privacy.

FIGURE 5. PRESENCE OF LEGAL/LIABILITY PROTECTIONS ("SAFE HARBOUR")

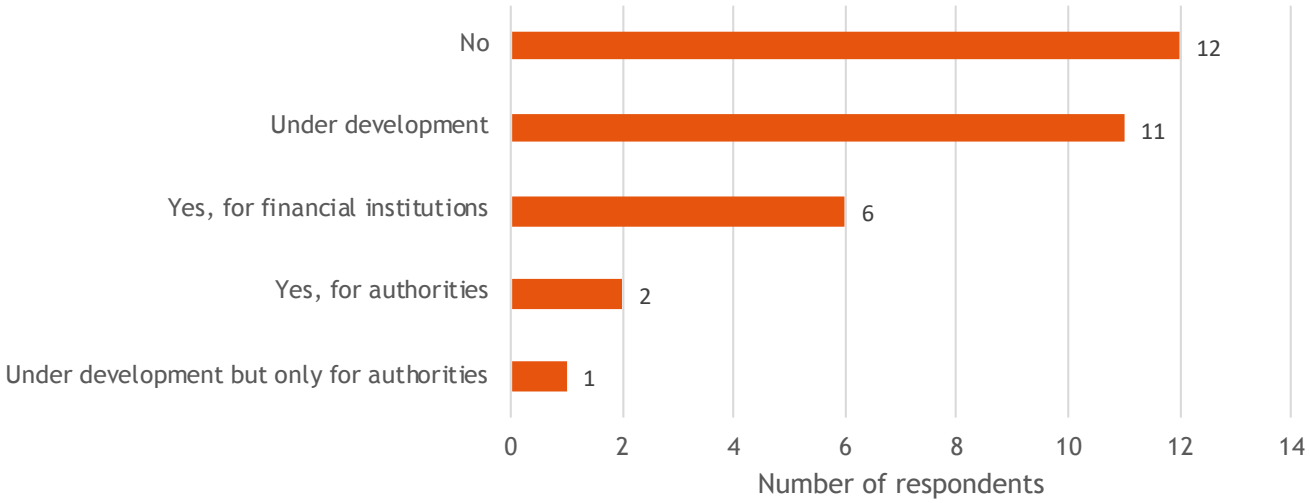
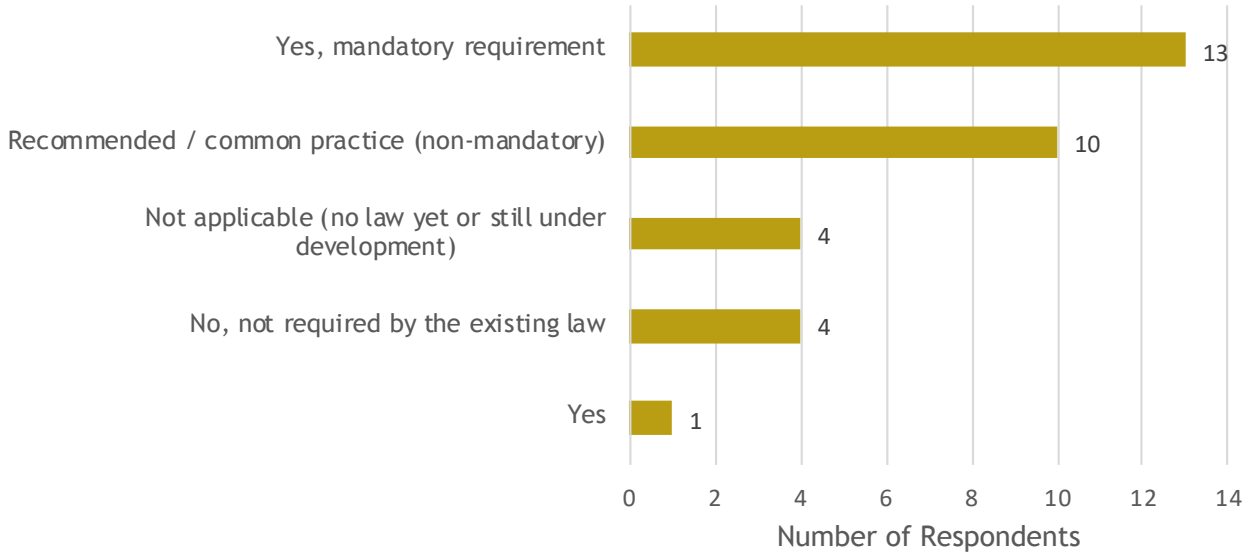


FIGURE 6. REQUIREMENTS FOR DATA ANONYMIZATION



Source: AFI Regional Survey; 2025

3.2. CYBERSECURITY GOVERNANCE AND STAKEHOLDER COORDINATION

Effective cybersecurity information sharing within the DFS ecosystem is strongly shaped by how cybersecurity functions are governed, organized, and coordinated across institutions and jurisdictions. For central banks and financial regulators, governance arrangements determine not only internal preparedness and incident response capacity, but also the ability to engage confidently in trusted information exchange with peers, sector participants, and national or regional counterparts. Discussions during the workshop reinforced that governance challenges are not only technical, but also institutional and relational. Participants emphasized that effective coordination depends heavily on trust, leadership, and clearly defined roles across institutions. In several countries, central banks are increasingly taking a leading role in convening stakeholders and driving sector-wide cybersecurity initiatives, although this often requires sustained efforts to align incentives and build confidence among public and private actors.

3.2.1. CSIRTs, SOC maturity, cross-agency coordination:

Dedicated cybersecurity units, CSIRTs, and SOCs form the operational backbone of effective cyber-incident management and information sharing. Their presence and maturity determine whether institutions can systematically detect incidents, analyse threats, and exchange timely, actionable information with trusted partners. At a regional level, interoperable and well-governed CSIRT/SOC structures are essential for enabling cross-border coordination, reducing fragmentation, and supporting collective responses to systemic DFS-related cyber risks.

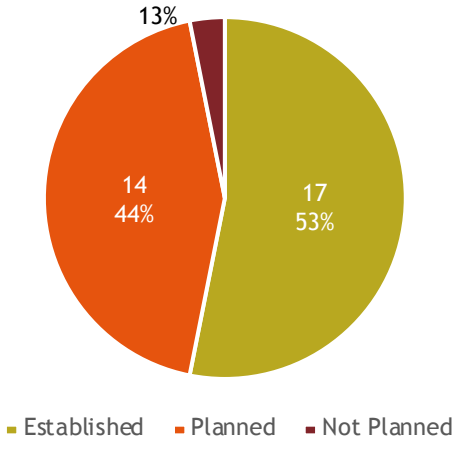
Our findings indicate that most responding jurisdictions have taken foundational steps toward formalizing cybersecurity governance. Fourteen respondents (44 percent) report having plans to establish a dedicated cybersecurity unit or team, while over half (53 percent) have already established an internal institutional CSIRT/CERT, many of which were created in the last five years, suggesting accelerated capacity building in response to rising cyber risks (see Figure 7).

However, maturity levels vary significantly. While some institutions report "established" or "interconnected" incident management capabilities, a substantial proportion still operate at ad-hoc or basic levels, with manual processes and limited external information exchange (see Figure 9). At the sector level, only a minority of respondents (37 percent) report an operational financial sector-wide CSIRT, with 53% of initiatives still in planning or development stages (see Figure 8). This results in uneven integration with national CSIRTs, and limited real-time coordination across the financial ecosystem.

Insights during the workshop illustrate different models of operationalization. Ghana, for example, has established a central bank-led financial sector SOC, with real-time monitoring capabilities and direct integration with multiple banks, while Kenya has created Banking Sector Cybersecurity Operations Centre (BS-SOC) to strengthen defences across the financial system, operated under the Cyber Fusion Unit. In South Africa, efforts are underway to transition from periodic coordination forums to a more dynamic financial sector CSIRT model, aimed at enabling real-time information sharing and broader inclusion of smaller institutions and fintechs. These examples demonstrate both progress and diversity in how countries are institutionalizing incident response and coordination structures.

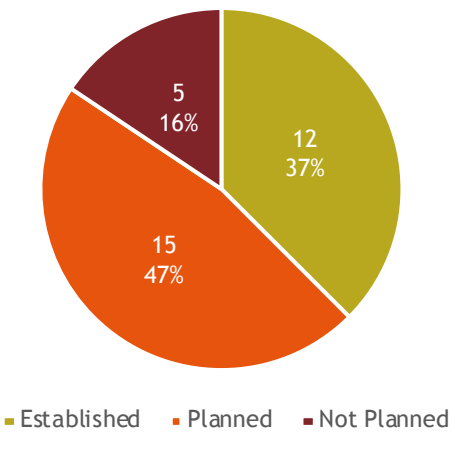
These findings point to both readiness and fragmentation. The growing number of institutional CSIRTs provides a strong foundation for regional information sharing, but disparities in maturity, and the limited coverage of sector-wide CSIRTs, constrain consistent participation. A regional initiative will therefore need to accommodate heterogeneous capabilities, support gradual onboarding, and emphasize minimum operational standards rather than advanced automation from the outset. Strengthening links between institutional, sectoral, and national CSIRTs, and clarifying coordination roles, will be critical to ensure that regional information sharing complements rather than bypasses existing governance structures within African financial systems (see Figure 10).

FIGURE 7. INSTITUTIONAL LEVEL CSIRT/CERT



Source: AFI Regional Survey; 2025

FIGURE 8. FINANCIAL SECTOR CSIRT/CERT



Source: AFI Regional Survey; 2025

FIGURE 9. MATURITY LEVEL OF INCIDENT MANAGEMENT CAPABILITIES

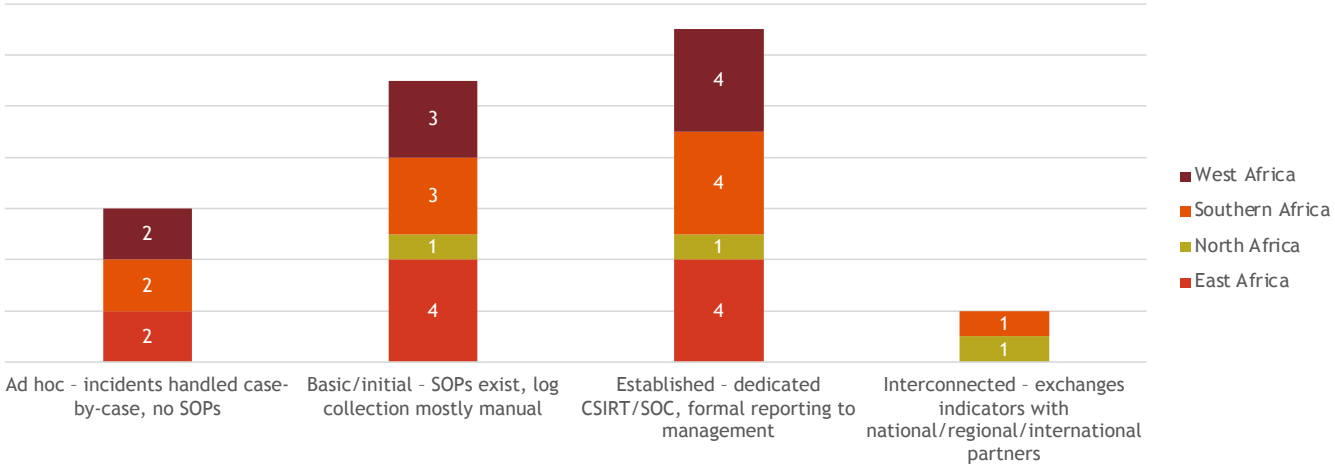
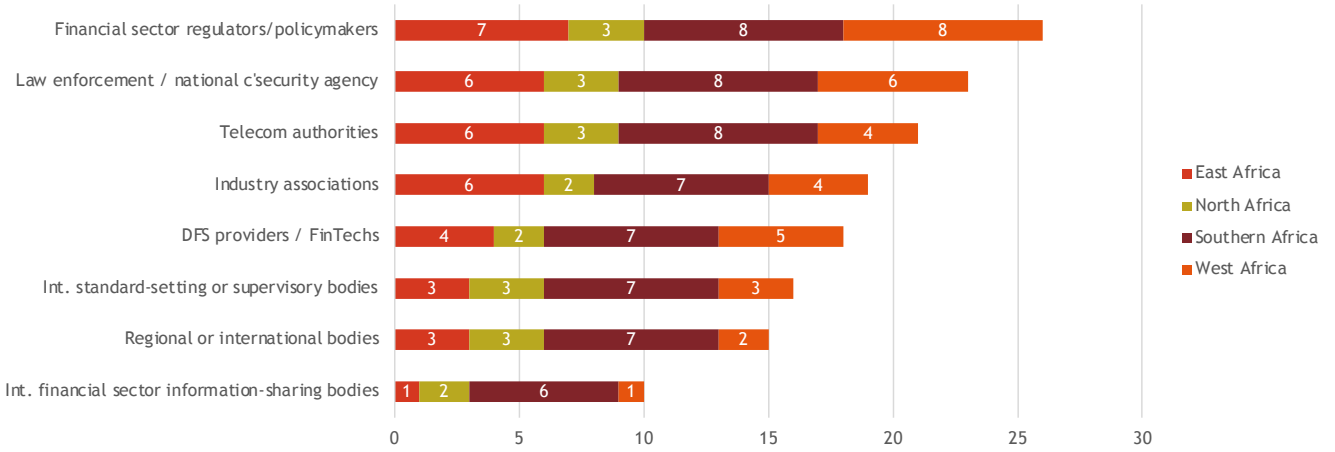


FIGURE 10. ENTITIES COORDINATED WITH ON CYBERSECURITY MATTERS



Source: AFI Regional Survey; 2025

3.2.2. Participation in national, regional, or global information-sharing mechanisms

Cybersecurity information sharing is fundamentally a collaborative activity that depends on trusted relationships, clear mandates, and regular engagement across agencies and borders. Participation in inter-agency committees and regional or global working groups allows financial authorities to align responses, share threat intelligence, and learn from peers facing similar risks. For DFS, where cyber incidents can quickly propagate across payment systems and markets, such coordination is essential to maintaining financial stability and consumer trust.

Our analysis indicates a minimal level of engagement by African financial authorities in inter-agency and multi-stakeholder coordination mechanisms. Most respondents participate in national cybersecurity committees, financial sector working groups, or operational coordination forums involving national CERTs, security agencies, communications regulators, and data protection authorities. Some institutions also engage in sub-regional platforms particularly within SADC, EAC, and West African arrangements, as well as selected global initiatives and ISACs. These mechanisms serve as key channels for information exchange, policy coordination, and capacity building, although in practice, information sharing is often conducted through a mix of formal structures and informal channels, including direct peer-to-peer communication among trusted counterparts.

The breadth of existing coordination mechanisms demonstrates strong institutional willingness to collaborate, and provides a valuable entry point for a continental or AFI-facilitated information-sharing initiative. However, the diversity of forums and overlapping mandates also risk fragmentation

and uneven information flows. Discussions further highlighted that limited trust, under-reporting of incidents, and lack of standardized processes can constrain the effectiveness of existing platforms, even where formal structures are in place. A future regional mechanism should therefore aim to complement and connect existing national and sub-regional structures, rather than replace them. Clear alignment with established coordination bodies, streamlined information-exchange practices, and well-defined participation roles will be essential to ensure coherence, avoid duplication, and build trust among participating institutions across Africa.

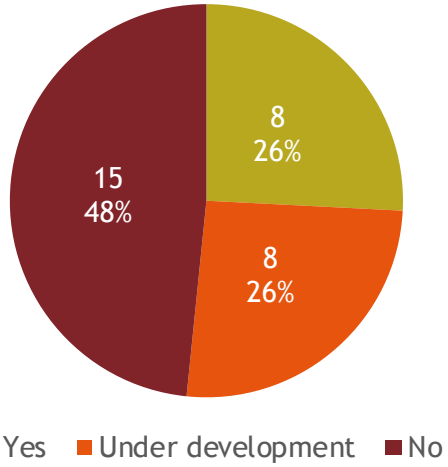
3.3. EXISTING CYBERSECURITY INFORMATION-SHARING MECHANISMS

Effective information sharing allows financial regulators and DFS providers to detect emerging threats early, respond more quickly to incidents, and learn collectively from attacks and vulnerabilities. In an environment where cyber threats are increasingly sophisticated and cross-border in nature, the availability of trusted platforms for timely exchange of incident information and threat intelligence is a key enabler of operational resilience, financial stability, and consumer protection. Our findings show that such platforms are not yet widely established across the region. Only 8 of the 31 respondent jurisdictions (26 percent) report having an operational platform or formal technological mechanism in place for sharing cyber incident information among DFS stakeholders. A similar proportion (26 percent) indicate that these mechanisms are still under development, while nearly half of respondents (48 percent) report having no platform at all (see Figure 11). This pattern highlights a significant implementation gap: although awareness of the importance of information sharing is growing, many jurisdictions are still in the early stages of translating policy commitments into functioning systems that support day-to-day cyber risk management.

Workshop insights confirm that, even where formal platforms are absent, information sharing often occurs through informal and trust-based channels. Participants reported relying on direct communication between counterparts, including phone calls and messaging applications, particularly during active incidents. While these practices enable rapid response, they also reinforce the need for more structured, secure, and scalable mechanisms that can support consistent participation and institutional memory across jurisdictions.

These findings are particularly relevant in the context of efforts to establish a regional cybersecurity information-sharing and peer-learning initiative. The uneven maturity of national platforms suggests that a regional initiative could play a catalytic role by providing a common, trusted space for collaboration, especially for jurisdictions that currently lack domestic systems. Such a mechanism can help accelerate learning, promote good practices, and facilitate early warning across borders, while also supporting countries that are in the process of developing their own platforms. In doing so, a regional approach can strengthen collective resilience, and contribute to a more coordinated and proactive cybersecurity posture across Africa's DFS ecosystem.

FIGURE 11. EXISTING PLATFORM FOR CYBER INCIDENT INFORMATION SHARING



Source: AFI Regional Survey; 2025

3.3.1. Platforms, channels, standards, and participation roles

The channels used to share cybersecurity information matter, for they directly affect how quickly, securely, and effectively stakeholders can respond to cyber threats. In the DFS space, timely access to incident information and threat insights is essential for limiting impact and preventing the spread of attacks. While informal channels can enable fast communication, more structured and secure platforms are better suited for sustained, trusted, and scalable information sharing across institutions.

Our findings show that most jurisdictions rely on basic and familiar communication tools. Email and mailing lists are used by 27 of 31 respondents (about 87 percent), and ad-hoc reports by 21 jurisdictions (68 percent). Messaging applications are also common, used by 15 jurisdictions (48 percent). In contrast,

more advanced platforms are far less prevalent: only 6 jurisdictions (19 percent) report using encrypted web portals, and just 2 jurisdictions (6 percent) use secure API-based data exchange (see Figure 12). Several respondents note that such platforms are still under development, indicating interest but limited current adoption.

This reliance on informal channels has clear implications for regional information-sharing efforts. A regional mechanism can provide a secure and standardized space that complements existing practices while gradually reducing dependence on email and messaging apps. In practice, several countries are beginning to transition toward more structured approaches. For instance, Mozambique is developing a dedicated web-based platform to support information sharing within the financial sector, while Ghana's SOC model integrates automated data collection from participating institutions, to enable near real-time analysis. At the regional level, discussions within the East African Community highlight the need for a "regional spine" supported by standardized templates and trust frameworks, moving beyond reliance on informal tools such as email and messaging applications. This will be supporting common standards and flexible participation roles, a regional platform ultimately helping jurisdictions strengthen information sharing in a way that is both practical and aligned with their current levels of technical maturity.

3.3.2. Nature of information shared, format and sharing frequency

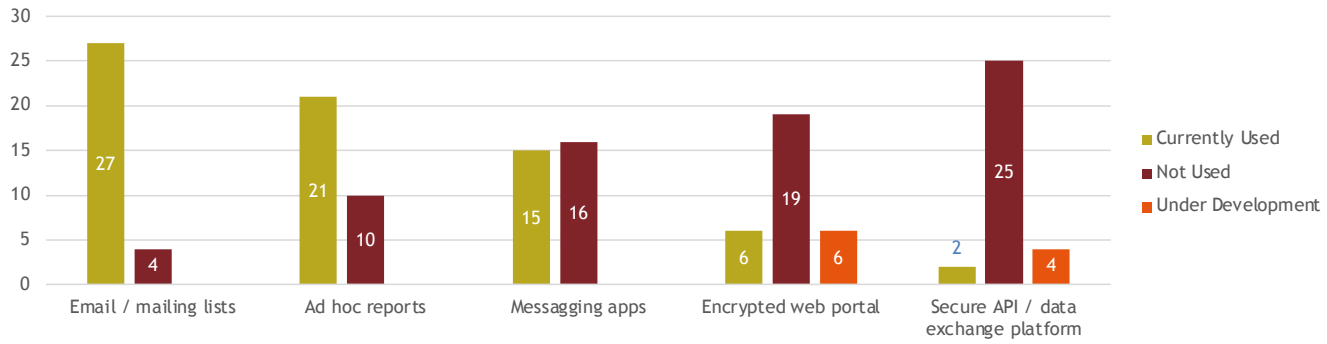
What type of information is shared, and how often it is shared, offers a practical view of how cybersecurity information sharing works on the ground. For DFS stakeholders, timely access to threat alerts and incident information is especially important for early warning and rapid response, while the regular exchange of lessons learned and best practices supports longer-term resilience. The formats and standards used also matter, as they influence how easily information can be understood, reused, and shared across institutions and borders.

Our findings show that information sharing in the region is focused primarily on immediate operational needs. Threat intelligence, alerts, and early warning information are the most shared, reported by 23 of 31 jurisdictions (around 74 percent), followed by incident reports (19 jurisdictions, or 61 percent). Best practices and lessons learned are shared by 17 jurisdictions (55 percent), while capacity-building materials (48 percent) and policy updates (45 percent) are somewhat less common.

The frequency and format of sharing further reflect the largely reactive nature of current practices. Most jurisdictions share information on an ad-hoc or incident-driven basis (13 jurisdictions, 42 percent), while 10 jurisdictions (32 percent) report no sharing in the past 12 months. Only a small number share information regularly through weekly bulletins or monthly updates, and just two jurisdictions (6 percent) report real-time or automated sharing (see Figure 14). In terms of format, the majority rely on email or PDF advisories (21 jurisdictions, 68 percent), with very limited use of structured standards such as STIX/TAXII or OpenIOC (each used by about 6 percent) (see Figure 13).

Insights from the workshop further illustrate a gradual shift toward more proactive practices. In Kenya, mandatory 24-hour incident reporting, combined with standardized templates, is enabling faster aggregation and analysis of threat data, while Ghana's centralized FICSOC supports continuous monitoring and real-time alerting across institutions. However, in many other jurisdictions, sharing remains largely incident-driven and informal, reinforcing the broader finding that structured, regular, and automated information

FIGURE 12. CHANNELS USED FOR CYBERSECURITY INFORMATION SHARING



Source: AFI Regional Survey; 2025

exchange is still at an early stage across the region.

Taken together, these findings suggest that cybersecurity information sharing in the DFS sector across Africa remains largely reactive, informal, and uneven. Information is most often exchanged after incidents occur, using basic formats that limit reusability and cross-border interoperability. The limited use of regular sharing cycles and structured standards indicates that threat intelligence is not yet being systematically aggregated, analysed, or disseminated in ways that support early warning or collective defense. For a regional information-sharing mechanism, this underscores the importance of moving beyond ad-hoc exchanges toward more predictable, trusted, and standardized practices, while recognizing current capacity constraints. A well-designed regional platform can help shift information sharing from episodic incident reporting to a more proactive and preventive model, strengthening collective cyber resilience across the DFS ecosystem.

FIGURE 13. FORMAT/STANDARD USED FOR CYBER-THREAT INFORMATION SHARING

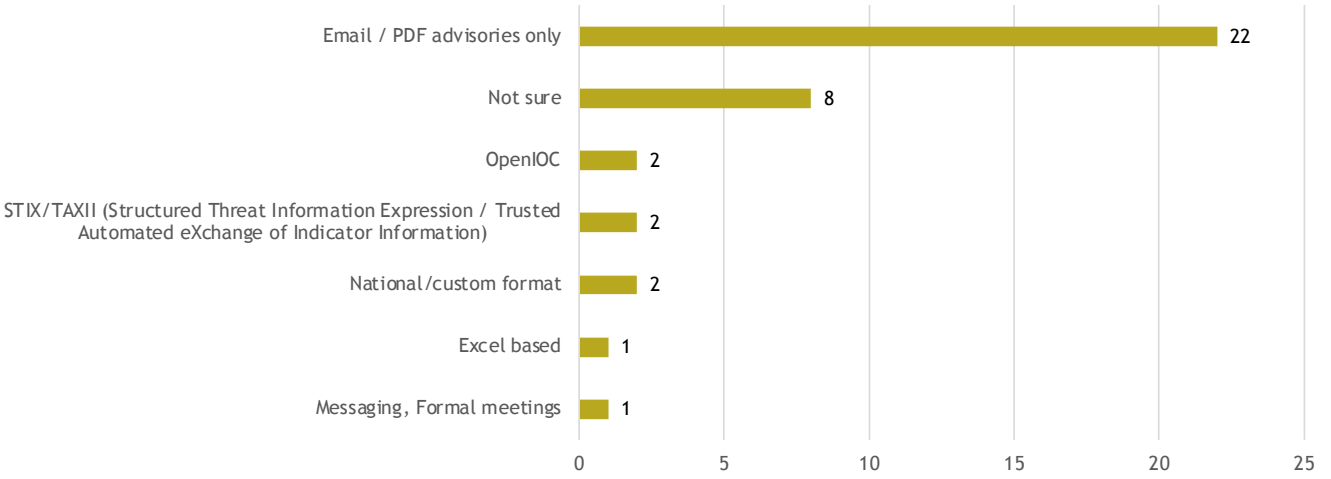
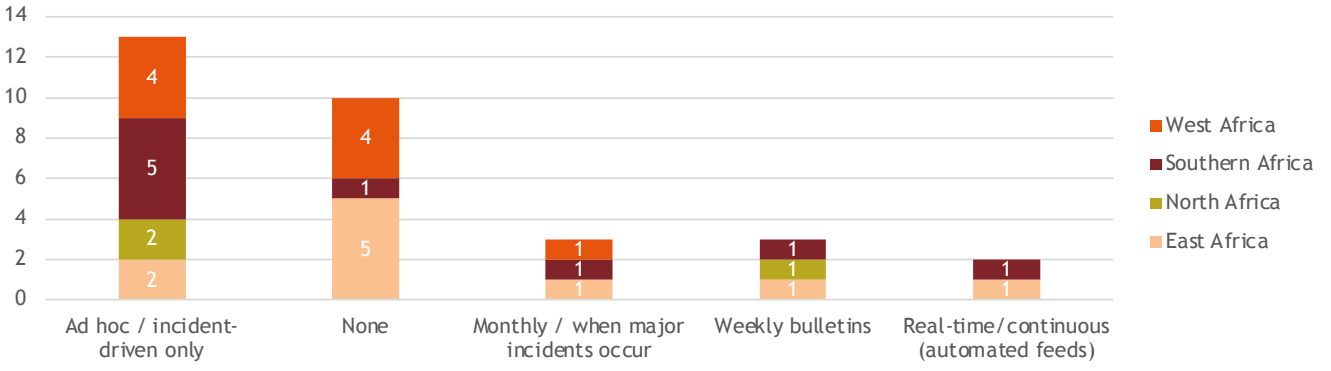


FIGURE 14. FREQUENCY OF SHARING IN THE LAST 12 MONTHS



Source: AFI Regional Survey; 2025

3.4. INCIDENT TRENDS AND OBSERVED PATTERNS

Cyber incidents targeting DFS represent a growing and evolving threat to financial stability, customer trust, and the broader digital economy in Africa. Understanding the types, frequency, and reporting practices of these incidents is critical to enabling regulators, financial institutions, and regional stakeholders to design effective risk management and information-sharing mechanisms. This section examines the patterns of cyber incidents affecting African DFS ecosystems, drawing on survey responses from AFI member institutions to highlight the most prevalent threats, reporting gaps, and policy-relevant insights that can inform regional collaboration and peer learning initiatives.

3.4.1. Cyber incident types most prevalent in financial systems

Identifying the most prevalent cyber incident types affecting financial systems is essential for prioritizing supervisory attention, capacity-building efforts, and information-sharing initiatives. Different categories of incidents, such as fraud, malware, insider abuse, or infrastructure attacks, require distinct prevention, detection, and response capabilities, as well as different forms of information exchange. For DFS in particular, the nature of incidents often reflects unique risk drivers, including agent-based distribution models, mobile channels, and extensive third-party dependencies. A clear understanding of dominant incident patterns provides a foundation for tailoring regional information-sharing mechanisms to the most pressing and recurrent threats.

Survey responses, as per the table below, indicate that social engineering and impersonation attacks are the most prevalent cyber incidents affecting financial systems, cited by 26 respondents. These include phishing, vishing, fake agents, and customer manipulation schemes, underscoring the central role of human and behavioural vulnerabilities in the DFS threat landscape. Mobile money-related fraud emerges as the second most common category (15 responses), highlighting risks such as agent fraud, SIM-swap-enabled fraud, fraudulent reversals, and wallet compromise that are closely linked to DFS business models in Africa. Malware and ransomware incidents (13 responses) and account takeover or credential compromise (11 responses) further indicate persistent weaknesses in endpoint security, authentication controls, and cyber hygiene across institutions and customers. Less frequently reported but still significant are insider threats, data breaches, and service disruption attacks, while incidents involving payment switch or API abuse, ATM/POS compromise, and third-party/ vendor compromise appear less common in the survey responses (see Figure 15).

These findings suggest that a regional information-sharing mechanism should prioritize the exchange of intelligence related to fraud typologies, social engineering campaigns, and mobile money-specific attack vectors, rather than focusing solely on traditional IT or infrastructure threats. Information-sharing frameworks must be capable of supporting rapid dissemination of indicators related to phishing campaigns, SIM-swap techniques, agent fraud patterns, and credential abuse methods, as well as practical

FIGURE 15. THE MOST PREVALENT CYBER INCIDENTS

Cyber Incident Types	East Africa	North Africa	Southern Africa	West Africa	Total
Social engineering/impersonation (phishing, vishing, fake agents, customer manipulation)	8	3	8	7	26
Mobile money-related fraud (agent fraud, SIM-swap-enabled fraud, fraudulent reversals, wallet fraud)	5	1	6	3	15
Malware / ransomware (infecting DFS endpoints, institution systems, or customers)	4	1	2	6	13
Account takeover / credential compromise (password compromise, credential stuffing, weak authentication)	2	1	4	4	11
Insider threat / credential abuse (misuse of privileged access, staff collusion)	3			3	6
Data breach / data exfiltration (customer data leakage, KYC or transaction data theft)	2		1	1	4
DDoS or service disruption attacks (targeting banks, mobile money, or national payment switches)	1		1	1	3
Payment switch / API abuse (API manipulation, unauthorized transactions, API key compromise)	2				2
ATM / POS compromise or e-skimming (card skimming, jackpotting, POS malware, web skimming)			1	1	2
Third-party / vendor compromise (fintech, aggregators, cloud providers, outsourced IT services)	1				1
Bot-driven or automated attacks (credential attacks, fake account creation, automated fraud)		1			1

Source: AFI Regional Survey; 2025

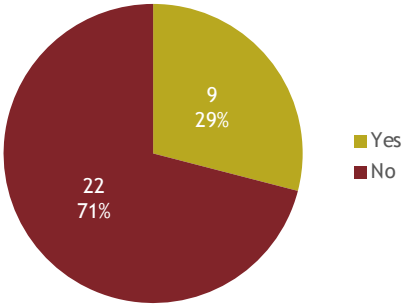
mitigation strategies. The prominence of DFS-specific fraud also reinforces the need for closer engagement with non-bank actors, such as mobile money operators, payment service providers, and fintechs, within any regional mechanism. Finally, the diversity of incident types observed underscores the value of structured peer learning, enabling institutions to share operational lessons learned and supervisory responses across jurisdictions facing similar threat profiles. The concentration of these threats also emphasizes the ongoing vulnerability of DFS ecosystems to customer-facing, human-facing, and transaction-based attack vectors. This pattern suggests that human-centric and operational weaknesses remain the primary cyber risk drivers in DFS, reinforcing the importance of consumer protection, agent oversight, and awareness-raising measures, alongside technical controls.

3.4.2. Known-vs-unreported gap

The effectiveness of cybersecurity information sharing depends not only on the existence of formal mechanisms but also on the willingness and ability of institutions to report incidents in a timely and transparent manner. Under-reporting of cyber incidents can significantly undermine situational awareness at national and regional levels, limit the effectiveness of coordinated responses, and weaken collective learning. In the context of DFS, where incidents can spread rapidly across platforms and borders, gaps between known and formally reported incidents pose risks to financial stability, consumer protection, and trust in DFS ecosystems.

Survey results reveal a notable reporting gap. While a majority of respondents (71%) indicated that they were not aware of additional DFS-related cyber incidents that went unreported, a substantial minority (29%) reported being aware of incidents that were not formally reported, but became known through other sources, such as media coverage, industry discussions, or informal networks (see Figure 16). This suggests that, even where formal reporting channels exist, some incidents circulate outside official supervisory or regulatory frameworks. The presence of such informal awareness points to latent information flows that are not systematically captured, analysed, or shared through institutional mechanisms.

FIGURE 16. AWARENESS OF UNREPORTED DFS-RELATED CYBER INCIDENTS BUT BECAME KNOWN THROUGH OTHER SOURCES



Source: AFI Regional Survey; 2025

These findings highlight the importance of addressing trust, legal, and incentive structures within any regional information-sharing framework. A successful initiative will need to create safe, well-governed environments that encourage candid reporting, including clarity around confidentiality, data protection, and safe-harbour provisions. The observed reliance on informal channels also suggests an opportunity: regional mechanisms can be designed to formalize and strengthen these existing networks, transforming ad hoc exchanges into structured, actionable intelligence flows. Integrating peer learning components such as anonymized case discussions, trusted forums, and non-punitive sharing arrangements may help reduce under-reporting and improve the overall quality and timeliness of information shared across the region.

3.4.3. Policy Relevant Insights

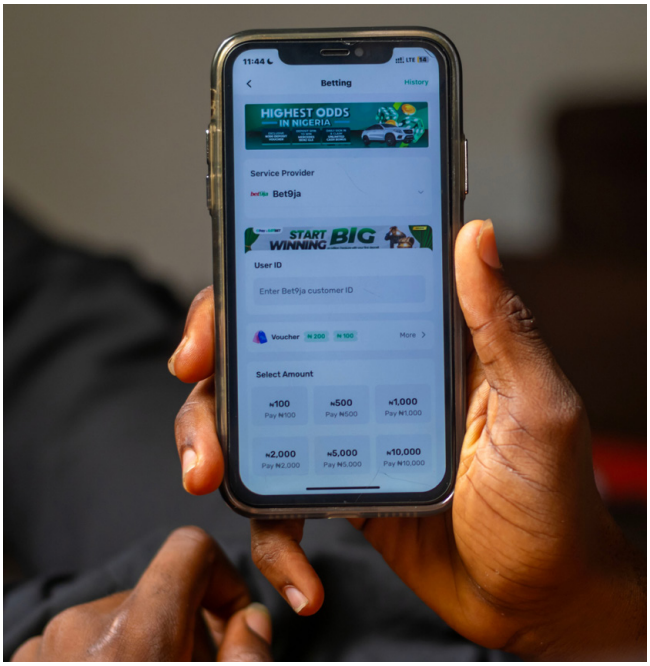
The analysis of DFS cyber incidents and reporting practices highlights several key policy implications for strengthening cybersecurity across African financial systems.

First, the prevalence of social engineering, mobile money-related fraud, and malware/ransomware underscores the need for targeted preventive measures, including multi-factor authentication, agent and customer awareness programs, and sector-specific guidance from regulators. Standardized reporting mechanisms, coupled with safe-harbour provisions, are essential to encourage timely disclosure of incidents while protecting institutions from reputational or legal risks.

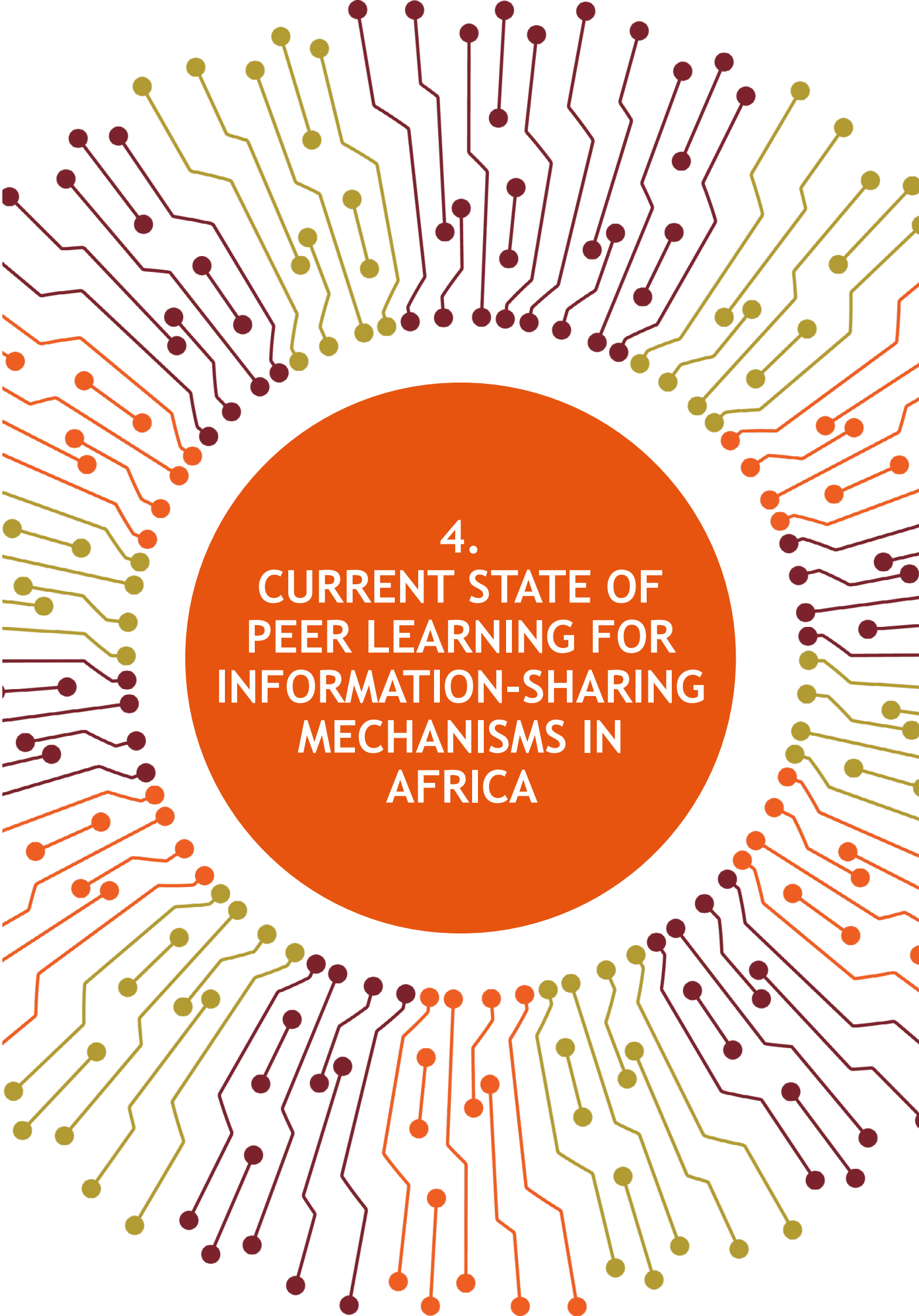
Second, the presence of unreported or informally shared incidents points to gaps in formal information-sharing channels and the potential value of leveraging existing informal networks. Regional coordination and secure, real-time platforms can enhance cross-border threat intelligence and early detection of emerging threats, particularly in mobile money and instant

payment systems. Workshop discussions also highlighted the importance of embedding these policy priorities within practical, country-level implementation models. For example, Mozambique and Kenya demonstrated how mandatory reporting frameworks and standardized taxonomies can significantly improve incident visibility and coordination. At the same time, experiences from The Gambia underscored the value of pre-existing bilateral relationships in enabling rapid cross-border support during cyber incidents.

These examples reinforce that combining regulatory measures with trust-based collaboration and capacity building is essential for achieving effective and sustained cybersecurity information sharing across Africa. Collectively, these findings emphasize the importance of capacity building, continuous peer learning, and data-driven regulatory oversight, enabling regulators and institutions to focus resources on the most critical vulnerabilities, and strengthen the overall resilience of the DFS ecosystem.



vic josh / Shutterstock



4. CURRENT STATE OF PEER LEARNING FOR INFORMATION-SHARING MECHANISMS IN AFRICA

As cybersecurity risks continue to evolve, peer learning has become an increasingly important mechanism and platform for financial-sector regulators and policymakers, helping to strengthen their understanding of threats, exchange practical experiences, and adapt supervisory and policy responses.

In the context of DFS, peer learning complements formal information-sharing mechanisms by enabling regulators and policymakers to learn from comparable jurisdictions, discuss challenges in a trusted setting, and build collective capacity over time.

This section examines the current state of peer learning related to cybersecurity information sharing among AFI member institutions in Africa. Drawing primarily on responses to the regional survey, the analysis is complemented by insights from Task Team discussions, regional workshops, and virtual stakeholder engagements. The survey findings reveal a landscape in which peer learning already takes place through a mix of domestic coordination, sub-regional collaboration, and participation in global forums, but where the depth, formality, and consistency of these engagements differ significantly across regions and institutions. Insights from the regional workshop further confirm that peer learning across African jurisdictions is often driven by practical, experience-based exchanges rather than formalized systems. Participants highlighted that learning frequently occurs through workshops, joint exercises, and direct engagement among peers, where real incident experiences and operational challenges are shared in trusted settings.

Overall, our findings highlight both strong interest and uneven practice in peer learning for cybersecurity. While many institutions are not yet actively engaged in structured information-sharing initiatives, there is widespread willingness to participate in regional platforms and a clear articulation of the tools and modalities that would enable more effective collaboration. This chapter unpacks these findings by examining how peer learning is organized domestically, how it extends across borders, the platforms and mechanisms currently in use, and the key barriers and opportunities that shape future peer learning initiatives across Africa.

4.1. DOMESTIC PEER LEARNING AND INSTITUTIONAL ARRANGEMENTS

At the national level, peer learning often begins within and among institutions responsible for financial sector regulations and oversight, cybersecurity, and payment systems. Understanding how AFI member institutions organize internal learning and coordination provides important insights into institutional readiness and the foundations upon which broader information-sharing initiatives can be built.

The survey results indicate that domestic peer learning arrangements related to cybersecurity information sharing remain uneven across AFI member institutions in Africa. Slightly over half of respondents reported not currently participating in any regional or international cyber information-sharing initiative, suggesting that for many institutions, peer learning is still largely confined to national or institutional boundaries. This points to varying levels of institutional maturity, mandates, and resourcing, as well as differences in how cybersecurity responsibilities are distributed across central banks, supervisors, payment system operators, and national cybersecurity agencies.

Among institutions that do participate in peer learning initiatives, engagement is often anchored in existing institutional or supervisory networks, particularly within central banking communities. Responses highlight participation in SADC-based workstreams, such as ISACs, CSIRT coordination groups, payment system operations centres, and committees of central bank governors, alongside involvement in global or functional forums including FS-ISAC, SWIFT ISAC, FIRST, IMF, World Bank, and BIS-related activities. These engagements are typically structured around working groups, periodic meetings, workshops, or conferences, rather than continuous or automated information-sharing mechanisms. This suggests that domestic peer learning often evolves organically from supervisory cooperation and capacity-building activities rather than from dedicated cyber intelligence frameworks.

Workshop discussions also revealed that, in several jurisdictions, domestic peer learning is increasingly being institutionalized through central bank–led coordination forums and sector-specific structures. For example, Kenya and Ghana have established formal coordination mechanisms, including sectoral SOCs and regulatory forums, which facilitate regular interaction among financial institutions, supervisors, and other stakeholders. In contrast, countries such as The Gambia noted that peer learning remains more informal, and often depends on external support or bilateral

relationships, highlighting differing levels of institutional maturity.
For the peer learning initiative, the findings imply that domestic arrangements form a critical foundation for broader regional collaboration, but are not yet consistently institutionalized across countries. Where strong internal coordination and routine peer exchanges exist, institutions appear better positioned to engage externally and contribute meaningfully to regional platforms. Conversely, the absence of structured domestic peer learning in many jurisdictions underscores the need for the initiative to support basic institutional readiness, clarify roles, and promote simple, practical entry points that can complement rather than overwhelm existing national coordination mechanisms.

4.2. CROSS-BORDER AND REGIONAL COLLABORATION

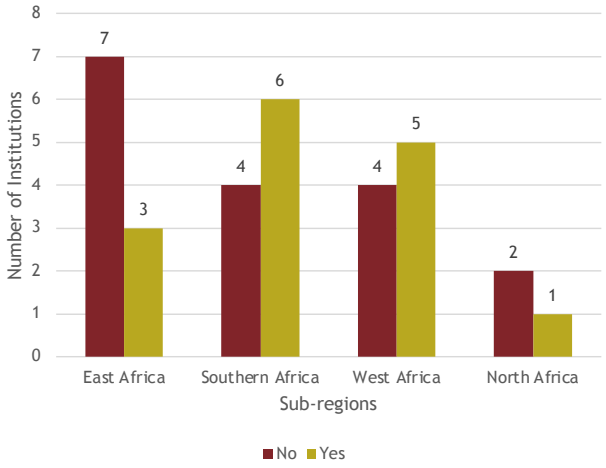
Given the cross-border nature of cyber threats, peer learning frequently extends beyond national boundaries. Sub-regional and regional platforms play a key role in facilitating dialogue, sharing experiences, and coordinating responses among financial-sector authorities facing similar risks.

The survey results highlight that cross-border peer learning on cybersecurity in Africa is already taking place, but primarily through sub-regional and thematic groupings rather than continent-wide platforms. Participation is strongest in regions with established financial and supervisory cooperation structures, notably Southern Africa (SADC) and West Africa (WAEMU/ECOWAS), where respondents cited regional coordination led by central banks, committees of supervisors, and payment system operators. These platforms provide important spaces for harmonizing supervisory approaches, discussing emerging risks, and sharing lessons learned, even if cybersecurity is not always their sole or primary focus (see figure 17).

Discussions during the workshop further illustrated that cross-border peer learning is often shaped by sub-regional dynamics and existing institutional relationships. For instance, collaboration within SADC has evolved through structured committees and working groups, while in the East African Community, information sharing remains more informal and reliant on direct communication between counterparts. In West Africa, the BCEAO highlighted both the opportunities and challenges of coordinating across a monetary union, particularly in the context of shared payment infrastructure and emerging cross-border cyber risks. These examples underscore the diversity of regional experiences and the need for a flexible, interoperable approach to peer learning.
Importantly, the survey reveals strong willingness among respondents to engage in a dedicated regional platform for cybersecurity information sharing and peer learning. Many institutions indicated a clear “yes,” with a smaller group expressing conditional interest pending internal policy review, and virtually no outright resistance. This demonstrates broad recognition of the cross-border nature of cyber risks affecting DFS, and an appetite for more structured collaboration that goes beyond ad hoc meetings or bilateral exchanges. The presence of “pending policy review” responses also highlights that legal, governance, or confidentiality considerations remain salient for some institutions.

For the CISPLI, these findings suggest a timely opportunity to build on existing regional networks, while offering a more focused, purpose-built peer learning platform for cybersecurity. Rather than replacing current arrangements, the initiative can leverage and provide the link with existing sub-regional experiences, promoting interoperability of practices, and enabling institutions with less exposure to regional collaboration to participate in a trusted environment. The strong stated willingness to engage provides a clear mandate to move from exploratory discussions toward practical implementation, while remaining sensitive to policy approval processes in certain jurisdictions.

FIGURE 17. INSTITUTIONS CURRENTLY PARTICIPATING IN REGIONAL OR INTERNATIONAL CYBER INFORMATION-SHARING INITIATIVES
SOURCE: AFI REGIONAL SURVEY



Source: AFI Regional Survey; 2025

4.3. PLATFORMS AND MODALITIES FOR PEER LEARNING

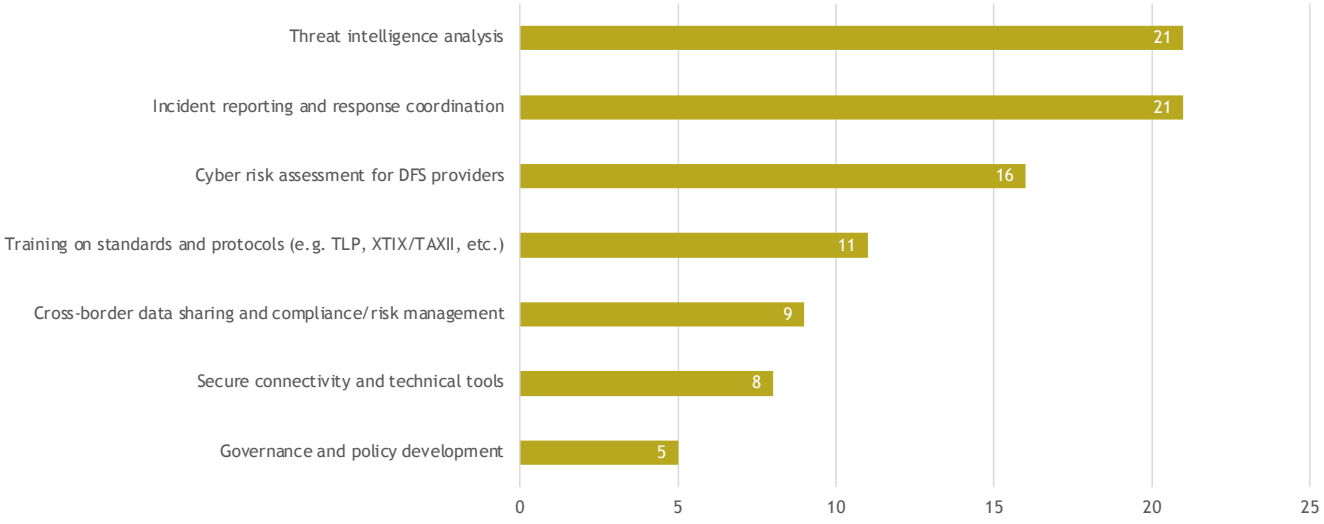
Peer learning can take many forms, ranging from formal, structured programs, to informal and ad-hoc exchanges. The choice of platforms and modalities influences the depth, trust, and continuity of learning as well as the level of trust and engagement among participants.

Survey responses provide valuable insight into the types of platforms and tools that institutions view as most useful for participating in a regional peer learning mechanism. The demand for playbooks, joint-exercise scripts, and curated starter threat-intelligence feeds suggests that peer learning is most effective when it is practical and experience-based. Institutions appear to value opportunities to learn from simulated incidents, real supervisory scenarios, and structured exchanges that translate abstract cyber risks into operational and supervisory actions. While training on frameworks such as TLP, STIX, and TAXII was also identified, it ranked alongside, rather than above, the more immediate, usability-focused tools, reflecting differing levels of technical maturity across the region (see Figure 18).

Workshop participants further emphasized the importance of experiential and practice-oriented learning modalities. Cyber-range simulations, joint incident-response exercises, and secondment programmes were identified as particularly effective in building operational capacity and trust among institutions. Countries such as South Africa have already implemented large-scale cyber simulation exercises, while others expressed interest in adopting similar approaches to complement traditional workshops and training sessions.

These preferences have important implications for the design of the peer learning initiative. The respondents point toward a phased and inclusive approach, starting with simple, common tools that lower barriers to participation and build confidence among members. Initial initiatives on templates, agreements, and guided exercises can foster trust, establish shared practices, and gradually introduce more advanced information-sharing modalities as institutional capacity grows.

FIGURE 18. CAPACITY BUILDING/TECHNICAL ASSISTANCE THAT WOULD MOST SUPPORT INSTITUTIONS



Source: AFI Regional Survey; 2025

4.4. BARRIERS, GAPS, AND OPPORTUNITIES

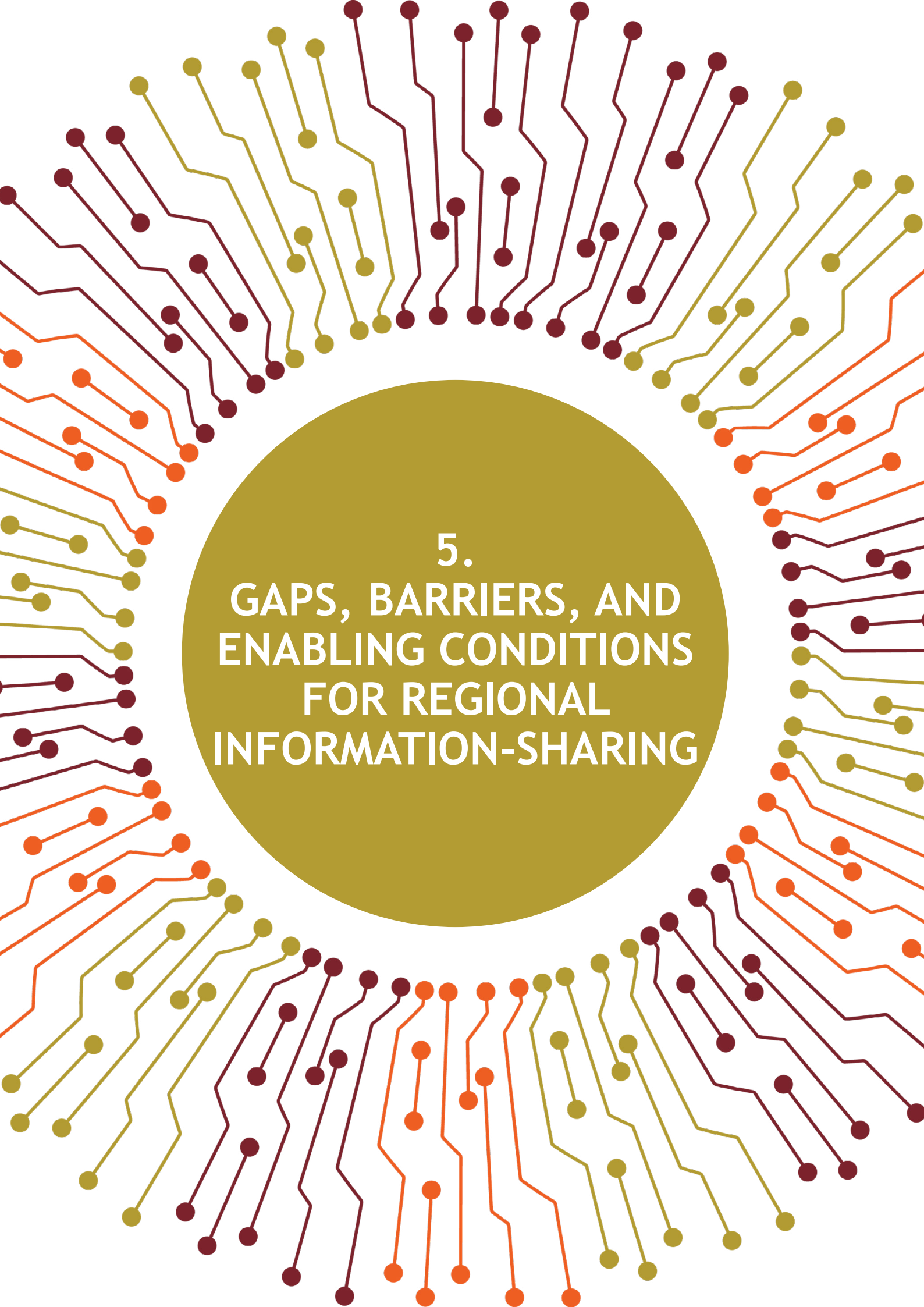
While peer learning is widely recognized as valuable, a range of constraints continue to limit its effectiveness and reach. The survey reflects strong interest in peer learning, and implicitly reveals several barriers that continue to limit effective collaboration. The fact that many institutions do not yet participate in regional or international cyber information-sharing initiatives points to challenges related to mandates, resources, legal constraints, and technical capacity. Concerns around confidentiality, data protection, and liability are reflected in the high demand for model NDAs and anonymization guidance which remain a key obstacle to more open and timely exchanges.

Survey responses highlighted a number of infrastructure and continuity gaps. Responses indicating the need for funding for secure connectivity and the reliance on meetings, workshops, or ad-hoc engagements, suggest that peer learning is often irregular rather than continued. This limits the ability of institutions to share time-sensitive information, track emerging threats, or build institutional memory over time. Additionally, varying levels of maturity across regions and institutions mean that some members may struggle to engage meaningfully without targeted support.

Workshop discussions also highlighted that peer learning is often constrained by structural and capacity-related challenges, including limited cybersecurity talent, funding constraints, and uneven access to training opportunities across institutions. Participants also noted that the absence of continuous engagement mechanisms, such as dedicated platforms or communities of practice, limits the sustainability of peer learning efforts. At the same time, there was strong consensus that structured capacity-building programmes, peer exchanges, and regional coordination platforms led by institutions such as central banks or AFI could significantly enhance both the reach and impact of peer learning across the continent.

These gaps point to clear opportunities for the initiative to add value. There is a need to address identified foundational constraints such as trust frameworks, standardized processes, and practical learning tools to support the peer learning platform and help level the playing field and enable broader participation. The strong willingness expressed by survey respondents, combined with concrete suggestions on needed tools, provides a roadmap for designing an initiative that is responsive, demand-driven, and grounded in members' realities.

vic josh / Shutterstock



5. GAPS, BARRIERS, AND ENABLING CONDITIONS FOR REGIONAL INFORMATION-SHARING

Effective cybersecurity information sharing is critical for detecting threats early, coordinating responses, and strengthening the resilience of DFS across Africa.

Timely and secure exchange of threat intelligence enables financial institutions and regulators to identify emerging risks, mitigate systemic vulnerabilities, and maintain trust in the DFS ecosystem.

This chapter examines the key factors shaping the effectiveness of cybersecurity information sharing in the region. It specifically explores the main barriers, including fragmented institutional arrangements, limited technical infrastructure, uneven human and technical capacity, and legal or trust constraints, that inhibit timely and comprehensive threat intelligence exchange. The chapter also assesses enabling conditions, such as governance frameworks, safe-harbour provisions, peer-learning initiatives, and cross-border cooperation, which can support the development of a trusted, efficient, and sustainable regional mechanism.

5.1. BARRIERS TO EFFECTIVE INFORMATION SHARING

Effective cybersecurity information sharing depends on clear rules, trusted relationships, and adequate technical, human, and financial resources. Legal frameworks provide clarity on what data can be shared, trust fosters timely disclosure, and sufficient technical and human capacity ensures actionable intelligence. Without these enablers, institutions adopt risk-averse behaviours, which can delay threat detection, impede coordination, and undermine the resilience of DFS ecosystems.

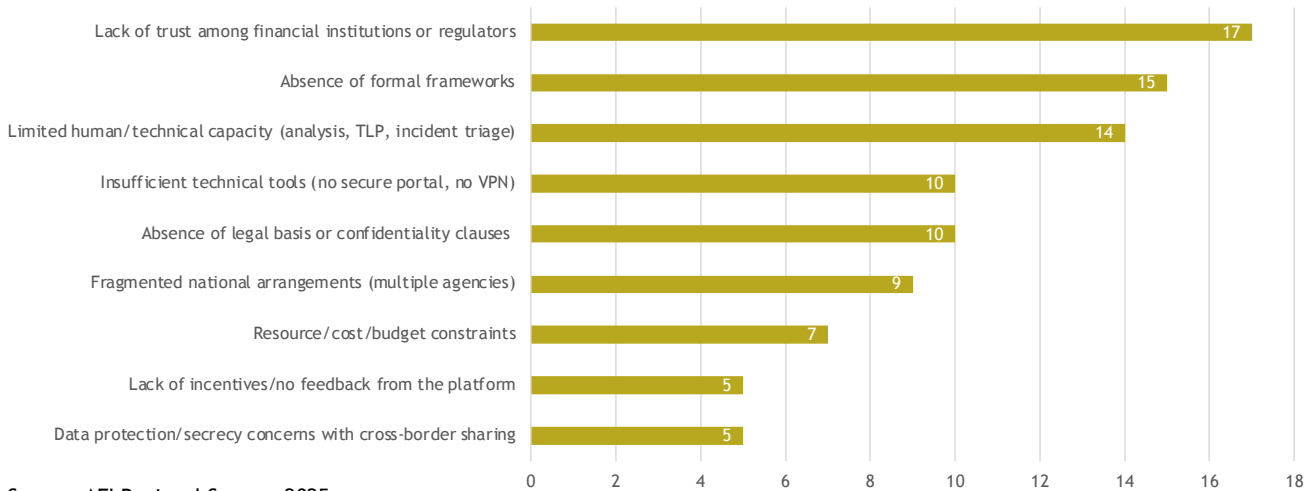
The survey responses highlight several key barriers. The most frequently reported challenge is lack of trust among financial institutions and regulators (53% of respondents), followed by absence of clear legal or regulatory frameworks (47%), which create uncertainty about liability, confidentiality, and supervisory consequences. Financial authorities' limited human and technical capacity (44%) and fragmented national arrangements (28%) further restrict the timeliness and quality of information exchange (see Figure 19).

Workshop insights further validate these findings, particularly the central role of trust and legal clarity as binding constraints. Participants emphasized that institutions are often reluctant to share sensitive information due to fear of reputational damage or regulatory consequences, especially in the absence of safe-harbour provisions. In several cases, reliance on informal communication channels was identified as a workaround to these constraints, reflecting both the importance of trusted relationships and the limitations of formal frameworks.

These findings indicate that institutional and governance constraints, combined with resource and capacity gaps, are the primary obstacles preventing effective cross-border cybersecurity collaboration. Respondents also highlighted gaps such as unclear reporting procedures, insufficient platforms, lack of incentives, and fear of reputational or regulatory consequences. These findings indicate that the primary constraints are institutional and governance-related, followed by technical and financial limitations.

Addressing these barriers requires a multi-dimensional approach. Regulators and policymakers should establish harmonized legal frameworks with appropriate

FIGURE 19. BARRIERS TO EFFECTIVE CYBERSECURITY INFORMATION SHARING SOURCE: AFI REGIONAL SURVEY



Source: AFI Regional Survey; 2025

safe-harbour provisions and implement a regional cybersecurity information-sharing mechanism that provides trusted governance, secure platforms, standardized procedures, and shared technical capacity. Strengthening inter-agency coordination, investing in technical infrastructure, and supporting capacity-building initiatives will reduce fragmentation, foster trust, and enable timely, actionable information sharing. Together, these measures will enhance cross-border cyber risk management, improve regulatory compliance, and strengthen the overall resilience of Africa's DFS sector.

5.2. INFRASTRUCTURE GAPS

Beyond policy and governance considerations, the effectiveness of information sharing is strongly influenced by the underlying technical infrastructure. Variations in tooling, interoperability, and adoption of common standards can create practical obstacles that slow down or compromise secure exchanges. Robust technical infrastructure allows institutions to share threat intelligence efficiently and reliably, supporting proactive risk management and coordinated incident response.

Global best practices include secure automated platforms, encrypted portals, and the use of standards such as STIX/TAXII and TLP, which enable structured, machine-readable, and actionable information exchange. In Africa, gaps in technical infrastructure can limit the effectiveness of regional information-sharing initiatives and reduce the speed and quality of responses to emerging cyber threats.

Survey responses indicate that information sharing remains largely manual and fragmented. Workshop discussions reinforced that infrastructure gaps are not only technical, but also linked to how information-sharing systems are designed and adopted. For example, countries such as Ghana are beginning to implement more advanced SOC-based data collection models that enable near real-time aggregation of incident data, while Mozambique is developing a dedicated web-based platform for financial sector information sharing. However, participants noted that many institutions continue to rely on basic tools due to cost, skills gaps, and uncertainty around standards adoption, highlighting the need for scalable and context-appropriate solutions rather than one-size-fits-all platforms. These findings reveal limited interoperability, low automation, and minimal adoption of international standards. Compared with global best practices, where structured, automated, and standardized sharing mechanisms are increasingly adopted, these institutions are largely at an early stage of technical maturity for cyber threat intelligence sharing, and face significant technical gaps that reduce the timeliness, consistency, and utility of shared cyber threat intelligence.

Addressing these gaps requires targeted investments in secure, interoperable, and standardized technical platforms for cybersecurity information sharing. Adoption of automated portals, secure APIs, and recognized standards such as STIX/TAXII and TLP will enable structured, timely, and actionable exchanges. Complementary training and capacity-building programs are also needed to ensure institutions can effectively use these tools. By strengthening technical infrastructure and aligning with global best practices, Africa can improve the efficiency, reliability, and scalability of information sharing, foster cross-border collaboration, and enhance the resilience of its DFS ecosystem against emerging cyber threats.

5.3. REGIONAL CYBER INFORMATION-SHARING READINESS

Assessing readiness for regional cybersecurity information sharing requires looking beyond individual country capabilities. Effective coordination depends on how governance models, operational preferences, and supporting conditions align across diverse jurisdictions. Differences in institutional arrangements, technical tools, and communication approaches can either facilitate or hinder timely, trusted, and actionable exchange of cyber threat intelligence.

Insights from the workshop further emphasize that readiness is uneven not only across countries but also across sub-regions, reflecting differences in institutional maturity, legal frameworks, and existing coordination mechanisms. While some jurisdictions have established operational structures and clearer governance models, others are still in early stages, relying on informal arrangements and external support. This diversity reinforces the importance of designing a regional approach that is flexible and capable of accommodating different starting points.

5.3.1. Preferred operational models

Operational models fundamentally shape how information-sharing mechanisms function and the degree of trust participants place in them. Different cyber information-sharing models (centralized, federated, or hybrid) each offer distinct advantages and trade-offs, depending on institutional capacity and regional dynamics. Centralized models consolidate data and oversight in a single hub, simplifying enforcement

but potentially raising liability or trust concerns. Federated models distribute responsibility across semi-autonomous entities, enabling local control but requiring robust coordination protocols. Hybrid models combine central oversight with decentralized execution, balancing consistency with local decision-making. Selecting the right operational model is critical to ensure regional cooperation, compliance, and resilience in DFS cybersecurity.

The survey results show a strong preference for a hybrid model, with 25 of 32 respondents (78%) favouring national platforms pushing anonymized data to a regional hub. Only 16% of the respondents preferred a fully centralized hub operated by AFI or partners, while one respondent favoured a federated approach (see Figure 20). These findings suggest that fully centralized or purely federated models may face challenges related to trust, liability, and coordination, whereas hybrid models offer a politically and operationally feasible balance between national ownership and regional integration.

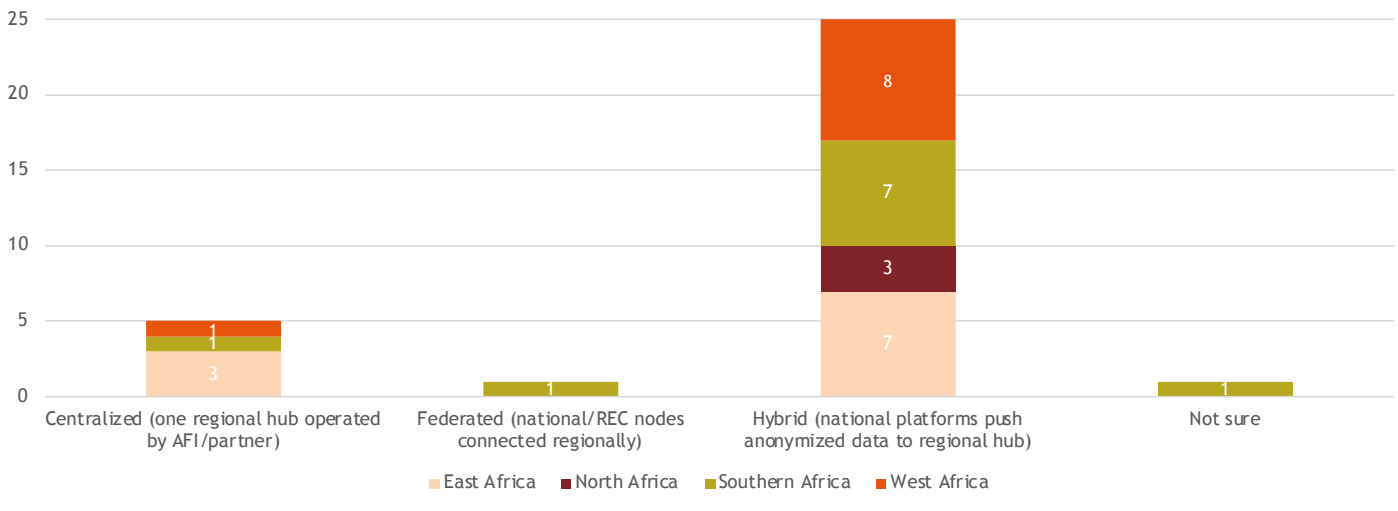
Workshop discussions strongly aligned with this preference, with participants advocating for a hybrid, multi-layered approach that links national, sub-regional, and continental mechanisms. For example, experiences from the East African Community highlighted the need for a "regional spine" to connect national systems, while SADC and West African participants emphasized building on existing sub-regional structures rather than replacing them. This reinforces the practicality of a hybrid model that preserves national sovereignty while enabling structured regional coordination.

The initiative should prioritize a hybrid operating model, enabling national authorities to retain control while contributing to regional situational awareness. Clear roles, standardized protocols, and secure channels for data exchange will support trust, transparency, and operational alignment. By adopting a hybrid model, the region can address governance, coordination, and standardization challenges, ensuring effective cross-border information sharing while maintaining local flexibility and accountability.

5.3.2. Language and localization needs

Language, terminology, and contextual relevance are critical for effective information sharing. The survey responses highlight Africa's linguistic diversity, with English, French, Portuguese, Swahili, and Arabic, among others, cited as predominant working languages. This indicates the need for multi-lingual platforms, consistent terminology, and culturally adapted communication strategies to ensure inclusivity, clarity, and actionable intelligence exchange across jurisdictions.

FIGURE 20. PREFERRED OPERATING MODEL FOR REGIONAL INFORMATION SHARING



Source: AFI Regional Survey; 2025

5.3.3. Enabling conditions

For regional cybersecurity information-sharing mechanisms to function in practice, they require sustained support beyond policy commitments. Funding, practical tools, shared templates, and clear guidance play a critical role in lowering participation barriers, promoting consistency, and enabling institutions to participate fully[5]. Clear governance frameworks and defined roles build trust among participants, ensuring that sensitive information is shared securely and responsibly.[6] Interoperable tools and standardized protocols (e.g., STIX/TAXII) support consistent, actionable exchange, while legal clarity on privacy, liability, and cross-border obligations reduces uncertainty and encourages participation.[7]

Strategic partnerships and financial resources will be essential to operationalize the mechanisms, particularly in the early stages of implementation. Workshop insights further highlighted that trust-building measures such as formal memoranda of understanding (MOUs), joint simulation exercises, and clear data-classification frameworks (e.g., TLP) are critical enablers for sustained participation. Participants emphasized that, beyond technical tools, consistent interaction and demonstrated value through real use cases are essential to encourage institutions to actively share information. These findings reinforce that a combination of resources, guidance, governance, trust, standards, and legal support is essential for sustainable, effective, and coordinated cyber threat information sharing.

i_am_zews / Shutterstock

[5] ISMS Online. Information Sharing Community. 2023. https://www.isms.online/glossary/information-sharing-community/
[6] Alotaibi, F., & Furnell, S. Trust in Cybersecurity Information Sharing: An Empirical Study. Cybersecurity, 11(1), 2022.
[7] Alzahrani, A. et al. Legal Challenges in Cyber Threat Information Sharing. Computers, 9(1), 2020. https://www.mdpi.com/2073-431X/9/1/18

6. RECOMMENDATIONS FOR A REGIONAL INFORMATION-SHARING APPROACH

The findings from this study highlight a clear opportunity for collective action.

While cybersecurity information-sharing practices for DFS across Africa remain fragmented and uneven, there is strong willingness among member institutions to engage in more structured collaboration. Building on these insights, this chapter sets out practical recommendations for establishing a regional cybersecurity information-sharing and peer-learning approach that is inclusive, trusted, and fit for purpose. This proposed approach should be situated within the broader ecosystem of cybersecurity collaboration initiatives across Africa. It is intended to complement, rather than duplicate, these efforts, with a specific focus on DFS regulatory coordination and peer learning within the financial sector.

Peer learning and information sharing should be treated as complementary pillars, where information sharing enables the exchange of cyber threat intelligence and incident data, and peer learning ensures that insights are translated into strengthened institutional capacity. The AFI platform is intended to serve as a trusted entry point for coordinating this dual function among its member DFS regulators.

6.1. STRATEGIC OBJECTIVES FOR REGIONAL INFORMATION SHARING AND PEER LEARNING

The regional cybersecurity information-sharing initiative should aim to transform fragmented, ad-hoc practices into a coordinated, trusted, and proactive ecosystem. Our findings show that unclear mandates, limited trust, and uneven technical capacity currently constrain effective sharing, while strong willingness exists to engage collaboratively. The initiative should therefore focus on creating a common, safe space where DFS regulators and financial institutions can exchange cyber threat intelligence, incident reports, and lessons learned, supported by clear governance, agreed protocols, and practical tools that reduce legal and reputational risks.

Equally important is embedding peer learning as a core objective. Given the diversity in institutional arrangements, oversight responsibilities, and technical maturity across jurisdictions, the mechanism should enable participation at multiple levels. This includes strengthening national supervisory capacities, promoting coordination with cybersecurity and data protection authorities, and providing structured opportunities for institutions to share experiences and adopt best practices.

These objectives are consistent with priorities identified during the regional workshop, where participants emphasized the need to move from informal, reactive exchanges toward structured, proactive, and trust-based collaboration. There was strong consensus on the importance of combining information sharing with peer learning, capacity building, and practical tools to ensure that the mechanism delivers tangible value to participating institutions. Together, these objectives aim to build trust, harmonize approaches, and improve collective resilience across Africa's DFS ecosystem.

6.2. POLICY AND LEGAL ENABLERS

Effective information sharing requires clear rules, legal clarity, and trust among participants. The findings show that absence of legal frameworks (47%) and weak trust (53%) are major barriers, while technical and human capacity gaps further limit collaboration. The regional mechanism should therefore support harmonized legal frameworks with safe-harbour provisions, clarify privacy and liability obligations, and provide templates and guidance that reduce uncertainty, allowing institutions to share information confidently and responsibly.

Financial and technical support is also key. Sustained funding, standardized tools, and interoperable data protocols help lower barriers to participation and promote consistent, actionable exchange. Combining legal safeguards with accessible operational resources ensures that information-sharing is not only compliant, but practical and sustainable across jurisdictions.

6.3. OPERATIONAL MODEL AND COORDINATION FRAMEWORK

Survey findings indicate a strong preference (78%) for a hybrid operating model that balances national ownership with regional coordination. Such a model allows jurisdictions to maintain control over sensitive data while contributing anonymized insights to a regional hub, building trust and facilitating standardization without imposing a fully centralized system. Clearly defining roles, responsibilities, and decision-making authority across stakeholders will be critical to the initiative's success.

The framework should foster stakeholder engagement and trust through transparent procedures, shared protocols, and agreed escalation paths. By combining national-level control with regional integration, the

initiative can coordinate cross-border cyber threat intelligence, support regulatory compliance, and ensure participants feel confident that shared information is protected and used responsibly.

6.4. TECHNICAL, OPERATIONAL, AND CAPACITY REQUIREMENTS

A regional platform must be supported by secure, interoperable technology that accommodates the current diversity of national capabilities. Survey results show heavy reliance on email and ad-hoc reports, with limited use of structured standards like STIX/TAXII. The mechanism should therefore offer secure portals, APIs, and standardized protocols, while providing practical onboarding pathways for jurisdictions at different technical maturity levels. Workshop discussions further emphasized that capacity building should be closely linked to practical application. Participants highlighted the value of hands-on approaches such as cyber-range simulations, joint incident-response exercises, and secondment programmes to more mature institutions.

Capacity building should complement technology, ensuring that staff can collect, analyze, and share cyber threat intelligence effectively. Operational guidance, templates, and training programs will help institutions adopt standardized formats and reporting cycles, while gradually moving toward more automated, real-time exchange. Together, these measures will ensure the platform is not only technically sound but usable and sustainable.

6.5. STRENGTHENING PEER LEARNING SYSTEMS

National-level peer learning provides a critical foundation for regional collaboration. Survey data indicate that most institutions are not yet engaged in formal regional or international sharing, highlighting the need to build domestic readiness first. The initiative should leverage existing supervisory and institutional networks to embed structured learning cycles that complement national arrangements.

Cross-border peer learning can then expand through workshops, digital platforms, and periodic exercises, allowing jurisdictions to share experiences, lessons, and best practices. This approach ensures that learning is continuous, practical, and scalable, supporting both individual capacity development and collective regional resilience.

6.6. GENERAL RECOMMENDATION TO DEVELOP A PHASED ROADMAP

A phased roadmap will allow the initiative to build momentum while accommodating varying levels of readiness. In the short term, focus should be on establishing governance structures, basic secure channels, and entry-level reporting templates. Medium-term priorities include integrating hybrid coordination models, expanding peer learning cycles, and gradually adopting structured standards like STIX/TAXII. As part of the roadmap, roles and responsibilities should be clearly defined and the necessary resources identified to support effective implementation.

In the long term, the goal should be to achieve automated, real-time information exchange across jurisdictions, fully institutionalized regional peer learning, and standardized reporting and analytics that enable proactive threat detection. Phasing ensures that jurisdictions can participate meaningfully from the start, while steadily increasing sophistication and integration. This phased approach reflects the consensus reached during the workshop, where participants agreed that early adoption should focus on willing and more mature jurisdictions, while others are progressively onboarded through targeted capacity-building support. Such an approach allows the initiative to demonstrate early value, build trust, and scale sustainably across the continent without excluding lower-maturity participants.

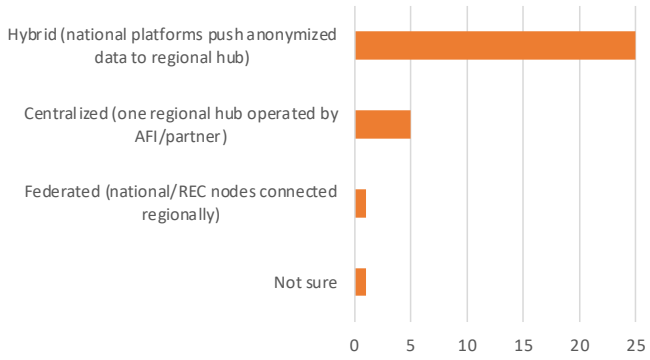
7. DESIGN OPTIONS FOR A REGIONAL INFORMATION-SHARING MECHANISM

This chapter explores practical design options for a regional cybersecurity information-sharing mechanism tailored to Africa's DFS ecosystem.

Drawing on findings that highlight uneven national capacity, fragmented arrangements, and strong preference for shared but non-centralized governance, the chapter compares three institutional models (centralized, federated, and hybrid) and assesses their suitability for the regional context. It also examines how DFS-specific risks can be integrated into each model, and how alignment with existing sub-regional structures can strengthen adoption and sustainability.

Rather than proposing a single prescriptive solution, this chapter outlines design choices and trade-offs, recognizing the diversity of institutional mandates, technical maturity, and legal environments across AFI member jurisdictions. The analysis aims to inform decision-making by highlighting which models best address current barriers while remaining flexible enough to evolve over time.

FIGURE 21. PREFERRED OPERATING MODEL



Source: AFI Regional Survey; 2025

7.1. OPTION 1: CENTRALIZED MODEL

Under a centralized model, a single regional entity such as a regional SOC or CSIRT would collect, analyze, and disseminate cybersecurity information from participating jurisdictions. This model can offer strong consistency, streamlined coordination, and easier enforcement of common standards and protocols. For jurisdictions with limited national capacity, a centralized hub could provide immediate access to expertise, analytics, and early-warning capabilities that might otherwise be difficult to establish domestically.

However, our findings suggest limited appetite for full centralization. Only a small minority of respondents favoured this model, reflecting concerns around data sovereignty, trust, legal liability, and control over sensitive incident information. In the African DFS context, where mandates for cybersecurity and data protection are often dispersed and legal gateways remain unclear, a fully centralized approach may face resistance and slow adoption unless accompanied by strong safeguards, clear legal authority, and high levels of institutional trust.

7.2. OPTION 2: FEDERATED MODEL

A federated model connects national-level platforms or nodes through agreed standards and protocols, allowing countries to retain full control over their data while enabling cross-border information exchange. This approach aligns well with national sovereignty concerns and allows jurisdictions to tailor information sharing to their legal frameworks, institutional arrangements, and capacity levels. It can also reduce the concentration of risk by avoiding a single point of failure.

Despite these advantages, survey results indicate limited support for a purely federated approach. Very few respondents preferred this model, likely due to concerns about coordination complexity, uneven maturity across nodes, and the difficulty of ensuring timely and consistent information sharing. In practice, a fully federated system may struggle to deliver regional situational awareness unless all participating nodes meet minimum technical and operational standards conditions that are not yet present across much of the region.

7.3. OPTION 3: HYBRID MODEL

The hybrid model combines a light regional coordination hub with national nodes and thematic working groups, balancing regional integration with national ownership. This approach was strongly favoured by survey respondents across all regions, reflecting its ability to address trust, governance, and capacity concerns, while still enabling meaningful regional collaboration. National authorities retain control over sensitive data, while anonymized or aggregated insights are shared regionally to support early warning and collective learning.

In practice, the hybrid model allows different participation roles based on institutional readiness. Jurisdictions with more mature platforms can contribute structured data, while others can participate through reports, alerts, or peer discussions. Thematic working groups focused on DFS, payment systems, or incident response can further deepen collaboration without overloading the core platform. This flexibility

makes the hybrid model particularly well suited to Africa's diverse regulatory and institutional landscape.

7.4. DFS INTEGRATION PATHWAYS

Any regional mechanism should explicitly integrate DFS-specific risks, given the central role of mobile money, e-money issuers, instant payments, and emerging open-finance ecosystems across Africa. Our survey findings show that current information-sharing arrangements often focus on general cybersecurity issues, with limited DFS-specific incident reporting. Design options should therefore include clear pathways for incorporating DFS providers, payment switches, and relevant fintech actors into information-sharing processes.

Furthermore, a phased integration approach is recommended. Initial focus can be placed on high-risk and high-impact segments such as mobile money platforms and national payment systems, followed by gradual inclusion of open-finance participants and third-party service providers. DFS-specific taxonomies, reporting templates, and threat scenarios can be developed through thematic working groups, ensuring that the mechanism remains relevant to the realities of Africa's DFS ecosystem.

7.5. ALIGNMENT WITH EXISTING SUB-REGIONAL STRUCTURES

Alignment with existing sub-regional structures is essential for avoiding duplication and leveraging established coordination channels. Survey responses indicate that many institutions already engage in sub-regional forums such as SADC and EAC working groups, often through periodic meetings rather than continuous information exchange. A regional mechanism should build on these foundations by enabling interoperability rather than replacing existing arrangements.

Sub-regional bodies can act as intermediate coordination layers within a hybrid model, supporting localized peer learning and gradual onboarding into the regional platform. This approach respects existing political and institutional dynamics while strengthening coherence across regions. By linking sub-regional initiatives into a common regional framework, the mechanism can enhance information flow, improve consistency, and support a more integrated continental cybersecurity posture for DFS.

Boijonell Pond / Shutterstock

REFERENCES

Carnegie Endowment for International Peace. (2024). Security and Trust in Africa's Digital Financial Inclusion Landscape.

Carnegie Endowment for International Peace. (n.d.). FinCyber Strategy Project: Cybersecurity and Financial Inclusion.

National Institute of Standards and Technology. (2016). Guide to Cyber Threat Information Sharing (NIST Special Publication 800-150). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-150.

INTERPOL (2024). African Cyberthreat Assessment Report (3rd edition). https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

INTERPOL (2025). Africa Cyberthreat Assessment Report 2025 (4th edition). https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf

World Bank. (2022). Cyber Threats to the Financial Sector in Africa.

ABBREVIATIONS

AFI - Alliance for Financial Inclusion

AfPI - African Financial Inclusion Policy Initiative

API - Application Programming Interface

CERT - Computer Emergency Response Team

CSIRT - Computer Security Incident Response Team

DFS - Digital Financial Services

DDoS - Distributed Denial of Service

EAC - East African Community

FSISAC - Financial Services Information Sharing and Analysis Center

IoC - Indicator of Compromise

MNO - Mobile Network Operator

SACCO - Savings and Credit Cooperative Organization

SOC - Security Operations Center

SADC - Southern African Development Community

STIX/TAXII - Structured Threat Information Expression/ Trusted Automated exchange of Intelligence Information

TLP - Traffic Light Protocol

WAEMU - West African Economic and Monetary Union

CISPLI TASK TEAM

1. Pedro Manjate (Banco de Moçambique)
2. Nuno Miguel Monteiro dos Santos (Banco Nacional de Angola)
3. Karima FATMI and Ghaffour Sana (Bank Al-Maghrib)
4. Ininahazwe Hugor (Bank of Burundi)
5. Daniel Klu (Bank of Ghana)
6. Linda Songiso and Awere Verry (Bank of Namibia)
7. Rashidatu Turay (Bank of Sierra Leone)
8. Medard Charles (Bank of Tanzania)
9. Collin Babirukamu (Bank of Uganda)
10. Ibrahima Sory BARRY (Banque Centrale de la République de Guinée)
11. Mariama Ouhoumoudou OUSMANE (Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO))
12. Mostafa ELHamshary (Central Bank of Egypt)
13. Mayibongwe Nkambule (Central Bank of Eswatini)
14. Fredrick Musili (Central Bank of Kenya)
15. Marcus Davis (Central Bank of Liberia)
16. Adedoyin Ademola Adeoba (Central Bank of Nigeria)
17. Descombes Elwin Daniel (Central Bank of Seychelles)
18. Mohamed Ahmed ALI (Central Bank of Somalia)
19. Edrissa Kanteh (Central Bank of The Gambia)
20. Kaoussou Kaba BALDE (Délégation Générale à l'Entreprenariat Rapide des Femmes et des Jeunes (DER F/J))
21. Andrianina Nantenaina RARIVONONA (Direction Générale du Trésor, Ministère de l'Economie et des Finances, Madagascar)
22. Mihlayenkosi SISA DLAMINI (Financial Services Regulatory Authority Eswatini)
23. Raafat EDDEREI (Ministère de l'Economie et des Finances (Maroc))
24. Souleymane DIEDHIOU (Ministère des Finances et du Budget du Sénégal)
25. Nakekelo Ginindza (Ministry of Finance – Eswatini)
26. Tendai Joana Tazvivinga (Ministry of Finance and Economic Development and Investment Promotion Zimbabwe)
27. Serge Mugiraneza (National Bank of Rwanda)
28. George Muya Ndirangu (Retirement Benefits Authority of Kenya)
29. Clever Murambwa Haparari (Reserve Bank of Zimbabwe)
30. Prester Mbiwa (Sacco Societies Regulatory Authority (SASRA) Kenya)
31. Sunthoshan Govender (South African Reserve Bank)

Alliance for Financial Inclusion
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org
Alliance for Financial Inclusion AFI.History @NewsAFI @afinetwork