BRICS
INDIA 2021

Compendium
BRICS BEST PRACTICES

Information Security Risks: Supervision and Control

India | 2021

BRICS Rapid Information Security Channel

Contents

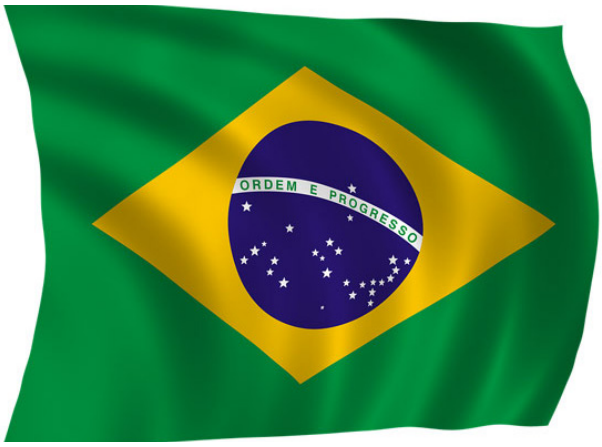
Foreword

Financial Institutions transmit private - sensitive data of end users in the course of doing business, and thus it becomes essential to protect such information as well as the systems those process or store this information. As the cyber security attacks have become more frequent and dynamic, the practices followed to identify the information security risks needs continuous upgradation. Better understanding of practices followed by different jurisdictions can help identify the gaps in existing practices and adopt best practices followed to identify specific security risks in best possible manner.

With an aim to build the knowledge network on digital information security in the finance sector across BRICS, among other activities of BRICS Information Security Channel (BRISC), the compilation of Best Practices in Information Security was envisaged to be carried out in four broad topics - 1. System of data exchange on information security risks 2. Information security risks supervision and control 3. Fintech information security strategy 4. Digital Payments Information Security Strategy. In the year 2021, the members have decided to compile the best practices in the area of “Information Security Risks – Supervision and Control”. This is mainly done by referring to - 1. Basic Governance Structure 2. Best practices followed in supervision by the individual regulator or supervisor 3. Best practices followed by banks based on learning from supervisory exercises.

It is hoped that this compilation will give 360-degree view of best practices followed in perspectives of both regulators as well as regulated entities.

Brazil

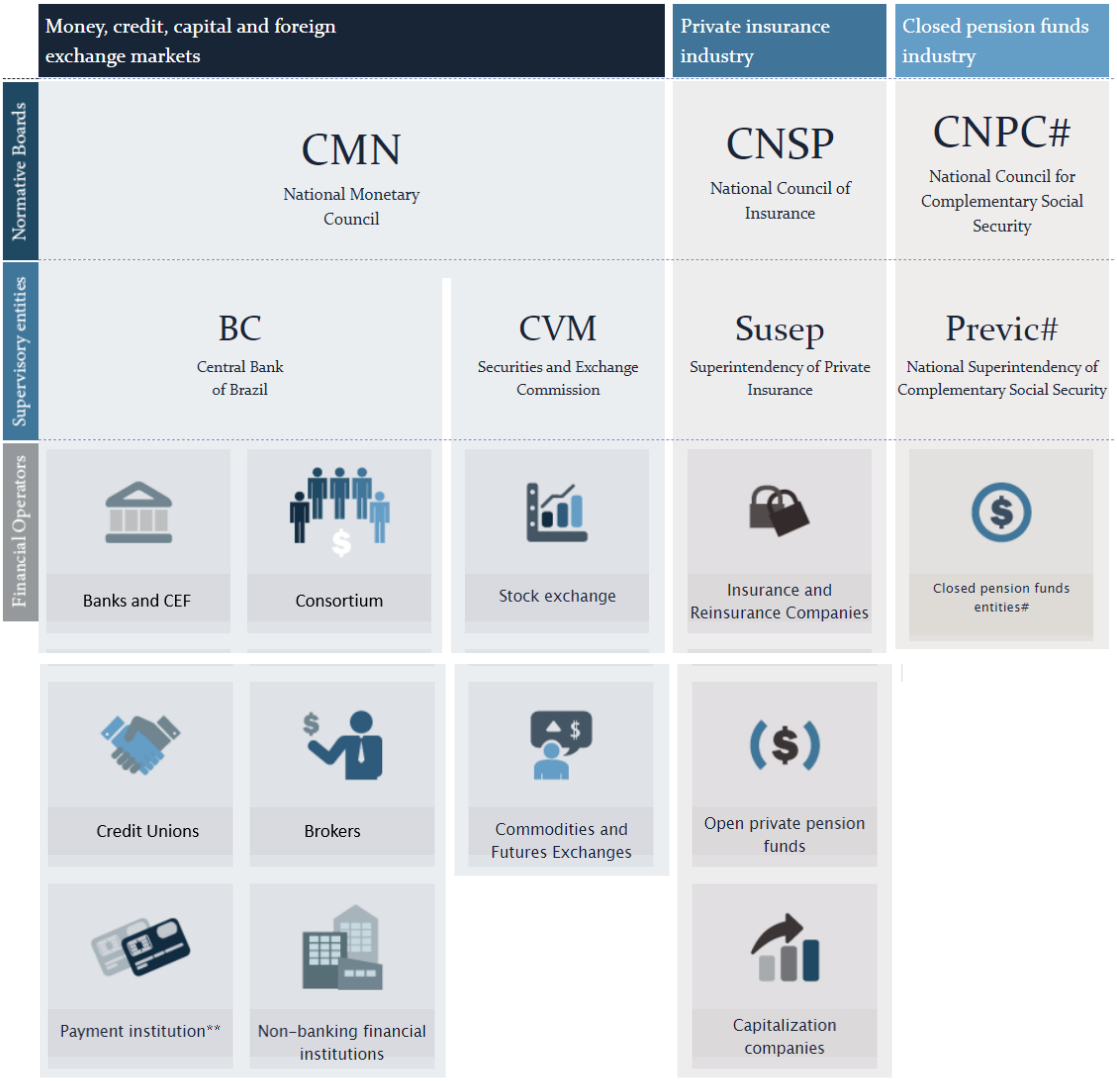


Develop Control Environment among Financial Institutions and guide them to mitigate the IT and cyber risk in order to disseminate cyber security culture in the country.

Section 1: Overview of Governance Structure

The Central Bank of Brazil (BCB) performs its functions as monetary, regulatory and supervisory authority in accordance with guidelines issued by the National Monetary Council (CMN).

The figure below illustrates the types of institutions regulated by the Central Bank of Brazil:



English version is not available for the moment.
* There may be shared regulatory competence with the CVM, depending on its activities.
** The payment institutions are not within the SFN, but are regulated and supervised by the CMN and the Banco Central do Brasil.

Within the BCB, the Prudential and Foreign Exchange Regulation Department (Dereg) and the Financial System Regulation Department (Denor) are responsible for the financial regulation, including cyber security topics considered within the operational risk management framework. The Departments under the Deputy Governor for Supervision are responsible for the Financial System monitoring and for the prudential supervision of supervised entities.

The BCB's supervision implements a risk-based approach. The supervisory teams continuously evaluate the risk profile and the implemented controls of supervised institutions. The procedures and controls related to the management of cyber inci-

dents by supervised institutions are evaluated within the IT risk assessment.

BCB's sanctioning process is provided by Law n° 13,506, of November 13, 2017, which provides for infractions, penalties, coercive measures, and alternative means of dispute resolution applicable to financial institutions and other institutions supervised by the Central Bank of Brazil and participants of the Brazilian Payment System.

Finally, it is important to highlight that BCB has no coercive, investigative, or criminal attributions related to cyber incidents/crimes. In addition, data protection issues are under responsibility of the National Data Protection Authority (ANPD).

Section 2: Best practices in Supervision

Due to the large discrepancy in size, complexity and maturity of institutions operating in the National Financial System (SFN), regulation and supervision are established considering the characteristics of financial institutions, the inherent risks of their operation, and the controls used to mitigate the risks incurred.

Institutions should have a control environment adequate to mitigate their exposures to the risks (e.g., IT risk) incurred. For instance, systemic institutions should have more robust controls than smaller institutions.

The table below shows the evolution of the BCB's supervisory universe:

Resolution CMN 4,553, of January 30, 2017[1] settled rules for allocation of financial institutions and other institutions licensed by the BCB into segments S1, S2, S3, S4 and S5 for the purposes of proportional implementation of prudential regulation. The segmentation classification is one of the variables considered when determining the supervisory cycle for banks, which duration can range from 1 to 3 years, where risks and controls are evaluated, with the participation of specialized teams and direct supervision teams. In addition, during periods between risk and control inspections, direct supervision teams updates and monitors institutions in the ongoing supervisory process. This risk and control information is used to build risk and controls matrix, calculate residual risk, and guide potential regulatory needs and specific supervisory actions according to the identified risks.

In a simplified way, more complex institutions typically have a greater the number of products offered to customers and use a greater the number of channels of interaction with customers and the financial system, resulting in increased inherent risk given its greater exposure to IT and cyber risk. The Brazilian Financial System regulation is typically principle-oriented, i.e., the required controls are not explicitly mentioned in its regulations. However, it provides the Guide to Supervision Practices (GSP), which cites the practices expected for risk mitigation, including information technology and information security.

When evaluating information security controls, the controls and practices adopted are evaluated, and their sufficiency is evaluated considering the risk profile of the FI.

Inspections consist of application of questionnaires, execution of tests, conducting interviews and meetings with those responsible for risk control and management. Meetings are also made with users of the systems to verify that the security and

1 https://www.bcb.gov.br/content/financialstability/Brazilian_Prudential_Financial_Regulation_Docs/ResolutionCMN4553.pdf

control policies are implemented as proposed in the manuals and internal policies of the FIs.

Regarding cyber security, The BCB does not require the implementation of specific controls but requires that they must be formalized and approved by the Board/ Senior Management. The Board and Senior Management are also responsible to extensively disseminate cyber security culture. The security policies should be widely disseminated for all employees, whether on the intranet, in training programs, or other sharing tools, and this dissemination must be verifiable.

The BCB does not determine that FIs should adopt any specific framework. Each framework has its own characteristics and benefits, so BCB seeks to consider the most up-to-date practices. BCB has its own assessment methodology, which uses concepts of COBIT 5, ITIL and NIST, among other frameworks. Similarly, BCB encourages FIs to analyze their own characteristics and use one or more frameworks, or either your custom framework, that are best suited to their risk and operational profiles.

Section 3: Best practices in the area of information security in banks

Recently, Resolution 4,893 of February 26, 2021, was published by replacing Resolution 4,658 of April 26, 2018 from July 1st, 2021. The updated regulation requires financial institutions to define and document the criteria/triggers considered when declaring an operational crisis. Similarly, the regulation for payment institutions was also updated with the publication of Resolution BCB No. 85, of April 8, 2021, which replaced Circular 3,909 of August 16, 2018.

When evaluating the cyber security policy and controls of a supervised institution, the BCB considers that:

- the scope of institution's information security and cybersecurity strategies/frameworks is not limited to the institution itself and includes relevant services eventually provided by third parties (i.e., outsourcing of IT services).
- the institution is responsible for data and systems hosted in IT environments operated by third-party companies such as cloud computing providers. The institution should adequately manage supply chain risks.
- Security management and recovery plans should provide for scenarios of events and incidents that have occurred in third-party companies.
- Institutions are expected to ensure cybersecurity of third-party contracted services, assessing the risks and controls related to such outsourcing.

The BCB assesses institution's cyber risk mitigation plans and measures, including issues related to cyber incident management such as information sharing on incidents/attacks and the implementation of measures to mitigate the impacts on the occurrence of relevant incidents.

The Financial Institutions should also elaborate an annual report on the implementation of the Incident Action and Response Plan, which should include:

I – The actions to be developed by the institution to adapt its organizational and operational structures to the principles and guidelines of its cybersecurity policy.

II – Routines, procedures, controls, and technologies to be used in incident prevention and response in compliance with cybersecurity policy guidelines.

III – The area responsible for recording and controlling the effects of relevant incidents.

This report shall be available to the BCB, which will make its analysis during the ongoing supervisory process.

During inspections, institutions may be asked to report incidents and attacks, as well as results of investigations and measures taken to correct incidents and correct/mitigate weaknesses found.

Financial Institutions are also required to define and document a policy for classifying the relevance of cyber events/incidents. Based on this policy, institutions should report relevant cyber events to the BCB, including relevant incidents that impacted services provided by third parties.

Institutions should also classify the relevance of data processing and storage services provided by third-party, including cloud computing services. The criteria used to classify the relevance of incidents should be registered and available for BCB consultation. The contracting of relevant services should be reported to BCB in an electronic form made available for this purpose. With this information, BCB can map concentration in certain relevant service providers, acting when a risk is detected in shared SFN providers, triggering closer monitoring by direct supervision. Thus, BCB is working on tools to monitor systemic risks arising from the concentration of suppliers, e.g. when relevant incidents with potential for dissemination occur.

Today BCB is developing several initiatives to promote the SFN cyber resilience in the face of accelerated innovation/digitization. These initiatives are part of the BC# Agenda, with emphasis on the Cyber Resilience Improvement Program of the SFN and the Brazilian Payment System (SPB) - Parc[2].

With the implementation of Parc, the BCB, in addition to the continuous evaluation of security controls of the most relevant supervised institutions (e.g., systemically important banks, relevant credit unions and FMIs), intends to:

- Establish risk profiles - scope: cyber risk and fraud risk in high-value payment systems.
- Set minimum cybersecurity controls based on the risk profiles.
- Define and coordinate cyber exercises focused on the financial sector.
- Identify enhancements to fraud detection in high-value payment systems.

Since 2020, BCB has also organized the Operational Resilience Forum, which is a group composed by financial system class entities, aiming at sharing best cybersecurity practices, and actively discussing common issues and concerns. As initial results, the BCB had:

- The organization of multisectoral roundtables between the financial sector and relevant sectors such as Telecom.
- Agreeing on the need to develop campaigns by financial institutions on information security, frauds, and phishing.
- The dissemination of good practices of digital onboarding of clients.

Among other means of dissemination of good practices, BCB has been providing studies and addressing the theme in articles published in Financial Stability Reports and partici-

2 Please refer to the Financial Stability Report (REF) published in May 2021- https://www.bcb.gov.br/en/publications/financialstabilityreport/202104

pating in events to disseminate information and practices related to cyber resilience.

The BCB has also been participating in the Annual Cyber Guardian Exercise. With 39 participating organizations and 211 observers at the last event (2019), the cyber exercise includes TableTop simulations, a study groups for discussions and stock propositions in the field of cyber security and a virtual simulated environment to test cyber incident response capabilities. This cyber warfare exercise is organized by the Brazilian army and the BCB is the crisis coordinator of the Financial Sector.

It is also important to monitor new trends and map emerging risks to information and cyber security. In this way, BCB is also developing some strategic initiatives:

- The Laboratory of Financial and Technological Innovations (LIFT).
- Regulatory SandBox – tracking disruptive innovations, seeking to early identify the risks involved.
- CBDC - study of digital currencies for the possible creation of Real Digital.

Finally, the Financial Stability Report published in October 2020[3] has a study that consolidates the security controls implemented by supervised institutions considering the NIST functions. Although it is a non-exhaustive study, this work can provide good insights regarding the capabilities implemented by Brazilian financial institutions to respond to cyber risk. The table below shows the results of the study:

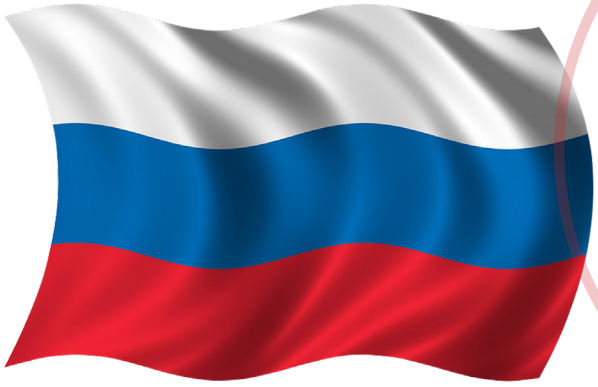
3 https://www.bcb.gov.br/content/publications/financialstabilityreport/202010/fsrFullRep.pdf

Table 2.4.4.1 – Percentage of institutions that declared to implement IS controls, grouped by NIST functions

Function	Practices / Procedures / Information Security Controls	S1	S2	S3	S4	S5	Credit Union (System)	Payment Institutions
Identify	Vulnerability analysis (IT environment)	100%	100%	89%	53%	57%	67%	85%
	Pentest - Penetration Testing	100%	100%	86%	42%	33%	67%	85%
	Vulnerability analysis (IT systems)	100%	100%	81%	42%	59%	67%	85%
	Evaluation of security controls prior to contracting relevant services	100%	83%	92%	68%	60%	33%	46%
	Red Teaming	83%	50%	38%	10%	2%	0%	62%
Protect	Protection against malicious software (antivirus, antimalware, others)	100%	100%	100%	94%	83%	83%	92%
	Backup of data and information	100%	100%	97%	92%	79%	100%	100%
	Computer network segmentation / segregation of environments	100%	100%	95%	75%	61%	83%	85%
	Management of cryptographic keys and digital certificates	100%	100%	89%	57%	56%	83%	69%
	Logical Access Management	100%	83%	97%	76%	58%	100%	92%
	Cryptography	100%	83%	86%	56%	54%	100%	77%
	MDM - Mobile Device Management	100%	83%	76%	25%	5%	33%	54%
	Patch Management	83%	100%	89%	68%	49%	83%	85%
	Secure systems development	83%	100%	51%	33%	51%	50%	69%
	Password vault	67%	67%	73%	33%	11%	50%	46%
	Network Access Control (NAC)	67%	33%	49%	41%	46%	50%	62%
	Web Application Firewall (WAF)	50%	67%	62%	52%	29%	83%	85%
Protect / Detect	Prevention of DDoS (Distributed Denial of Service) attacks	100%	83%	81%	60%	47%	100%	69%
	Data Loss Prevention - DLP	83%	50%	68%	32%	16%	33%	38%
	Anti-APT (APT - Advanced Persistent Threat)	83%	17%	51%	25%	10%	33%	31%
	Cloud Access Security Broker (CASB)	33%	17%	24%	11%	4%	17%	38%
Detect	Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)	100%	100%	95%	68%	47%	100%	69%
	Traceability mechanisms, including audit trails and log implementation	100%	100%	89%	74%	55%	83%	85%
	Log correlator / Security Information and Event Management (SIEM)	100%	67%	65%	26%	7%	33%	69%
Detect / Respond	Cyber incident management	100%	100%	76%	72%	63%	33%	77%
	Security Operations Center (SOC)	100%	67%	68%	29%	27%	33%	54%
Respond	Mitigation of impact of relevant incidents	100%	67%	73%	63%	54%	50%	77%
Respond / Recover	Establishment of procedures to be followed in case of interruption of relevant services	67%	67%	51%	45%	51%	33%	54%
Recover	Procedures for reporting crisis situations to the BCB	100%	100%	81%	62%	54%	67%	62%
	Definition of RTO (Return to Operation) for relevant activities or services	100%	100%	78%	72%	60%	67%	62%
	Definition of incident scenarios to be considered in business continuity tests	100%	83%	65%	64%	57%	67%	69%

Universe of surveyed institutions: 6 institutions in the S1 segment, 6 institutions in the S2 segment, 37 institutions in the S3 segment, 236 institutions in the S4 segment, 237 institutions in the S5 segment, 6 cooperative systems and 13 payment institutions.

Russia



Establish information security requirements and monitoring compliance to ensure financial resilience and operational reliability.

Section 1: Overview of Governance Structure

The Bank of Russia's mandate with regard to Information Security covers establishing mandatory information security requirements and monitoring compliance therewith.

The mandatory information security requirements cover the following:

1) for conducting banking activities, with a view to countering unauthorized money transfers, except for the information security requirements set forth by federal laws and other regulatory acts adopted thereunder, as per Article 57.4 of Federal Law No. 86-FZ, dated 10 July 2002, "On the Central Bank of the Russian Federation (Bank of Russia)" ("Federal Law No. 86-FZ").

2) for conducting activities in financial markets envisaged by Article 76.1, Part 1 of Federal Law No. 86-FZ, with a view to countering illegal financial transactions, except for the information security requirements set forth by federal laws and other regulatory acts adopted thereunder, as per Articles 76.1 and 76.4-1 of Federal Law No. 86-FZ.

3) for performance of money transfers by money transfer operators, bank payment agents (subagents), information exchange services operators, payment applications providers, payment systems operators, payment infrastructure services providers, with a view to ensuring information security in the payment system, as per Article 27, Part 3 of Federal Law No. 161-FZ, dated 27 June 2011, "On the National Payment System" ("Federal Law No. 161-FZ").

The Bank of Russia establishes mandatory information security requirements for the cases specified under Items 1-3 in coordination with the federal executive body authorized to ensure information security as well as the federal executive body authorized to counter gathering of technological intelligence and maintain technological information security (as per Article 27, Parts 2 and 3 of Federal Law No. 161-FZ; Articles 57.4, 76.1 and 76.4-1 of Federal Law No. 86-FZ.).

In order to improve and specify provisions for every case described in Items 1-3, dedicated by-laws have been developed and implemented, along with respective standardization documents.

Section 2: Best practices in Supervision

Key objectives, tools, and the scope of best supervision and control practices

In accordance with best supervisory and control practices in the field of information security, the regulator pursues the following key objectives:

- ensuring financial resilience and operational reliability both of financial institutions and financial ecosystems, and of the national financial market as a whole;
- ensuring that the actual level of risk of information threats materializing does not exceed the tolerated level as per applicable risk level benchmarks;
- integrating a system designed to manage the risk of information security threats materializing into the financial institution's overarching risk and capital management system;
- promptly responding and adapting to the transformations of relevant information threats (within the institution and beyond) that could be tolerated in accordance with the risk level benchmarks in use.

The tools for implementing best practices include the following:

- Regulation;
- Standardization;
- Operational risk management.

The subject of regulation is information protection.

Standardization is aimed at developing technical tools and building infrastructure, including platforms for standardization and compliance assessment (voluntary certification systems), in the following areas: managing the information security risk, operational reliability, and information protection.

Scope covers credit institutions, non-credit financial institutions, financial cooperatives, and ecosystems.

Subject matter of regulation can be divided into three core domains:

1. Information infrastructure security;
2. Financial applications security;
3. Financial technologies security.

Key areas of supervision and regulation

We distinguish seven (7) key areas of the Bank of Russia's regulatory and supervisory activities with regard to information security risk in finance, namely:

1. Identifying infrastructure;
2. Establishing and monitoring risk indicators;
3. Corporate governance;
4. Risk assessment;
5. Response and recovery;
6. Cyber drills;
7. Registering incidents.

1. Identifying information infrastructure

The Bank of Russia designs and introduces reporting forms, and develops the standard determining the procedure for identifying information infrastructure.

This helps shape the scope of regulation in order to conduct monitoring activities for further assessment.

This stage also lays the groundwork for developing a system of risk level benchmarks, as well as for building a system of key information risk management indicators (including key indicators of risks that are subject to monitoring and control).

2. Establishing and monitoring indicators

Information security risk (cyber risk) is a part of the operational risk. In view of this and in line with its regulating activities, the Bank of Russia has established corresponding requirements in a dedicated regulatory act on managing the operational risk – Bank of Russia Regulation No. 716P, dated 8 April 2020, "On the Requirements for the Operational Risk

Management Systems in Credit Institutions and Bank Groups" ("Regulation No. 716-P"). Regulation No. 716-P contains requirements for proper management of the operational risk, including the information security risk (Chapter 7). One of such requirements demands setting risk level benchmarks, which are determined with regard to the information security risk as well. Compliance with such risk level benchmarks is essential for proper management of the information security risk.

3. Corporate governance

It is mandatory to build organizational systems and design processes aimed at managing the operational risk with respect to information security. The institution may be held responsible for improper management of its operational risk, including the information security risk.

4. Assessing information security risks

It is also mandatory for a corporate governance body to establish and review control and signal values for risk level benchmarks related to the institution's operations. In the course of its supervisory activities, the Bank of Russia conducts an assessment of whether such benchmarks were properly set, taking into account the specificities of the particular business.

5. Response and recovery

The capacities of a financial institution to respond and recover should a cyber risk materialize are also subject to evaluation.

6. Cyber drills

Cyber drills are designed to hone personnel's skills with respect to detecting and responding to incidents connected with information security risks. Besides, it is necessary to assess the credibility of a financial institution's risk profile with respect to information security; the risk profile is drafted on the basis of data submitted to the Bank of Russia through regularly scheduled reporting and incident reporting, and during inspections.

7. Registering incidents (prompt information exchange)

The Bank of Russia has set up a procedure for reporting information security incidents, computer attacks, etc. in order to ensure prompt response and appropriate measures. Furthermore, important measures to mitigate major information security risks include developing and introducing a voluntary certification system (VCS) in order to monitor the quality of assessment with regard to conformity and compliance with the requirements under applicable standards. We expect that the creation and implementation of a VCS will contribute to efficient application of standards related to the technologies standardized by the Bank of Russia and the professional community. The closest equivalent to this set-up is the system of voluntary certification of conforming to the standards issued by the PCI Security Standards Council, ISO/IEC 27001, and similar standards that also provide for a conformity assessment system and certification.

In terms of approaches to putting together a particular set of information security requirements, a good example could be Bank of Russia Regulation No. 719-P, dated 4 June 2020, "On the requirements for ensuring information security when executing money transfers and on the procedure for monitoring the compliance with information security requirements when executing money transfers".

The requirements under this regulation include:

1. Requirements for the information infrastructure used to execute money transfers;
   - compliance with National Standard of the Russian Federation GOST R 57580.1-2017 "Security of financial (bank) operations. Protection of financial institutions' information. Basic set of organisational and technical measures";
   - regular assessment of such compliance.
2. Requirements for automated systems' software and applications – certification or conformity assessment as per the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408, EAL4+).
3. Organizational requirements:
   - testing for breaches;
   - reporting incidents;
   - protecting personal data;
   - complying with the requirements for the use of cryptographic methods of information protection;
   - validating email addresses and other data.

4. Requirements for information protection functions engaged in the technological processes of executing money transfers:
   - client identification, authentication, and authorization;
   - generation (preparation), transfer and reception of electronic messages;
   - verifying that the clients are authorized to manage funds;
   - executing operations and recording the results of money transfers;
   - storing electronic messages and details regarding the money transfers executed.

Russia hosts Technical Committee No. 122 "Financial Operations Standards", Subcommittee 1 "Security of Financial (Banking) Operations" ("TC 122"; website: http://www.tk122.ru/pk1/about/), which is a mirror committee to ISO/TC 68/SC 2 "Financial Services, security" (website: https://www.iso.org/committee/49670.html).

TC 122 serves as a discussion platform for the Bank of Russia and financial market participants, allowing them to consider technical issues, including matters of cybersecurity. Following such discussions, TC 122 develops national standards of the Russian Federation, which are adopted in due course and reflected in the supervisory activities of the Bank of Russia.

Section 3: Best practices in the area of information security in banks[1]

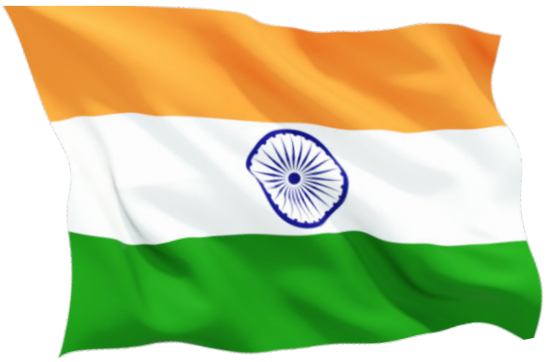
As part of its supervisory activities dedicated to ensuring information security of financial institutions, the Bank of Russia takes the following measures.

1. An individual risk profile is compiled for every financial institution regulated by the Bank of Russia. The Bank of Russia has developed and enacted methodological recommendations with regard to risk profiling of institutions under its supervision.

1 Based on learnings from supervisory exercises.

2. The data for calculating the risk profile indicator is drawn, among other sources, from the Bank of Russia Automated Incident Processing System (AIPS FinCERT). This system enables prompt interaction with information exchange participants (credit and non-credit financial institutions) on incidents that have taken place, including operational reliability incidents.
3. Bank of Russia's interaction with information exchange participants has been formalized under Bank of Russia Standard STO BR BFBO-1.5-2018 "Security of financial (banking) operations. Managing information security incidents. On the forms and timeframes for the Bank of Russia's interaction with information exchange participants when detecting incidents related to the violations of information protection requirements" ("STO BR BFBO-1.5-2018").
4. In addition, with a view to enhancing the effectiveness of measures for monitoring (supervising) the activities of financial institutions, the Bank of Russia conducts certain activities (cyber drills) as part of supervisory stress testing in the field of information security. The main objective of these activities is to assess the accuracy of the developed risk profile of supervised institutions and financial associations. These activities are aimed at examining various scenarios of computer attacks. That said, the transition from formal inspections to cyber drills will allow to promptly detect specific vulnerabilities of information security processes at supervised institutions and associated risks, which in turn will allow for effective advisory supervision with regard to the activities of a certain financial institution while taking into account its risk profile.

India



Enhance the cyber security posture of the banking and payments system with appropriate regulation to safeguard customer's interest and ensure financial stability.

Section 1: Overview of Governance Structure

Cyber Security as a subject matter is the responsibility of the Ministry of Electronics and Information Technology (MeitY), Government of India. MeitY formulated the Information Technology (IT) Act 2000 and is also the custodian of the IT Act. Under IT Act following two organizations were set up:

1) Indian Computer Emergency Response Team (CERT-In) was set up under Section 70B of the IT Act to deal with and respond cyber incidents. CERT-In works 24x7 proactively and reactively to secure the cyber space in the country. CERT-In is designated as the national nodal agency for 24x7 incident response. CERT-In is under the administrative control of MeitY.

2) National Critical Information Infrastructure Protection Centre (NCIIPC) was set up under Section 70A of the IT Act to protect critical information infrastructure in the country. It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection. NCIIPC is a unit of National Technical Research Organisation (NTRO), Government of India.

Cyber-crime as a subject matter comes under the purview of the Ministry of Home Affairs. Ministry of External Affairs, Government of India does cyber diplomacy with other countries and engages in cyber dialogue. They also participate in United Nations Group of Governmental Experts' (UNGGE) meetings. National Cyber Security Coordinator (NCSC) is responsible for coordination with all Ministries and Departments and agencies for cyber security in the country

The financial system in India is primarily regulated by four authorities – the Reserve Bank of India (banks, non-bank lenders and credit information companies), Securities and Exchange Board of India (securities and commodities market), Insurance Regulatory and Development Authority of India (insurance entities) and Pension Fund Regulatory and Development Authority of India (pension funds). The regulatory entities coordinate their activities at the Financial Stability and Development Council for a stable financial intermediation ecosystem and sound macro prudential regulation of the economy.

The Reserve Bank of India, in 2016, established an exclusive Cell in its supervisory vertical to assess and strengthen the cyber security posture of banks in the country. A Standing Committee on Cyber Security comprised of experts from academia and industry advises the Cell on regulatory and supervisory actions.

The regulatory authorities in the country work closely with agencies dedicated to strengthening the cyber security preparedness of India which include CERT-In, NCIIPC and other relevant agencies.

The following sections will concentrate on the central bank and the banking sector

Section 2: Best practices in Supervision

a) Regularly assessing the cybersecurity risk of regulated entities based on Key Risk Indicators (KRIs) covering key domains of cyber security. Analysing the data collated post analysis of the KRIs, tracking the deviations from baselines to derive a KRI score for each regulated entity and advising entities on corrective action.

b) Periodically assessing the compliance of regulated entities with supervisory instructions and communicating the areas of improvement to non-compliant entities.

c) Regular issuance of Advisories (based on learnings from cyber security incidents) and Alerts (market intelligence) to entities for improving and protecting the cyber security posture of the entities.

d) Regularly carrying out security audit of IT infrastructure, web applications and websites on periodic basis to check resilience of cyber assets against malicious attacks.

e) Frequently subjecting regulated entities to IT examinations/inspections touching upon broad areas of Application Security, Network Security, Database Security, Hardening of databases and servers, Electronic Fraud Risk Management etc and sharing a detailed report on the specific deficiencies observed and directing the entities to furnish the compliance to the observations within specific timelines.

f) Maintaining an open communication channel with the information security and compliance functions of regulated entities to articulate regulatory expectations, keep abreast with recent developments in the cyberspace and get feedback from the ground on challenges faced by regulated entities in strengthening their cyber security posture.

g) Conducting Cyber Drills to assess the incident response plan/management of the entities and analysing the responses with reference to benchmarks set by the respective regulated entities and communicate the areas of improvement in the incident response plan with the entities.

h) Investing in cutting edge supervisory technology solutions to streamline supervisory activities such as issuance of instructions, planning and managing of on-site supervisory assessments, collection of offsite data from regulated entities and easy incident reporting by regulated entities.

i) Reserve Bank of India has set up an Inter-disciplinary Standing Committee on Cyber Security to, inter alia, review the threats inherent in the existing/emerging technology; study adoption of various security standards/protocols; interface with stakeholders; and suggest appropriate policy interventions to strengthen cyber security and resilience.

Section 3: Best practices in the area of information security in banks[1]

a) Using multiple anti-virus solutions for security updates from multiple sources/channels.

b) Periodically conducting the Asset inventory review to facilitate early identification and off-loading of unused or unsupported assets thereby minimising attack surface area.

c) Subscribing to Threat intelligence and proactively hunting for threats.

d) Leveraging Global Security models and best practices from the parent organization and making them part of the software development process.

e) Following a security by design approach wherein application security [secure coding, OWASP (Open Web Application Security Project) Top 10 *etc.*] is ensured in software development life cycle.

f) Not allowing Screenshots to be taken during the ongoing session of mobile banking for

1 Based on learnings from supervisory exercises.

sensitive screens.

g) Customer education and awareness on platforms such as mobile application, website.

h) Having a robust and automated patch management policy for network devices, servers and applications.

i) Testing the disaster resilience and business continuity preparedness of the entity's IT systems by conducting drills during working days and for extended periods.

j) Ensuring strict separation of responsibilities and periodic rotation of personnel manning critical roles as a fraud prevention measure.

k) Taking a daily backup of network configuration to review configuration changes from previous day to today.

l) Implementing an ATM Terminal Security solution to enforce regulatory compliance in ATM terminals having such as Time-based Access Management, BIOS (basic input/output system) Password, USB (Universal Serial Bus) Protection, EJ(Electronics Journals) Pulling, Operating Systems and Access Privileged Management, LAN (Local Area Network) Monitoring, Application Whitelisting, Full Hard Drive Encryption

m) Allowing customers to set Personalized transaction limits depending on the nature of the transaction.

n) Disabling user logins during weekends and long holidays to prevent unauthorized access to the application during such periods.

o) Exchanging a key for every session between application and the server, which expires when the session terminates, thereby eliminating any possibility of session duplication

p) Implementing defence in depth wherein multiple security controls are deployed such as Firewall, IPS (intrusion prevention system), anti-DDoS (Distributed Denial of Service) solutions, CDN (Content Delivery Network) for static site etc.

q) Customer centric malware detection solution to mitigate client-side vulnerabilities, which helps to ascertain the presence of malware in the system, while the customer uses online banking account. In case of any identified infection, impacted customers are called and advised to get the infected malware removed by using legitimate anti-virus tools.

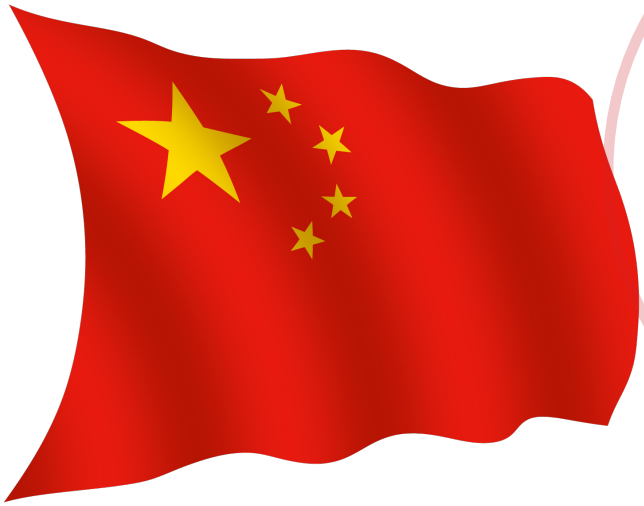
r) Implementation of Domain-based Message Authentication, Reporting and Conformance (DMARC) in "block mode", across all domains.

s) Real-time risk assessment engine is deployed for evaluating the risk of each transaction against the rules defined in the system such as negative accounts/ blacklisted IPs etc.

t) The remote connections to the network and security devices are encrypted. The devices accept remote connections only from identified hardened systems designated for the business purpose.

u) All the default credentials configured by the Original Equipment Manufacturer (OEM) are changed before implementing the devices in production environment.

China



Formulate the development plans, rules, regulations and standards to strengthen the protection of network security of financial institutions.

Section 1: Overview of Governance Structure

At national level, Cyberspace Administration of China is responsible for the overall coordination of cyber security work and related supervision and management. The public security authorities are responsible for the supervision, inspection, and guidance of graded protection of cybersecurity, as well as preventing and punishing cybercrimes. In terms of laws related to cyber security, with the formal implementation of the *Cyber-Security Law of the People's Republic of China* in June 2017, a top-level architecture for cyber-security was established.

The People's Bank of China (PBC) is responsible for directing the cybersecurity and informatization work in the financial sector, taking the lead in formulating the development plans, rules and regulations, and standards related to cybersecurity and data security, coordinating and directing cybersecurity incident notification, emergency drills and the protection of network security of critical information infrastructure.

China Banking and Insurance Regulatory Commission (CBIRC) is responsible for supervision and inspection of information technology risks of banking and insurance institutions. China Securities Regulatory Commission (CSRC) is responsible for information security management, supervision and inspection of the securities and futures industry.

Section 2: Best practices in Supervision

The PBC is responsible for directing the cybersecurity and informatization in the financial sector. Aiming at strengthening management policies, technical means and talent cultivation, the PBC keeps improving the quality of regulation and enhancing the cybersecurity capacity of the financial industry.

Firstly, improving the regulatory and standardization system. The PBC earnestly implements the *Cybersecurity Law of the People's Republic of China* and other domestic laws, establishes and improves the financial cybersecurity policies, so as to set the compliance bottom line for financial institutions. Besides, the PBC makes efforts to coordinate the national and local financial supervision authorities to form a supervision synergy with clear division of supervision duties among various authorities.

Secondly, enhancing technical capabilities. On the one hand, the PBC has been improving cyber threat information sharing and the mechanism for joint prevention of risk events in the financial sector. On the other hand, supervisory technology is employed to strengthen cybersecurity risk monitoring and early warning. These efforts gradually reinforce the supervision for the financial cybersecurity. Thirdly, enhancing the cybersecurity talents team. The PBC has been exploring the training mechanism of cybersecurity talents in financial sector, and training financial cybersecurity talents through skills training, cybersecurity attack and defense drills and other activities. With these efforts, the PBC aims to organize a dedicated team with strong technology background, to improve the cyber emergency support and advance the ability of rapid response in case of cyber threats.

Lastly, innovating cybersecurity supervision approaches. The PBC conducts unannounced emergency drills, which simulates real-world emergency scenarios, to carry out stress tests on financial institutions. Unlike the conventional drill mode, where the drill date is confirmed and the personnel are put in place in advance, the unannounced emergency is

featured with unexpected issuing of instructions and temporary assembling of personnel.

Section 3: Best practices in the area of information security in banks

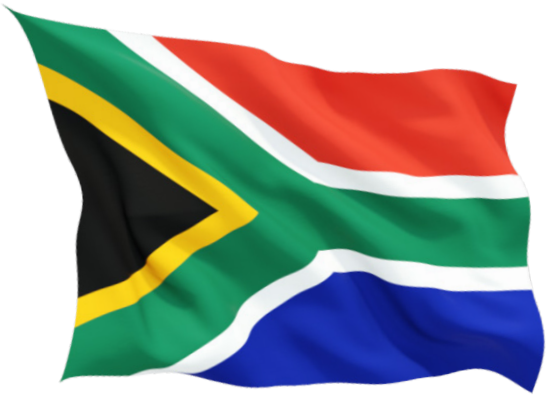
The banking sector takes the following measures to enhance regulatory compliance and management.

- ensure sufficient funds, resources and personnel for cybersecurity and strengthen the security of information infrastructure.
- coordinate the work among information technology department, risk management department, and internal audit department.
- establish internal cybersecurity supporting system, covering cybersecurity strategy, IT organizational structure, asset management, system development and maintenance, outsourcing management, emergency management, risk management.
- carry out dedicated training programs to enhance employees' awareness of cybersecurity. Banks launch online training platforms which offer compulsory courses for all employees and dedicated training program for personnel in key posts, such as registered information security personnel.
- build emergency response capacity. In addition to emergency drills related to infrastructure, network, system, banks also carry out recovery drills simulating interruptions in systems, application, business operation.

In terms of technical protection and control, a multi-perspective network security technology system was established in the banking sector.

- from the perspective of security management, with the help of the centralized log analysis and traffic threat awareness platform, security personnel in banks are able to detect access anomalies, virus events, and malicious attacks, internal wrongdoings in time.
- from the perspective of business operations, banks incorporate cybersecurity into the entire life cycle of IT construction, covering planning, design, development, testing, operation and maintenance.
- from the perspective of attack and defense, banks employ deceptive defense methods to deploy camouflage agents and tracing systems on the Internet and set up traps on the only route hackers use to initiate attacks. Once attacks are launched, security personnel in banks are able to identify and paint portraits of the attackers, facilitating real-time interception and tracing of attacking sources.

South Africa



Adopt a risk-based approach to its supervisory practices that contribute to effective information and cybersecurity risk supervision.

Section 1: Overview of Governance Structure

The South African Reserve Bank (SARB) plays a crucial role in ensuring the resilience of the financial services sector. The SARB's supervisory approach is risk-based, meaning that it is proportionate to the systemic risks posed by the supervised institutions. The Prudential Authority (PA) is an authority within the SARB responsible for the supervision and regulation of the financial sector, i.e. banks, insurers and market infrastructures, to promote and enhance their safety and soundness and support financial stability.

Ministries such as the Department of Communications and Digital Technologies (formerly the Department of Telecommunication and Postal Services) and the State Security Agency (SSA) are involved in national cybersecurity initiatives.

The SARB has established a cyber-resilience governance structure at the financial services industry level, namely the Cybersecurity Resilience Sub-committee (CRS). The financial sector supervisors and regulators are also members of the sub-committee, and the platform is used for cooperation and collaboration as per the terms of reference of the CRS. There are further financial sector associations that specifically focus on their financial entities, including:

a. The SARB:
   - Prudential Authority (PA)
   - Financial Stability (FinStab)
   - Financial Markets Department (FMD)
   - National Payment System Department (NPSD)
   - Group Security Management Department's (GSMD) Cyber and Information Security Unit (CISU)
   - Financial Services Department (Finserv)

b. National Treasury: National Treasury aims to promote economic development, good governance, social progress and rising living standards through accountable, economic, efficient, equitable and sustainable management of South Africa's public finances. As per the Financial Sector Regulation Act 9 of 2017, the National Treasury is a member of the Financial Sector Oversight Committee (FSOC), the Financial Sector Contingency Forum (FSCF) and its related CRS.

c. CyberSecurity Hub: The CyberSecurity Hub is mandated by the National Cybersecurity Policy Framework (NCPF), and is South Africa's National Computer Security Incident Response Team (CSIRT).

d. Financial Critical Infrastructures (FCI) - Cyber (computer) Security Incident Response Team (CSIRT): – The FCI-CSIRT consists of two stock exchanges (JSE and A2X), Strate and BankserveAfrica, SARB (NPSD and CISU), and is an informal grouping. Its primary purpose is to facilitate cyber and information security collaboration to equip its members to be better prepared and able to prevent and respond to cyber security incidents.

e. Financial Sector Conduct Authority (FSCA): The FSCA is the market conduct regulator of financial institutions that provide financial products and financial services, financial institutions that are licensed in terms of a financial sector law, including banks, insurers, retirement funds and administrators, and market infrastructures.

f. Financial Intelligence Centre (FIC): The Financial Action Task Force (FATF) identifies high-risk jurisdictions that have significant strategic deficiencies in their re-

gimes to counter money laundering, terrorist financing, and financing of proliferation. FATF engages in an ongoing process to monitor jurisdictions that have strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. To this end, the FIC issued Public Compliance Communication 42 (PCC 42) which provides clarity on certain provisions of the FIC Act that allow certain supervisory bodies access to facts or information regarding reports submitted in terms of section 29 of the FIC Act 38 of 2001.

g. Banking Association of South Africa (BASA): BASA advises on and acts in the interests of the industry through its engagements with regulators, legislators and stakeholders, to make banking sustainable, profitable and better able contribute to the social and economic development and transformation of the country.

h. South African Banking Risk Information Centre (SABRIC): SABRIC focuses on commercial banks, and it has 20 member banks, ATM provider and two cash-in-transit companies. SABRIC's focus is to keep their clients informed about the latest banking scams and fraudster activities that target the commercial banks.

i. The Association for Savings and Investment South Africa (ASISA): ASISA represents the majority of South Africa's asset managers, collective investment scheme management companies, linked investment service providers, multi-managers and life insurance companies.

j. The South African Insurance Association (SAIA): SAIA is the representative body of the non-life insurance industry. It represents the industry to all relevant stakeholders to ensure a sustainable and dynamic industry. SAIA has 58 members, comprising all categories of non-life insurers, including reinsurers. Its members abide by the SAIA Code of Conduct, which ensures adherence to best-practice industry standards and self-regulation.

k. State Security Agency (SSA): The SSA is the regulator and oversight body for all government departments, agencies and national key points (i.e. critical infrastructures) security (physical, information and personnel security).

Section 2: Best practices in Supervision

The SARB adopts a risk-based approach to its supervisory practices that contribute to effective information and cybersecurity risk supervision. Systemic cyber-related matters are reported to the Financial Stability Committee (FSC), the statutory Financial Sector Oversight Committee (FSOC) and Financial Sector Contingency Forum (FSCF).

The PA has also developed various regulations, guidance, and supervisory practices for the financial sector that address cybersecurity.

a. Although the PA does not prescribe any industry standards and frameworks, it has been recommended to the supervised FIs that they should adopt and adapt established industry standards and frameworks that are fit for purpose to manage their cyber risk. In addition, the standards and frameworks used should be aligned to the institution's internal enterprise risk management frameworks.

b. The PA issued a memo to the BASA in 2013, which was intended to provide a high-level investigation into mobile and internet banking fraud within the South African banking industry.

c. The PA issued an IT risk questionnaire to the banking industry in 2016 as well as to the entire financial sector in 2020, which was intended to provide, among others, an analysis of the IT security and infrastructure risks, including the IT controls that have been

deployed to mitigate existing control weaknesses. In addition, a risk assessment, which is a cyber assessment tool that uses different frameworks such as NIST and ISO 27000, was procured and customised for the SABRIC member banks. The banks that are not members of SABRIC were also requested to complete the assessment tool to determine their cyber risk posture against the principles detailed in Guidance Note (GN) 4 of 2017[1] issued by the PA.

d. Cybersecurity was discussed with Boards of all registered banks in 2016[2] and market infrastructures (MIs) in 2019 as one of the PA's flavour-of-the-year topics to assess cybersecurity risk management practices of the financial services sector.

e. The IT Risk Task Group was established in March 2019 at the BASA to collaborate with the banking industry on issues relating to IT risk management, which would coincidentally include cybersecurity. Similar conversations/ suggestions are being considered for the SAIA and the ASISA.

f. The Operational Resilience Group (ORG), sub-committee of Basel's Standard and Implementation Group (SIG), issued the cyber-resilience range of practices in December 2018. The PA will leverage these learnings to decide further requirements that may be introduced or complement current practices in South Africa.

g. The Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions (CPM-IOSCO) issued cyber resilience guidance for market infrastructures in 2016. The guidance provides authorities with a set of internationally agreed guidelines to support consistent and effective oversight and supervision of FMIs in the area of cyber risk. The PA believed that this was also applicable to banks and as a result, issued GN 4 of 2017.

h. The Financial Stability Board (FSB) was asked to perform a stock-take in 2017 of relevant existing regulations and supervisory practices in G20 jurisdictions, as well as of existing international guidance, including the mandate to identify effective practices to enhance cross-border co-operation. The cyber lexicon was subsequently issued in November 2018 to address cybersecurity and cyber resilience in the financial sector.

The PA is in the process of developing a joint cybersecurity standard as well as an IT risk standard with the FSCA. Furthermore, a cybersecurity questionnaire will be issued to banks, insurers and MIs. A material IT/ cyber incident reporting process will be standardised across the industries.

As part of its supervisory review, the PA monitors policies, processes and practices related to cyber risk and cyber resilience by regulated institutions; 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 conducts on-site as well as off-site reviews through questionnaires, surveys, data centre walkthroughs and industry trend analysis, with the below being some key activities conducted:

a. Information and cybersecurity are discussed as part of the PA's IT risk supervisory programme and included in the agenda for the IT risk on-site meetings. Institutions provide an overview of their frameworks, policies, processes and practices, etc.

b. Ongoing assessment of supervised entities on business / operational resilience.

c. Ongoing assessment of third-party concentration and/or systemic risk in the financial

1 https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-guidance-notes/2017/7803

2 https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-guidance-notes/2016/7109

sector.

d. Recovery and resolution planning (RRP) reviews included in the supervisory programme.

e. Continued involvement in supervised entities' crisis simulation tests where a cyber-attack has been identified as the crisis event.

During the supervisory programme, challenges experienced are discussed either bilaterally or through industry associations to identify possible mitigations. Some of the challenges noted include:

- The continued drive for the use of emerging technologies to gain competitive advantage without assessing the underlying cybersecurity risks.
- Unavailability of data with regard to cybersecurity risks for certain emerging technologies.
- Limited skills, competence and capability for certain emerging technologies both locally and internationally.
- Evolving cyber-attacks and the fact that most supervised Financial Institutions (FI) cannot define insurance requirements for their cyber-risk exposure.
- Segregation of duties between the information security operations and oversight functions.
- The rising cyber dependency outside of the financial sector, spilling into the financial system.
- The lack of research into the interconnectedness and interoperability of institutions, especially the financial sector with the non-financial sector.
- The probable high replacement costs, falling profitability and negative impact on balance sheets of FIs in the event of a cyber-attack, which may become systemic.

Section 3: Best practices in the area of information security in banks

The PA observed that the South African financial services sector continually implemented controls to mitigate against emerging trends such as data breaches, business disruption and fraud. It has been observed through various interactions with the regulated FIs that disparate frameworks or standards such as NIST, CIS Critical Security Controls, ISO 27001, ISO 27002, COBIT, Information Security Standard of Good Practice, and PCI-DSS are used. In addition, institutions are required to follow the CPMI-IOSCO cyber resilience guidance as per GN4/2017.

Some of the common practices that FIs have adopted based on the above frameworks includes:

Governance

- The governance processes are measured in terms of the effectiveness and efficiency of security in delivering business value.
- The bigger financial institutions have appointed a Chief Information Security Officer (CISO) to execute cybersecurity strategy and framework.
- Information security governance had been strengthened to include the cyber-attack team (red team). The red team includes the "Ethical Hackers", which are employed to try and compromise IT systems; the emergency team (blue team) for responding and

recovering in the event of an attack as well as the governance team (purple team) for intelligence gathering and policy / procedure formulation.

- Most institutions have implemented security policies according to their appetite and defined and documented the institution's established position about the security risks.

Information Classification and Protection

- Most institutions have identified their "Crown jewels". They have also established an inventory of assets that support business and the delivery of services, including those managed by third parties.
- Information assets classification are based on the sensitivity, business criticality, and the impact that a compromise could result in.
- The inventory is reviewed periodically, but at least annually and updated whenever there are changes.

Identity and Access Management

- Identity and Access Management is automated in most institutions, where role definition is performed by both business and IT.
- Users are assigned roles based on their job functions and responsibilities.
- User access is revoked in instances where changes occurred to any user profile.
- User access are reviewed periodically.

Vulnerability and Patch Management

- Institutions have established processes for identifying, assessing and resolving security weaknesses in their IT environment;
- Institutions ensure that security patches are applied to address vulnerabilities to every IT system;
- Instituttions ensure that security controls are instituted to reduce any risk posed where there is no security patch available to address vulnerabilities identified; and
- Institutions ensure that patches are tested before they are applied to the IT systems in the production environment to ensure compatibility with existing IT systems or they do not introduce problems to the IT environment.

Secure Configurations

- Most institutions ensure that there is a written set of security standards for hardware and software (e.g. operating systems, databases, network devices and endpoint devices).
- Security standards are in place that outline the configurations that will minimise their exposure to cyber threats and are reviewed periodically for relevance and effectiveness.

Incident Management

- Institutions have established incident response and management plans to swiftly isolate and neutralise a cyber threat and to securely resume affected services. The plans describe communication, coordination and response procedures to address plausible cyber threat scenarios.

Information Systems Security

- Institutions ensure that appropriate controls are implemented to secure the information and technology systems that support business operations, to protect these against exploitation or compromise.

- Institutions ensure that appropriate measures are taken to reduce the risk of breach, damage, service disruption, and other impacts that can result from negligence / attack.

Application Development

- Institutions implement processes that enable the development, implementation and maintenance of applications that meet business needs, and guard against vulnerabilities and software bugs. Institutions place emphasis on both functionality and security, to support development teams in creating and deploying software securely, efficiently, and at scale.

Mobile Device Security

- Institutions implement controls to secure the increasing use of mobile devices, privately owned or company issued to access, store and process data to ensure that data is appropriately protected, safeguarding critical information.

Third Party Management

- Institutions perform relevant due diligence, as well as assess and manage the risk associated with the use of third parties and IT service providers. Assurance is obtained on the controls by both internal and external companies.
- Most institutions have implemented a third party cyber risk framework.

Awareness and Training

- Most institutions have to establish a comprehensive cybersecurity awareness training programme to maintain a high level of awareness among all users.

Annex

BRICS Rapid Information Security Channel (BRISC)
Members

Members	***Position, Organisation***
Brazil Central Bank	
Mr Marcio Rodrigues Alves dos Santos	Head of Division, Information Technology Department
Mr Carlos Eduardo Gomes Marins	Coordinator, Information Technology Department
Mr Rodolfo de Fontes Oliveira	Head of Division, International Affairs Department
Mr Estenio do Nascimento Sobral	Advisor, Information Technology Department
Mr Alexander Bulbow	Coordinator, Strategic Management and Specialized Supervision Department
Mr Eduardo Urbanski Bueno	Advisor, International Affairs Department
Mr Ricardo Terranova Favalli	Coordinator, Strategic Management and Specialized Supervision Department
Mr Marcelo Jose Oliveira Yared	Analyst, Executive Secretariat
Mr Caue Mello da Silva	Analyst, Corporate Risks and Benchmarks Department
Ms Suely Haruko Takahashi Iwamoto	Analyst, International Affairs Department
Central Bank of Russian Federation	
Mr Maxim Leonov	Chief Economist, International Cooperation Department
Mr Artem Sychev	First Deputy Director, Information Security Department
Ms Olga Kraeva	Deputy Head of Division, Information Security Department
Mr Igor Dobrovoltsev	Head of the Financial CERT of the Information Security Department
Mr Nikolay Peremyshlennikov	Head of the Analysis Center of Cyber Attacks, Information Security Department
Mr Alexander Chuburkov	Consultant, Information Security Department
India	
Dr Sanjay Bahl	Director General, Indian Computer Emergency Response Team (CERT-In)
Mr Noorul Ameen	Scientist “D”, CERT-In
Mr Vinod Kumar Chouhan	Scientist “D”, Ministry of Electronics and Information Technology (MeITY)
Dr Mohua Roy	Adviser-in-Charge, International Department, Reserve Bank of India (RBI)
Mr T K Rajan	Chief General Manager, Department of Supervision, RBI

Ms Darshana S Kulkarni	General Manager, Department of Information Technology, RBI
Mr Maulik Shengal	Manager, International Department, RBI
People's Bank of China	
Mr Teng Rui	Deputy Division Chief, International Department,
Ms Fan Shilei	Staff, International Department
South African Reserve Bank	
Mr Gerhard Cronje	Head of the Cyber Information Security Unit, Group Security Management Department
Mr Jacques Theron	Financial Sector Cybersecurity Liaison, Group Security Management Department
Mr Martin Van Deventer	Head of the Security Governance, Risk and Compliance Division, Security Management Department
Mr Jacques Henning	Divisional Head: Operational Risk and IT Risk, Risk Support Department, Prudential Authority
Mr Elias Mashego	Senior Analyst: IT Risk, Risk Support Department, Prudential Authority
Mr Denzil Phillips	Manager: IT Risk, Risk Support Department, Prudential Authority
Ms Linda Motsumi	Senior Manager, International Economic Relations and Policy Department
Ms Crystal Huntley	Economic Policy Analyst, International Economic Relations and Policy Department
Ms Shanthessa Ragavaloo	Junior Economic Policy Analyst, International Economic Relations and Policy Department
Basani Mabaso	Analyst: IT Risk, Risk Support Department, Prudential Authority

BRISC - Editorial Team

Participant	*Position, Organisation*
Chair Coordination Team – Reserve Bank of India	
Ms Smita Sharma	Director, International Department
Mr Giridharan Gopalarathnam	Deputy General Manager, Department of Supervision
Mr Maulik Shengal	Manager, International Department
Mr Shekhar Iyer	Manager, Department of Supervision
Brazil Central Bank	
Mr Estenio do Nascimento Sobral	Advisor, Information Technology Department
Mr Alexander Bulbow	Coordinator, Strategic Management and Specialized Supervision Department
Central Bank of Russian Federation	
Mr Alexander Chuburkov	Consultant, Information Security Department
India	
Mr Vinod Kumar Chouhan	Scientist "D", Ministry of Electronics and Information Technology
People's Bank of China	
Lu Songdian	Staff, International Department
Xia Lei	Staff, Technology Department
Dai Chen	Staff, Technology Department
South African Reserve Bank	
Mr Elias Mashego	Senior Analyst: IT Risk, Risk Support Department, Prudential Authority
Mr Denzil Phillips	Manager: IT Risk, Risk Support Department, Prudential Authority

Published by

Reserve Bank of India