INTERNATIONAL MONETARY FUND

IMF Country Report No. 22/181

SOUTH AFRICA

FINANCIAL SECTOR ASSESSMENT PROGRAM

June 2022

TECHNICAL NOTE ON CYBERSECURITY RISK SUPERVISION AND OVERSIGHT

This technical note on Cybersecurity Risk Supervision and Oversight was prepared by a staff team of the International Monetary Fund in the context of a joint IMF-World Bank Financial Sector Assessment Program (FSAP). It is based on the information available at the time it was completed in June 2021.

Copies of this report are available to the public from

International Monetary Fund • Publication Services
PO Box 92780 • Washington, D.C. 20090
Telephone: (202) 623-7430 • Fax: (202) 623-7201
E-mail: publications@imf.org Web: http://www.imf.org
Price: $18.00 per printed copy

International Monetary Fund
Washington, D.C.

INTERNATIONAL MONETARY FUND

SOUTH AFRICA

FINANCIAL SECTOR ASSESSMENT PROGRAM

June 2, 2022

TECHNICAL NOTE

CYBERSECURITY RISK SUPERVISION AND OVERSIGHT

Prepared By
Monetary and Capital Markets Department

This Technical Note was prepared in the context of the Financial Sector Assessment Program in South Africa during June 2021 mission led by Jennifer Elliott, IMF and Eva Gutierrez, World Bank and overseen by the Monetary and Capital Markets Department, International Monetary Fund, and the Finance, Competitiveness and Innovation Global Practice, World Bank. It contains technical analysis and detailed information underpinning the FSAP's findings and recommendations. Further information on the FSAP can be found at http://www.imf.org/external/np/fsap/fssa.aspx

CONTENTS

Glossary

BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
BCP	Business Continuity Plan
CABS	Community of African Banking Supervisors
CCP	Central Counterparty
CERES	Central Bank and Regulator Supervisor Forum
CERT	Community Emergency Response Team
CLS	CLS Bank International
CPMI	Committee on Payments and Market Infrastructures
CRS	Cybersecurity Resilience Sub-Committee
CSD	Central Securities Depository
CSP	Critical Service Provider
DDoS	Distributed-Denial-of-Service
DD4BC	Distributed-Denial-of-Service for Bitcoin
FIC	Financial Intelligence Centre
FinStab	Financial Stability Department
FI	Financial Institution
FMI	Financial Market Infrastructure
FSC	Financial Stability Committee
FSCA	Financial Sector Conduct Authority
FS-ISAC	Financial Services Information Sharing and Analysis Center, Inc
FSCF	Financial Sector Contingency Forum
IOSCO	International Organization of Securities Commissions
IT	Information Technology
JSE	Johannesburg Stock Exchange
MI	Market Infrastructure
MISP	Malware Information Sharing Platform
NPS	National Payment System
NPSD	National Payment Systems Department
OSINT	Open-Source Intelligence
OTC	Over the Counter
PRA	Prudential Regulation Authority
PASA	Payments Association of South Africa
PCH	Payment Clearing House
PFMI	Principles for Financial Market Infrastructures
PS	Payment Systems
PSMB	Payment System Management Body
RAM	Risk Assessment Matrix
RTGS	Real-Time Gross Settlement
SABRIC	South African Bank Risk Information Centre

SADC-RTGS	South African Development Community Real-Time Gross Settlement
SAMOS	South African Multiple Option Settlement
SARB	South African Reserve Bank
SIFI	Systemically Important Financial Institutions
SIPI	Systemically Important Payment Systems
SSS	Securities Settlement System
SWIFT	Society for Worldwide Interbank Financial Telecommunication
ZAR	South African Rand

EXECUTIVE SUMMARY

The domestic cyber threat landscape[1] is evolving, posing challenges for risk management. Cybersecurity risk continues to grow both in complexity and severity and is a function of an increasingly open and interconnected cyber and financial ecosystem. The South African financial system has a long history of incorporating technology and as for many financial systems across the globe, digitalization has become a strategic priority. For risk management to keep pace with the dynamic nature of cyber threats and threat agents, systemically important financial institutions (SIFIs) have made substantial investments in cyber resilience programs (e.g., establishing cyber strategies, frameworks, and governance structures). Consistent with many jurisdictions, and partly a result of widespread remote working arrangements implemented in response to the global pandemic, cybersecurity threats to financial stability increased. However, high standards of risk management meant threats did not materialize into significant losses and/or disruptions.

The South African authorities have established a robust institutional framework to strengthen cyber resilience of the financial system. Cybersecurity and cyber resilience are critical for national financial stability within the South African financial sector. The South African cybersecurity framework is well established and based upon four principles: protect, detect, respond, and recover. A formal committee structure involving numerous public and private stakeholders is charged with responsibilities of detection, escalation, coordination and response and recovery. The South African Reserve Bank (SARB) has direct responsibility in terms of financial stability, playing a pivotal role. The Prudential Authority (PA) implements the regulatory framework and supervisory processes to monitor policies, processes and practices related to cybersecurity risk and cyber resilience by regulated entities. SARB's and Financial Sector Conduct Authority's (FSCA) oversight, supervision, and regulation of financial market infrastructures (FMIs) is based on global standards.[2]

Cooperative platforms have been established to effectively detect and manage cyber-attacks on a national level, and thereby supporting financial stability. These platforms facilitate cooperation between authorities, sector-based Computer Emergency Response Teams (CERTs) and public and private businesses. The South African Banking Risk Information Centre (SABRIC) provides an interface between the public and private sectors in relation to information sharing. Financial institutions—particularly SIFI's—have made significant investments in people, processes, and systems to enhance cybersecurity risk management standards and governance across their respective enterprises. Examples include cybersecurity risk and maturity assessments, threat simulation exercises and a continued effort to improve maturity of controls.

[1] Terms commonly used in cybersecurity work are defined in Annex I.

[2] Cybersecurity standards in the financial sector are typically sets of rules that organizations comply with to interface with each other such as the payments sector, for storing client data and so on. Examples of global industry standards for cybersecurity include (but not limited to): National Institute of Standards and Technology (NIST), ISO/IEC 27001/27032, etc.

There is scope to strengthen cybersecurity supervision and oversight and a need for additional dedicated resources. Onsite examinations should be more frequent, performed at least annually for SIFIs, with more comprehensive verification of cybersecurity risk management capabilities. SARB and the PA should commit additional resources to this area, in particular by recruiting and retaining more cybersecurity risk specialists. The addition of more specialist resources will help arm supervisors with the necessary skills, time and first-hand knowledge to identify vulnerabilities, assess the effectiveness of controls and verify the effectiveness of risk management. The PA has done important work to develop and implement new supervisory tools (such as a cybersecurity risk management questionnaire); the next step will be to focus on collecting and analyzing information prior to the onsite examination. This would help supervisors to focus on issues identified and to explore threats and vulnerabilities in more depth during the on-site examination. Taken together, these resources and tools will provide an opportunity for the PA to provide regulated entities with benchmarking relative to wider industry experience and risk management standards, in turn assisting regulated entities with prioritization.

Moving toward a consistent and consolidated regulatory framework for cybersecurity (based on prudential standards) should be a priority. While guidance notes have been used by the PA historically, moving toward fully articulated standards will strengthen application and enforceability and influence behavior through giving additional weight to the regulatory framework and signal to industry the importance of this topic, mirroring the PA's approach in relation to the other Pillar 1 risks (credit and market risk). Furthermore, the recent publication of the Basel Committee's guidance covering operational risk management and operational resilience provides the PA with a good instrument to leverage the move towards a regulatory framework for cyber resilience.

Third-party risk management should be strengthened through ongoing banking supervision and FMI oversight. Third-party service providers play an integral role for SIFIs and while dependency on providers is not unique to South Africa, in some cases these providers exhibit high levels of concentration, low substitutability and fragilities (outside of scenarios of cyber incidents) which could act as amplifiers in the event of a cyber incident. SARB and the PA should continue to mine the information gained from mapping for connections/ dependencies/ concentrations and use that to inform next steps (potential third-party oversight, etc.). Second, the SARB makes identification of critical third parties a priority outcome of the mapping exercise. Third, engage with SIFIs on their management of third-party service providers, evaluating the ongoing risk management standards and due diligence to understand their standards of operational resilience, and lastly, for the SARB and PA to prioritize management of third parties during forums for private and public sector cooperation, e.g., SABRIC and others.

FMIs have room to systematically evolve and achieve more mature states of cyber resilience. While FMIs recognize the importance of cyber resilience, there are gaps against international standards that should be remediated. Expediting the National Payment Systems (NPS) Act into law will formally adopt the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) and establish explicit regulatory, supervisory, and oversight powers for the SARB, forming the basis for implementing the CPMI-IOSCO Guidance on Cyber Resilience for PS FMIs. Formalizing a cyber

resilience framework for all systemically important FMIs, particularly the real-time gross settlement system, regional cross-border transfer system, and capital market FMIs (Strate, JSE Clear), would be the next step. Metrics and maturity models would allow the FMIs to benchmark and assess their cyber resilience maturity against a set of predefined criteria, such as operational reliability objectives. Benchmarks would require FMIs to analyze and correlate findings from audits, management reviews, incidents, recovery time objectives, near misses, tests, and exercises as well as external and internal intelligence gathered. Also, such metrics help identify gaps in the cyber resilience framework for remediation. Finally, all FMI critical service providers, in addition to messaging providers, should be assessed against the CPMI-IOSCO Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers. This is to safeguard against risk from other third-party service providers, particularly information technology firms.

Response and recovery capabilities, including information sharing, critical to managing cyber threats on a continuous basis also require improvements. The current formal escalation processes for cyber incidents appears to be overly complex, although it is supplemented by informal senior-level communications networks. SARB could sponsor or lead an industry-wide crisis management exercise to test and further deepen formal and informal relationships across the sector. In addition, the SARB should support implementation of an industry-wide platform designed to share cybersecurity threat intelligence. Furthermore, as noted above, the SARB is the home supervisor for many banks with cross-border presence and there may be a greater regional role that SARB could undertake to improve information sharing, building on the Community of African Banking Supervisors (CABS) CABS cyber resilience sub-committee arrangements. SARB should also strengthen penetration testing capabilities across the financial sector by engaging with regulated entities to ensure that their penetration testing is robust. The various stakeholders within the SARB may also wish to determine the best approach for the implementation of regulator-led penetration testing (based on, for example, global frameworks such as TIBER-EU and UK CBEST).

Table 1. South Africa: Key Recommendations	
Recommendations and Authority Responsible for Implementation	**Time[1]**
Cybersecurity Risk Supervision	
Move toward implementing a consistent, cross-sectoral regulatory framework for cybersecurity (based on prudential standards)	MT
Strengthen cybersecurity supervision and oversight with greater supervisory intensity and frequency for SIFIs and new supervisory tools.	ST
Strengthen bank and FMI third-party risk management through ongoing supervision and oversight.	ST
Strengthen the PA's resources for cybersecurity supervision with dedicated specialists	ST
Monitor intraday liquidity management and stress test payment system	ST
Help strengthen response and recovery capabilities for the financial sector, including: (i) support implementation of an industry-wide crisis management exercise, ideally hosted and/or sponsored by SARB as a way to further deepen formal and informal relationships across the sector; (ii) support implementation of an industry-wide platform designed to share cybersecurity threat intelligence; and (i) strengthen penetration testing capabilities across the financial sector.	MT
Cybersecurity Risk Oversight	
Expedite the adoption of the revised National Payment Systems Act to establish explicit regulatory, supervisory and oversight powers for the SARB.	ST
Formalize the cyber resilience frameworks for all systemically important FMIs with metrics for benchmarking.	MT
Monitor the compliance of SAMOS and SADC-RTGS participants with the mandatory controls of the SWIFT Customer Security Program, and ensure self-attestations are audited.	I
Assess all FMI critical service providers against the CPMI-IOSCO Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers.	ST
1/ I Immediate (within 1 year); ST Short term (within 1–2 years); MT Medium Term (within 3–5 years)	

INTRODUCTION[3]

1. Growing threats from cyber-attacks and links to financial stability have elevated cyber resilience to a top policy priority for the financial sector. Operational risks—including cybersecurity risks—are among the top risk categories considered by financial institutions and regulators/supervisors. While risks of internet and communication technology outages have been considered important operational risks for financial institutions for some time, the confluence of increased dependence on technology, increased interconnectedness of the financial sector, concentration in technologies and, crucially, the significant increase in accessibility of hacking technology over the past several years, have pushed cybersecurity risk to the fore.

2. In response, the IMF embarked on a pilot exercise to determine the feasibility of an evaluation of cyber resilience and recovery and crisis management capabilities as part of surveillance activities. Cybersecurity risk poses a unique threat to financial stability, which differs from traditional financial shocks; a successful attack could affect otherwise robust institutions. Furthermore, a disruption to the ability of payment and settlement systems to function, counterparties to trade and assets to be priced could have systemic implications.[4] To test the feasibility of integrating cyber into surveillance, the IMF joined with the South African authorities to undertake a pilot exercise to analyze cybersecurity risks and potential threats to financial stability as part of the FSAP process and as a standalone workstream. The pilot worked closely with the SA authorities at all stages of the process to agree scope and information requests and to formulate policy recommendations.

3. This note focuses on the review of the supervisory and oversight frameworks for systemically important financial institutions (SIFIs), including banks and financial market infrastructures (FMIs) in South Africa. This report contains the assessment of South Africa's cybersecurity risk[5] supervision and oversight. It includes the work of the South African Reserve Bank (SARB) and the Prudential Authority (PA) in the areas of cyber threat intelligence gathering, financial

[3] This Technical Note (TN) was prepared by Chris Wilson, Tanai Khiaonarong (both IMF staff) and (Nick Strange, IMF short-term expert on temporary secondment from the Bank of England).

[4] For instance, a cyber incident has the potential to disrupt critical functions like credit provision and access to deposits and disruption of payments messaging services could cause the failure of payments and technical defaults (particularly if the disruption extended over several days) if the incident impacts multiple financial institutions, critical infrastructure or a common technology or technology provider on which a significant portion of the sector relies. For further detail see "The Future of Financial Stability and Cyber Risk," SIPA, published by the Brookings Institute, October 2018. See https://www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/.

[5] Cybersecurity, cybersecurity risk, and cyber resilience are widely but imprecisely used terms. In this note we use the Financial Stability Board's Cyber Lexicon definition of cybersecurity ("Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved"), which is broad and considers cyber incidents irrespective of their cause, and where "cyber" relates to the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems. Thus, for all practical purposes, the term cybersecurity is the same as information security that has been broadly used for some time. Similarly, cyber resilience can be considered a new term referring to the existing concept of business continuity management but with a focus on cyberthreats.

sector and cyber mapping, cybersecurity risk related information sharing, cybersecurity risk regulation and supervisory/oversight practices, as well as response and recovery capabilities of critical financial sector participants and public sector agencies. The review is based on a detailed questionnaire sent to the SARB, and SIFIs, thorough interviews with both authorities and supervised banks and FMIs, as well as the study of relevant national laws and reports published by the authorities. Interviews with selected banks and FMIs informed the assessment of the effectiveness of the South African regulatory framework and supervisory assessments with regards to cybersecurity risk. Due to Covid-19, the mission was delivered remotely.[6]

4. The basis for the review of the South African cybersecurity risk supervisory and oversight approach was derived from international standards and regulatory good practice. As there are no binding international regulatory standards on cybersecurity risk, the mission team used guidance material developed by standards-setting bodies and regulatory good practice as the basis of this Note. For cybersecurity risk supervision of financial institutions (FIs) the following benchmarks were used: the BCBS's '*Principles for Operational Resilience* and the revision of the *Principles for the Sound Management of Operational Risk*' (both March 2021) and BCBS *Cyber resilience: Range of practices* (December 2018); the FSB '*Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices*'; the World Bank Group's '*Financial Sector's Cybersecurity: A Regulatory Digest*'; the IMF Departmental Paper on Cybersecurity Risk Supervision and the G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector. The CPMI-IOSCO '*Guidance on cyber resilience for financial market infrastructures*' (June 2016), is the basis of recommendations on the oversight of cybersecurity risk in FMIs.

CYBERSECURITY RISK SUPERVISION AND OVERSIGHT

A. Overview of the South African Financial System

5. The South African financial system is large, concentrated and highly interconnected, with cross-border linkages. Banking sector assets account for 31 percent of total financial sector assets (the share of banks' assets as a proportion of GDP is 115 percent), exceeding that of most other emerging economies. The banking sector in South Africa is highly concentrated with the sector dominated by five large banks accounting for more than 91 percent of the banking sector assets and the large banks are highly interconnected with other segments of the financial sector such as insurance and asset management. While South African banks' cross-border operations represent a small part of consolidated balance sheets,[7] operations continue to grow and are systemically important in many host countries (e.g., Botswana, Lesotho, Malawi, Mauritius,

[6] The scope of the work undertaken by the mission team included the prudential and systemic implications of cybersecurity risk for large domestic banks and PFMIs with a focus on regulations and supervision. The scope did not extend into impacts on conduct supervision or other broader areas of impact.

[7] Less than 5 percent of the exposures of the six largest banks is booked abroad.

Mozambique, Namibia, Swaziland, Uganda, and Zambia). Thus, domestic shocks could generate outward spillovers, with a significant impact on the region.

6. There are six systemically important FMIs that are subject to the PFMI (Figure 1). This includes four payment systems (PS), one central securities depository (CSD)/securities settlement system (SSS), and one central counterparty (CCP).[8] There are no trade repositories. The ZAR is a CLS-eligible currency, which is operated by an FMI located in a foreign jurisdiction.

- **PS.** These are: (i) the South African Multiple Option Settlement (SAMOS) system, the real-time gross settlement (RTGS) system owned and operated by the SARB; (ii) the large-value payment system within STRATE, a privately operated SSS; (iii) the BankservAfrica retail payment system privately operated by BankservAfrica; and (iv) the South African Development Community RTGS (SADC-RTGS) system, which settles cross-border payments and is owned by SADC central banks and operated by the SARB. At least 15 SADC member countries participate in the SADC-RTGS system.

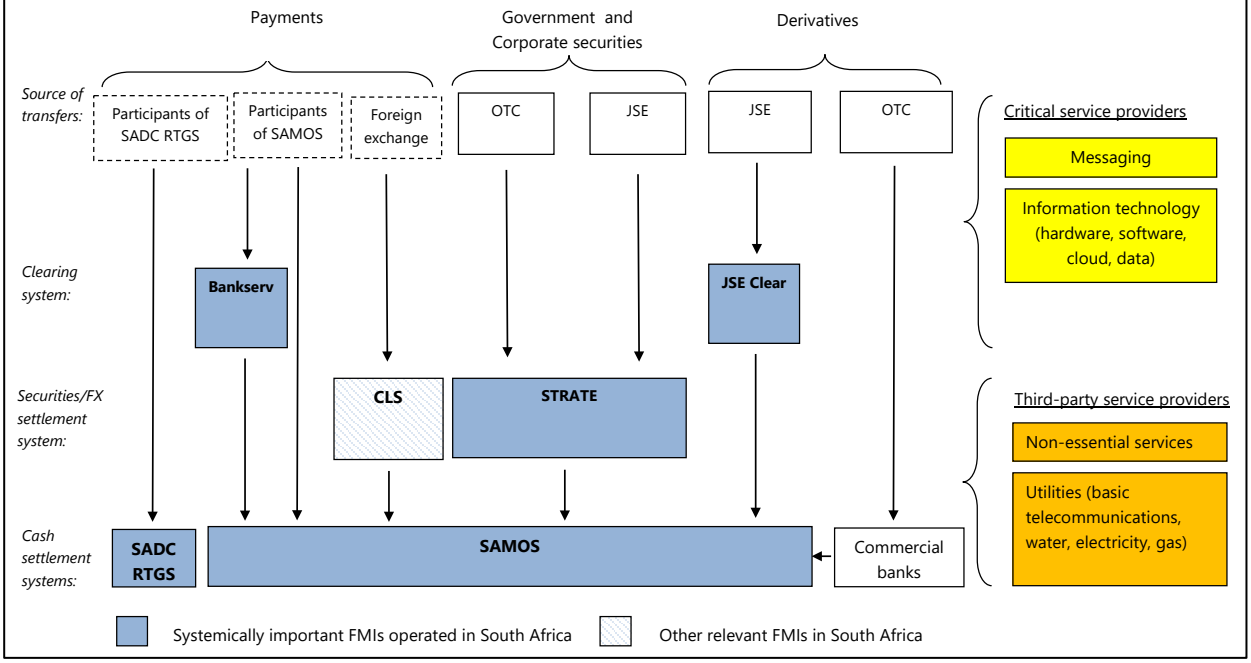
- **CSD/SSS.** STRATE is also the sole operational CSD/SSS in South Africa. It facilitates the settlement of equities, bonds, and money market transactions.

- **CCP.** JSE Clear is the sole licensed clearing house in South Africa. JSE Clear acts as the settlement authority for the exchange-traded equities market and as the clearing house for the exchange-traded derivatives market.

7. The characteristics of the South African financial system (such as interconnectedness and fragilities of third-party service providers) could act as amplifiers to financial instability risks in the event of a cyber incident. The financial sector performs a critical function in the economy including allocating credit, facilitating settlement and payments and disruptions to these functions can cause financial instability. Characteristics such as a concentrated financial sector, a high level of interconnectedness and a lack of IT substitutability may act as amplifiers in the event of a cyber incident, transforming operational disruptions into risks to financial stability. It is therefore necessary to strengthen FI's ability to absorb operational risk-related events, such as cyber incidents, which could cause significant disruptions in financial markets.

[8] See CPMI-IOSCO (2015) Assessment and Review of Application of Responsibilities for Authorities, November.

Figure 1. Systemically Important Financial Market Infrastructures in South Africa



B. Institutional Structure for Cyber Resilience

8. The SARB and PA are the leading public sector agencies in terms of strengthening cyber resilience for the financial sector. The SARB has responsibility for overseeing the stability of the financial system, the provision of liquidity assistance to FIs and oversight of the national payment system (NPS). Within the South African financial sector, cybersecurity and cyber resilience is critical for national financial stability. Given its role for overseeing financial stability, the SARB compiles a risk assessment matrix (RAM) that serves at the Financial Stability Oversight Committee[9] and frames the analysis and assessment of the financial stability of the domestic financial system. Cybersecurity risks have featured as systemic risk in the RAM for the past two years. The SARB's oversight and supervisory process of the payment system and FMIs is based on global standards and is risk-based and proportionate to the systemic risks posed by the supervised entity or system.

9. The financial sector recognizes the importance of developing cyber resilience and have implemented various measures. In addition to their established risk management processes, SIFIs have undertaken various initiatives to strengthen cyber resilience, including identifying and quantifying cybersecurity risks; implementing practices to protect most critical IT assets (i.e., 'crown

[9] The Financial Stability Oversight Committee is a central part of the SARB's structure for dealing with operational and cybersecurity risks. It is chaired by the SARB Governor and is constituted with representatives from the public and private sector.

jewels'); develop intelligence-led defenses; collaboration and cooperation; and, engage in industry-wide activities.

10. In terms of prudential supervision, cyber is a subset of operational risk which falls into the remit of the PA responsible for consolidated supervision. The PA is responsible for the prudential regulation and supervision of banks, insurance companies and capital market infrastructures (MIs).[10] As part of its supervisory review, the PA monitors policies, processes, and practices related to cybersecurity risk and cyber resilience by regulated entities and further relies on outcomes of work done by independent parties such as internal and external audit as well as external cyber experts. The PA also conducts on- and off-site reviews through questionnaires, surveys, data center, walk-throughs,[11] and industry trend analysis.

11. The authorities responsible for the regulation, supervision, and oversight of FMIs include the SARB, PA and FSCA. The SARB's National Payment System Department (NPSD) is responsible for the operations, oversight, supervision, and policy of payment systems. The PA is responsible for the supervision of capital market FMIs (CSD, SSS, CCP) from a prudential perspective. The FSCA is responsible for the supervision of CSD/SSS, CCPs and trade repositories from a conduct perspective. These responsibilities fall under the Financial Sector Regulation Act 9 of 2017 (FSRA), which is the overarching financial regulatory framework governing supervised financial firms. This Act specifies the financial sector regulators as the PA, FSCA, and Financial Intelligence Centre (FIC), while the SARB assumes an oversight function.

12. The Payments Association of South Africa (PASA) also has a key role in rulemaking. Under the NPS Act, the SARB was mandated to recognize a Payment System Management Body (PSMB), to organize, manage and regulate its members participating in the NPS. PASA is a self-regulatory body that develops legal constructs such as payment clearing house (PCH) agreements, clearing rules, and service level agreements. PASA also develops policies and position papers relating to clearing activities which are aligned to the overall NPS legislation.

13. There are well established mechanisms for domestic cooperation and coordination between the SARB and PA. To effectively detect and manage cyber-attacks on a national level, and thereby supporting financial stability, several cooperation platforms between authorities, sector CERTs,[12] and public and private businesses have been established. The SARB and PA have a mature framework for domestic cooperation and coordination across a range of topics that includes the

[10] "Market infrastructures" comprise: (a) a central counterparty; (b) a central securities depositary; (c) a clearing house; (d) an exchange; and (d) a trade repository. The PA is preparing to develop its prudential regulatory and supervisory framework to promote and enhance the safety and soundness of MIs. The biggest focus is on operational risk, liquidity risk management, and capital adequacy for unforeseen events.

[11] Data center walk-throughs are typically used by supervisors to gain comfort regarding the security and control processes of third-party service providers, especially where the supervisor does not have a direct mandate over the provider.

[12] CERT stands for computer emergency response (or readiness) team and CSIRT stands for computer security incident response team. And CIRT can also stand for either computer incident response team or, less frequently, cybersecurity incident response team. CSIRT, CERT and CIRT are often used interchangeably in the field.

area of cybersecurity and have entered into a number of MOUs for coordination of cross-border bank supervision with foreign authorities. Formal mechanisms exist for domestic sharing of information, coordination of activities, and working together across a range of topics. Protocols have been tailored for the risks associated with cybersecurity.

14. The SARB gathers threat intelligence through cooperation with other organizations and public sector agencies. Directive 2, issued by the PA in September 2019, requires banks to formally report material IT and/or cyber events and is currently the SARB/PA's most direct source of cyber threat information. SARB is a member of the Central Bank and Regulator Supervisor Forum (CERES), which is a program of the Financial Services Information Sharing and Analysis Center, Inc. (FS-ISAC). SARB has also established a cyber resilience governance structure at the financial services industry level: the Cybersecurity Resilience Sub-committee (CRS), which is a sub-committee of the Financial Sector Contingency Forum (FSCF). The CRS meets quarterly to discuss pertinent cybersecurity matters within the financial sector and to monitor, evaluate and guide cybersecurity efforts. SARB also uses some open-source intelligence (OSINT) and subscription feeds for threat information and intelligence.

15. At the international level cyber threat information is shared by a malware information-sharing platform (MISP) driven by SABRIC which is maintained by the CERT-EU (France). South Africa is a member of the Community of African Banking Supervisors (CABS) that was established to assist regulators with the sharing of information or discussion of critical matters that have an impact across the African continent and/or other pertinent information. A CABS cyber-resilience subcommittee was recently established where the intention is to share information around cyber threats, intelligence gathering, cyber resilience supervisory frameworks, standards, and practices as well as any other information.[13]

16. In addition to the public sector mechanisms for information sharing, SABRIC plays a vital role for the private sector which connects with the public sector structures. SABRIC's role is to ensure that their members are represented, contribute to and receive valuable insights from information shared by other participants, in the interest of creating cyber resilience within the financial services sector. SABRIC works closely with the Cybersecurity Hub in SA and with a mandate from members, intends to share information that can assist other sectors or Government, once the MISP, which is currently a proof of concept and includes commercial banks and insurers, is up and running. SABRIC has several stakeholder relationships that contribute to a data pool and perform global research, assisting with early detection of emerging trends so that they may alert members.

Threat Landscape

17. The cyber threat landscape presents challenges for the South African financial sector. The South African financial services sector's experience with cyber-attacks is consistent with many jurisdictions globally. Although SABRIC does not currently record annual statistics on cyber-attacks on its member banks, this capability is envisaged, and would include insurers and FMIs. Cyber risk

[13] At the time of the mission, no actual incident information had been shared.

incidents continue to grow in terms of frequency and volume, however, the methods used by cyber threat actors have remained relatively unchanged over the recent period. Nonetheless, the severity and frequency are a function of an increasingly open and interconnected cyber and financial ecosystem. The change in work arrangements caused by the Covid-19 pandemic has exacerbated the threat landscape as teleworking and increased reliance on digitalization have exposed new risks, with several banks reporting material increases in cyber-attacks.

18. Motivation for cyber-attacks is predominantly for financial enrichment, with phishing attacks being typical and threat actors mainly organized crime. Cyber-attacks on the financial system are mainly focused on financial crime, i.e., stealing (credit card skimming, internet banking scams, card fraud, automated teller machine fraud, etc.), extortion (ransomware, DD4BC),[14] money laundering, etc. There has also been an increase in spam/scam attacks on employees and customers (phishing, vishing, smishing, social engineering, etc.) and some successful ransomware attacks. The most recent and successful cyberattack on Nedbank where 1.7 million bank clients had personal details exposed due to a breach of one of their service provider's IT systems.[15] Cyber threat actors have also taken advantage of the changes to work processes as a result of Covid-19, though similar techniques (e.g., phishing) are being used.

Transmission Channels and Systemic Risk Propagation

19. As cyber-attacks can impact financial institution's systems and data through three main channels, effective security controls need to protect the following:

- **Integrity** to guard against illicit alterations or destruction of information and assuring non-repudiation and authenticity;
- **Confidentiality** to guarantee restrictions on information access, including methods to secure privacy and proprietary information (e.g., data breaches); and
- **Availability** to preserve timely and dependable access and use of information against internet service provider outages of DDoS attacks.[16]

20. Furthermore, financial interconnectedness and operational dependencies can function as contagion channels when wide-scale or major incidents occur. Many banks and FMIs depend on a few key IT service providers that provide and maintain critical systems and hardware. In some cases, these providers exhibit high levels of concentration and low substitutability and exhibit fragilities outside of scenarios of cyber incidents which could act as amplifiers to financial instability in the event of a cyber incident. Concentration of key nodes can act as transmission channels of risks

[14] DD4BC- (DDoS for Bitcoin). Armada Collective executed a Distributed-Denial-of-Service (DDoS) attack on four of South Africa's major banks during November 2015. This was the first recorded incident of DDoS attacks on SA commercial banks aimed at extorting Bitcoins as ransom payment—DD4BC.

[15] Nedbank advised customers of the incident after it was identified. For details see https://www.nedbank.co.za/content/nedbank/desktop/gt/en/info/campaigns/nedbank-warns-clients.html

[16] See "The Future of Financial Stability and Cyber Risk," SIPA, published by the Brookings Institute, October 2018.

to financial stability in the event of an operational disruption such as a cyber-attack. In this way, a disruption of one financial institution or FMI can lead to disruptions at other financial institutions resulting in potential financial risks, ultimately weakening confidence in the financial system.

21. FMI interdependencies with other entities are potential transmission channels (Figure 1). This includes connection between the SAMOS and CLS, and foreign RTGS systems to the SADC RTGS. Interdependencies also exist with other settlement banks (commercial banks), liquidity providers (domestic banks providing ZAR committed liquidity facilities for CLS), and service providers. For the latter, this includes messaging and information technology providers used by FMIs and/or FMI participants. Other third-party service providers include non-essential services and utilities, which could also impact the operations of FMIs and/or FMI participants.[17] South African FMIs recognize this importance and make transparent such interdependencies as part of their framework for the comprehensive management of risks. Such reviews help spot material risks the FMI bears from and poses to other entities. Responses to the CPMI-IOSCO Disclosure Framework for FMIs are also publicly disclosed. As a CPMI-IOSCO member, South Africa participates in the implementation monitoring of the PFMI, which includes self-assessments and peer reviews.[18]

22. High concentration of transactions in PS could pose liquidity risks in a cyber incident. The mission observed relatively high transaction volume and value concentration ratios in two systemically important PS. This is based on the market share of the five largest senders of payment messages. A prolonged outage caused by a cyber incident at a major participant (bank) in the payment system could disrupt its incoming and/or outgoing payments and create liquidity pressures to other direct participants, or disable its access to central bank intraday liquidity facilities and interbank settlement services—calling for monitoring of intraday liquidity management and stress-testing of intraday liquidity stress scenarios.[19]

23. Endpoint security for wholesale payments is monitored domestically and follow-ups are planned with foreign central banks connected to the SADC-RTGS. The SARB's NPSD Oversight and Supervision Division receives completed self-attestation reports from SWIFT. This helps ensure customer security for connection to SAMOS. If deficiencies are identified, an escalation process is made to the relevant competent authority. The NPSD plans to engage the relevant central banks through the SADC-RTGS annual user group meetings to obtain views on any outstanding self-attestations by banks in the region. While the mission observed during industry interviews that bank

[17] Unless otherwise indicated by the relevant authorities, activities not directly related to essential operations of the FMI and utilities (such as basic telecommunication services, water, electricity, and gas) are out of scope when identifying critical service providers. See CPMI-IOSCO (2014) Principles for Financial Market Infrastructures: Assessment Methodology for the Oversight Expectations Applicable to Critical Service Provider, December.

[18] CPMI and IOSCO members have committed to adopting the principles and responsibilities contained in the PFMI in line with the G20 expectations.

[19] See BCBS (2013) Monitoring Tools for Intraday Liquidity Management, April. The BCBS recommends that this tool is for monitoring purposes only and is required for internationally active banks. Additionally, national supervisors will determine the extent to which the tools apply to non-internationally active banks within their jurisdictions.

size determined resource availability to address cybersecurity issues, there was insufficient information to observe its role in the completion of self-attestations.

C. Cybersecurity Risk Regulatory Framework and Supervisory Practice

Oversight Arrangements for FMIs

24. Authorities recognize the importance of cyber resilience and have issued regulatory instruments to set supervisory and oversight expectations for FMIs. Guidance Note 4 on the cyber resilience for FMIs was issued to the banking industry in 2017. The guidance is legally-binding. The PA is of the view that the principles and risk management categories are applicable to banks in addition to FMI, although since banks are not named in the guidance there is cause for some uncertainty. Additionally, the NPSD instructed all systemically important payment systems, through official correspondence, to implement and comply with the CPMI-IOSCO Guidance on Cyber Resilience for FMIs. The mission observed that the PA plans to issue a prudential or joint standard on cyber resiliency with the FSCA, which would be applicable to regulated financial institutions.

25. The NPS Act 78 of 1998 empowered the SARB to manage, administer, operate, regulate, and supervise payment, clearing, and settlement systems in South Africa. Amendments made in 2004 stipulated additional powers to withdraw the recognition of a payment system management body, designate settlement systems, enable payments to third persons, and issue directives. A major review of the NPS Act 78 of 1998 in 2018 further recommended that the SARB's regulatory, supervisory and oversight responsibilities in the payment system and adoption of the PFMI be made explicit in the NPS Act, among others. As a CPMI member country, South Africa was expected to have formally adopted the PFMI by the end of 2012. The SARB has published a position paper and a supporting information paper broadly expressing its commitment to adopting the PFMI within the regulatory framework of the National Payment System as of September 2013. While the SARB could use moral suasion as a mechanism to effect change, it lacks formal powers to induce change or enforce corrective action in an FMI that is not complying with relevant regulations or policies relating to cyber resilience.

26. FMIs have started to implement the international guidance for cyber resilience and are at different levels of maturity.[20] At the time of the mission, the SARB's NPSD Risk Division was in collaboration with the Cyber and Information Security Unit to formalize a cyber resilience framework for the SAMOS and SADC-RTGS. BankservAfrica completed self-assessments on cyber resilience and identified remedial actions for the retail payment system. STRATE has plans to align its cyber resilience framework with international standards, having used the frameworks established by NIST and the Center for Internet Security.

27. FMI critical service provider assessments have been implemented inconsistently across FMIs. While oversight expectations are clear and self-assessments forthcoming for messaging

[20] The mission was not in a position to assess the implementation progress on cyber resilience for JSE Clear due to insufficient information.

providers (SWIFT) where a foreign authority serves as the lead overseer, further improvements could be made for information technology providers or other third-party service providers that have been identified as critical service providers. Such identification would indicate what is considered non-essential services and clarify if certain utilities (such as basic telecommunication services and electricity) would fall under the category of critical service providers to FMIs in the context of South Africa. The mission observed that in one case, multiple external suppliers and vendors were reported but without identifying if they were critical service providers to the FMI.

PA's Regulatory Framework for Cybersecurity

28. The PA has a long history of implementing a principles-based regulatory framework for cybersecurity based on global standards. Cybersecurity is a subset of operational risk containing general requirements for risk management and governance. Specifically in relation to cyber, however, Guidance Note 4 of 2017 refers to cyber resilience for FMIs and was issued to the banking industry, representing the PA's expectations. The PA relies upon the principles in this Guidance Note—as set out by the CPMI and IOSCO—as applicable to the banking industry. This Guidance Note is complemented with several targeted guidance materials. The complete regulatory framework for cyber for FIs is below (Figure 2).

Figure 2. Prudential Authority's Regulatory Framework for Cyber for Financial Institutions

Theme	Banks	Insurance	FMIs
Cyber-resilience	Guidance Note 4/2017: Cyber Resilience	None	Guidance Note 4/2017: Cyber Resilience
IT Incident Reporting	D2/2019: Reporting of material information technology and/or cyber incidents	None	None
Outsourcing	The Financial Sector Regulation Act 9 of 2017 (FSRA) gives the PA the ability to request information from or conduct an inspection at the third-party service provider. Directive 8/2016: Reporting requirements relating to material outsourced service providers and critical third-party service providers Guidance note 5/2014: Outsourcing of functions within banks	FSRA GOI 5: Outsourcing by insurers GOG: Outsourcing by insurers groups GOB: Outsourcing by branches of foreign reinsurers GOL: Outsourcing by Lloyd's GOM: Outsourcing by micro-insurers	FSRA
Cloud	Directive 3/2018: Cloud computing and the offshoring of data Guidance Note 5/2018: Cloud computing and the offshoring of data	None	None
Business Continuity Management	None	GOI 3.2: Business Continuity Management (BCM)	None

Main Findings and Recommendations Pertaining to the Regulatory Framework

29. The mission recommends the PA moves toward a consistent regulatory framework (based on prudential standards) for cyber regulation. While guidance notes have been used by the PA historically, the mission recommends the PA move toward a consistent multi-sectoral

regulatory framework (based on prudential standards) for cybersecurity and operational resilience. The production of prudential standards rather than a guidance note will strengthen the application and enforceability to influence behavior through the full weight of the regulatory framework. The use of prudential standards will also signal to industry the importance of this topic. The recent publication of the BCBS's "*Principles for Operational Resilience* and the revision of the *Principles for the Sound Management of Operational Risk*" gives the PA the opportunity to codify this guidance into regulation for consistency, enforceability, applicability of the regulations to bring about changes in behavior of firms, to get them to fully internalize systemic risks into higher standards of risk management consistent with the SA's / PA's expectations risk tolerance consistent with financial stability responsibilities.

30. The mission recommends the revised National Payment System Act be expedited into law to further establish explicit regulatory, supervisory and oversight powers for the SARB. This would form the basis for formally adopting the CPMI-IOSCO PFMI, observing the CPMI-IOSCO Guidance on Cyber Resilience for FMIs, and identifying and overseeing critical service providers to systemically important PS. For the latter, this would cover risk identification and management, robust information security management, reliability and resilience, effective technology planning, and strong communication with users.[21] Explicit powers would enhance the SARB's ability to obtain timely information and to induce change or enforce corrective action if an FMI is not complying with relevant regulations or policies.

31. The mission recommends formalizing the cyber resilience frameworks for all systemically important FMIs with metrics for benchmarking. This is applicable for the SAMOS, SADC-RTGS, STRATE, and JSE Clear. Metrics and maturity models would allow the FMIs to benchmark and assess its cyber resilience maturity against a set of predefined criteria, such as operational reliability objectives. Benchmarks would require FMIs to analyze and correlate findings from audits, management reviews, incidents, recovery time objectives, near misses, tests, and exercises as well as external and internal intelligence gathered. Also, such metrics help identify gaps in the cyber resilience framework for remediation.

32. The mission recommends that all FMI critical service providers, in addition to messaging providers, should be assessed against the CPMI-IOSCO Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers. Ratings could be considered in the annual self-attestations submitted by FMI CSPs to support the continuation of critical services for the FMIs and external audits should be completed against acceptable national or international standards. This could safeguard against risk from other critical service providers, particularly information technology firms and/or third-party service providers, that performs, on a continuing basis, activities essential to the operations of the FMI. The continuous, secure, and efficient delivery of these services by the third-party service provider may be critical to the operations of the FMI or, in some cases, multiple FMIs. Furthermore, a rating for each oversight

[21] See CPMI-IOSCO (2012) Principles for Financial Market Infrastructures, Annex F on Oversight Expectations Applicable to Critical Service Providers, April.

expectation can be assigned and applied to reflect the gravity and urgency of the need to remedy identified issues of concern.

Supervision Arrangements of the PA

33. The PA implements a risk-based approach to supervising cybersecurity risk, employing a mix of off-site and onsite analysis. The PA follows a risk-based approach to supervising cybersecurity risk and has a long history of supervising operational risk and IT security risk (see Figure 3 for a summary of the PA's approach to IT Risk supervision).[22] The PA conducts detailed institution specific assessments of SIFI's business continuity plans (BCPs) with a focus on operational resilience. The PA follows a thorough approach to assessing operational risk of which BCPs are included. The PA expects BCPs to be developed with operational resilience in mind, such that banks and FMIs take into account the unavailability of third-party providers under various scenarios in order to be able to fulfill their obligations in the event of a cyber incident or other operational disruptions.

34. Cybersecurity risk supervision is a subset of the PA's risk-based approach to operational risks. The PA's overall approach is a mix of onsite and offsite analysis. Line supervisors collect material throughout the supervision cycle used as inputs into an onsite examination. In addition to the routine reporting, the PA has implemented a 'Flavor of the Year' questionnaire to facilitate a deep dive on a specific topic, of which cyber has been a recent focus. The supervisory cycle for SIFIs is typically between one to two years for an onsite examination of operational risk.

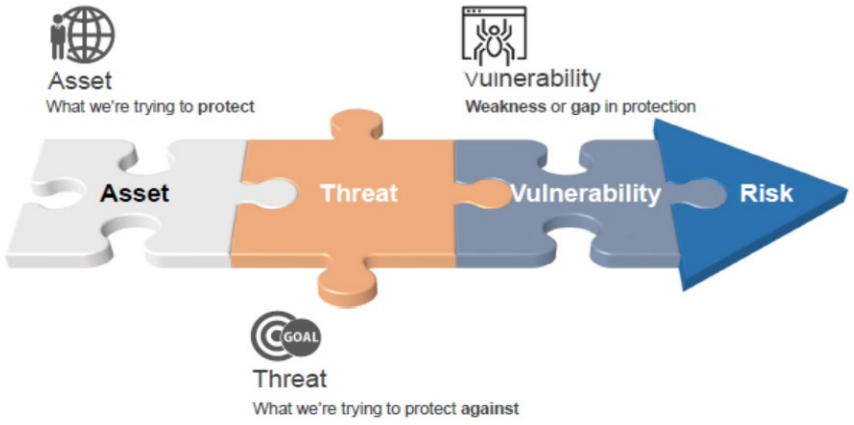
35. For SIFIs (the five largest banks), the PA will undertake a two to three-day onsite examination of operational risk. Pre-visit material is requested and evaluated by the PA prior to the onsite. The onsite will cover all aspects of operational risk such as: third-party risk management, disaster recovery, business continuity, governance, etc. Cybersecurity risk will be covered in all operational risk onsite examinations for SIFIs and will consist of a dedicated session with bank management evaluating the issues identified during offsite analysis such as: internal audit reports and results of work undertaken by the external auditor. To date, the PA has relied mainly on supervisors with an operational risk background to undertake onsite examinations and recently hired a cyber expert to complement the existing team of operational risk specialists.

36. The PA plans to enhance the information gathering process by implementing an annual questionnaire to be completed by SIFIs. The questionnaire is designed to assess the institution's cybersecurity posture and maturity. The design of the questionnaire leverages global best practice and will be an input into the PA's risk-based approach to supervision.

[22] Annex II provides an overview of two approaches to cybersecurity risk and operational resilience by the Australian Prudential Regulation Authority and the United Kingdom's Bank of England.

Figure 3. Prudential Authority's Approach to Information Technology Risk Supervision

The PA's approach to IT risk supervision is a four-part process: (i) identify the IT assets that are required for IT security; (ii) assess the threat landscape; (iii) undertake a vulnerability analysis; and (iv) conclude with a risk assessment. SIFIs' cyber posture is assessed against 8 criteria: governance, identification, protection, detection, response and recovery, testing, situational awareness, and learning and evolving. Aggregating the results of interviews with FIs, the PA will develop a heat map across these eight criteria.



Main Findings and Recommendations Pertaining to the Supervisory Approach

37. There is scope to strengthen cybersecurity supervision and oversight, for which additional resources are needed. There is need for greater supervisory intensity and, in particular, onsite examinations. This would help ensure supervisors are armed with sufficient knowledge, skills, time, and support to challenge management decisions. To get more out of each visit, major factual discoveries should take place before the visit. A program—based on a cybersecurity questionnaire evaluating maturity such as the cyber resilience questionnaire[23] (CQUEST) used in the UK or TIBER-EU—would help inform preparation for the examination in advance, as would penetration-testing (firm's own or regulator-led).[24] With this information pre-analyzed, onsite conversations could focus on issues identified and to explore threats and vulnerabilities in more depth.

38. To support greater frequency and intensity of supervision, the mission recommends additional specialist resources. Recruitment of additional cybersecurity risk specialists, to allow more time during on-sites, which should be at least annual for SIFIs. The addition of risk specialists will provide an opportunity for the PA to provide regulated entities with benchmarking of industry experience and risk management standards to assist with prioritization. Furthermore, this will allow

[23] See Financial sector continuity | Bank of England

[24] The mission has made reference to the supervisory tools used by the UK PRA and the EU SSM. Other tools are available and should also be explored for applicability to the needs of the SA financial sector and cyber threats.

the PA to shift its reliance away from outcomes of work completed by independent parties (such as internal and external audit as well as external cyber experts) to onsite work conducted by in-house risk specialists.

39. The mission recommends monitoring the compliance of SAMOS and SADC-RTGS participants with the mandatory controls of the SWIFT Customer Security Program, and ensuring self-attestations are audited. This should aim to protect the endpoint security of wholesale payments. Cooperation among the relevant FMI and banking authorities would be necessary to exchange information in relation to SWIFT CSP compliance.

D. Third-Party Vulnerabilities and Vendor Risk Management

40. Third-party service providers play an integral role for South African SIFIs. Part of a FIs technology supply chain include third-party vendors which can be classified into two broad groups: (i) vendors common across the entire financial sector, e.g., PASA, Visa/Mastercard, SWIFT messaging network, credit bureaus and utility providers (such as telecommunication and electricity); and (ii) vendors specific to a particular FIs, e.g., software and hardware providers, internet service providers, etc.

41. The SARB has identified the following payment FMIs as SIPS in terms of the PFMI criteria: The South African Multiple Option Settlement (SAMOS) system which is a real-time gross settlement (RTGS) system owned and operated by the SARB. A retail payment system that clears retail transactions in respect of all the payment streams, excluding the card stream, owned and operated by BankservAfrica. A large value payment system that clears the delivery and payment legs of equities, bonds, and money market transactions, owned and operated by Strate (Pty) Limited. CLS system, which settles foreign exchange transactions in designated currencies, including the ZAR—owned and operated by the CLS Bank International. SADC-RTGS system, which settles cross-border transfers that require immediate settlement—owned by SADC central banks and operated by the SARB.

42. To manage dependencies on third-party service providers, FIs have implemented an enterprise-wide approach to governance and risk management. FIs recognize the need to manage dependencies effectively and employ a range of risk management practices, including:

- Identifying and cataloguing all critical vendors, via full mapping of systems, infrastructures, and suppliers;
- Implementing self-identified maturity gap analysis;
- Service level agreements (SLAs) in legal contracts to test and manage resilience of critical service providers;
- Ongoing monitoring and measuring of the performance of vendors against SLA's; and
- Disaster recovery failovers tested regularly (e.g., quarterly).

43. While dependency on third-party providers is not unique to South Africa, in some cases these providers exhibit high levels of concentration, low substitutability, and fragilities (outside of scenarios of cyber incidents) which could act as amplifiers in the event of a cyber incident. Management of third-party service providers is a priority, particularly where the FI does not have leverage to negotiate with large global ICT service providers. In terms of the utility service providers, there are vulnerabilities and fragilities, some of which are specific to South Africa, in particular telecommunications and electricity.

44. The SARB undertook an integrated mapping initiative to map the markets and payments systems to provide insights into cyber resilience. A "cyber map" identifies the main technologies, services, and connections between financial sector institutions, service providers, and in-house or third-party systems. At a conceptual level, mapping aims to highlight key financial and technological connections between financial institutions (including FMIs) and between these firms and third-party technology and service providers. Even a basic map will identify systemic institutions, service providers, and technology providers and their relationships in the financial system and thus provide a valuable reference for supervisors to identify key vulnerabilities and allocate resources.[25] There is currently no single high-level view of the end-to-end South African financial sector vis a vis financial and cyber networks. To address this gap, the SARB contracted a service provider to develop a high-level map for the national payment and market systems. The aim of the mapping exercise is fourfold:

- Defining the critical services executed by the financial sector;
- Collecting data on systematically important institutions;
- Identifying the critical system used to carry out the critical services; and
- Mapping the connections between the institutions.

45. At the time of the mission, the SARB and PA were researching options to take forward the mapping exercise. While conceptually appealing, the dynamism and complexity of the financial sector and the technologies it uses can make cyber mapping challenging. It can be expensive and time-consuming to build detailed maps. However, mapping exercises that do not aspire to completeness and apply thresholds for inclusion, as well as qualitative approaches, have proved to be a useful tool. Cyber mapping is nascent across national supervisors though some have commenced this effort. The initial mapping exercise was still in development at the SARB and PA with next steps to be determined.

[25] Comparative examples from other national authorities that have commenced this process aim to map the financial sector that sets out fundamental functions. Based on these functions, critical objects, infrastructures, and information systems have been defined at the national level. Sectoral agencies have then added further detail to the initial map, which is used to inform both supervision and financial stability analysis.

Main Findings and Recommendations Pertaining to Third-Party Vulnerabilities

46. The mission recommends the PA press for strong bank management of risks associated with third parties. Understanding the financial and ICT connections between SIFIs is a valuable input into supervision, as well as understanding transmission channels for risks to financial stability. There are four observations:

- First, the SARB/PA should keep mining the information gained from mapping, overlaid with information already known, for connections/ dependencies/ concentrations and use that to inform their next steps (third-party oversight, etc.).
- Second, make identification of critical third parties a priority outcome of the mapping exercise.
- Third, engage with SIFIs on their management of third-party service providers, evaluating the ongoing risk management standards and due diligence to understand their standards of operational resilience, and,
- Fourth, to prioritize discussion of third-party risk during forums for private and public sector cooperation, e.g., SABRIC and others.

E. Response and Recovery Capabilities

47. The SARB plays a pivotal role in the response and recovery framework. The SARB has established a cyber-resilience governance structure at the financial services industry level, namely the Cybersecurity Resilience Sub-committee (CRS), which is a sub-committee of the Financial Sector Contingency Forum (FSCF). The primary objective of the CRS is to monitor, evaluate and guide cybersecurity efforts within the financial sector, including national structures and other critical service providers by:

- Fostering trust and collaboration: and
- Facilitating joint initiatives reinforcing the operational resilience of the financial sector.

48. The CRS is a key mechanism for threat information-sharing and collaboration between public and private sector stakeholders. The CRS meets quarterly to discuss pertinent cybersecurity matters within the financial sector. Participants include the PA (as regulator), SARB, national financial structures and associations, commercial banks and insurers. While all cyber incidents need to be reported to the PA, the CRS adds an additional layer of information sharing specifically related to cyber. In addition to the CRS, the local banking industry collaborates through SABRIC and the National Cybersecurity Hub to develop and assist with intelligence gathering and knowledge sharing. The CRS is the main hub by which escalation of cyber incidents will occur and whereby response and recovery decisions will be coordinated. The structure for coordination and escalation contains several committees between the FSCF and the Government. In the event a cyber incident is

designated systemic, however, there is a potential short-cut for the FCFS to escalate cyber incidents to the FSOC/ Government/ Governor.

49. Mechanisms and processes for cross-border coordination and cooperation are less developed. While there are plans underway to facilitate information sharing cross-border, there is currently no or limited sharing of information with other jurisdictions. South Africa is a member of the CABS that was established to assist regulators with the sharing of information or discussion of critical matters that have an impact across the African continent and/or other pertinent information. While various activities have been initiated, processes and protocols to encourage cyber resilience remain at early stages, such as cybersecurity crisis management exercises.

50. SIFIs are strengthening internal response and recovery protocols that help maintain critical business functions during disruptions, such as through penetration testing. SIFIs have raised recovery and response capabilities to a main priority as part of risk management frameworks for cyber resilience conducting in-house cyber-attack simulations as part of crisis management exercises. Simulations and crisis exercises are continually updated and informed by incidents (such as the October 2019 industry-wide DDoS attack on internet infrastructure). Threat-led penetration tests are typically conducted on a periodic basis with the results feeding back into cybersecurity risk management frameworks.

51. Each institution in the financial sector has an independent responsibility for ensuring acceptable risk in their own business. This includes, among other things, the responsibility for secure and stable operating solutions, good backup and emergency solutions and actively contributing to a robust financial infrastructure. Assessment of the business continuity management of FIs and FMIs are done as part of the PA's risk assessment and on-site inspections, and through oversight assessments against Principle 17 of the PFMIs. Firms are required to monitor and test their capabilities regularly such as disaster recovery and business continuity plans and more sophisticated risk management such as penetration testing.

52. FMIs have largely set recovery time objectives at two hours with end-of-day settlement following disruptive events, but actual experiences present implementation challenges. Prolonged power outages could disrupt the FMI and/or other entities that have interdependencies with the FMI (such as other FMIs, settlement banks, liquidity providers, service providers). While most SIPS closely align with the two hours recovery time objective, this is varied for the retail payment system where multiple time objectives could be set by banks for different payment and settlement services. As payments increasingly move towards near real-time environments for retail transactions and cross-border for both retail and large-value payments, this presents a challenge on setting clear and achievable recovery time objectives in the context of fast-moving cyber incidents where settlements must be achieved by end-of-day.

Main Findings and Recommendations Pertaining to Response and Recovery Capabilities

53. The mission recommends strengthening response and recovery capabilities including information sharing. There are three observations:

- First, support implementation of an industry-wide crisis management exercise, ideally hosted and/or sponsored by SARB as a way to further deepen formal and informal relationships across the sector.
- Second, support implementation of an industry-wide platform designed to share cybersecurity threat intelligence.
- Third, strengthen penetration testing capabilities across the financial sector (such as a UK CBEST or TIBER-EU threat-led penetration testing framework for testing firms' cyber resilience).

Annex I. Commonly Used Terminology in Cyber (Cyber Lexicon)

Term[1]	Definition
Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems. Source: Adapted from CPMI-IOSCO (citing NICCS)
Cyber Event	Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring. Source: Adapted from NIST (definition of "Event")
Cyber Incident	A cyber event that (i) jeopardizes the cybersecurity of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. Source: Adapted from NIST (definition of "Incident")
Cyber Resilience	The ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents. Source: Adapted from CERT Glossary (definition of "Operational resilience"), CPMI-IOSCO and NIST (definition of "Resilience")
Cyber Risk	The combination of the probability of cyber incidents occurring and their impact. Source: Adapted from CPMI-IOSCO, ISACA Fundamentals (definition of "Risk") and ISACA Full Glossary (definition of "Risk")

[1] The terms used in this annex is a subset of the work undertaken by the Financial Stability Board to develop a cyber lexicon, published November 12, 2018. The objective of the lexicon is to support the work of the FSB and standard-setting bodies to foster a common understanding of relevant cybersecurity and cyber resilience terminology across the financial sector, including banking, financial market infrastructures, insurance and capital markets, and with other industry sectors. For further information regarding the lexicon see - https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Term	Definition
Cybersecurity	Preservation of confidentiality, integrity, and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. Source: Adapted from ISO/IEC 27032:2012
Information Sharing	An exchange of data, information and/or knowledge that can be used to manage risks or respond to events. Source: Adapted from NICCS
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system or interconnected information infrastructure. Source: NIST
Threat Actor	A person or element that has the power to carry out a threat. Source: Mark Ciampa (2019) "Security Awareness: Applying practical security in your world" Fifth edition. An individual, a group or an organization believed to be operating with malicious intent. Source: Adapted from STIX
Threat Intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted or enriched to provide the necessary context for decision-making processes. Source: NIST 800-150
Vulnerability Assessment	Systematic examination of an information system, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation. Source: Adapted from NIST

Annex II. Overview of Approaches to Cybersecurity Risk Supervision and Operational Resilience

United Kingdom: Bank of England's Approach to Operational Resilience

1. The UK's central bank and regulator has issued operational resilience policy statements requiring financial firms to:

a. identify the **important business services** that they provide to their customers and to the U.K. economy more generally;

b. set tolerances for disruption—'**impact tolerances**' including time limits within which they will need to resume the delivery of these services; and

c. invest to build resilience such that they can stay within these tolerances in **severe but plausible** scenarios.

2. The UK defines operational resilience as the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover, and learn from operational disruptions. Cyber resilience is a key component of operational resilience. This Policy will roll out over the next few years.

3. The UK has established CBEST (a threat-led penetration testing framework), combining ethical hackers with the latest threat intelligence. CBEST remains the UK's flagship testing program for cyber resilience and is now well into its second cycle.

4. When assessing a firm's operational risk management, the Prudential Regulation Authority (PRA) considers the extent to which firms: have reduced the likelihood of operational incidents occurring; can limit losses in the event of severe business disruption; and whether they hold sufficient capital to mitigate the impact when operational risks crystallize.

5. In addition, the UK's Financial Policy Committee continues to develop a new type of regular assessment, first piloted in 2019, called a cyber-stress test to assess firms' operational resilience. Whilst CBEST focusses more on detection, the stress test looks at the response and in particular the ability to restore functioning after an incident. The stress test helps the UK's financial authorities to examine a firm and a system's ability to recover within the timeframe implied in their impact tolerance in a severe but plausible scenario. The UK's next cyber stress test will be in 2022 and will involve a scenario where data integrity has been compromised within the end-to-end retail payments chain.

6. The UK also carries out a high-profile biannual sector-wide simulation exercise (SIMEX), designed to validate the effectiveness of the sector response framework against severe but plausible

sector-wide operational incidents. Exercise scenarios over the past few years have included a pandemic, an extended outage at the Bank's High Value Payment System—RTGS, and a significant cyber-attack which incorporated a data-integrity scenario.

Australian Prudential Regulation Authority's Approach to Supervising Cybersecurity Risk

7. APRA's role is to ensure regulated institutions are resilient to cyber-attacks through prevention, detection and response capabilities. The collection of data drives the supervisory process to prioritize and tailor supervisory activities, including frequency and nature of onsite examinations. The data is also intended to be used to inform baseline metrics against which APRA regulated institutions will be benchmarked and held to account for maintaining their cyber defenses.

8. The regulatory requirements for cyber are principally contained within a regulation CPS 234 which is a legally binding minimum standard. This Prudential Standard aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats. A key objective is to minimize the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties.

9. In addition to CPS 234, APRA has issued several other standards in relation to operational risks, including:

- CPS231 Outsourcing;
- CPS 232 Business Continuity Management; and,
- CPS 235 Managing Data Risk.

10. APRA uses IT risk specialists to complement line supervisors and bolsters their organizational capacity with third party experts for deeper assessments where necessary. In terms of coordination with other regulators, APRA cooperates with the Council of Financial Regulators' Cybersecurity Working Group and engages with the Australian Federal Government to consult on the development of the next national cybersecurity strategy to ensure the best response to this evolving threat.

11. APRA issued a Cybersecurity Strategy that builds on previous strategic initiatives including the delivery of APRA's information security prudential standard and prudential guidance and establishing a notification and response process for material cyber incidents. The Strategy was informed by consultation with the Department of Home Affairs, as well as Treasury, ASIC, and the Reserve Bank of Australia, and is designed to complement Australia's Cybersecurity Strategy 2025.

12. The Strategy comprises three primary focus areas.

- First priority is to establish a baseline of cyber controls by reinforcing the embedding of non-negotiable cyber practices, facilitating better sharing of cyber information and enabling more effective incident response processes.
- Second priority is to enable boards and executives of financial institutions to oversee and direct correction of cyber exposures.
- Third branch of APRA's new Strategy is to rectify weak links within the broader financial eco-system and supply chain by fostering the maturation of provider cyber-assessment and assurance and harmonizing the regulation and supervision of cyber across the financial system.

13. APRA has also implemented a one-off tripartite independent cybersecurity reviews across all regulated industries. Starting 2022, APRA will ask boards to engage an external audit firm to conduct a thorough review of their CPS 234 compliance and report back to both APRA and the board.