DIGITAL FINANCIAL SERVICES (DFS) WORKING GROUP

BRINGING
SMART
POLICIES
TO LIFE

CYBERSECURITY FOR FINANCIAL INCLUSION: FRAMEWORK & RISK GUIDE

Guideline Note No.37
October 2019

GUIDELINE NOTE

CONTENTS

ACKNOWLEDGMENTS

AFI expresses its thanks to the chair of the cybersecurity subgroup, Komitas Stepanyan of the Central Bank of Armenia, for his excellent leadership. We would also like to thank the following member countries who contributed to the work: Bank of Ghana; Bank Al-Maghrib; Central Bank of Nigeria; Bank of Namibia; Central Bank of Sudan, and Reserve Bank Fiji. AFI is also thankful to Paul Makin for helping the subgroup conduct relevant research and draft the document.

AFI also acknowledges and appreciates the private partners, experts and stakeholders who contributed to the document. Among them are the European Central Bank, GSMA, Mastercard, Visa, IMF, ITU, CGAP and the World Economic Forum.

Ali Ghiyazuddin Mohammad and Kennedy Komba from the AFI management unit also provided inputs and comments for the framework.

The digital financial services workstream is supported by AFI's Funding Partners.

1 INTRODUCTION

1.1 BACKGROUND

In recent years, regulators and financial sector supervisors have become increasingly aware that financial services aimed to address financial inclusion (FI) challenges around the world are becoming vulnerable to cyber threats, primarily due to the increasing role of digital services (including mobile and other technologies) in the delivery of financial services.

As financial services become increasingly digitized, the volume of sensitive digital data grows exponentially and with it, the potential for personal and system impacts of data breaches. As such, the need for safeguards from illicit access to this data becomes increasingly important.

In the course of implementing their facilitatory and coordinating role to enhance financial inclusion through leveraging on digital financial services targeting the underbanked and unsophisticated consumers, AFI members have realized that they need specific guidance on addressing cyber security risks from the demand side. Also needed are supply-side perspectives focusing on the peculiarity of financial service provisions targeting the bottom segment of the pyramid. In this regard, AFI's Digital Financial Services (DFS) Working Group has set up a subgroup on cyber security to ascertain cybersecurity risks in light of digital/ FinTech innovations. Further, the subgroup will also provide policy recommendations to monitor, identify, manage and mitigate cybersecurity risks, including the development of a Cybersecurity Risk Guide, i.e. this document.

1.2 CYBERSECURITY RISK GUIDE

1.2.1 PURPOSE

The primary purpose of this document is to provide key principles and best practices that will offer guidance to assist regulatory and supervisory authorities in devising tools for the financial sector to deal with cybersecurity risks. The Guide is also useful for financial service providers to help them strengthen their cyber-risk management in the provision of financial services that target the last-mile, underserved consumers at the bottom of the pyramid.

1.2.2 METHODOLOGY

Development of this Risk Guide involved the following:

- Interviews with stakeholders, including AFI members active in cybersecurity, international payment schemes, supra-national regulatory authorities, developers of other cybersecurity frameworks, and independent industry experts.
- Meta-analysis of existing frameworks, with a specific focus on those highlighted by stakeholders.
- Development of a generic digital payments and financial services model with a significant component of financial inclusion.
- Derivation of a set of recommendations for use by regulators in the development of cybersecurity policy.

2 DIGITAL PAYMENTS AND FINANCIAL SERVICES MODEL

Financial services with a significant financial inclusion element differ from mainstream financial services in a number of key areas, including:

> **Customer segment:** services are offered to hitherto unserved or underserved segments of the population who previously conducted the majority of their transactions through informal means.

> **Medium of transaction:** this is typically technology-heavy involving self-service or agent-assisted transactions conducted through a digital device.

> **Channel**: transactions are either carried out through agents, or directly through an electronic channel such as a mobile phone.

> **Characteristics of user segments:** many are low-income customers with limited digital or financial literacy (though it is recognized that it would be a gross simplification to characterize all customers in this way, it is important to understand that it applies to a significant proportion).

> **Transactions:** these are typically low value, and low volume per customer - service providers generally seek to compensate for this by trying to achieve an overall high volume across the service.

Consequently, cybersecurity risks that such services face are somewhat different, reflecting the different attack opportunities and the limited defence opportunities available. In addition to risks directly addressed by mainstream cybersecurity frameworks developed and applied successfully in the industrialized world, there are very specific classes of risk that those frameworks do not address, given the context in which they were developed. These frameworks generally do not include the considerations of financial inclusion. The risks mentioned here are discussed in detail in Section 3, along with mitigation strategies.

In order to understand these additional risks, it is important to have a model or framework to serve as both as a reference and a means of classification. This section therefore presents an abstracted service model for a financial service aimed partially or wholly at the underserved. This model is intended to serve two main purposes:

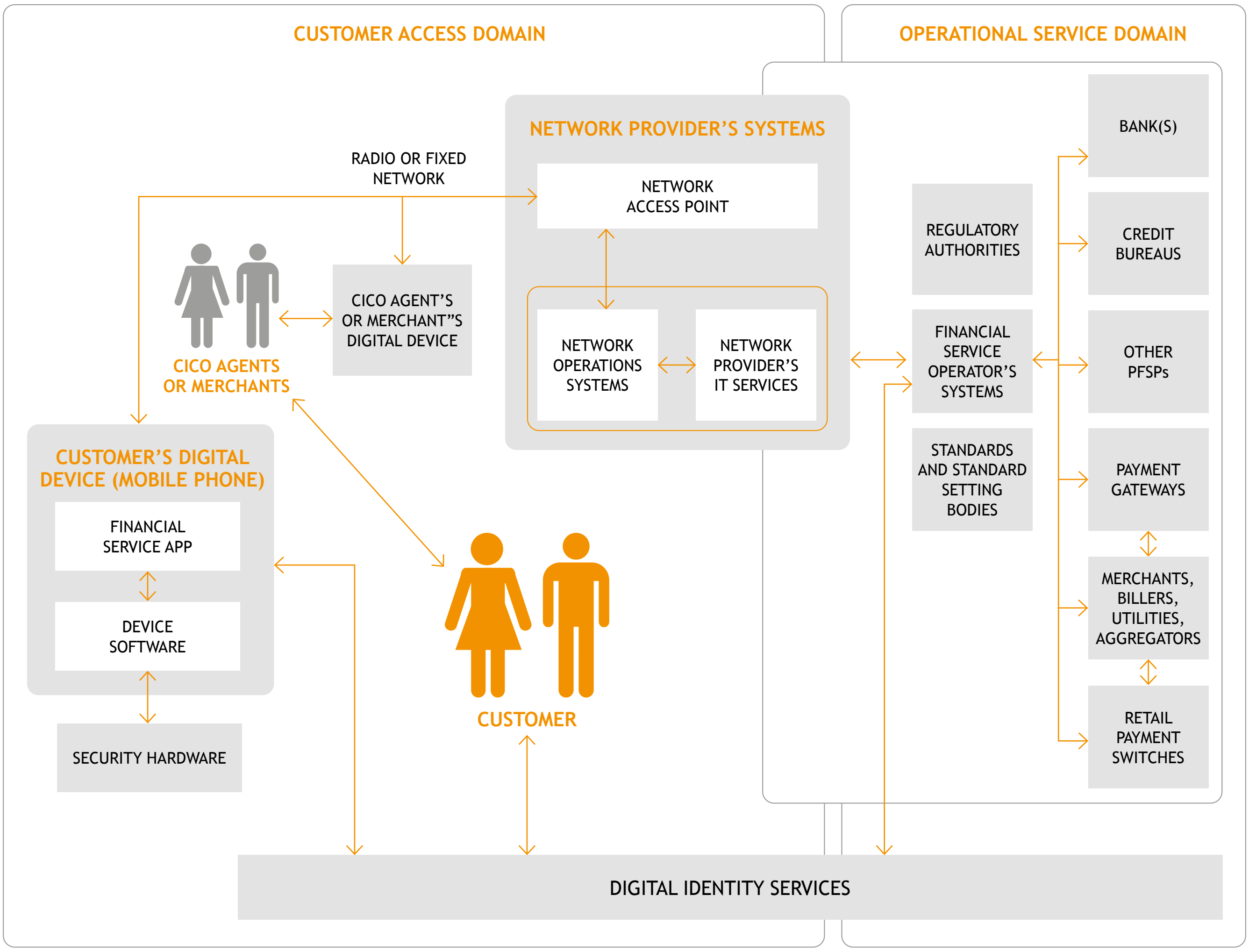
> To promote a common understanding of what a service looks like – including the “service ecosystem” in which it operates;

> To serve as a reference point for the recommendations themselves, giving context to each element.

The diagram presented in Figure 1 sets out the service model used in the analysis of cybersecurity risks for financial inclusion.

The model, which is presented from the consumer’s perspective, illustrates the range of actors involved in the delivery of services, and the varied means of interconnection and interaction between them. It has been slightly abstracted in order to highlight the elements and relationships that interoperate to deliver a financial service with a significant element of financial inclusion. In particular, a consumer’s use of either a digital device (such as a mobile phone) or an OTC service is assumed to be a characteristic of a service that supports financial inclusion.

FIGURE 1: DIGITAL PAYMENTS AND FINANCIAL SERVICES MODEL


CUSTOMER ACCESS DOMAIN
OPERATIONAL SERVICE DOMAIN
NETWORK PROVIDER'S SYSTEMS
RADIO OR FIXED NETWORK
NETWORK ACCESS POINT
CICO AGENT'S OR MERCHANT"S DIGITAL DEVICE
CICO AGENTS OR MERCHANTS
NETWORK OPERATIONS SYSTEMS
NETWORK PROVIDER'S IT SERVICES
REGULATORY AUTHORITIES
FINANCIAL SERVICE OPERATOR'S SYSTEMS
STANDARDS AND STANDARD SETTING BODIES
BANK(S)
CREDIT BUREAUS
OTHER PFSPs
PAYMENT GATEWAYS
MERCHANTS, BILLERS, UTILITIES, AGGREGATORS
RETAIL PAYMENT SWITCHES
CUSTOMER'S DIGITAL DEVICE (MOBILE PHONE)
FINANCIAL SERVICE APP
DEVICE SOFTWARE
SECURITY HARDWARE
CUSTOMER
DIGITAL IDENTITY SERVICES

3 PRINCIPLES OF CYBERSECURITY

3.1 INTRODUCTION

This Guide provides seven key principles for cybersecurity aimed specifically at financial inclusion initiatives.

> Two principles are for regulatory and supervisory authorities, to enhance their supervisory frameworks, regulatory approaches and cooperation on matters related to the cybersecurity of financial services with a significant component intended to address financial inclusion challenges.

> The remaining five principles set out the requirements to be placed on service providers and are intended to assist regulatory authorities in their supervision of service providers' activities.

3.2 PRINCIPLES FOR REGULATORS, POLICY MAKERS AND SUPERVISORY AUTHORITIES

Cybersecurity is not just an issue for service providers. Two essential principles in ensuring the security of services and the protection of customers are fulfilled by regulatory and supervisory authorities.

PRINCIPLE I: REGULATION AND COMPLIANCE

Establishing and maintaining the regulatory requirements that service providers must comply with; informing and assisting service providers in demonstrating their compliance with the regulatory environment; adapting regulations to changing environments; applying principle-based approaches, and monitoring the safety of critical public infrastructure.

PRINCIPLE II: COOPERATION

Ensuring that action is taken in concert with international counterparts; cooperating with multiple national agencies that are active in the field of cybersecurity; sharing information about threats and incidents, and ensuring that FSPs have appropriately skilled human resources to deal with cybersecurity threats.

3.3 PRINCIPLES FOR SERVICE PROVIDERS

These principles place requirements on service providers when delivering financial services with a significant financial inclusion element, and are aimed at supporting regulators in their supervision of service providers' fulfilment of these requirements:

PRINCIPLE III: PROTECTING CUSTOMERS

Understanding customers' financial service capacities; identifying customers; keeping their data private, and ensuring their effective identification during client on-boarding and in transactions.

PRINCIPLE IV: SECURE DELIVERY OF SERVICES

Understanding the service delivery channels and infrastructure that interface between FSPs customers, and ensuring that information remains private and transaction integrity is maintained.

PRINCIPLE V: MANAGING INTERNAL RISKS

Ensuring that the integrity of FSPs' service is preserved through internal controls and processes that provide effective enterprise-wide risk management for secure service provision.

PRINCIPLE VI: UNDERSTANDING YOUR PARTNERS

Making sure that partners are engaged through appropriate process without significantly increasing the risks to either customers or your service.

PRINCIPLE VII: THE LONGER TERM

Ensuring that your service maintains its security as new threats emerge; that regulatory authorities are informed of both existing risks and your plans to address these; carrying out audits regularly, and ensuring that all reporting requirements are met etc.

3.4 REGULATORS

3.4.1 PRINCIPLE 1: REGULATION AND COMPLIANCE

Establishing and maintaining the regulatory requirements that service providers must operate within; informing and assisting service providers in demonstrating their compliance with the regulatory environment; adapting regulations to changing environments; applying principle-based approaches and monitoring the safety of critical public infrastructure.

REFERENCE	RECOMMENDATION
R-1	Develop or adopt a cybersecurity framework to guide FSPs as to what is expected of them. Such a framework should take into account appropriateness to the size of the regulated institution and the risks it presents to customers.
R-2	Consider liability issues that may arise if security standards are not followed by FSPs, especially if non-compliance results in financial loss. Issues to consider include: > Mandatory communication to both the authority and affected customers > Requirements to refund losses from customers' accounts > Potential liabilities for customers' consequent losses
R-3	Consider allowing lower technical security standards (including, for example, USSD) by balancing the higher risk with stricter liability – see also Recommendation Reference C-10.
R-4	Develop a policy to address the practical aspects of implementation of oversight procedures, to include the development or adoption of a cybersecurity assessment framework.
R-5	Place particular emphasis on assessing the quality, availability and continuous transaction monitoring facilities by FSPs. This is especially in the context of additional risk incurred by using USSD and SMS for mobile financial services.
R-6	Where possible, appoint a Chief Information Security Officer (CISO). This individual will be responsible for developing and implementing an information security program to protect both internal systems and data, as well as the sensitive data provided by FSPs as part of their reporting obligations. The CISO role should exist outside any IT or MIS departments. The benefit of sch a role will be derived only from a direct reporting function to the Directors, thus avoiding the risk of cybersecurity concerns being filtered through the interests of specific departments. This industry best practice applies as much to regulatory authorities as it does to FSPs.
R-7	Sensitive data supplied by FSPs to supervisory authorities, including data about their customers, should be subject to many of the same internal cybersecurity measures that are required of FSPs. To this end, regulatory/oversight authorities should consider the adoption of international best practice technical cybersecurity controls for internal use, both where they offer digital services, and where they are the recipient or repository of confidential data from regulated entities.
R-8	Establish a national baseline for a common assessment of cyber-readiness reports across the financial sector. FSPs are required to conduct annual assessments of their level of cyber-readiness and provide the resulting reports to the supervisory authority.
R-9	Develop an approach to providing a proper, standardized assessment of each FSP's proposed approach to addressing any identified shortcomings. Shortcomings identified in an FSP's cyber-readiness assessment are commonly addressed in an addendum to the annual assessment report.
R-10	Review suspicious transaction reports (STRs) received from individual FSPs, comparing them to those received from the rest of the financial sector, and act if they differ significantly either in expected numbers of reports, or the level of detail provided.
R-11	Visit FSPs' operational centers on a regular basis to verify that the documented processes and control points are being followed. Also verify that active transaction monitoring (including AML monitoring) is in place, where appropriate.
R-12	Build internal capacity to satisfy the supervisory requirements set out in this document.
R-13	Develop cybersecurity awareness programs for delivery to the staff of both FSPs and regulatory/supervisory authorities.
R-14	Incorporate enforcement clauses in all national cybersecurity guidelines and frameworks, such that an FSP's non-compliance will result in sanctions according to national regulations.
R-15	Take measures to monitor the safety of critical digital infrastructure, including digital identity systems, payments systems, financial switches etc. and act to alert FSPs if an issue is identified.

3.4.2 PRINCIPLE II: COOPERATION

Ensuring that action is taken in concert with international counterparts; cooperating with multiple national agencies that are active in the field of cybersecurity; sharing information on threats and incidents, and ensuring that FSPs have appropriately skilled human resources to deal with cybersecurity threats.

REFERENCE	RECOMMENDATION
O-1	Where an FSP suffers a failure in cybersecurity that leads to a data breach, or in the case of fraud being reported to supervisory authorities, those authorities should review the associated cyber threat and, if appropriate, warn other regulated entities of the attack.
O-2	The creation of a national cyber-awareness and warning body should be considered; if the supervisory body feels there is insufficient capacity for this, then it should consider identifying regional or international partners to establish such a service.
O-3	Set up an industry-wide Cybersecurity Operations Centre (CSOC) and Computer Emergency Response Team (CERT).
O-4	Facilitate cooperation between the national CSOC/CERT and regional/international CSOC/CERT that is in place.

3.5 FINANCIAL SERVICE PROVIDERS

The requirements set out in this section specifically apply to the activities expected of FSPs with a specific financial inclusion element. They are also intended to assist regulatory authorities in their supervision of service providers' activities in the fulfilment of their requirements.

3.5.1 PRINCIPLE III: THE CUSTOMER

Understanding customers' financial service capacities; identifying them; keeping their data private, and ensuring you know who they are when they return.

REFERENCE	RECOMMENDATION
C-1	**Financial Service Capacity** FSPs should have a program of support and education in place for customers with limited digital and/or financial literacy. The program should include relevant aspects of cybersecurity risks and associated steps customers can take to mitigate them.
C-2	**Proportionate, Risk-Based KYC and Due Diligence** It is vitally important that every customer of an FSP is subject to a robust identification and verification process during registration, making appropriate use of technological innovations such as analysis of a customer's digital footprint and shared or utility-based KYC services. This does not mean that every customer must present robust evidence of their identity. Instead a proportionate approach to KYC should be adopted: every customer must present whatever identity documentation they have. This should then be subject to verification, and their degree of access to financial services should be built on the output of that process, in a model that follows the FATF Recommendations. This way, a potential customer with a digital identity, issued by a government and subject to robust biometric authentication, who can also provide a passport and evidence of their residential address, would typically be offered the full range of financial services (subject to further checks on a case-by-case basis, such as determining credit worthiness). In contrast, a customer who is only able to provide a single paper-based identity document, such as a voter's card, and is unable to provide any additional documentation, will be offered only basic access to a transactional account, with strict balance and transaction limits. It is assumed that there would be a gradation of access between these two extremes, possibly consisting of three to five levels. In all cases, these should be defined in accordance with the requirements set out in national regulation, or in agreement with the regulatory authorities (if this is not otherwise defined).
C-3	It should be possible for customers to "upgrade" the level of service they are able to access, by providing additional identity documentation to the FSP.
C-4	Consideration should also be given to providing service to customers who are not able to produce any form of identity documentation, as long as an existing customer of the financial service provider presents an attestation of their identity. Naturally this must be subject to strict provisos: > It must take place only in agreement with, and under the supervision of, the appropriate authorities; > If the attesting customer becomes subject to investigation for any reason (identity comes under question; links to fraud, or money laundering or the funding of terrorism), then the attested customer's account should be immediately suspended.

REFERENCE	RECOMMENDATION
C-5	Once a decision has been made to grant service to a customer, a customer 'registration account' should be created. This will effectively be a digital identity that is used to access services. It is distinct from financial service accounts and is used to facilitate management of the customer relationship rather than the management of the services provided to the customer. The primary purpose of this is to ensure that all of a customer's relationships with an FSP are properly managed. This is so a customer-focused approach is adopted, rather than a product-focused approach, supporting the FSP's AML and transaction monitoring activities. This registration account should be identified by a customer identity, issued to a customer as a customer number or another identifying token. The use of a customer's mobile phone number is acceptable, though this should be backed with procedures to manage the change of mobile phone numbers over time. Controls should also be put in place given that a mobile phone number is subject to attacks, such as SIM Swap.
C-6	**Authentication** Whenever initiating a transaction or accessing private data (such as their account or transaction details), customers should be required to authenticate themselves using the tools provided by the FSP. Single-factor authentication might be sufficient for lower value transactions or simple account viewing, but multiple factors (including biometrics) should be considered for account changes, initiating larger transactions, or when overall volume over a longer period of time has reached a defined threshold.
C-7	**Data Privacy and Protection** Customer data, such as that presented during onboarding and that generated during the lifetime of the relationship with the FSP (including transaction data) must be soundly protected. It must be stored only in encrypted form, and only ever disclosed to the customer or to properly authorized members of the FSP's staff. Selections of cryptographic algorithms, key lengths, key management tools etc. should only be made on the advice of cybersecurity experts.
C-8	Over the counter (OTC) transactions should be allowed if a country's specific context necessitates it. However, this must be done in a carefully planned manner, such that every party to a transaction is properly identified. This includes the initiating customer, the initiating agent, the receiving agent and the receiving customer. A situation in which only agents are linked to a transaction, and customers remain anonymous, is not acceptable.
C-9	If the limitations of financial literacy mean that a customer is not yet ready to conduct their transactions themselves, and would benefit from assistance (sometimes – though not always – the reason for the use of OTC services), then they should be offered such services; but in a manner in accordance with the previous recommendation.
C-10	**Customer Liability** Customer liabilities should be defined by both the capacities of customers and the feasibility of their influence over the reliability and security of the service. During interviews conducted, some stakeholders observed that a number of FSPs have a customer agreement that sees customers liable for any losses in the customer access domain (see Figure 1). The unfortunate result is that there has been little or no investment in better cybersecurity in that domain, even though customers have no influence over, for example, the security of a mobile network. This approach is not acceptable or sustainable, as it affects customer confidence in the FSP, and, more broadly, the whole financial sector. Customers may not be aware of this liability, and this reinforces the need to have robust consumer protection mechanisms in place. One remedy would be a liability shift, in a manner similar to that seen in the European Union's PSD2 initiative. This would mean that any loss is automatically assumed to be the FSP's liability until proved otherwise and should be refunded to the customer immediately. However, if a subsequent investigation reveals it is in fact the customer's liability, the refund should be reversed. In some cases, this might necessitate a reserve of funds dedicated to refunds – but in return for this, cases should be resolved quickly, ideally within three business days.
C-11	**Digital Literacy** It is incumbent upon customers to be vigilant and ensure that others cannot gain access to their account and carry out unauthorized transactions. They should not, under any circumstances, divulge their PIN or password to anyone else, no matter how much they trust them. If they use a smartphone, they should be required to install security updates as soon as they become available. This message should be communicated clearly – and emphasized – to the customer during registration.

3.5.2 PRINCIPLE IV: DELIVERING THE SERVICE

Understanding the service delivery channels and infrastructure that interface FSPs and their customers, and ensuring that information remains private and transaction integrity is maintained

REFERENCE	RECOMMENDATION
S-1	FSPs should make best efforts to ensure that end-to-end security is in place between the customer and their own internal systems. FSPs should refer to both national and international cybersecurity frameworks and standards. The security of external systems and networks should not be relied upon. These are rarely designed and developed with financial-service grade security in mind. For example, the security of mobile phone networks was designed to: > Ensure that mobile operator revenue was protected from unauthorized access; > Keep mobile phone conversations and data private. The cybersecurity requirement of a financial service is significantly higher. It is therefore incumbent on the FSP to ensure the security, privacy and integrity of their service themselves.
S-2	As was highlighted in Section 2, the use of USSD for the delivery of financial services presents major security vulnerabilities: > There is no security from the customer's handset right through to a mobile operator's back office systems, allowing hackers to eavesdrop on account details and PINs, potentially leading to loss of customer funds; > A cyber-attacker can push a USSD session to the customer in a way that looks like the FSP is contacting them. They can use this to ask the customer to change their PIN, which can then be captured, leading to account hijacking and loss of funds. Much the same concern applies to the use of SMS, which should not be used for one-time PINs (OTPs) because they can be intercepted by cyber-attackers. The sole exception is the use of SIM Toolkit Apps that do their own encryption of SMS, but only where that encryption has been independently reviewed. The recommendation is not that USSD and SMS should be abandoned, though that would be preferable. However, in the light of the highlighted vulnerabilities, the recommendation is first, that where USSD/SMS are used, detailed, active transaction monitoring is put in place in the FSP's central systems to identify and stop fraudulent transactions. Second, a strategy should be put in place to manage migration away from these exposed services. For regulatory authorities, the recommendation is that where a service relies on USSD or unencrypted SMS for delivery, the terms of service imposed on customers should not be such that they are liable for fraud that occurs in the customer service domain.
S-3	As smartphone penetration increases, FSPs should consider the provision of a suitably-secured app for customers to access their services. Access to the app should be secured using a PIN or a biometric (where available), and the developers of the app should include technical defenses against cyber-attack. For example: > The app should be encrypted, in order to ensure that an attacker cannot reverse-engineer the app to extract data and keys. > Any cryptographic keys (for example, for use in end-to-end encryption) should be broken up and distributed (hidden) around the app, and only reconstructed when needed. > The purpose of all data used in the app should be obfuscated, using suitable development tools. > The app should be developed to operate in a smartphone's sandbox where available. This is a technological sandbox for cryptographic protection of live services and is different from a regulatory sandbox. > Where such a sandbox is available, the app should make use of a mobile phone's Secure Execution Environment (SEE). This might be the phone's SIM, or a dedicated SEE in a smartphone. > A requirement should be placed on the customer by the FSP to ensure that their smartphone operating system software is always up to date; the app should not launch if the operating system does not offer the level of security it requires. Further, the app should never launch if the mobile phone has been 'jailbroken'. The CIS-20 Controls are a useful resource in this area.
S-4	Where an FSP is not also a mobile network operator (MNO), that FSP should foster a good relationship with all of the MNOs in their country, in order to restrict and monitor SIM swaps. Swaps should be disabled for SIMs that belong to prominent individuals or those that are part of the FSP service (SIMs of agents and employees). This is unless FSP senior management approval is obtained, as these individuals' mobile phone numbers are often made available as part of their normal activities, and thus are vulnerable to cyber-attacks based on SIM swaps. Multiple SIM swaps against a single account within a short period should be disabled.
S-5	Where a national Cybersecurity Operations Centre (CSOC) and Computer Emergency Response Team (CERT) are in place, the FSP is expected to contribute to and participate in their activities. This is in addition to the base requirement of compliance with national and international cybersecurity standards issued by the respective regulatory authorities.

3.5.3 PRINCIPLE V: MANAGING INTERNAL RISKS

Ensuring that the integrity of an FSP's service is preserved through internal controls and processes, and that staff are appropriately managed, etc.

REFERENCE	RECOMMENDATION
I-1	The cybersecurity of a financial service can be undermined by malicious staff. FSPs should therefore conduct appropriate country-specific background checks when recruiting staff in sensitive positions, including: > Properly identifying staff through the same identification and verification processes used when onboarding customers; > Requesting and referring to appropriate police or criminal records to avoid the employment of known fraudsters or cyber criminals; > Staff should be subject to credit reference checks where these are available, in order to identify those with excessive debt who might therefore be vulnerable to bribery. These background checks should apply to all staff in senior positions, including senior staff, any staff at any grade involved in accessing or configuring the DFS platform, or financial activities either with banking partners or customer accounts, and those in customer-facing roles who would be in a position to identify accounts for targeting by cyber-attackers. Further, these background checks should be repeated on a periodic basis.
I-2	Employers should apply robust risk mitigation with regard to access to IT systems for its critical employees in sensitive positions (defined in I-1). This access includes authorization rules, access procedures, restricted use of unauthorized electronic devices in certain office premises including personal laptops, mobile phones, tablets etc.
I-3	It is essential that all staff interaction with the FSP's platform is logged, and that those logs are authoritative. This implies that all staff access to IT systems is subject to strong authentication, such as two-factor authentication; for example, a username and password, together with a QR code that is scanned using their mobile phone. SMS for OTPs is not recommended. Staff in sensitive positions (who should preferably not have their mobile phones with them: see I-2) should be issued with a key fob that generates temporary passcodes, and its use should be enforced for all logins. For reasons of auditability, all activities carried out by all staff should be logged/recorded, whether or not these activities are successful. The resulting audit trail should not be editable, and access to these logs should be restricted. These logs should be subject to periodic audit.
I-4	All operational and management functions that the FSP's service platform provides should be subject to role-based access, so that, for example, if their role does not involve the movement of funds or the examination of customer accounts, they should be barred from accessing such functionality.
I-5	The role-based access described in I-4 should be used to implement maker/checker controls (sometimes referred to as "four eyes" controls) particularly with regard to funds transfer and other sensitive transactions. This kind of access allows one staff member to "make", or create the details of, a funds transfer transaction, and another to "check/approve" the transaction. No single individual should ever be granted both roles. These controls should be reinforced by recording logins and by making investigation and auditing tools available to senior management and external authorities.
I-6	An important element of business continuity planning is the definition and operation of detailed business processes. It is recommended that this is undertaken as they improve a business's operations, and mitigate the issues of staff error, over-reliance on key staff, and lack of knowledge-sharing amongst staff. A business process management system (BPMS) should be adopted, which when properly implemented, can manage the smooth day-to-day operations of a financial service provider and reduce reliance on critical personnel.
I-7	The FSP should identify a set of control points, which can be incorporated into the business processes in order to enhance the basic cybersecurity of the service. These might include: > The specification of a transaction value beyond which additional authorization is required; > A particular person whose authenticated presence is required to carry out a function; > Restrictions on when a specific function may be performed (e.g. during office hours).
I-8	Regular reconciliation of transactions across customer accounts and the FSP's own bank accounts is an essential activity, crucial to maintaining the integrity of a financial service. In this context, reconciliation has two main functions: > Ensure all customer balances are secure. > Provide an early indicator of potential fraud perpetrated by breaching cybersecurity controls and controls for the creation of value, either internal or external.

REFERENCE	RECOMMENDATION
I-9	Cryptography is crucial for the operation of DFS and for data protection and privacy. It helps ensure the confidentiality and integrity of communications among: > An FSP and its customers, suppliers, and other external parties; > An FSP's staff and inter-process systems; > An FSP's inter-process systems (to avoid replay attacks). All data must be encrypted in transit and at rest. With regard to data at rest, the intent is that all customer data, personal and transaction, should be encrypted before storing so that anyone who can obtain access to the system cannot see the data. This underpins role-based access, so only someone who has authenticated themselves as having the right credentials can see the data in clear. All transactions and staff activities must be logged for future auditing or investigations.
I-10	Physical security is the first step in ensuring cybersecurity and limits the opportunity for the subversion of cyber-controls. Well-managed FSPs focus equally on physical and cybersecurity. At a minimum, physical security involves the following: > One, strictly controlled entrance to an FSP's premises. > Ensuring that other entrances are secured, and fire exits have alarms. > Ensuring that all rooms are secured with biometric locks, and that they require both "touch in" and "touch out" to avoid tailgating. This also means ensuring that access to all rooms is restricted based on job function (role). > Enabling video surveillance and 24-hour recording of all areas. This is essential for deterring and detecting crimes. It must be emphaised that cameras should not face screens that may display sensitive information. - As a minimum, these recordings should be available for a period of one month; however, a year is preferable. - It should be possible for authorized investigators to download and archive recordings for the purposes of fraud investigation.
I-11	It is recommended that an FSP should implement active, automated transaction monitoring and alert functions. In addition to the detection and prevention of fraud, active, automated transaction monitoring can contribute to an FSP's anti-money laundering/combatting the financing of terrorism (AML/CFT) compliance obligations.
I-12	A Fraud Officer should be appointed. The role is to monitor transactions, submit suspicious transaction reports to the regulatory authorities and support further investigations in cooperation with those authorities.
I-13	The FSP should implement modern transaction investigation tools with "follow the money" functionality, which can be leveraged for rapid, effective investigation of potential crimes.
I-14	Larger organizations with a market share of above 10% should appoint a Chief Information Security Officer (CISO), responsible for developing and implementing an information security program.
I-15	FSPs should provide all operational and development staff with cybersecurity skills and development training.

3.5.4 PRINCIPLE VI: UNDERSTANDING YOUR PARTNERS

Ensuring that partners are engaged through appropriate processes without significantly increasing the risks to either customers or the service.

REFERENCE	RECOMMENDATION
P-1	There are additional physical security measures that apply to visitors to an FSP's premises, beyond those that apply to members of staff: > All visitors must be identified (with reference to an identity card or similar) and logged. > Visitors must not be permitted to take any electronic equipment into operational or sensitive areas. > Visitors can be permitted to take mobile phones and laptops into non-operational areas only. However, the serial numbers of laptops should be logged, and FSP staff should use this information to verify that visitors leave with the same equipment they brought, to avoid the switching of laptops. > Visitors must be accompanied at all times by a staff member who is responsible for their conduct. > Appointed staff members must remain aware of visitors' activity at all times. In particular, visitors must not be allowed to: - Wander around the building unaccompanied; - Insert USB drives or similar devices into company laptops, printers, etc.
P-2	A process should be developed and incorporated into the operation of an FSP for the onboarding of suppliers and the subsequent management of the relationship. The aims of this process should be: > To enable the FSP's management team to develop an understanding of the risks that might arise from the supplier's internal activities; > To understand the supplier's relationships with third parties which might, for example, make them subject to coercion to provide improper access to the FSP's operational or customer information; > To identify relationships with key staff within the FSP, which might have the potential to lead to collusion and fraud. As well as being a vital component of supplier onboarding, this vetting process should also be a regular part of annual due diligence, applied to all supplier relationships.
P-3	When establishing a relationship with a supplier, an FSP should take measures to satisfy itself that there is a common understanding of the division of responsibilities and liabilities in case of fraud.

3.5.5 PRINCIPLE VII: THE LONGER TERM

Ensuring that an FSP service maintains its service security as new threats emerge; that regulatory authorities are informed of both existing risks and the plans to address these; ensuring that audits are carried out regularly, and all reporting requirements are met, etc.

REFERENCE	RECOMMENDATION
L-1	The management and board of an FSP should adopt and implement international best practices in cybersecurity. Used appropriately, this will make compliance with emerging national regulatory and supervisory requirements more straightforward.
L-2	In order to assist in the continuing development of cyber-readiness, every FSP should adopt an international best practice cybersecurity assessment tool and integrate the use of that tool into its core business processes, with the aim of driving up the level of cybersecurity readiness over time.
L-3	The IT Director/Manager of every FSP should adopt and implement international best practice technical cybersecurity controls to enhance the technical cybersecurity of their systems and services.
L-4	Building on L-1 to L-3, an FSP should develop a capability to identify and address new cybersecurity threats as they emerge.
L-5	FSPs should assess their level of cyber-readiness, determined by using the FFIEC Cybersecurity Assessment Tool. This review process should be conducted at least annually, and regulatory and supervisory authorities should be informed of the results.
L-6	Where an FSP's level of cyber-readiness falls short of expected standards, the FSP should inform the regulatory and supervisory authorities of their plans to address the gap, with particular reference to the FSSCC CSP.
L-7	Any failing in cybersecurity that leads to a data breach or fraud should be reported to the relevant authorities immediately.

3.6 RISK SUMMARY

The following table lists the principal actors; describes their role in the delivery of financial services; highlights the key risks to which they are exposed, and sets out the high-level impacts or implications of those risks being realized.

TABLE 1: DIGITAL PAYMENTS AND FINANCIAL SERVICES: ACTORS, ROLES, RISKS AND IMPACTS

ACTOR	DESCRIPTION	KEY RISKS	IMPACTS
Customer	The customer may or may not use a digital device such as a mobile phone to access services.	> Low financial, digital and/or cyber literacy > Social engineering, enabling fraud against the customer > Mistakes	> Loss of funds > Loss of personal data
Customer's digital device	The customer might use a device to access the service, or use an OTC service.	> Hacking > Eavesdropping	Loss of customer's funds
Financial service app	> An app that the customer might use in his/her interactions with the service, including transactions. > Might be provided by the FSP or by a FinTech.	> Hacking > Interception/Eavesdropping	> Loss of funds > Loss of personal data
Merchant	Wants to sell to the customer and is willing to accept payment via a digital device.	> Low digital literacy > Inadequate training	Reduced service availability; reduced confidence.
Merchant's digital device	The merchant's digital device might be a mobile phone.	> Hacking > Eavesdropping	Loss of customer's or merchant's funds
Agent	> Provides services to the customer. Such services might include customer registration, cash in/cash out (CICO) services, or a full range of financial services via an over the counter (OTC) model. > In some circumstances, a merchant might also take on the role of an agent.	> Low digital literacy > Inadequate training > Unreliable staff	> Reduced service availability and reliability > Fraud against customer > Fraud against agent (by staff)
Agent's digital device	Used to provide service to customers and to manage service provision. This may be a mobile phone.	> Hacking > Eavesdropping	Reduced service availability; reduced confidence
Digital identity service	Used to establish the identity of the customer during onboarding. In some countries, this service also offers authentication services for use during financial transactions, but generally, the authentication function is performed by the FSP.	> Weak registration > Weak authentication during onboarding > Consequent link to incorrect credit bureau records, enabling fraud	> Unreliable customer identification > Untraceable fraud (or other crimes) > Inappropriate lending by FSP
Regulatory authorities	Define the regulatory and supervisory environment in which services may be offered, and identify the personnel who must ensure that those expectations are met.	Lack of familiarity with technical risks (fintech, digital financial services, mobile networks)	> Inappropriate distribution of liability > Diminished customer protection > Loss of trust in services
Standards & standard setting bodies	Define how different partners in service delivery may interoperate, and set out the expectations placed on the quality of that service.	Inappropriate standards resulting in insecure, inappropriate or unreliable services	> Diminished reliability > Loss of trust in services

Communications network	This might be a mobile phone or Wi-Fi network, or a similar setup.	> Eavesdropping > Interception > Redirection > Spoofing > Phishing	> Loss of customer, agent or merchant funds > Customer account hijacking > Loss of customer or merchant data
A network operator's systems	These are made up of: > The operational network base stations, located around the country, which provide local access to a backbone that interconnects the entire network; > A central network operations center, which is itself made of network operations systems (these provide the communications service) and the network operator's internal IT systems, which administer the operational systems and provide back office support.	> Phishing > Spoofing > Eavesdropping > Interception	> Loss of customer, agent or merchant funds > Customer, agent or merchant account hijacking > Loss of customer, agent or merchant data
The FSP's systems	Used to provide financial services to customers, potentially including the underserved.	> Inadequate internal controls > Internal malicious actors > Lack of business continuity planning > Poor fraud investigation tools	> Data breaches; loss of service data, both financial and non-financial > Unreliable service > Loss of reputation > Inability to combat financial crime
Banks	> Holds the customers' funds. > Note that the bank and the FSP may be the same organization, though it is not unusual for them to be separate.	> Failure to conduct adequate reconciliation, giving rise to additional fraud risk > Funds concentration; potential bank failure leading to loss of customers' funds > Internal malicious actors	Systemic failure
Other external service providers	Support the FSP in the delivery of their service. For example, this might include technical partners, such as server/ hosting services, or logistical partners responsible for managing networks of agents.	> Disruption of services > Hacking > Spoofing	Loss of reputation and, therefore, trust
Credit Bureaus	Support the FSP in the delivery of their services	Credit record errors	Financial risk to FSP from inappropriate lending

3.7 OF SPECIAL NOTE: USSD, SMS AND CYBER RISK

USSD is widely used in the delivery of financial services to the underserved, and it is recognized that this is often necessary for a range of reasons that are beyond the scope of this document. However, USSD has major security vulnerabilities:

> There is no security from the customer's handset right through to a mobile operator's back office systems, allowing hackers to eavesdrop on account details and PINs, potentially leading to loss of customer funds;
> A cyber-attacker can push a USSD session to the customer in a way that looks like the FSP is contacting them. They can use this to ask the customer to change their PIN, which can then be captured, leading to account hijacking and loss of funds.

Much the same concern applies to the use of SMS, which should not be used for one-time PINs (OTPs) because they can be intercepted by cyber-attackers; the sole exception being the use of SIM Toolkit Apps that do their own encryption of SMS.

Until the technology to fully secure private data is available to customers and FSPs, and transactions become more affordable, there must be careful and sustained monitoring of transactions by FSPs. Through this, FSPs must prioritize the identification of anomalies and appropriate intervention. Approaches to mitigating these risks are included in Section 3.5.2 of this document.

4 BACKGROUND: EXISTING FRAMEWORKS

4.1 INTRODUCTION

Regulators and financial sector supervisors will be well aware that there is already a wide range of cybersecurity frameworks in existence: some generalized, some aimed at protecting a nation's critical infrastructure, some formalized in national or international standards, and some specific to a particular sector of the economy, including the financial sector.

It is not the purpose of this document to offer an alternative to these frameworks. Instead, as was highlighted in Section 1.2.1, this Guide is intended to supplement the frameworks, by highlighting and emphasizing the risks that arise from adopting practices and technologies that have become common practice when a service is focused on the priorities of financial inclusion.

In the pursuit of this objective, it is important to highlight the landscape of cybersecurity frameworks against which this document should be viewed. Based on interviews with a wide range of stakeholders, a consensus view of the broad set of supranational cybersecurity frameworks relevant to regulatory authorities and FSPs is presented in this section.

In addition, the regulatory authorities in a number of countries have taken the initiative in developing national cybersecurity frameworks that relate to the entire financial sector in their country, without specific emphasis on financial inclusion. Some of these are also summarized in this section.

4.2 SUPRANATIONAL FRAMEWORKS

With regard to supranational cybersecurity frameworks, stakeholders repeatedly highlighted the importance and relevance of the frameworks in the following subsections.

4.2.1 NIST

The USA's National Institute of Standards and Technology (NIST) published their first cybersecurity framework in 2014. This is an influential framework, which underpins many of the other cybersecurity frameworks published by other bodies around the world. NIST published[1] the updated version (1.1) of their Framework for Improving Critical Infrastructure Cybersecurity on 16 April, 2018.

Since the publication of version 1.0 in February 2014, the NIST Framework has become the default starting position for many organizations wishing to address issues of cybersecurity. Notwithstanding its foundational and influential status, the NIST Framework is very general; it is aimed at improving critical infrastructure cybersecurity across all sectors of an economy and cannot be used directly by FSPs without being made more specific. The following sections document some approaches to this.

4.2.2 FFIEC

The Federal Financial Institutions Examination Council (FFIEC) built on the NIST cybersecurity framework and developed a cybersecurity assessment tool, specifically aimed at the financial sector, allowing institutions to assess their own cybersecurity readiness. The tool was published[2] in May 2017, in response to the increasing volume and sophistication of cyber threats. The development of the tool was shaped by the NIST cybersecurity framework.

The aim of the tool is to help financial institutions identify their risks and determine their cybersecurity preparedness. Further, it is structured to provide those institutions with a repeatable, standardized process to measure the development their cybersecurity preparedness over time.

The FFIEC approach is widely admired and adopted, and has been influential on a range of initiatives, including the European Central Bank's CROE, which is summarized later in this section.

4.2.3 CPMI-IOSCO

The Committee on Payments and Market Infrastructures (CPMI) at the Bank for International Settlements (BIS), in collaboration with the Board of the International Organization of Securities Commissions (IOSCO), developed the document[3] for "Guidance on cyber resilience for financial market infrastructures" (Cyber Guidance) in June 2016. The Guidance applies to a complete national Financial Market Infrastructure (FMI), defined as "critically important institutions responsible for providing clearing, settlement and recording of monetary and other financial transactions".

The Guidance is based on principles rather than the setting of specific standards, in recognition of the dynamic nature of cybersecurity and the threats posed to systems and services. An important aspect to emphasize is that it is intended to supplement - and not replace - IT-focused cybersecurity guidance. Conversely, it emphasizes that cybersecurity is more than just IT.

[1] https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

[2] https://www.ffiec.gov/cyberassessmenttool.htm

[3] https://www.bis.org/cpmi/publ/d146.htm

Thus, it suggests that an organization needs both a principles-based framework and an IT cybersecurity framework, working in concert to ensure the security of a financial institution against cyber threats.

4.2.4 ECB CROE

The European Central Bank (ECB) published[4] their "Cyber resilience oversight expectations for financial market infrastructures"(CROE) in December 2018. In developing the CROE, the ECB considered a range of international guidance documents and frameworks - notably CPMI–IOSCO, NIST and FFIEC. The purpose of the CROE is to assist supervisory/oversight authorities in their task of reviewing compliance with the CPMI-IOSCO guidance as part of their oversight function; in essence, it is akin to an assessment framework.

The ECB CROE is an important document that provides an extremely useful bridge from the requirements set out in CPMI-IOSOC, NIST and elsewhere, to the processes that financial institutions must have in place to achieve compliance. It does so in a manner that is relevant to the state of evolution of the institution, and the environment in which it operates.

However, it is not designed as or intended to be a formal cybersecurity framework. This reflects its primary role as a tool for use by supervisory/oversight authorities. The CROE assists authorities in assessing the cybersecurity frameworks used by organizations whose oversight they are responsible for. Essentially, it helps develop the capacity of authorities to assess the cybersecurity of the institutions they oversee, an essential element of the cybersecurity jigsaw.

4.2.5 FSSCC CYBERSECURITY PROFILE

The USA's Financial Services Sector Coordinating Council (FSSCC) was established in 2002 by representatives of the financial sector in the United States. It works collaboratively with US government agencies to protect critical infrastructure in the US financial sector from cyber and physical incidents. FSSCC released version 1[5] of their Cybersecurity Profile (CSP) on 25 October, 2018. The framework is based heavily on the NIST Framework and CPMI-IOSCO Guidance. Assessment questions are based on relevant supervisory guidance and frameworks, and mappings to ISO/IEC 27001/2 controls.

The development of the FSSCC CSP arose, at least in part, as a response to the piecemeal approach of existing regulations and frameworks. The majority of these are derived from the NIST Framework's Functions, Categories and Subcategories, but they either provide only partial coverage, or take such an arbitrary approach that the utility is compromised.

The FSSCC set out to avoid this by taking a comprehensive, pan-industry direction. Despite this, it should be remembered that its genesis is in the United States financial sector, which could be expected to have a different capacity to financial institutions (particularly smaller ones) and supervisory agencies in emerging economies.

4.2.6 CENTER FOR INTERNET SECURITY – THE CIS 20 CONTROLS

Reflecting the CPMI-IOSCO recommendation that an organization needs both a principles-based framework and an IT cybersecurity framework, a number of stakeholders highlighted the value of the "CIS 20" as a leading example of the latter.

The Center for Internet Security (CIS) is a non-profit entity based in the US. In their words, they "harnesses the power of a global IT community to safeguard private and public organizations against cyber threats". This is of particular interest because of its "bottom-up" approach to cybersecurity. Rather than a set of principles mandated by regulators, supervisory authorities or consortiums of leading banks, the CIS approach relies on the donated expertise of those dealing with cybersecurity in an ongoing, active capacity. It is therefore a useful complement to other approaches.

Of particular relevance to this Guide is what has become known as the "CIS 20 Controls". This refers to a set of 20 cybersecurity controls and guidelines which, when taken together, address the cybersecurity needs of the majority of organizations, including those in the financial sector. The current version at the time of writing is 7.1[6], released on 1 April, 2019. A separate publication documenting the alignment with the NIST Cybersecurity Framework is available from CIS, though it has not been reviewed in the preparation of this Guide.

[4] https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

[5] https://www.ffiec.gov/cyberassessmenttool.htm

[6] https://www.cisecurity.org/controls/

4.3 NATIONAL FRAMEWORKS

4.3.1 INTRODUCTION

When considering national, regulatory authority-led cybersecurity frameworks, stakeholder interviews identified three in particular as reflecting a growing sophistication in national agency responses to increasing concerns in cybersecurity in the financial sector:

> Armenia's "CyberSecurity Maturity Assessment Tool";

> Ghana's "Cyber & Information Security Directive";

> Nigeria's "Risk-Based Cybersecurity Framework".

Coincidentally, all three of these were published in 2018, reflecting both the growing urgency felt by regulatory authorities in emerging economies, and their willingness to engage actively with the financial sector to address the issues.

The nature of these frameworks varies considerably, as has already been seen with the supranational frameworks. This is in part related to the priorities of each individual national authority. The Nigerian and Ghanaian frameworks provide a clear specification of what is expected from financial institutions (and in this, they are akin to the FSSCC CSP), whilst the Armenian framework focuses on how – through detailed individual activities – a financial institution can achieve the necessary degree of cybersecurity (akin to the FFIEC framework).

4.3.2 ARMENIA

During the period 2007 to 2010, in order to improve IT and information security governance, processes and procedures, the Central Bank of Armenia (CBA) adopted the ISO 27001 standard for information security management systems, leading to certification in 2012. During this period the CBA defined cybersecurity regulations for regulated financial institutions, using a simplified set of requirements based on ISO 27001. In 2013, the CBA extended this to include a requirement that all financial institutions be ISO 27001-certified by 2015, with certification being carried out by a recognized international certification body.

More recently, the CBA's Internal Audit department has developed a cybersecurity self-assessment tool, initially for use internally, and subsequently for use by regulated financial institutions. This tool is intended to assist them (and supervisory authorities) in developing an understanding of their inherent risk profile and cybersecurity maturity.

This is a valuable instrument which, through its automation of the FFIEC framework, offers a significant step forward in the usability of that framework. Its use by financial institutions should therefore be promoted. However, how it might be used by supervisory/oversight authorities has not been determined.

4.3.3 GHANA

In October 2018, the Bank of Ghana published[7] the "Cyber & Information Security Directive", which is aimed at the financial services industry in Ghana, and which:

> "…provides a framework for establishing Cyber and Information Security protocols and procedures for; routine and emergency scenarios, delegation of responsibilities, inter- and intra-company communication and cooperation, coordination with government authorities, establishment of reporting mechanisms, physical security measures for IT Datacentres and Control Rooms, and assurance of data and network security"

With regard to international regulations and standards, the document makes particular reference to ISO27001[8] (information security), ISO27032[9] (guidelines for cybersecurity), PCI-DSS (security of card transactions) and the cybersecurity framework and guidelines[10] published by the US-based NIST, whose expertise in this area is widely acknowledged.

The Directive is broken down into multiple parts, setting out requirements for systems and services, and defining the responsibilities of the principal actors. These requirements cover a broad range and each contains a great deal of highly relevant, useful advice.

The Directive represents a significant step forward in ensuring the cybersecurity of FSPs in Ghana, with regard to both the approaches recommended and the breadth of its vision.

4.3.4 NIGERIA

Recognizing both the rapid growth in transactions across Nigeria financial sector (including the emergent fintech sector), and the increasing prevalence of cyberattacks on financial institutions, the Central Bank of Nigeria (CBN) issued their Risk-Based Cybersecurity Framework[11], applicable to all deposit-taking banks and payment service providers, on 10 October, 2018, and the date for full compliance was set for 1 January, 2019. This followed an earlier draft issued in June 2018, which was revised following industry consultation.

[7] https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

[8] A specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

[9] Background: ISO 27032 is not a standard that you can certify; this is one of the most important differences with respect to ISO 27001, which is aimed at the certification of an ISMS. The principal objective of ISO 27032 is to provide a guide for cybersecurity through specific recommendations. So, the focus of ISO 27001 is an organization and its ISMS, while ISO 27032 focuses on cyberspace and is a framework for collaboration.

[10] https://www.nist.gov/cyberframework

[11] https://www.cbn.gov.ng/out/2018/bsd/risk%20based%20cybersecurity%20framework%20final.pdf

CBN's Framework takes a different approach to that instituted by Ghana: that of establishing broad guidelines, with reference to international experts/ authorities such as NIST and PCI-DSS, for detailed guidance.

Some important aspects of the CBN Framework are:

- The Chief Information Security Officer (CISO) of a financial institution must report directly to the CEO. Under no circumstances should the CISO report to the Head of IT. Although it is an accepted industry best practice, the significance of this aspect cannot be over-emphasized.
- As part of a cybersecurity resilience self-assessment, the Framework includes a requirement for institutions to determine both their current cybersecurity profile, and the desired/target state, together with a detailed roadmap to achieve the target within a stipulated time frame.
- Minimum requirements for establishing and developing cybersecurity operational resilience are set, including requirements to understand an institution's operational, technology and business environments; to continually enhance cybersecurity resilience, and to develop a cyber-threat intelligence capability.
- There is a requirement placed on all institutions to report all cyber-attacks to CBN, whether or not they are successful, within 24 hours of their occurrence. It is unclear what the scope of this is. Presumably, it does not include the general 'probing' attacks that occur continuously on the Internet, as attackers probe systems to detect obvious electronic doors that have been left open[12]. It would be useful to attain some clarity on the threshold before a report is required or generated.

The CBN Framework, as might be expected, is an important and valuable resource, establishing clear principles and providing a great deal of guidance to FSPs on how they might ensure compliance.

[12] Any device connected to the Internet can expect to see its Internet connection probed many times in a day, relying on a firewall to protect it.

GLOSSARY

TERM	DESCRIPTION
AFI	Alliance for Financial Inclusion
AML	Anti-Money Laundering
API	Application Programming Interface
BIS	Bank for International Settlements
BoG	Bank of Ghana
BPMS	Business Process Management System
CA	Competent Authority
CAF	Cyber Assessment Framework
CBA	Central Bank of Armenia
CBN	Central Bank of Nigeria
CERT	Computer Emergency Response Team
CFT	Combatting the Financing of Terrorism
CICO	Cash In, Cash Out
CII	Critical Information Infrastructure
CIS	Center for Internet Security
CISO	Chief Information Security Risk Officer
CNI	Critical National Infrastructure
CPMI	Committee on Payments and Market Infrastructures
CROE	Cyber Resilience Oversight Expectations
CSA	Cyber Security Agency
CSIRT	Computer Security Incident Response Team
CSOC	Cybersecurity Operations Centre
CSP	Cybersecurity Profile
DFS	Digital Financial Services
DFS WG	Digital Financial Services (DFS) Working Group
DGSSI	General Directorate of Information Security Systems
ENISA	EU Network and Information Security Agency
EU	European Union
FATF	Financial Action Task Force
FFIEC	Federal Financial Institutions Examination Council
FI	Financial Inclusion or Financial Institution, depending on context
Fintech	Financial technology products
FinTech	Financial technology company or service provider
FMI	Financial Market Infrastructure
FSP	Financial Service Provider

TERM	DESCRIPTION
FSSCC	Financial Services Sector Coordinating Council
IGP	Indicator of Good Practice
IOSCO	International Organization of Securities Commissions
ISMS	Information Security Management System
MAS	Monetary Authority of Singapore
MFI	Microfinance Institution
MNO	Mobile Network Operator
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
NIS	Network and Information Systems
OES	Operators of Essential Services
OTC	Over the Counter
OTP	One-Time PIN
PEP	Politically Exposed Person
PIN	Personal identification Number
PFMI	Principles for Financial Market Infrastructures
RegTech	Regulatory Technology
RFP	Request for Proposal
SACCO	Savings and Credit Cooperative Organization
SEE	Secure Execution Environment
SME	Small- or Medium-sized Enterprise
SMS	Short Message Service
SOC	Security Operations Centre
STR	Suspicious Transaction Report
SupTech	Supervisory Technology
TRM	Technology Risk Management
USSD	Unstructured Supplementary Service Data

ANNEX A
STAKEHOLDER INTERVIEWS

The following stakeholders were interviewed during the preparation of this document.

NAME	TITLE	ORGANIZATION	ROLE
Komitas Stepanyan	Deputy Head of Internal Audit	Central Bank of Armenia	Regulatory Authority
Daniel Klu, CISO	Chief Information Security Officer	Bank of Ghana	Regulatory Authority
Hakima El Alami	Deputy Director in charge of the Supervision of Systems and Method of Payment, and Financial Inclusion	Bank Al-Maghrib, Morocco	Regulatory Authority
Fadwa Jouali	Head of Fintech and Payment Development	Bank Al-Maghrib, Morocco	Regulatory Authority
Mustapha Hadadi	Organization and Information System Department	Bank Al-Maghrib, Morocco	Regulatory Authority
Stephen Mathew Ambore	Head, Digital Financial Services	Central Bank of Nigeria	Regulatory Authority
Candy Ngula	Deputy Director	Bank of Namibia	Regulatory Authority
Thomas Lammer	Principal Market Infrastructure Expert, Oversight Division	European Central Bank	Regulatory Authority
Klaus Löber	Head of Division, Market Infrastructures and Payments	European Central Bank	Regulatory Authority
Killian Clifford	Director of Policy & Advocacy	GSMA	Industry Body
Munir Bello	Mobile Money Certification Technical Lead	GSMA	Industry Body
Brian Muthiora	Regulatory Director, Mobile Money	GSMA	Industry Body
Juliet Maina	Advocacy and Regulatory Manager, Mobile Money	GSMA	Industry Body
Daniel Schwartz	Director, Global Policy Affairs	Mastercard	Industry Body
Amina Tirana	Lead for Policy, Research and Measurement, Social Impact	Visa	Industry Body
Michael Nunes	Head of Government Advisory	Visa	Industry Body
Frank Adelmann	Financial Sector Expert (Cyber Security)	IMF	International Body
Vijay Mauree	Programme Coordinator, Study Group Dept, TSB	ITU	International Standards Body
David Medine	Senior Advisor	CGAP	International Body
Seán Doyle	Project Lead, Cybersecurity Governance and Policy	World Economic Forum	International Body
Leon Perlman	-	Independent	Industry expert
David Cracknell	-	First Principles	Industry expert
Abbie Barbir	-	FIDO Alliance	Industry expert
Dave Birch	-	Consult Hyperion	Industry expert

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