INFORMATION SECURITY REGULATIONS IN FINANCE

Russian Federation I 2024

CONTENTS

INTRODUCTION

Digital connectivity has led to the expanding and deepening of transactions in the financial sector. The increasing reliance on digital channels for financial transactions offers greater choices, more flexibility and improved convenience to the stakeholders. However, the increasing levels of interconnectedness, if unchecked, could pose serious security threats to the stability of the financial sector. Financial sector is among the sectors most susceptible to cyber-attacks. Large scale digital adoption, while providing tremendous convenience, also comes with increased risk in the form of cyber risk. National boundaries have lost their relevance, thereby posing difficulties in controlling cyber risks and recovering lost funds in the event of a cyber-attack. Cyber risk is now recognized as a potential risk to financial stability globally. It is therefore essential to enhance the resilience of the finance sector, by continuously monitoring and mounting the defenses against cyber risks. Many countries and international bodies have formulated cybersecurity regulations and legislations to effectively manage the cybersecurity-related risks responsibly. However, constant upgradation and refinements to the cybersecurity frameworks and a harmonious approach by regulators will be the key to contain the impact of the cybercrimes.

To facilitate the exchange of information and sharing of experiences for building a resilient cyber security system, the BRICS Finance and Central Bank Deputies Meeting, held on May 14, 2020 under the Russian Chair, approved the setting up of the BRICS Rapid Information Security Channel (BRISC). Under Workstream 1 of the BRISC, it was proposed to come out with an e-booklet on BRICS Digital Information Security Regulation, to build the knowledge network on digital information security in the financial sector across BRICS. This e-booklet would act as a guiding document for policy makers to understand the regulatory approaches followed by the BRICS members in financial sector to contain the impacts of the cyberattacks.

The information security regulations given in the booklet have been classified as per the National Institute of Standards and Technology (NIST) framework. Accordingly, it is attempted to categorise the information under these 5 broad categories:

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a security event.
- **Respond:** Develop and implement the appropriate activities when facing a detected security event.
- **Recover:** Develop and implement the appropriate activities for resilience and to restore any capabilities or services that were impaired due to a security event.

Category-wise sharing of information will help in identifying regulations followed by each jurisdiction in each of the five functional areas, as mentioned above. While not all countries follow this method of classification, all efforts have been made to ensure that the booklet provides a comparative glimpse of the regulations.

The document represents the outcome of collaborative efforts undertaken by the members and the editorial teams of the BRICS Rapid Information Security Channel (BRISC). The names of the BRISC members and the editorial team are set out in Annex. It is hoped that this e-booklet would serve as a single point reference document for the readers, to gain an overview of the cybersecurity-related regulations in the BRICS countries.

BRAZIL

THE BRAZILIAN CYBER SECURITY RESOLUTIONS ARE APPLIED TOGETHER WITH INTERNAL CONTROLS SYSTEM AND RISK MANAGEMENT FRAMEWORK

A. REGULATIONS

The Brazilian regulatory framework provides for the cyber security policy that, together with the regulations that provide for the internal controls system and the risk management framework of supervised institutions, consolidates a solid foundation for the establishment of cyber risk management.

Regulation on cyber security policy

This regulation provides for the cyber security policy and the requirements for contracting services of data processing, data storage and cloud computing to be observed by supervised institutions.

- Resolution CMN 4,893, of February 26, 2021 – banks and financial institutions.
- Resolution BCB 85, of April 8, 2021 – payment institutions, securities brokerage firms, securities distribution companies and exchange brokerage firms.

Regulation on internal controls system

Supervised institutions should implement and maintain internal control systems compatible with their nature, size, complexity, structure, risk profile and business model.

This regulation establishes that institutions' internal control systems should provide for periodic security testing of information and technology systems.

- Resolution CMN 4,968, of November 25, 2021 – banks and financial institutions.
- Resolution BCB 260, of November 22, 2022 – payment institutions, securities brokerage firms, securities distribution companies, exchange brokerage firms and consortium administrators.

Regulation on risk management framework

This regulation provides for the structure for risk management and the structure for capital management.

In the context of operational risk management, supervised institutions should implement an IT governance structure consistent with the risk appetite established.

- Resolution CMN 4,557, of February 23, 2017 – prudential conglomerates Type 1.
- Resolution BCB 198, of March 11, 2022 – prudential conglomerates Type 2.
- Resolution BCB 265, of November 25, 2022 – prudential conglomerates Type 3.

Prudential conglomerates:

- Type 1: individual financial institutions or conglomerates led by a financial institution, not classified in Type 2 and 3 conglomerates.
- Type 2: payment institutions or prudential conglomerates consisting exclusively of payment institutions and investment funds.
- Type 3: prudential conglomerates led by a payment institution and integrated by at least one financial institution.

Resolution BCB 304, of March 20, 2023 – Financial Market Infrastructures

Approves the Regulation that disciplines, within the scope of the Brazilian Payment System, the operation of settlement systems, the exercise of registration and centralized deposit of financial assets and the constitution of burdens and encumbrances on registered or deposited financial assets, and consolidates rules on the matter.

Provides for the cyber security policy and the requirements for contracting critical services to be observed by financial market infrastructures.

Guide to Supervision Practices (GSP)

Finally, the Guide to Supervision Practices consolidates BCB Supervision's expectations about the controls environments of financial institutions, payment institutions and other institutions licensed by the BCB, according to the institution's risk exposure and the size and complexity of its operations.

The Guide to Supervision Practices aims to provide greater transparency to the aspects considered in the assessment of supervised entities, providing them with a better understanding of the practices expected by the supervisory body. It is noteworthy that the GSP does not represent a set of new requirements imposed by the regulation, but a compilation of the expectations of the Supervision, which is based on the best practices in risk management and Prevention of Money Laundering and Financing Terrorism (PML/FT).

The broad coverage of the Brazilian Financial System Regulation related to IT (Information Technology) and cyber risks are given below. The translation of these regulations is given in Appendix A1.

B. FUNCTIONAL CATEGORIZATION

The National Financial System (SFN) regulation has a series of provisions that addresses issues present in the functions of NIST, although their references are not organized as established in the cybersecurity framework. A broad categorization of these regulations are illustrated below:

IDENTIFY

Regulation on cyber security policy:

- Information sharing about relevant incidents.
- Establishment of the objectives of the cybersecurity policy and definition of guidelines to be considered in the identification of relevant services of data processing and storage, and cloud computing.
- Vulnerability assessments.

Regulations on internal controls system and risk management framework:

- Definition of risk appetite.
- Identification of critical business processes and potential evaluation effects resulting from the interruption of these processes.
- Continuous evaluation of the different risks associated with the activities of the institution.
- Periodic security testing of information systems.

Guide to Supervision Practices:

- Identification of IT risks, including cyber risk.
- Establishment information security management system.
- Alignment between security strategy and business strategy.
- Implementation of vulnerability analysis.

PROTECT

Regulation on cyber security policy:

- Implementation of mechanisms for dissemination of cybersecurity culture.
- Senior management commitment to continuous improvement of procedures related to cybersecurity.
- Dissemination and training.
- Implementation of security controls – encryption, information leak prevention, protection against malicious software, among others.
- Access control implementation.
- Security measures for transmission and data storage.
- Segregation of data and access controls to protect customer information.
- Development of initiatives for sharing information about relevant incidents.

Regulations on internal controls system and risk management framework:

- Establishment of strategies to ensure continuity of activities and limit losses arising the interruption of critical business processes.
- Implementation of information protection and security mechanisms with objective to preventing, detecting, and reducing vulnerability to digital attacks.

Guide to Supervision Practices:

- Implementation of mechanisms for dissemination of risk and security cultures.
- Establishment of information security management system.
- Establishment of policies: data and information classification, cyber, among others.
- Segregation of IT environments.
- Implementation of audit track.
- Implementation of mechanisms of physical and logical security.

DETECT

Regulation on cyber security policy:

- Controls for intrusion prevention and detection.
- Handling of information on incidents occurred in service providers.

Regulations on internal controls system and risk management framework:

- Information protection and security mechanisms aiming to prevent, detect and reduce vulnerability to digital attacks.

Guide to Supervision Practices:

- Monitoring and attack prevention.

RESPOND

Regulation on cyber security policy:

- Establishment of Incident Response Plans.
- Reporting to the BCB on occurrence of relevant incidents.
- Analysis of the root-cause and impact of incidents.
- Mitigation of the effect of relevant incidents.

Guide to Supervision Practices:

- Incident management.

RECOVER

Regulation on cyber security policy:

- In line with actions aimed at continuity business: execution of procedures in case of interruption of contracted relevant services, setting recovery time for restart or normalization of interrupted relevant activities or services.

Regulations on internal controls system and risk management framework:

- Establishment of continuity plans for restart and recover the activities.

Guide to Supervision Practices:

- Establishment of business continuity management.

C. REFERENCES

- Resolution CMN 4,893, of February 26, 2021 (Portuguese version) – https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893
- Resolution BCB 85, of April 8, 2021 (Portuguese version) – https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=85
- Resolution CMN 4,968, of November 25, 2021 (Portuguese version) – https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4968
- Resolution BCB 260, of November 22, 2022 (Portuguese version) – https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=260
- Resolution CMN 4,557, of February 23, 2017 (Portuguese version) – https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4557
- Resolution BCB 198, of March 11, 2022 (Portuguese version) – https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=198
- Resolution BCB 265, of November 25, 2022 (Portuguese version) – https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=265
- Resolution BCB 304, of March 20, 2023 (Portuguese version) – https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=304

CHINA

A. REGULATIONS

In terms of laws related to cyber security in China, after the implementation of Cyber-Security Law of the People's Republic of China in June 2017, Data Security Law of the People's Republic of China and Personal Information Protection Law of the People's Republic of China were carried out in 2021. In addition to the national laws, "Regulations on Security Protection of Critical Information Infrastructure" came into effect in 2021, defining the responsibilities of supervision authorities and critical information infrastructure and relevant requirements like risk assessment. Besides, in 2022, "Cybersecurity Review Measures" was implemented, it clarifies the cybersecurity review requirements for the procurement of network products or services by critical information infrastructure operators and the data processing by network platform operators when national security is or may be affected. Furthermore, in 2023, the revised "Regulation on the Management of Commercial Cryptography" was announced. It refines and improves the compliance management requirements for critical information infrastructure operators to use commercial cryptography for security protection of critical information infrastructure.

The PBOC has been establishing regulations and standards based on the national laws. The major cybersecurity regulation issued by the PBOC is the Notice of the People's Bank of China on Issuing the Reporting System for Computer Security Incidents of Banks, which defines the cyber incident cases that banks must report and the key elements, process as well as timelines of incident reporting. The Standard, Implementation guidelines for classified protection of cybersecurity of financial industry–Part 1: Fundamentals and vocabulary, introduces the basic requirements in cyber incident reporting for financial institutions. The standard, Financial Cyber Security Guidelines of Implementation for Crowdsourced Cyber Security Testing, defines the organizational structure and process of implementing Crowdsourced Cyber Security Testing as well as the responsibilities of relevant parties during the implementation.

THE REFERENCES TO CIRCULARS ON CYBER SECURITY

1. Yinfa No. 280 [2002], Notice of the People's Bank of China on Issuing the Reporting System for Computer Security Incidents of Banks (http://www.pbc.gov.cn/en/3688253/3689009/3788456/4006036/index.html).

2. Financial Cyber Security Guidelines of Implementation for Crowdsourced Cyber Security Testing (available in Chinese: https://std.samr.gov.cn/hb/search/stdHBDetailed?id=BD16B32D9D96D084E05397BE0A0A9E14).

3. Implementation guidelines for classified protection of cybersecurity of financial industry – Part 1: Fundamentals and vocabulary" (JR/T 0071.1–2020) (available in Chinese: https://std.samr.gov.cn/hb/search/stdHBDetailed?id=B62CB2BE711F1CD5E05397BE0A0A83BC).

B. FUNCTIONAL CATEGORIZATION

IDENTIFY

- Computer security incidents of banks shall include:
  - hardware and software failure of the information system;
  - failure of the network communication system;
  - failure of the power supply system;
  - the infection of the system with a computer virus;
  - the flood, fire, and lightning suffered by the data processing center;
  - invasion or attack of the bank network;
  - the disclosure of sensitive data in the information system;
  - the data theft from the information system; and
  - the theft of the bank data processing equipment.
- A computer security incident that meets any of the following requirements must be reported:
  - Interruption or abnormal operation of the computer information system for more than 4 hours.
  - Causing a direct economic loss of more than RMB 1 million.
  - Seriously threatening the security of bank funds.
  - Causing the bank to be unable to operate normally, and affecting more than one county-level administrative region.

PROTECT

- Financial institutions (FIs) should establish a video monitoring system and an environment monitoring system for the server room to implement comprehensive monitoring of important facilities such as air-cooled equipment, water and electricity equipment, firefighting facilities, and access control systems in the server room. Video records and server room access records should be kept for at least 3 months.
- Different network areas should be divided and network addresses be assigned to each network area for the purpose of easy management and control. Deployment of critical network areas at borders should be avoided. Reliable technical isolation should be adopted between important network areas and other network areas.
- FIs should use validation technology to ensure the integrity of data in the process of network communication as well as transmission and storage.
- Access and data flow across the boundaries should be communicated through a controlled interface provided by network boundary control devices.
- Access control rules should be set up between network boundaries or areas according to access control policies. Except for allowed communications, the controlled interface should reject all communications by default.
- Encryption or other protective measures should be employed to ensure the confidentiality of authentication information during the transmission and storage process.
- Local data backup and recovery function for important data should be available. Off-site data backup function which uses communication network to transfer important data to the backup site in batches at regular intervals should be provided.

DETECT

- FIs should be able to detect intrusions into critical nodes and provide alerts in the event of a serious intrusion.
- FIs should be able to detect possible known vulnerabilities and patch them in a timely manner after adequate testing and evaluation.
- FIs should install anti-malicious software or configure software with corresponding functions, and ensure that upgrades and updates to the anti-malicious library are carried out regularly and consistently.

RESPOND

- A bank where a computer crime occurs shall, in accordance with the relevant provisions, report the case to the security department of the local branch of the PBOC, and send a copy thereof to the computer security department.
- The report on a computer security incident shall include:
  - when and where the computer security incident occurs, the entity and its person in charge and his or her contact information;
  - the category of the computer security incident, the software and hardware systems involved, and the cause of the incident;
  - the consequences and coverage of the computer security incident;
  - the reasons for the occurrence of the computer security incident;
  - the liable persons or the persons involved in the case; and
  - emergency measures taken after the occurrence of the computer security incident .
- After a computer security incident occurs in a bank, the bank shall, according to escalation procedures, report it to the superior entity of the system within 12 hours after the occurrence of the incident, and at the same time send a report to the computer security department of the local branch or sub-branch of the PBOC. If the entity where an incident occurs has no superior entity, it shall directly send a report to the computer security department of the local branch or sub-branch of the PBOC.
- After receiving the report on a computer security incident from the banking system, the branch or sub-branch of the PBOC shall, within 12 hours, report it to the computer security departments of the branches and operation offices of the PBOC, and central subbranches of the PBOC in capital cities of provinces (autonomous regions). The branches, operation offices, and central sub-branches of the PBOC in capital cities of provinces (autonomous regions) that have received the report shall, within 24 hours of occurrence of the incident, send a report to the computer security department of the PBOC.
- Any entity or individual shall have the right to report to the local branch or sub-branch of the PBOC the hidden dangers of computer security existing in the bank. The relevant department of the PBOC that receives the report shall, in no time, make a preliminary assessment of the report and, if necessary, immediately organize the inspection and disposal of the hidden dangers of computer security.
- Computer security incidents must be reported in a timely manner, the content shall be complete, objective and accurate. The implementation of the reporting system for computer security incidents of banks shall be subject to computer security inspection.
- There are also several requirements for financial institutions operating “Classified Security Protection Level II” systems, mainly:
  - Financial institutions should report the identified cyber security vulnerabilities and suspicious events.

– Financial institutions should establish incident reporting and disposal management systems, which define the reporting, handling and response process of different cyber incidents, and specific management duties.
– Financial institutions should analyse the causes of the incidents, collect evidence, document the response process, and summarise experiences, in the process of cyber incidents reporting and response.

EGYPT

EGYPT FINANCIAL CYBERSECURITY FRAMEWORK BESIDES THE INTERNET BANKING REGULATION ALONG WITH OTHER LAWS SUCH AS EGYPT LAW FOR INFORMATION TECHNOLOGY CRIMES, EGYPT ANTI-MONEY LAUNDERING IN ADDITION TO EG-FINCIRT THAT RESPOND TO INCIDENTS, PERFORM FORENSICS ANALYSIS, AND THREAT HUNTING

Central bank of Egypt (CBE) has established a comprehensive cybersecurity framework in December 2021, tailored to cover the unique requirements of the Egyptian financial sector and serves as the guidance for cybersecurity capability development within Egyptian Banking & Financial sector. Moreover, CBE has published internet banking regulations in order to regulate electronic services and digital channels provided by banks and financial institutions, in addition to the establish of Computing Incident Response Team for the Financial Sector (EG-FinCIRT) which is a key pillar in the framework for implementing the strategy of the Central Bank to reduce different risks associated with the banking systems, paving the road for investment inflows into the banking & financial sector in Egypt.

A. REGULATIONS

- **Egypt Financial Cybersecurity Framework (EGY-FIN CSF) V1.0 published in December 2021**

This framework aims to provide guidance and mandated controls in order to elevate the Cybersecurity Readiness through determining the maturity levels according to risk exposure and controls effectiveness in banks and financial institutions. This framework represents an intentionally detailed document, allowing every Licensed Entity under the CBE supervision the flexibility to architect and implement the relevant controls in a manner consistent with existing and emerging industry best practices and standards.
The CBE has developed a structured assessment, training, and maturation model that builds off this framework. As organizations evolve and enhance their cybersecurity programs, thus reaching a more mature state, the CBE will continually refine expectations and update the framework accordingly to meet the emerging landscape.

- **Central bank of Egypt Circular dated October 2021 "Rules Regulating Services for Instant Payment Network Inside the Arab Republic of Egypt"**[1]

The circular aim to develop a framework for banks and mobile phone application service providers regarding the Instant Payment Network to allow customers and banks to carry out instant transfers through electronic payment tools and provide all segments of society with appropriate banking services.

- **Central bank of Egypt's Directions based on Governor letter dated 2 September 2021 "Recovery Plan Directions"**[2]

- **Egypt Law No. 194 of 2020 "Central bank and Financial Sector Law" to regulate and ensure the independency of Central bank of Egypt and the supervision of banks and financial institutions**[3]

[1] Source: https://www.cbe.org.eg/-/media/project/cbe/listing/circulars/payments-regulations/ipn-services-regulations_en.pdf

[2] Source: https://www.cbe.org.eg/-/media/project/cbe/file/long-context/laws-and-regulations/book-3/%D8%A7%D9%84%D9%81%D8%B5%D9%84-%D8%A7%D9%84%D8%B1%D8%A7%D8%A8%D8%B9-%D8%B9%D8%B4%D8%B1-%D8%AA%D8%B9%D9%84%D9%8A%D9%85%D8%A7%D8%AA-%D8%AE%D8%B7%D8%B7-%D8%A7%D9%84%D8%AA%D8%B9%D8%A7%D9%81%D9%8A.pdf

[3] Source: https://www.cbe.org.eg/-/media/project/cbe/page-content/other-links/cbe-law-no,-d-,-194-of-2020.pdf

The provisions of Law No. 194 for the year 2020, any unregistered individual, entity or establishment is prohibited from performing any banking business, excluding the public legal entities that conduct one of these businesses within the limits of their establishment documents. Banking Business means any activity deals primarily and regularly with accepting deposits, obtaining financing and investing those funds in providing financing and credit facilities, contributing to corporate capital, and any other acts customarily known as banking business. Also, according to the provisions of the aforementioned law, any unregistered establishment is prohibited from using the word bank or any similar expression in any language, whether in its own name, trade address, or advertisement. This law sets specific conditions for licensing to open such offices, whereas the activity of representation offices is limited to study markets and investment possibilities and being a link with the main head office abroad to overcome the problems and difficulties that may face its correspondent banks in Arab Republic of Egypt. Such offices cannot engage in any banking or commercial activity, including the activity of commercial agents and financial intermediation. Furthermore, The Central Bank of Egypt examines the requests of foreign banks to open offices to represent them in Arab Republic of Egypt.

- **Egypt Law No. 151 of 2020 "The Protection of Personal Data Law"**

This law aims to safeguard individuals' personal information, setting a new standard for data protection and significantly impacting cybersecurity in Egypt. The provisions of this law and the annexed law shall apply to whoever commits any of the violations stipulated in the annexed law if the offender is an Egyptian residing inside or outside the Arab Republic of Egypt, a non-Egyptian residing inside the Arab Republic of Egypt, or a non-Egyptian outside the Arab Republic of Egypt provided that the act is punishable under any legal form in the country where it occurred, and the data subject of the crime belongs to Egyptians or foreigners residing inside the Arab Republic of Egypt.

- **Egypt Law No. 175 of 2018 "Anti-Cyber and Information Technology Crimes Law"**

This law forms the backbone of cybercrime legislation in Egypt. It outlines penalties for unauthorized access, data privacy infringements, and other forms of cyber malfeasance. On the other hand, this law is designed to secure digital spaces, but it also has direct implications for corporate governance. Companies are now required to adopt strict data management and cybersecurity protocols to avoid penalties.

- **Central bank of Egypt Regulation Published dated 09 November 2014, "Governance Rules for the provision of online banking services in the Egyptian banking sector"**[4]

The Regulation establishes requirements for establishing and operate different digital channels which contain different enables for customers to connect, use and modify their banks accounts, and the ability to transfer money and use different bank's services digitally.

- **Egypt Law No. 10 of 2003 on The Telecommunication Regulation**[5]

This law lays down regulations concerning digital communication, which also includes guidelines for secure data transmission. This law has a significant impact on the telecommunication, media and technology sectors in Egypt and have aided in noticeable and tangible growth in these sectors over the last few years. The development that resulted from the enactment of this law has succeeded in attracting a number of key players into the local market, mainly mobile operators. This movement entailed the issuance of other related legislations in the last couple of years to support the sector, adapt to market needs and complement Egypt Law No. 10 of 2003.

[4] Source: https://www.cbe.org.eg/-/media/project/cbe/listing/circulars/files/cbeinterne_216_en.pdf

[5] Source: https://www.tra.gov.eg/wp-content/uploads/2020/11/Law-No-10-of-2003.pdf

B. FUNCTIONAL CATEGORIZATION

The Egypt Financial Cybersecurity framework and Central Bank of Egypt laws and directions set the baseline roles and functions in order to unify and protect the cybersecurity cultures and set a defined maturity levels and process and align with different international standards requirements.

IDENTIFY

- Define the overall cybersecurity strategy shall focus on the required structure to execute that strategy.
- The organizational structure component shall focus on the roles, responsibilities, and associated skill sets per job function and the structure's alignment with the documented strategy.
- Define Policies are codified, agreed-upon standards endorsed by executive leadership to hold employees and supporting business elements accountable for a minimum set of expected behaviors.
- Policies are shaped by the needs of the business culture, regulations, and industry. Policies are reviewed, validated, and refined on a periodic basis to ensure relevance with the organization's mission, vision, and goals.
- Define the Risk Management Operations that aims to frame, assess, monitor, mitigate, and respond to risks across business components, processes, and people.
- Risk appetite and risk acceptance decisions shall be driven by a strategic determination and expression of organizational risk tolerance.
- Risk Management Operations shall be used to plot risks on a graph using either a quantitative or qualitative model to inform decision prioritization by probability and impact.
- Define an Asset Management program that shall encompass all systems, functions, applications, or business services. Including but not limited to physical assets, cybersecurity-centric assets, and digital assets.
- The organization shall build a comprehensive understanding of all of the systems it requires and their functional dependencies.

PROTECT

- Define a comprehensive Security Awareness and Training provides employees, third parties, contractors and customers with the baseline knowledge and understanding of their responsibility for protecting the organization from threats to its assets and data.
- Define Network Security Program that focuses on the logical structure, policies, processes, and technologies to protect data in transit and remote connectivity to physical or virtual systems.
- Protect data and information in transit, ensure proper network visibility, limit network access to only authorized endpoints, and take corrective actions on malicious activity discovered.
- Protect servers, desktops, and workstations that employees, third parties, and contractors use to connect to the organization's network.

- Define the required level of security controls needed and account for common and unique risks posed by on-premises, off-premises, cloud, third-party, and telework devices.
- Reduce systemic risk exposure inherited from the use of software applications required to support business operations.
- Calculate organization risk while considering different Application types, architecture, and design decisions before introduction on the production network.
- Define requirements for acceptable electronic communications, use of email security safeguards, data protection, and data classification.
- Address security concerns introduced by electronic mail technologies needed to support business operations and communications with internal employees and external entities.
- Stemming from physical access to the organization's facilities and data centers and environmental conditions affecting operations and its underlying technologies within their physical environment.
- Define Data protection measures that focus on safeguarding client and business data, intellectual property, and personally identifiable information belonging to employees and clients while ensuring the protection of availability, integrity and privacy of data.
- Data protection must be maintained when the data leaves the organizational boundaries such as when it is provided to customers or cloud providers.
- Define an Identity and Access Management (IAM) program that aims to provision or revoke access for users and systems to operate on the organization's enterprise in addition to ensure that users are only granted the minimal level of access needed to perform core job functions.
- Define a Physical and Environmental Security program to protect against threats.

DETECT

- Define a Vulnerability and Patch Management aim to identify, prioritize, and take corrective action to protect the organization against exploitation from internal and external threats.
- The Vulnerability and Patch Management shall Identify and catalog system versions and configurations to determine whether the assets are susceptible to exploitation.
- The Vulnerability and Patch Management shall apply patches or compensatory controls to mitigate risk exposure.
- The Vulnerability and Patch Management prioritization decisions should be informed by cyber threat intelligence.
- Define a comprehensive Cyber Threat Intelligence (CTI) program to guide organization's cybersecurity program, defense operations, and vulnerability management decisions.
- The CTI program shall provide and maintain situational awareness on threats, vulnerabilities, and risks while overlaying applicable environmental, business, and operational knowledge in a formal cyclical manner.
- The organization shall have a security operation center that continuously monitor and improve an organization's cyber defense posture while preventing, detecting, analyzing, and responding to incidents.
- The Security Operations Center (SOC) shall be the central point of collaboration for identifying suspicious activities to investigate using a centralized system to view data collected, aggregated, and indexed from endpoints, network appliances, applications, and cybersecurity controls.
- The organization shall define a process to safeguard intellectual property, prevent financial theft and fraud, protect brand reputation, and ensure the safety of personnel from employees or contractors misusing their access to the organization's systems or workspace.
- The Insider Threat Management focuses on monitoring authorized individuals such as employees and contractors to proactively identify, understand, and address risky and unintended behaviors.

RESPOND

- Define an incident management program to provide the organization with the ability to oversee, control, communicate, and recover from a variety of incidents, disruptions, or disasters. The incident management program shall be focused on the overarching organizational capabilities outside of what is handled within the Cybersecurity team's incident response.
- Define a solid Incident Response program to determine the scope and scale of a potential compromise and then take action to minimize the impact to business operations.
- The incident response program shall document and apply all lessons learned from a compromise to work with asset and application owners, the Network Operations team, and other SOC elements to improve the organization's overall security posture.
- The incident response program shall cover the process of investigating suspected intrusion attempts to determine whether they were successful and to what extent.
- The Incident Response team works with the SOC and other stakeholders to remediate the intrusion by containing and cleaning the compromised systems, eradicating attacker tools, and revoking attacker access, before taking preventative steps to ensure the attacker does not return.

RECOVER

- The organization shall devise a strategy that would allow an organization to withstand, adapt, and thrive in the event of an incident, disruption, or disaster.
- The business resilience strategy shall account for incidents, disruptions, or disasters that could impact the organization's operational ability, IT systems, people, brand, and finances.
- The organization shall contain the effect of shocks to business operations to ensure the critical assets identified retain their Availability, Integrity, and Confidentiality.
- The organization shall document process that incorporates recovery-level objectives defined as part of the Business Impact Analysis (BIA) to prioritize the resumption of business-critical processes, systems, and services.
- The organization shall perform simulation exercise at regular intervals at least annually to test the organization's incident response, business continuity, and disaster recovery plans.

ETHIOPIA

THE CYBERSECURITY REGULATION TO BE ISSUED AND ALREADY ISSUED DIRECTIVE OF REQUIREMENT FOR IT MANAGEMENT BY NBE

A. REGULATIONS

With respect of a cyber security, there is a cyber security strategy issued by government security agency named Information Network Security Administration (INSA) recently. A cyber security strategy also issued by National Bank some 7 years ago. This strategy tries to address on three pillars. The first one is on Regulatory framework which will be done by National Bank of Ethiopia which address the finance sector issued directive where all financial institutions need to follow it. The second pillar also addresses using shared platform. This address institutions instead of implementing different technology related to cyber security on each institution it advisable to implement centrally where all finance institutions used this technology. Recently a common Security Operation Center for all financial institutions is underway as a project. The third pillar is to on capacity building where staffs of the sector need to get regular training with respect of cyber security. There is also issued proclamation No. 1321/2024 about to provide for personal data protection. In general, it will focus on people, Process and Technology.

A directive of Information Technology (IT) Management issued on 2022. This directive addresses as:

General requirements

- The bank should describe and include the role of IT in business strategy.
- The bank should develop and implement IT strategy.
- The IT strategy should cover:
  - the bank vision, mission, and strategic objective;
  - assessment of information technology opportunity, threats and internal strengths and weakness and weaknesses to manage information technologies;
  - assessment of stock of exiting IT and planned ones to be introduced in future;
  - IT Objective to be pursued;
  - key performance indicators in achieving IT objectives;
  - strategies to ensure security in the usage of IT;
  - identified IT initiatives to achieve indicated objectives; and
  - requirements provided by Information Network Security Administration.

Management of IT Risks

- A bank shall put in place and implement IT risk management program aligned with the institutions risk management program and at least cover:
  - types or categories and definitions of IT risks to which the bank is exposed;
  - IT risk management and culture and objectives;
  - IT risk identifications, assessment, measurement, reporting and monitoring mechanisms;

- duties and responsibilities of board and /or its committees, senior management and or/its committees, risk management function, and operational units in managing risk;
- IT risk management policies, procedures and standards; and
- duties and responsibilities of internal auditor to asses and ensure the adequacy of IT risk management process and overall program;
- in the course of automating its various business and developing program to manage related risks, a bank shall take in account cyber security risk management requirement by Information Network Security Administration.

IT Risks Management Polices

A bank shall develop and implement IT risk management strategies, plan and policies and at least cover:

- physical access and network securities;
- customer data privacy;
- password, data transfer security, user right access, antivirus, and firewall security.

IT Audit

The scope of IT audit shall at least include:

- carryout at least annual cyber threat test or conducting other IT audit activities as provided by INSA or other competent authority;
- IT audit shall conduct at least quarterly base.

There is a cyber security directive that will be released soon, which address the following points:

- governance;
- Cyber Security Policy to have on institutions and suggest also points to be considered;
- cloud computing;
- outsourcing;
- reporting.

A circular also issued for financial sector before they implement any technology should pass Information Network Security Administration penetration test.

B. FUNCTIONAL CATEGORIZATION

IDENTIFY

Cyber security incidents of banks shall include:

- identifying physical and software assets;
- identifying cybersecurity policies;
- identifying asset vulnerabilities;
- identifying a Risk Management Strategy;
- identifying a Supply Chain Risk Management strategy.

PROTECT

- Protections for Identity Management and Access Control.
- Empowering staff within the organization through Awareness and Training.
- Establishing Data Security protection consistent with the organization's risk strategy.
- Protecting organizational resources.

DETECT

- Ensuring Anomalies and Events are detected, and their potential impact is understood.
- Implementing Security Continuous Monitoring capabilities to monitor cybersecurity events and verify the effectiveness of protective measures including network and physical activities.
- Maintaining Detection Processes to provide awareness of anomalous events.

RESPOND

- Ensuring Response Planning process are executed during and after an incident.
- Managing Communications during and after an event with stakeholders, law enforcement, external stakeholders as appropriate.
- Analysis is conducted to ensure effective response and support recovery activities including forensic analysis, and determining the impact of incidents.
- Mitigation activities are performed to prevent expansion of an event and to resolve the incident.
- The organization implements Improvements by incorporating lessons learned from current and previous detection / response activities.

RECOVER

- Ensuring the organization implements Recovery Planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents.
- Implementing Improvements based on lessons learned and reviews of existing strategies.
- Internal and external Communications are coordinated during and following the recovery from a cybersecurity incident.

INDIA

Indian Computer Emergency Response Team (CERT-In) and Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) respond to cyber incidents, issue alerts, guidelines and directions for mitigation. In addition, the Cyber Security and Information Technology Risk Group (CSITEG) in RBI issues cyber-security directions and guidelines and also supervises through onsite and offsite surveillance mechanisms.

In India, the CERT-In under Ministry of Electronics and Information Technology (MeitY), Government of India is the national agency for responding to cyber security incidents. The CERT-In supports all sectors including financial sector. The functions of CERT-In include strengthening of cyber-security by providing proactive & reactive services as well as guidelines, threat intelligence and assessment of preparedness of various agencies across the sectors, including the financial sector.

CSIRT-Fin has been established under CERT-In and is made operational from 15th May 2020. CSIRT-Fin is a nodal sectoral CSIRT which provides Incident Prevention and Response services as well as Security Quality Management Services to the entities of the Indian financial sector. It manages cyber incidents and coordinate responses across banking, securities market infrastructure, insurance, and pension funds entities. CERT-In provides the requisite leadership for the CSIRT-Fin (Computer Security Incident Response Team-Finance Sector) for responding to containment and mitigation of cyber security incidents reported from the financial sector. The CSITEG of Department of Supervision in the Reserve Bank of India, regulates and supervises area of cybersecurity and IT, in the banks, urban co-operative banks, non-banking financial companies, credit Information companies and select All India financial Companies in the country. To strengthen the cyber security of the supervised entities, referred to as “entities” hereinafter, CSITEG takes regulatory measures on IT and cyber security by issuance of directions/ guidelines in the form of circulars and advisories. On the supervisory front, CSITEG conducts onsite IT examinations and monitors the cyber security posture of these entities through various offsite surveillance mechanisms.

A. REGULATIONS

- The Information Technology Act, 2000 is an Act of the Indian Parliament notified on 17 October 2000. It is the Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce” (https://www.meity.gov.in/content/information-technology-act-2000).
- CERT-In Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet (https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf).
- Cyber Security Framework in Banks dated 2 June 2016 (https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF).

- Select portions relevant to cyber security of Master Direction – Information Technology Framework for the NBFC Sector dated 8 June 2017 (https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD53E0706201769D6B56245D7457395560CFE72517E0C.PDF).
- Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) dated 19 October 2018 (https://rbidocs.rbi.org.in/rdocs/Notification/PDFs/NT636E1566334F9A4F998C838D5AC6173A96.PDF).
- Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach dated 31 December 2019 (https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI129BB26DEA3F5C54198BF24774E1222E61A.PDF).
- Cyber Security controls for Third party ATM Switch Application Service Providers dated 31 December 2019 (https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT13060CC89309DEC4BFB8B7CBC33FAA05FE5.PDF).
- Master Direction on Digital Payment Security Controls dated 18 February 2021 (https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF).
- Master Direction on Outsourcing of Information Technology Services (https://rbidocs.rbi.org.in/rdocs/notification/PDFs/102MDITSERVICES56B33FD530B1433187D75CB7C06C8F70.PDF).
- Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (https://rbidocs.rbi.org.in/rdocs/notification/PDFs/107MDITGOVERNANCE3303572008604C67AC25B84292D85567.PDF).

B. FUNCTIONAL CATEGORIZATION

The regulations enumerated in this booklet cover the regulations under the central bank. The key aspects of these regulations are categorized as per the 6 functions enumerated under NIST cybersecurity framework, viz., govern, identify, protect, detect, respond, recover.

GOVERN

- To apply security best practices and strengthen security of IT infrastructure.
- Establish appropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor/outsourcing activities shall be put in place.
- Develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators. Some illustrative metrics include coverage of anti-malware software and their updating percentage, patch latency, extent of user awareness training, vulnerability related metrics, etc.
- Formulate a policy for digital payment products and services with the approval of their Board. The contours of the policy, while discussing the parameters of any “new product” including its

alignment with the overall business strategy and inherent risk of the product, risk management/ mitigation measures, compliance with regulatory instructions, customer experience, etc., should explicitly discuss about payment security requirements from Functionality, Security and Performance (FSP) angles.

- Put in place a fully effective Incident Response programme with due approval of the Board / Top Management.
- Develop a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.
- Define roles and responsibilities of stakeholders (including third-party personnel) involved in IT risk management. Areas of possible role conflicts and accountability gaps must be specifically identified and eliminated or managed.
- Create an inventory of services provided by the service providers (including key entities involved in supply chains). Further, Regulated Entities shall map their dependency on third parties and periodically evaluate the information received from the service providers.
- REs shall put in place a Risk Management framework for Outsourcing of IT Services that shall comprehensively deal with the processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with Outsourcing of IT Services arrangements.
- Banks shall ensure and demonstrate that the service provider (including another bank) adheres to all regulatory and legal requirements of the country. Banks may necessarily enter into agreement with the service provider that amongst others provides for right of audit by the Bank and inspection by the regulators of the country.
- Banks shall carefully evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment.
- Among others, banks shall regularly conduct effective due diligence, oversight and management of third-party vendors/service providers & partners.
- Background checks, non-disclosure and security policy compliance agreements shall be mandated for all third-party service providers.
- In order to mitigate the risk of unexpected termination of the outsourcing agreement or insolvency/ liquidation of the service provider, REs shall retain an appropriate level of control over their IT outsourcing arrangement along with right to intervene, with appropriate measures to continue its business operations.
- The Outsourcing of IT Services policy shall contain a clear exit strategy with regard to outsourced IT activities/ IT enabled services, while ensuring business continuity during and after exit. The strategy should include exit strategy for different scenarios of exit or termination of services with stipulation of minimum period to execute such plans, as necessary. In documenting an exit strategy, the RE shall, inter alia, identify alternative arrangements, which may include performing the activity by a different service provider or RE itself.
- REs shall define suitable metrics for system performance, recovery and business resumption, including Recovery Point Objective (RPO) and Recovery Time Objective (RTO), for all critical information systems.
- On an annual or more frequent basis, REs shall proactively assess capacity requirement of IT resources. REs shall ensure that IT capacity planning across components, services, system resources, supporting infrastructure is consistent with past trends (peak usage), the current business requirements and projected future needs as per the IT strategy of the RE.
- REs shall have a separate IS Audit function or resources who possess required professional skills and competence within the Internal Audit function. Where the RE uses external resources for conducting IS audit in areas where skills are lacking within the RE, the responsibility and

accountability for such external IS audits would continue to remain with the competent authority within Internal Audit function.

- Identify a Supply Chain Risk Management strategy including priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated with managing supply chain risks.
- REs shall have a documented data migration policy specifying a systematic process for data migration, ensuring data integrity, completeness and consistency. The policy shall, inter alia, contain provisions pertaining to signoffs from business users and application owners at each stage of migration, maintenance of audit trails, etc.
- REs shall carry out IS Audit planning by adopting a risk-based audit approach.
- REs may consider, wherever possible, a continuous auditing approach for critical systems, performing control and risk assessments on a more frequent basis.
- Prepare and implement a Cyber Crisis Management Plan (CCMP) of the bank including detailed contingency plan for dealing with crisis arising out of cyber-attacks in respective areas.

IDENTIFY

- Maintain an up-to-date inventory of assets, including business data/information containing customer data/information, business applications, supporting IT infrastructure and facilities – hardware/software/network devices, key personnel, services, etc. indicating their business criticality. The banks may have their own framework/criteria for identifying critical assets.
- Software/Application development approach should be based on threat /modelling and security testing based on global standards and secure rollout.
- Maintain an up-to-date and preferably centralised inventory of authorised/unauthorized software(s).
- Have a clearly defined framework including requirements justifying the exception(s), duration of exception(s), process of granting exceptions, and authority for approving and for review of exceptions granted on a periodic basis by officer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s).
- Prepare and maintain an up-to-date network architecture diagram at the organization level including wired/wireless networks.
- Maintain an up-to-date/centralised inventory of authorised devices connected to bank's network (within/outside bank's premises) and authorised devices enabling the bank's network. The bank may consider implementing solutions to automate network discovery and management.
- Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling are required to be clearly specified at the initial and ongoing stages of system development/acquisition/implementation.
- Ensure that adoption of new technologies shall be adequately evaluated for existing/evolving security threats and IT/security teams of the Bank reach reasonable level of comfort and maturity with such technologies before introducing for critical systems of the Bank.
- Follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches, so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.
- Periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between (i) different VLANs in the Data Centre (ii) LAN/WAN interfaces (iii) Bank's network to external network and interconnections with partner, vendor and service provider networks are to be securely configured.

- In respect of critical business applications, banks may consider conducting source code audits by professionally competent personnel/service providers or have assurance from application providers/OEMs that the application is free from embedded malicious/fraudulent code.
- Banks should act as the identity provider for identification and authentication of customers for access to partner systems using secure authentication technologies.
- Document and implement email server specific controls.
- Banks shall be accountable for ensuring appropriate management and assurance on security risks in outsourced and partner arrangements.
- Regularly carry out security audit of IT infrastructure, web applications and websites on periodic basis to check resilience of cyber assets against malicious attacks.
- Reserve Bank of India shall have access to all information resources (online / in person) that are consumed by banks, to be made accessible to RBI officials by the banks when sought, though the infrastructure / enabling resources may not physically be located in the premises of banks.
- Further, banks have to adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders.
- Banks shall thoroughly satisfy themselves about the credentials of the vendor / third-party personnel accessing and managing the Bank's critical assets.
- Define and implement policy for restriction and secure use of removable media / BYOD on various types/categories of devices, including, but not limited to workstations PCs / laptops / Mobile devices/servers, etc. and secure erasure of data on such media after use.
- Consider implementing centralised policies through Active Directory or Endpoint management systems to whitelist/ blacklist /restrict removable media use.
- Periodically conduct VA/PT of internet facing web/mobile applications, servers & network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.).
- Penetration testing of public facing systems as well as other critical applications are to be carried out by professionally qualified teams.
- Periodically conduct application security testing of web/mobile applications throughout their lifecycle (pre-implementation, post implementation, after changes) in environment closely resembling or which is a replica of the production environment.
- Red Teams may be used to identify the vulnerabilities and the business risk, assess the efficacy of the defences and check the mitigating controls already in place by simulating the objectives and actions of an attacker.
- Identification of critical information systems of the organization and fortification of the security environment of such systems.
- Periodicity of DR drills for critical information systems shall be at least on a half-yearly basis and for other information systems, as per RE's risk assessment.

PROTECT

- Appropriately manage and provide protection within and outside organization borders/ network, taking into consideration how the data/information are stored, transmitted, processed, accessed and put to use within/outside the bank's network, and the level of risk they are exposed to, depending on the sensitivity of the data/information.
- Continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply the security patches as per the patch management policy of the bank. If a patch/series of patches is/are released by the OEM/manufacturer/vendor for protection against well-known / well publicised / reported attacks exploiting the vulnerability patched, the banks must have a mechanism to apply them expeditiously following an emergency patch management process.
- Ensure that all the network devices are configured appropriately and periodically assess whether the configurations are appropriate to the desired level of network security.

- Put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.
- Establish Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network.
- Document and apply baseline security requirements / configurations to all categories of devices (end-points / workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically.
- Periodically evaluate critical device (such as firewall, network switches, security devices, etc.) configurations and patch levels for all systems in the bank's network including in data centres, third party hosted sites, shared-infrastructure locations.
- Incorporate/Ensure information security across all stages of application life cycle.
- Secure coding practices may also be implemented for internally/collaboratively developed applications.
- The development, test and production environments need to be properly segregated.
- Ensure that software/application development practices proactively address the vulnerabilities based on best practices baselines such as Open Web Application Security Project (OWASP) and adopt principle of defence-in-depth to provide layered security mechanism.
- Consider implementing measures such as installing a "containerized" app on mobile/ smart phones for exclusive business use that is are encrypted and separated from other smartphone data/applications; implement measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.
- Put in place systems and processes to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems / databases / applications / middleware, etc.
- Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes, configuration baseline that ensure integrity of any changes thereto.
- Provide secure access to the Bank's assets/services from within/outside Bank's network by protecting data/information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. using technologies such as VPN or other secure web protocols, etc.).
- Carefully protect customer access credentials such as logon user id, authentication information and tokens, access profiles, etc. against leakage/attacks.
- Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a need to know basis and for specific duration when it is required following an established process.
- Implement centralised authentication and authorisation system or accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/ multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.
- Implement appropriate (e.g. centralised) systems and controls to allow, manage, log and monitor privileged/super user/ administrative access to critical systems (Servers/OS/DB, applications, network devices etc.).
- Implement controls to minimize invalid logon counts, deactivate dormant accounts.
- Implement measures to control installation of software on PCs/laptops, etc.
- Implement controls for remote management/wiping/locking of mobile devices including laptops, etc.

- Implement measures to control use of VBA/macros in office documents, control permissible attachment types in email systems.
- Implement multi-factor authentication framework/mechanism to provide positive identify verification of bank to customers.
- Customer identity information should be kept secure.
- Implement secure mail and messaging systems, including those used by bank's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.
- Limit media types and information that could be transferred/copied to/from such devices.
- As default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorised for defined use and duration of use.
- Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise.
- Implement anti-malware, antivirus protection including behavioural detection systems for all categories of devices – (endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), web/internet gateways, email-gateways, wireless networks, SMS servers etc. including tools and processes for centralised management and monitoring. Employ end-point detection and response system for all such end-points.
- Consider implementing whitelisting of internet websites/systems.
- Consider implementing secure web gateways with capability to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web/internet gateway.
- Subscribe to anti-phishing/anti-rouge app services from external service providers for identifying and taking down phishing websites/rouge applications.
- This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.
- Similar arrangements need to be ensured at the vendor managed facilities as well.
- Define and communicate to users/employees, that vendors' & partners' security policy is covering secure and acceptable use of Bank's network/assets including customer information/ data, educating them about cybersecurity risks and protection measures at their level.
- Encourage them to report suspicious behaviour incidents to the incident management team.
- Conduct targeted awareness/training for key personnel (at executive, operations, security related administration/operation and management roles, etc.).
- Evaluate the awareness level periodically.
- Establish a mechanism for adaptive capacity building for effective Cybersecurity Management. Making cyber security awareness programs mandatory for new recruits and web-based quiz & training for lower, middle & upper management every year. (Recent and past cyber-attacks show; cyber adversaries are also targeting bank employees).
- Board members may be sensitised on various technological developments and cyber security related developments periodically.
- Board members may be provided with training programmes on IT Risk / Cybersecurity Risk and evolving best practices in this regard so as to cover all the board members at least once a year.
- Improve and maintain customer awareness and education with regard to cybersecurity risks.
- Encourage customers to report phishing mails / phishing sites and on such reporting take effective remedial action.
- Educate the customers on the downside risk of sharing their login credentials/passwords etc. to any third-party vendor and the consequences thereof.
- For digital payment applications that are licensed by a third party vendor, entities shall put in place a source code escrow arrangement or other arrangements to adequately mitigate the risk

of default by the vendor. Entities shall ensure that all product updates and programme fixes are included in the source code escrow arrangement.

- The security controls for digital payment applications must focus on how these applications handle, store and protect payment data. The APIs for secure data storage and communication have to be implemented and used correctly in order to be effective. Entities shall refer to standards such as Open Web Application Security Project – Mobile Application Security Verification Standard (OWASP-MASVS), Open Web Application Security Project – Application Security Verification Standard (OWASP-ASVS) and other relevant OWASP standards, security and data protection guidelines in ISO 12812, threat catalogues and guides developed by NIST (including for Bluetooth and Long-Term Evolution (LTE) security), for application security and other protection measures. Such testing has to necessarily verify for vulnerabilities including, but not limited to OWASP/ OWASP Mobile Top 10, application security guidelines/ requirements developed/ shared by operating system providers / OEMs.
- Entities shall mention/ incorporate a section on the digital payment application clearly specifying the process and procedure (with forms / contact information, etc.) to lodge consumer grievances. A mechanism to keep this information periodically updated shall also be put in place. The reporting facility on the application shall provide an option for registering a grievance. Customer dispute handling, reporting and resolution procedures, including the expected timelines for the response should be clearly defined.
- Entities shall provide digital payment products and services, to a customer only at her/ his option based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions.
- Entities may explore the feasibility of implementing a code that checks if the device is rooted/ jailbroken prior to the installation of the mobile application and disallow the mobile application to install/ function if the phone is rooted/jailbroken.
- Implement Information Security Management System (ISMS) in particular ISO27001 best practices in the bank.
- Incident Response and recovery plan, Business Continuity Disaster Recovery plan shall be put in place and tested periodically.
- Participate in cyber drills.
- In case Security Operations Centre is being outsourced, REs to ensure adequate oversight and ownership overrule definition, customisation and related data/logs, meta data and analytics.
- The key length, algorithms, cipher suites and applicable protocols used in transmission channels, processing of data and authentication purpose shall be strong. REs shall adopt internationally accepted and published standards that are not deprecated/demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions.
- Ensure that there is no manual intervention or manual modification in data while it is being transferred from one process to another or from one application to another, in respect of critical applications.
- Data transfer mechanism between processes or applications must be properly tested, securely automated with necessary checks and balances, and properly integrated through “Straight Through Processing” methodology with appropriate authentication mechanism and audit trails.
- Ensure that the systems used and the remote access from alternate work location to the environment hosting RE’s information assets are secure.
- REs shall ensure that their rights and obligations and those of each of their service providers are clearly defined and set out in a legally binding written agreement.
- Access to data at RE’s location / data centre by service providers shall be on need-to-know basis, with appropriate controls to prevent security breaches and/or data misuse.

DETECT

- Have mechanisms to centrally/otherwise control installation of software/ applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. and mechanisms to block /prevent and identify installation and running of unauthorised software / applications on such devices/ systems.
- Put in place mechanisms for monitoring of breaches / compromises of environmental controls relating to temperature, water, smoke, access alarms, and service availability alerts (power supply, telecommunication, and servers), access logs, etc. Appropriate physical security measures shall be taken to protect the critical assets of the Bank.
- Have mechanisms to identify authorised hardware / mobile devices like laptops, mobile phones, tablets, etc.
- Have mechanism to automatically identify unauthorised device connections to the bank's network and block such connections.
- Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.
- Security Operation Centre to monitor the logs of various network activities and to have the capability to escalate any abnormal / undesirable activities.
- Enable logs of all ICT systems and maintain them securely for a rolling period of 180 days within the Indian jurisdiction.
- Deploy a Security Information and Event Management (SIEM) system in SoC for management of log from security devices and critical servers. The SIEM may be configured to automate event correlation between multiple devices and alert and threat generation.
- Monitor any abnormal changes in the pattern of logon.
- Get the removable media scanned for malware/anti-virus prior to providing read/write access.
- Consult all the stakeholders before finalising the scope, frequency and storage of log collection.
- Manage and analyse audit logs in a systematic manner so as to detect, understand or recover from an attack.
- Enough care is to be taken to capture audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be.
- Implement and periodically validate settings for capturing appropriate logs / audit trails of each device, system software and application software, ensuring that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or event and/or transaction.
- Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all delivery channels.
- Entities should provide a mechanism on their mobile and internet banking application for their customers to, with necessary authentication, identify/ mark a transaction as fraudulent for seamless and immediate notification to his entities. On such notification by the customer, they may endeavour to build the capability for seamless / instant reporting of fraudulent transactions to the corresponding beneficiary / counterparty's entities; vice-versa have mechanism to receive such fraudulent transactions reported from other entities.
- REs shall accurately define minimum monitoring requirements in the cloud environment.

RESPOND

- Report the incidents to RBI and CERT-In as per extant guidelines.
- Regulated Entities shall maintain updated contact details of service providers, intermediaries, external agencies and other stakeholders (including other entities) for coordination in incident response. Entities shall put in place a mechanism with the stakeholders to update and verify such contact details and shall also formulate specific SOPs to handle incidents related to payment ecosystem to mitigate the loss either to the customer or Entities.
- Define incidents, method of detection, methods of reporting incidents by employees, vendors and customers and periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type, allocate and communicate clear roles and responsibilities of personnel manning/handling such incidents, provide specialised training to such personnel, post incident review, periodically test incident response plans, incident management procedure.
- As a threat mitigation strategy, identify the root cause of incident and apply necessary patches to plug the vulnerabilities.
- Responding to cyber incidents: have written incident response procedures including the roles of staff / outsourced staff handling such incidents; response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication & co-ordination with stakeholders during response.
- Responding to cyber incidents: have a mechanism to dynamically incorporate lessons learnt to continually improve the response strategies.
- The vulnerabilities detected in the incident are to be remedied promptly in terms of the bank's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.
- The bank should notify the customer, through alternate communication channels, of all payment or fund transfer transactions above a specified value determined by the customer.
- Have support/arrangement for network forensics/forensic investigation/DDOS mitigation services on stand-by.
- Document and communicate strategies to respond to advanced attacks containing ransom ware/cyber extortion, data destruction, DDOS, etc.
- Contain the level of cyber-attack by implementing shielding controls/quarantining the affected devices/systems.

RECOVER

- Recovery from cyber incidents: in terms of improvements or lessons learnt from the incident, bank's BCP/DR capabilities shall adequately and effectively support its cyber resilience objectives and designed to enable the bank to recover rapidly from cyberattacks/ other incidents and safely resume critical operations aligned with recovery time objectives, while ensuring security of processes and data is protected.
- Recovery from cyber incidents: banks shall ensure such capabilities in all interconnected systems and networks, including those of vendors and partners and readiness demonstrated through collaborative & co-ordinated resilience testing, that meet the Bank's recovery time objectives.
- Such testing shall also include testing of crisis communication to customers and other internal and external stakeholders and also test the reputation management. Adequate capacity shall be planned and maintained, in consideration thereof.

IRAN

A. REGULATIONS

The Central Bank of the Islamic Republic of Iran (CBI), with the aim of centralized management and guidance of information security within banking infrastructures and information, as well as expanding, deepening, and optimizing cooperation and coordination with banks and credit institutions on one hand, and with other active governmental institutions and organizations in the field of information security on the other hand, is tasked with enhancing the security and resilience of the infrastructures and services of banks, financial and credit institutions, and the unorganized monetary market of the country through monitoring, evaluating, directing interactions and sharing information. The main components of these missions are defined as follows:

- Defining and documenting objectives and supervising the proper implementation of high-level policies, strategies, and "information security requirements."
- Defining and documenting the framework for managing and monitoring "information security risks."
- Research and development in the field of information security.
- Integrated coordinating and managing information security-related incidents within the banking system in a hierarchical structure and in cooperation with active "CERTs" in banks, financial and credit institutions, and the unorganized monetary market.
- Designing and providing an incident and information security status reporting system.
- Increasing the level of security awareness in the banking system through the dissemination and sharing of information related to threats, vulnerabilities, and information security incidents.
- Coordinating to provide necessary training regarding the objectives, structures, high level policies, strategies, and information security requirements.

The following are the information security regulations applicable to banks and non-banking credit institutions, developed and announced by CBI under the missions of setting objectives, supervising the proper implementation of high-level policies, strategies and information security risks and setting the framework for managing and monitoring information security risks.

a) The Requirements for Information Security Organization in Banks and Credit Institutions with Document ID BIS RG 100-10 as per Circular No. 49751/97 dated 20/02/1397 (2018)
This document outlines the requirements that banks and credit institutions must adhere to in organizing information security and assigning information security roles. Additionally, the necessary guidelines for adhering to these requirements are provided in a document titled "Information Security Organization Guide".

Due to the achieving the expected maturity resulting from at least three years of implementing the information security organization requirements, an addendum was issued in 1402. This addendum mandates the establishment of a separate Organizational unit for information security under management of the Chief Executive Officer (CEO), Direct reporting of the Chief Information Security Officer (CISO) to the CEO and the essential functions of the information security unit, as per Circular No. 49804/1401.

b) The Organizational and Information System Security Controls Framework for Banking Industry (OISSCF) with Document ID BIS RG 100-15 as per Letter No. 6073/4/02/m/d dated 21/01/1402 (2023)

The security control framework has mainly been extracted from the standards such as NIST SP 800-53, PCI DSS, and ISO 27001 and has been communicated to banks and non-banking credit institutions under the title "Coordinated Program for Enhancing Security in the Monetary and Financial Sector". The OISSCF is a comprehensive set of over 1133 controls containing various domains and maturity levels, both for organizational and system-based perspectives.

The organizational and information system security controls are classified into 6 domains, 16 categories, and 62 subcategories. The domains of security controls include Cybersecurity Governance (G), Cyber Resilience (R), Cyber Development and Maintenance (D), Cyber Intelligence (I), Cyber Protection (P), and Cyber Business Relations (B).

The method of implementing these security controls in each bank is based on the risk management framework using NIST SP 800-37 and mandates a set of security controls as a baseline, based on the "bank's inherent risk" and "business impact" level of the information system.

c) Requirements for Reporting Information Security Incidents with Document ID BIS RG 200-10, as per Circular Number 49488/97 dated 20/02/1397 (2018)

The main objectives of information security incident reporting system developed by CBI are:

- coordinated and integrated management of information security-related incidents at the level of the banking system, within a hierarchical structure and with the collaboration of bank's CERTs;
- developing an incident reporting and information security status system.

This Requirement includes obligations for:

- reporting information security incidents to CBI CERT;
- responsibilities and authorities of the banks and credit institutions;
- disciplinary process.

d) Requirements for Strong Customer Authentication in Remote Electronic Banking Services with Document ID BIS RG 300-18, as per Circular Number 311417/99 dated 01/10/1399 (2020)

In order to safeguard and protect the bank customers' assets against attacks such as brute force, phishing, keystroke logging, session hijacking, man-in-the-middle attacks, tampering, and social engineering, CBI has issued regulations for implementing "strong customer authentication" in the following cases:

- access to remote electronic banking services;
- initiating electronic payment transactions;
- performing high-risk actions, and
- any other actions that, at the discretion of the financial institution or according to notified laws and regulations by relevant authorities, may lead to fraud or misuse of a customer's bank account.

e) Requirements of the Banking Security Operations Center with Document ID BIS RG 200-12, Subject to Circular Number 49804/1401 dated 08/11/1401 (2023)

Security Operations Center (SOC) aims to meet the objectives such as maximizing the utilization of common security tools, integrating and correlating the information gathered by

each of tools, and helping the organizations to get a comprehensive insight of overall security status. For stablishing an effective SOC, banks need to develop policies, procedures and employ specialized and competent human resources and also related technologies.

For insuring effectiveness of SOC's in banks, CBI issued the Requirements of the Banking Security Operations Center. These requirements include CBI expectations in technology, process and people aspects.

B. FUNCTIONAL CATEGORIZATION

Some of the issued regulations are under the category of Governance and will cover the other functions:

- **The requirements for Organizing Information Security in Banks and Credit Institutions are considered entirely within the governance function;**
- **The preparation step in the OISSCF;** the purpose of this step is to conduct essential activities to enable the organization to start risk management process. In this step, roles and responsibilities of risk management, risk assessment, risk treatment strategy, determination of inherent risks of business, and prioritization of information systems for risk management must be defined.

IDENTIFY

- **The following topics from the OISSCF fall under the "identify" functional category:**
- **Preparation, Information Systems categorization and Control Selection Steps:**
  - The purpose of preparation step is to conduct essential activities to enable the organization to start risk management process.
  - The purpose of the categorization step is to identify the security requirements of the information system to determine its necessary control baseline. The information system's control baseline is determined based on a combination of the information system's security impact level and the bank's inherent risks of business level.
  - In the control selection step, the security controls that the bank needs to implement based on the system's security classification or risk assessment are determined and, if necessary, customized.
- **Controls set within the Cybersecurity Governance (G) domain – Supervision Category:**
  - Controls including the requirement for security objectives, security strategies, security architecture (non-technical), high level security policies (-Irrelevant), effectiveness indicators, etc.;
  - Controls related to risk management;
  - Controls related to the allocation of financial and human resources;
  - Controls addressing structural security requirements and high-level roles and responsibilities.

- **Controls set within the Cybersecurity Development and Maintenance (D) domain – Asset Management Category:**
  - Controls for creating, maintaining, and detailing asset lists.
- **Controls set within the Cybersecurity Protection (P) domain – Asset Management Category:**
  - Controls related to the security classification of information and information assets
- **Controls set within the Cybersecurity Development and Maintenance (D) domain – Security Testing Category:**
  - Requirements related to identifying vulnerabilities of information systems;
  - Penetration testing requirements.

PROTECT

- **The following topics from the Banking Organizational and Information Systems Security Control Framework fall under the "Protect" functional category:**
  - **Controls set within the Cybersecurity Protection domain (P) – Access Management Category:**
    - Controls related to mechanisms (including the number of factors) and quality of authentication operations;
    - Authorization controls, including authorization policies; (principles of least privilege, etc.), authorization procedures, monitoring, and reviewing access permissions, etc.;
    - Identity management requirements, including definition, assignment, and administration of identities;
    - Controls that must be considered in the information system login process, such as notification of usage responsibilities, response to failed login attempts, etc.;
    - User session management controls, such as session timeout restrictions, closing or locking inactive sessions;
    - Management, delivery, and removal or adjustment of authenticators (including passwords);
    - Controls related to the quality of authenticators (length, complexity, and lifetime for passwords, quality of algorithms, etc., for authentication tokens);
    - Authorization controls for network connections;
    - Authorization controls for privileged access;
    - Authorization controls for remote access and telecommuting;
    - Authorization controls for installation and use of software.
  - **Controls set within the Cybersecurity Protection domain (P) – Data Protection Category:**
    - Controls for protecting the confidentiality and integrity of stored data;
    - Controls for protecting the confidentiality and integrity of data in transit and data exchange agreements and procedures.
  - **Controls set within the Cybersecurity Protection domain (P) – System Hardening Category:**
    - Controls for hardening equipment and systems by establishing configuration baselines and applying secure configurations;
    - Controls for malware protection;
    - Controls for security patch management procedures.
  - **Controls set within the Cybersecurity Protection domain (P) – Network Security Category:**
    - Network segmentation and traffic monitoring controls;
    - Controls related to intrusion detection and prevention systems;

  - Security controls for wireless networks, including specific settings and configurations for wireless networks.
- **Controls set within the Cybersecurity Protection domain (P) – Physical Security Category:**
  - Controls for physical access to buildings and secure environments;
  - Controls to counter incidents and adverse environmental conditions, such as fire, temperature, humidity, etc.;
  - Physical protection of assets, including storage and operation areas, access to equipment (or its outputs and functions), detecting and countering physical tampering or sabotage of assets;
  - Requirements related to backup equipment and facilities, such as backup power sources, cooling equipment, etc.
- **Controls set within the Cybersecurity Business Relationships (B) domain – Human Resource Security Category:**
  - Controls to mitigate risks arising from the bank's personnel, including contractual requirements, behavioral frameworks, security responsibilities, role and duty segregation, screening, termination requirements, qualifications;
  - General security training and awareness controls.
- **Controls set within the Cybersecurity Intelligence domain (I) – Event Management and Logging category:**
  - Requirements for log generation;
  - Requirements for preserving and maintaining logs;
  - Controls related to forensic;
- **Controls set within the Cybersecurity Development and Maintenance (D) domain – System Development Lifecycle Category:**
  - Requirements related to identifying security needs, system design and technical architecture;
  - Software development environment requirements, including data exchange methods and secure development process;
  - System development policies and secure development process requirements, including procedures and responsibilities;
  - Controls for maintaining the integrity of source code and system runtime files;
  - Controls related to managing the risks of outsourcing system development, including technical and intellectual property requirements;
  - Controls related to system and software testing (including avoiding common and known weaknesses and vulnerabilities) and pre- release and post-release requirements.
- **Requirements for Strong Customer Authentication in Remote Electronic Banking Services**

DETECT

- **The following topics from Banking Organizational and Information Systems Security Control Framework fall under the "detect" functional category:**
  - **Controls set within the Cybersecurity Intelligence (I) domain – Security Insight Category:**
    - Requirements for reviewing and responding to event logs, events and information correlation, and extracting patterns or supplementary information;
    - Requirements related to threat intelligence and threat information sharing.
- **Requirements for the Banking Security Operations Center**

RESPOND

- **The following topics from the Banking Organizational and Information Systems Security Control Framework fall under the "respond" functional category:**
  - **Controls set within the Cybersecurity Resilience (R) domain – Incident Management Category:**
    - Incident management processes and requirements, including roles and responsibilities, response procedures, etc.;
    - Training, testing, and preparation for incident response, and mechanisms for employee participation in incident management (including incident identification and reporting);
    - Controls related to incident analysis and learning from incidents.
- **Requirements for Information Security Incident Reporting**

RECOVER

- **The following topics from the Banking Organizational and Information Systems Security Control Framework fall under the "recover" functional category:**
  - **Control sets within the Cybersecurity Resilience domain (R) – Continuity Management Category:**
    - Controls for identifying requirements, planning, preparing, executing continuity plans, testing and training, and related capabilities;
    - Controls related to backing up information;
    - Controls related to managing risks arising from equipment failures and the existence of single points of failure.

RUSSIA

In the Russian Federation the main directions of the state policy in the field of security are determined by the President of the Russian Federation (Federal Law No. 390-FZ, dated 28 December 2010, "On Security" (as amended on 10 July 2023), the source of the publication "Rossiyskaya Gazeta", No. 295, dated 29 December 2010).

The Bank of Russia, being an industry mega-regulator, establishes information security requirements for regulated entities, as agreed with the federal executive authority responsible for ensuring information security.

The Bank of Russia has created a special structural unit, FinCERT.

On the basis of FinCERT, a system of information exchange has been created between financial market participants, law enforcement agencies, telecom providers and operators, system integrators, anti-virus software developers and other companies engaged in information security.

Information exchange participants inform about threats they have identified and attacks committed on them, and Financial CERT provides recommendations on how to address these risks.

Detailed information about FinCERT on the official website of the Bank of Russia http://www.cbr.ru/information_security/fincert/

The information security regulations issued by the Bank of Russia cover (but are not limited to) three main areas of application:
1. Information security requirements covering technological aspects of processing protected information (technological guarantees of information security);
2. Information security requirements applicable to the application software of automated systems and applications;
3. Information security requirements that apply to the information technology infrastructure.

The regulations within this structure affect three large groups of participants:
1. National payment system participants, including participants of the Payment System of the Bank of Russia, regarding money transfers (Regulations No. 821-P and 802-P);
2. Credit institutions, regarding banking issues (Regulation No. 683-P);
3. Non-credit Financial Institutions, regarding financial market activities (Regulation No. 757-P);

This material has been prepared as a follow-up to Information Security Regulations in Finance BRICS e-Booklet published by Reserve Bank of India.

Functional categorization of documents in the field of information security of financial market participants according to the main information security functions (The CSF Core Functions) and according to The NIST Cybersecurity Framework (CSF) 2.0 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf**) you can find in the attached file:** Mapping to the NIST CSFs 2.0 function**).**

Below you will find a more detailed description of the documents from the Mapping, namely: the details of the document, the source of the publication, the main idea of the document.

Doctrines, strategies, concepts

"The Guidelines for the Advancement of Information Security in the Financial Sector for 2023–2025" (approved by the Bank of Russia Board of Directors on 22 May 2023).

Publication source: official website of the Bank of Russia http://www.cbr.ru

Function: Govern
Category: Organizational Context

Decree of the President of the Russian Federation No. 646, dated 5 December 2016, "On the Approval of Information Security Doctrine of the Russian Federation".

Publication source: official Internet portal of legal information http://www.pravo.gov.ru

Function: Govern
Category: Organizational Context

Decree of the President of the Russian Federation No. 400, dated 7 February 2021, "On National Security Strategy of the Russian Federation".

Publication source: official Internet portal of legal information http://www.pravo.gov.ru

Function: Govern
Category: Organizational Context

Regulatory Legal Acts

Federal Law No. 187-FZ, dated 26 July 2017 (as amended on 10 October 2023), "On Security of the Critical Information Infrastructure of the Russian Federation".

Publication source: official Internet portal of legal information http://www.pravo.gov.ru

Function: Govern
Category: Roles, Responsibilities and Powers

Decree of the President of the Russian Federation No. 250, dated 1 May 2022 (as amended on 3 June 2024), "On Additional Measures to Ensure Information Security of the Russian Federation".

Publication Source: the official Internet portal of legal information http://www.pravo.gov.ru

Function: Govern
Category: Roles, Responsibilities and Powers

Decree of the Government of the Russian Federation No. 1272, dated 15 July 2022, "On Approval of the Model Regulation on the Deputy Head of the Body (Organization) Responsible for Ensuring Information Security in the Body (organization) and the Model Regulation on the Structural Unit in the Body (organization) Ensuring Information Security of the Body (Organization)".

It defines the powers, rights and obligations of the body (organization) responsible for ensuring information security in the body (organization), including for detecting, preventing and eliminating the consequences of computer attacks, and responding to computer incidents (responsible person).

Publication source: official Internet portal of legal information http://www.pravo.gov.ru

Function: Govern
Category: Roles, Responsibilities and Powers

National standards

National Standard of the Russian Federation GOST R 57580.1-2017 "Financial (Bank) Transaction Security. Data Protection in Financial Organisations. Core Arrangements and Controls" (approved and put into effect by Rosstandart Order No. 822-st, dated 8 August 2017).

Publication source: Standartinform, 2017

Function: Identity
Category: Risk Assessment – item 7.4 Process 3 "Monitoring the Integrity and Security of Information Infrastructure"
Category: Improvement – item 8.5 Direction 4 "Improvement of the Information Security System Process"
Category: Risk Assessment – item 7.4 Process 3 "Control of the Integrity and Security of the Information Infrastructure"

Function: Protect
Category: Identity Management – access management process
Category: Awareness and Training – Direction 2 "Implementation of the Information Security System Process" – item 8.3.1
Category: Data Security
Category: Platform Security
Function: Detect
Category: Continuous Monitoring – item 7.7.1 Subprocess "Monitoring and Analysis of Information Security Events"

In order to ensure the information security requirements of IT infrastructures, the standard provides for the following information protection processes (and subprocesses) that implement the detection function:

- Detection of violations and attacks on the network, which should ensure:
  - monitoring the content of network traffic;
  - registration of information security events related to the results of monitoring the content of network traffic;
- Verification of the integrity and security of the IT infrastructure, which should provide:
  - monitoring of the occurrence of any known (described) vulnerabilities in the protection of information of the IT systems;
  - organization and control of the placement, storage and updating of software of the IT infrastructure;

- monitoring of the content and integrity of the software of the IT infrastructure;
- registration of the information security events related to the results of monitoring the integrity and protection of the information infrastructure.

Function Respond
Category – item 7.7.2 Subprocess "Detection of Information Security Incidents and Response to Them"
Category – Incident Mitigation – item 7.7.2 Subprocess "Detection of Information Security Incidents and Response to Them"

National Standard of the Russian Federation GOST R 57580.2-2018 "Security of Financial (Banking) Operations. Information Protection of Financial Organizations. Conformity Assessment Methods" (approved and put into effect by Rosstandart Order No. 156-st, dated 28 March 2018).

Publication source: Standartinform, 2018

The standard establishes requirements for the methodology and design of the results of assessing the compliance of information protection in a financial organization when choosing and implementing organizational and technical information protection measures to the requirements of GOST R 57580.1, used by financial organizations to meet the information protection requirements established by the regulations of the Bank of Russia.

Function: Govern
Category: Oversight

National Standard of the Russian Federation GOST R 57580.3-2022 "Security of Financial (Banking) Operations. Information Threat Risk Management and Ensuring Operational Resilience. General Principles' Methods" (approved and put into effect by Rosstandart Order No. 1548-st, dated 22 December 2022).

Publication source: M.: FSBI Russian Standardization Institute, 2023

This standard defines the requirements for the composition and content of measures to manage the risk of information threats for the levels of protection that are used by financial organizations as part of the planning, implementation, control and improvement of the risk management system, as well as management systems defined within the standards on operational reliability and information protection. The standard is intended for use by credit institutions and non-credit financial institutions.

In order to reduce the likelihood of adverse consequences for the smooth functioning of the payment system, as well as to ensure the proper provision of services to banks and their customers, it is recommended that operators of payment infrastructure services and operators of information exchange services apply measures within a number of processes of the information threat risk management system. In addition, the standard can be applied by other organizations implementing innovative business and technological processes related to the provision of financial and banking services, including money transfer services and (or) information services.

Function: Identify
Category: Risk Assessment
Function: Protect
Category: Technology Infrastructure Resilience
Function: Respond
Category: Incident Mitigation
Function: Recover
Category: Incident Recovery Plan Execution, Incident Recovery Communication

National Standard of the Russian Federation GOST R 57580.4-2022 "Security of Financial (Banking) Operations. Ensuring Operational Resilience. Basic Set of Organizational and Technical Measures" (approved and put into effect by Rosstandart Order No. 1549-st, dated 22 December 2022).

Publication source: M.: FSBI Russian Standardization Institute, 2023

The standard establishes requirements for the composition and content of operational reliability measures for those levels of protection that financial organizations apply when determining the basic composition of such measures. The standard is intended for use by credit institutions and non-credit financial institutions. In order to reduce the likelihood of negative consequences for the smooth functioning of the payment system, as well as the proper provision of services to banks and their customers, it is recommended that operators of payment infrastructure services and information exchange service providers apply operational reliability measures defined by the standard. In addition, the standard can be applied by other organizations implementing innovative business and technological processes related to the provision of financial and banking services, including money transfer services and (or) information services.

Function: Govern Category
Risk Management Strategy
Function: Identify
Category: Risk Assessment

National Standard of the Russian Federation GOST R ISO/IEC 27000-2021 "Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary" (approved and put into effect by Rosstandart Order No. 392-st, dated 19 May 2021).

Publication source: Standartinform, 2021

The standard is identical to ISO/IEC 27000:2018 "Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary", IDT).

Function: Govern
Category: Organizational Context
Function: Protect
Category: Awareness and Training

National Standard of the Russian Federation GOST R ISO/IEC 15408-3-2013.

"Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 3. Security Assurance Requirements" (approved and put into effect by Rosstandart Order No. 1340-st, dated 8 November 2013).

Publication source: Standartinform, 2014

The standard is identical to ISO/IEC 15408-3:2008 “Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3. Security Assurance Components”.

Function: Identify
Category: Risk Assessment

Regulatory Acts of the Bank of Russia

Bank of Russia Regulation No. 822-P, dated 30 August 2023, “On the Requirements for the Security of Information in the Automated Information System of Insurance”.

Publication source: official website of the Bank of Russia http://www.cbr.ru/

The Regulation establishes requirements for ensuring the protection of information contained in the automated insurance information system.

Function: Identify
Category: Asset Management
Function: Protect
Categories: Access Control, Data Security, Platform Security
Function: Respond
Categories: Incident Analysis, Incident Management

Bank of Russia Regulation No. 821-P, dated 17 August 2023, “On the Requirements for the Protection of Information Relating to Funds Transfers and on the Procedures for the Bank of Russia to Control Compliance with the Requirements for the Protection of Information Relating to Funds Transfers” (registered with the Ministry of Justice of the Russian Federation on 6 December 2023 No. 76286).

Publication source: official website of the Bank of Russia http://www.cbr.ru/

The Regulation establishes requirements for providing money transfer operators, bank payment agents (subagents), information exchange service operators, payment application providers, payment system operators, payment infrastructure service operators, operators of electronic information protection platforms when making money transfers, as well as the procedure for the Bank of Russia to monitor compliance with protection requirements information when making money transfers.

Function: Identify
Category: Asset Management
Function: Protect
Categories: Platform Security, Data Security
Function: Respond
Categories: Incident Management, Incident Response Reporting and Communication

Bank of Russia Regulation No. 802-P, dated 25 July 2022, “On the Requirements for Information Security” (together with “Rules for Material and Technical Support of Electronic Message Generation and Control of Electronic Message Details in the Information Infrastructure of

the Exchange Participant in the Course of Money Transfers in the Bank of Russia Payment System Using the Urgent Transfer Service and the Non-urgent Transfer Service, as well as the Rules for Material and Technical Support of Electronic Message Processing and Control of Electronic Message Details in the Information Infrastructure of the Operational Center, Payment Clearing Member") (registered with the Ministry of Justice of the Russian Federation on 25 November 2022 No. 71124).

Publication source: official website of the Bank of Russia http://www.cbr.ru/

Function: Identify
Category: Asset Management
Function: Protect
Categories: Identity Management, Data Security, Platform Security
Function: Respond
Categories: Incident Management, Incident Analysis, Incident Response Reporting

Bank of Russia Regulation No. 716-P, dated 8 April 2020, "On the Requirements for the Operational Risk Management System in a Credit Institution or a Banking Group" (as amended on 25 March 2022 (registered with the Ministry of Justice of the Russian Federation on 3 June 2020 No. 58577).

Publication source: official website of the Bank of Russia http://www.cbr.ru/

Function: Govern, Categories: Risk Management Strategy, Cybersecurity Supply Chain Risk Management

Bank of Russia Regulation No. 683-P, dated 17 April 2019, "On Mandatory Requirements for Credit Institutions to Ensure Data Protection in Banking to Counter Unauthorised Funds Transfers" (as amended on 6 December 2023, registered with the Ministry of Justice of the Russian Federation on 16 May 2019 No. 54637).

Publication source: official website of the Bank of Russia http://www.cbr.ru/

The Regulation establishes mandatory requirements for credit institutions to ensure the protection of information in banking activities in order to counter unauthorized money transfers. These requirements apply to data infrastructure facilities, application software for automated systems and applications, and secure data processing technologies. The requirements are applied to protect data prepared, processed and stored in automated systems that are part of data infrastructure facilities and are used in banking transactions related to money transfers.

Function: Identify
Category: Asset Management
Function: Protect
Categories: Data Security, Platform Security
Function: Respond
Categories: Incident Management, Incident Analysis, Incident Response Reporting and Communication

Regulation of the Bank of Russia dated 20 April 2021 No. 757-P (rev. dated 20 April 2021) "On Establishing Mandatory Requirements for Non-Credit Financial Organizations to Ensure Protection of Information in the Course of Activities in the Field of Financial Markets in order to Counteract Illegal Financial Transactions" (registered in the Ministry of Justice of the Russian Federation 15 June 2021 No. 63880).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The Bank of Russia has established mandatory requirements for non-banking financial institutions (NBFIs) in terms of information protection to prevent illegal financial transactions. The requirements are basically similar to the requirements for credit organizations established by Regulation 683-P. The document also contains a list of types of protected information, information protection requirements for data infrastructure objects, software and technologies for processing protected data. The requirements are differentiated depending on the level of data protection applicable to a particular NBFI.

Function: Identify
Category: Asset management
Function: Protect
Category: Data security, Platform security
Function: Respond
Category: Incident Management, Incident Analysis, Incident Response Reporting

Regulation of the Bank of Russia dated 17 October 2022 No. 808-P "On requirements to ensure protection of information when carrying out activities in the field of professional services on the financial market in order to counteract the implementation of illegal financial transactions, mandatory for persons providing professional services on the financial market, to ensure that credit history bureaus protect information specified in Article 4 of the Federal Law "On Credit Histories" during its processing, storage and transmission by certified means of protection, as well as to the safety of information, and to ensure that the information is protected by certified means of protection (registered in the Ministry of Justice of the Russian Federation 7 December 2022 No. 71409).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The Regulation establishes mandatory requirements for persons providing professional services in the financial market to ensure the protection of information when carrying out activities in the field of professional services in the financial market in order to counteract the implementation of illegal financial transactions, requirements to ensure the protection of information by credit history bureaus, during its processing, storage and transmission by certified means of protection, requirements to the safety and protection of information obtained in the process of credit rate activity.

Function: Identify
Category: Asset management
Function: Respond
Category: Incident Management, Incident Analysis, Incident Response Reporting
Function: Identify
Category: Asset management
Function: Protect
Category: Data security, Platform security

Regulation of the Bank of Russia dated 7 December 2023 No. 833-P "On Requirements to Information Protection for Digital Ruble Platform Participants" (together with "Requirements to Information Protection applicable to the technology of processing and transmission of electronic messages in transactions with digital rubles", "Requirements to Information Protection applicable to the client's application") (registered in the Ministry of Justice of the Russian Federation 29 December 2023 No. 76729).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The Regulation establishes requirements for ensuring information protection for participants in the digital ruble platform.

Function: Identify
Category: Asset management
Function: Respond
Category: Incident Management, Incident Analysis, Incident Response Reporting
Function: Protect
Category: Data security, Platform security

Regulation of the Bank of Russia dated 12 January 2022 No. 787-P (rev. dated 6 October 2023) "On mandatory requirements for credit organizations to operational reliability in banking activities in order to ensure continuity of banking services" (registered in the Ministry of Justice of the Russian Federation 8 April 2022 No. 68140).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The Regulation establishes mandatory requirements for credit organizations for operational reliability in carrying out banking activities in order to ensure continuity of banking services.

Function: Identify
Category: Asset management
Function: Protect
Category: Resilience of technological infrastructure

Regulation of the Bank of Russia dated 15 November 2021 No. 779-P "On Establishing Mandatory Requirements for Non-Credit Financial Institutions for Operational Reliability in Conducting Types of Activities Provided for by Part One of Article 76.1 of the Federal Law dated 10 July 2002 No. 86-FZ "On the Central Bank of the Russian Federation (Bank of Russia)" to Ensure Continuity of Financial Services (Except for Banking Services)" (registered in the Ministry of Justice of the Russian Federation 28 March 2022 No. 67961).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The Regulation establishes mandatory requirements for non-credit financial organizations to operational reliability in order to ensure continuity of financial services (except for banking services).

Function: Identify
Category: Asset management
Function: Protect
Category: Resilience of technological infrastructure

Regulation of the Bank of Russia dated 30 June 2023 No. 819-P "On Requirements to Operational Reliability of the Operator of the Automated Insurance Information System" (registered in the Ministry of Justice of the Russian Federation 3 August 2023 No. 74588).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The Regulation establishes requirements for the operational reliability of the operator of the automated insurance information system.

Function: Identify
Category: Asset management
Function: Protect
Category: Resilience of technological infrastructure

Decree of the Bank of Russia dated 15 April 2015 No. 3624-U (rev. dated on 6 October 2023) "On Requirements to the Risk and Capital Management System of a Credit Organization and a Banking Group" (together with "Requirements to the Organization of Procedures for Managing Certain Types of Risks") (registered in the Ministry of Justice of the Russian Federation 26 May 2015 No. 37388).

Publication source: "Bank of Russia Bulletin", No. 51, 15 June 2015.

Function: Govern
Category: Risk management Strategy

Decree of the Bank of Russia dated 25 September 2023 No. 6540-U "On the list of security threats relevant to the processing of biometric personal data, vectors of the unified biometric system, verification and transmission of information on the degree of compliance of vectors of the unified biometric system with the provided biometric personal data of a natural person during the interaction of information systems of financial market organizations with the unified biometric system" (registered in the Ministry of Justice of the Russian Federation 26 October 2023 No. 75742).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

Function: Identify
Category: Asset management

Decree of the Bank of Russia dated 25 September 2023 No. 6541-U "On the list of security threats relevant in the processing of biometric personal data, vectors of the unified biometric system, verification and transmission of information on the degree of compliance of vectors of the unified biometric system with the provided biometric personal data of an individual in the information systems of financial market organizations that carry out authentication on the basis of biometric personal data of individuals, except for the unified biometric system, as well as relevant in the processing of biometric personal data, vectors of the unified biometric system, and also relevant in the processing of biometric personal data, vectors of the unified biometric system (registered in the Ministry of Justice of the Russian Federation 26 October 2023 No. 75743).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

Function: Identify
Category: Asset management

Decree of the Bank of Russia dated 30 August 2023 No. 6515-U "On Determination of Security Threats in Processing Personal Data in the Automated Insurance Information System" (registered in the Ministry of Justice of the Russian Federation 23 November 2023 No. 76079).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The Guideline defines security threats in the processing of personal data in the automated insurance information system.

Function: Identify
Category: Asset management

Standards, recommendations of the Bank of Russia

"Standard of the Bank of Russia "Security of Financial (Banking) Operations. Ensuring the security of financial services using digital fingerprint technology" STO BR BFBO-1.7-2023" (adopted and enacted by Order of the Bank of Russia No. OD-335 dated 1 March 2023).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The standard provides for the formation of a unique digital fingerprint of user devices in order to take measures to counteract money transfers without customer consent (antifraud measures) in banking and financial transactions using untrusted devices that do not act in full compliance with expectations and do not do what they are supposed to do, to detect fraud and chains of related transactions, to deal with information security incidents and transactions made by the customer, and to identify and detect fraudulent transactions.

Function: Detect
Category: Adverse Event Analysis
Function: Respond
Category: Incident Analysis

"Bank of Russia Standard "Security of Financial (Banking) Operations. Application program interfaces. Ensuring security of financial services at initiation of openid connect by client of authentication flow through a separate channel. Requirements" STO BR FAPI.PAOK-1.0-2021" (adopted and enacted by Order of the Bank of Russia No. OD-1536 dated 23 July 2023).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The standard is based on the OpenID Connect Client Initiated Backchannel Authentication Flow – Core and Client Initiated Backchannel Authentication Profile specifications of the OpenID Foundation (OIDF), an organization that promotes and supports the OpenID community and technologies (OpenID Connect Core (OIDC), OpenID Connect Discovery (OIDD) and others) and defines the use of the application programming interface (API) model with structured data to enhance the security of financial technologies in the case of OpenID Connect client initiated backchannel authentication flow.

Function: Protect
Category: Identity management

"Bank of Russia Standard "Security of Financial (Banking) Operations. Applied program interfaces to ensure the security of financial services based on the OpenID protocol. Requirements" STO BR FAPI.SEC-1.6-2020" (adopted and enacted by Order of the Bank of Russia No. OD-1650 dated 9 October 2020). The standard is developed on the basis of specifications of the OpenID Foundation (OIDF), which promotes and supports the OpenID community and technologies (OpenID Connect Core (OIDC), OpenID Connect Discovery (OIDD) and others), and defines the procedure for using the model of application programming interfaces (API) with structured data and token model to improve the security of financial technology.

Function: Protect
Category: Identity management

"Bank of Russia Standard "Security of Financial (Banking) Operations. Management of incidents related to the realization of information threats and operational reliability incidents. About forms and terms of interaction of the Bank of Russia with credit organizations, non-credit financial organizations and subjects of the national payment system in identifying incidents related to the implementation of information threats and incidents of operational reliability" STO BR BFBO-1.5-2023" (adopted and put into effect by Order of the Bank of Russia dated 8 February 2023 No. OD-215).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The standard allows financial organizations to inform the Bank of Russia of actions taken to address an information protection incident and also allows the Bank of Russia to provide recommendations on possible actions in relation to the incident.

This standard establishes the procedure for interaction between the Bank of Russia and credit organizations, non-credit financial organizations and subjects of the national payment system in identifying violations of information protection requirements. Forms for requesting and submitting information are provided. The Bank of Russia's regulations provide for mandatory registration of any incidents related to violations of information security requirements, including incidents that have led or may lead to unauthorized banking operations or failure to provide services, in particular incidents included in the list of incident types ("information protection incidents").

Function: Respond
Category: Incident management, Incident Analysis, Incident response reporting

"Standard of the Bank of Russia "Ensuring Information Security of Organizations of the Banking System of the Russian Federation. Information Security Risk Management in Outsourcing" STO BR IBBS-1.4-2018" (adopted and enacted by Order of the Bank of Russia dated 6 March 2018 No. OD-568) (adopted and put into effect by Order of the Bank of Russia dated 6 March 2018 No. OD-568).

Publication source: “Bank of Russia Bulletin”, No. 27, 30 March 2018

The purpose of the standard is to establish requirements for managing and controlling the risk of IS breach in outsourcing, the fulfillment of which creates a basis for ensuring that the level of IS breach risk in outsourcing business functions corresponds to the level of IS breach risk accepted independently by the BS RF organization, as well as a basis for mitigating such risk.

Function: Govern
Category: Supply chain risk management

“Standard of the Bank of Russia “Ensuring Information Security of Organizations of the Banking System of the Russian Federation. Collection and analysis of technical data when responding to information security incidents in the process of money transfers” STO BR IBBS-1.3-2016” (adopted and put into effect by Order of the Bank of Russia dated 30 November 2016 No. OD-4234).

Publication source: “Bank of Russia Bulletin”, No. 107, 8 December 2016

The standard applies to organizations that perform the functions of money transfer operators or payment infrastructure service operators, and establishes recommendations for organizational, technological and technical approaches related to the collection, processing, analysis of information security incidents in the process of money transfers.

Function: Respond
Category: Incident Analysis

“Standard of the Bank of Russia “Ensuring information security of organizations of the banking system of the Russian Federation. General Provisions” STO BR IBBS-1.0-2014” (adopted and put into effect by the Order of the Bank of Russia dated 17 May 2014 No. R-399).

Publication source: “Bank of Russia Bulletin”, No. 48-49, 30 May 2014

The standard applies to the Bank of Russia, credit institutions and representative offices of foreign banks. To manage information security risks, each institution creates an authorized body – its information security service, which may be a separate unit or persons responsible for information security. Thus, an information security policy is developed, as well as threat and intruder models and relevant procedures.

Special attention is paid to the processing of personal data. The information security management system is described in detail. The procedure for the development of internal documents related to information security, as well as the general procedure for self-assessment and auditing in terms of information security are established.

Function: Govern
Category: Organizational context
Function: Detect
Category: Continuous monitoring

“Standard of the Bank of Russia “Ensuring Information Security of Organizations of the Banking System of the Russian Federation. Methodology for assessing compliance of information security of organizations of the banking system of the Russian Federation with the requirements of STO BR IBBS-1.0-2014” STO BR IBBS-1.2-2014” (adopted and put into effect by the Order of the Bank of Russia dated 17 May 2014 No. P-399).

Publication source: “Bank of Russia Bulletin”, No. 48-49, 30 May 2014

The standard establishes methods for determining the degree of compliance with the requirements of the Bank of Russia’s standard STO BR IBBS-1.0-2014 “Ensuring information security of organizations of the banking system of the Russian Federation. General Provisions”, as well as the final level of compliance of information security with the requirements of the Bank of Russia standard STO BR IBBS-1.0-2014 “Information Security of Organizations of the Banking System of the Russian Federation. General Provisions” during information security audit and information security self-assessment.

Function: Govern
Category: Oversight

“Standard of the Bank of Russia “Ensuring Information Security of Organizations of the Banking System of the Russian Federation. Information Security Audit” STO BR IBBS-1.1-2007” (adopted and put into effect by Order of the Bank of Russia dated 28 April 2007 No. R-345).

Publication source: “Bank of Russia Bulletin”, No. 29, 18 May 2007

The standard applies to organizations of the banking system, as well as to organizations that audit information security of banking organizations, and establishes requirements for the external audit of information security of banking organizations.

Function: Detect
Category: Continuous monitoring

“Standard of the Bank of Russia “Security of Financial (Banking) Operations. Ensuring security of financial services during remote identification and authentication. Composition of information protection measures” STO BR BFBO-1.8-2024” (adopted and put into effect by Order of the Bank of Russia dated 28 February 2024 No. OD-326).

Publication source: official website of the Bank on Russia http://www.cbr.ru/

The standard establishes the composition and content of measures to ensure confidence in the results of identification and authentication of customers – recipients of services in the remote provision of financial products and services by providers of financial products and services in order to implement the requirements of the Bank of Russia at the technological section of identification, authentication and authorization of customers in the implementation of banking activities, activities in the field of financial markets, provided for by part one of Article 76.1 of the Federal Law dated 10 July 2002 No. 86-FZ “On the Central Bank of the Russian Federation (the Bank of Russia)”.

Function: Protect
Category: Identity management

“Recommendations in the field of standardization of the Bank of Russia “Ensuring Information Security of Organizations of the Banking System of the Russian Federation. Methodology of Information Security Risk Assessment” RS BR IBBS-2.2-2009” (adopted and put into effect by Order of the Bank of Russia dated 11 November 2009 No. R-1190).

Publication source: “Bank of Russia Bulletin”, No. 71, 11 December 2009

The current standard of the Bank of Russia “Ensuring Information Security of Organizations of the Banking System of the Russian Federation. General Provisions” (hereinafter referred to as “STO BR IBBS-1.0”) for the purpose of creating and maintaining at an appropriate level the system of ensuring information security of organizations of the banking system of the Russian Federation defines the requirement to assess the risks of information security breach. The document establishes recommended methods and procedure for assessment of risks of information security breach of the banking system organization, which is an integral part of the information security management system.

Function: Identify
Category: Risk assessment

“Recommendations in the field of standardization of the Bank of Russia “Ensuring information security of organizations of the banking system of the Russian Federation. Prevention of Information Leaks” RS BR IBBS-2.9-2016” (adopted and put into effect by Order of the Bank of Russia dated 11 April 2016 No. OD-1205).

Publication source: “Bank of Russia Bulletin”, No. 41, 27 April 2016

The document establishes recommendations, the implementation of which is aimed at ensuring by the organization of the banking system of monitoring and control of information flows, carried out to identify and prevent information leaks as a result of the actions of the organization’s employees and (or) other persons with legal access to information – possible internal violators of information security.

Function: Identify
Category: Asset management
Function: Detect
Category: Continuous monitoring
Function: Respond
Category: Incident management

“Recommendations in the field of standardization of the Bank of Russia “Ensuring information security of organizations of the banking system of the Russian Federation. Information Security Incident Management” RS BR IBBS-2.5-2014” (adopted and put into effect by the Order of the Bank of Russia dated 17 May 2014 No. R-400)

The document establishes approaches to the implementation by the banking system organization of the process of detection and response to information security incidents, which is an integral part of the information security management system of the banking system organizations.

Function: Respond
Category: Incident management, Incident Analysis, Incident response reporting, Incident management

"Recommendations in the field of standardization of the Bank of Russia "Ensuring information security of organizations of the banking system of the Russian Federation. Guidelines for self-assessment of compliance of information security of organizations of the banking system of the Russian Federation with the requirements of STO BR IBBS-1.0" RS BR IBBS-2.1-2007" (adopted and put into effect by the Order of the Bank of Russia dated 28 April 2007 No. R-347)

Publication source: "Bank of Russia Bulletin", No. 29, 18 May 2007

The Guidelines apply to banking organizations conducting self-assessment of compliance of information security with the requirements of the Bank of Russia standard and establish approaches to conducting such self-assessment.

Function: Detect
Category: Continuous monitoring

"Methodological document. Protection profile of application software of automated systems and applications of credit organizations and non-credit financial organizations" (approved by the Bank of Russia).

Publication source: official website of the Bank of Russia http://www.cbr.ru/

The document is intended for organizations carrying out work on the development of application software of automated systems and applications of credit organizations and non-credit financial organizations (hereinafter referred to as developers), applicants for product certification (hereinafter referred to as applicants), as well as for bodies for the certification of products (hereinafter referred to as applicants).

Function: Protect
Category: Identity management, Data security

SOUTH AFRICA

The South African Reserve Bank (SARB) established a cyber-resilience governance structure at the financial services industry level, called the *Cyber Resilience Sub-committee*, with the objective of cooperation and collaboration at the financial sector level.

The Prudential Authority, mandated with promoting and enhancing the safety, soundness, and integrity of financial institutions and market infrastructures, has also developed various regulations, guidance, and supervisory practices for the financial sector that directly and indirectly address cybersecurity.

A. REGULATIONS

1. **Guidance Note 5 of 2014: Outsourcing of functions within banks**
Published Date: 2014-07-11
Last Modified Date: 2020-10-01
Link: https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-guidance-notes/2014/6320

2. **Directive 2 of 2019: Reporting of material information technology and/or cyber incidents**
Published Date: 2019-09-12
Last Modified Date: 2020-10-01
Link: https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-directives/2019/9487

3. **Guidance Note 4 of 2017: Cyber resilience**
Published Date: 2017-05-19
Last Modified Date: 2020-10-01
Link: https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-guidance-notes/2017/7803

4. **Prudential Standards: Financial Soundness standards (FS) and Governance and Operational standards (GO)**
Governance and Operational Standards for Insurers 5
Governance and Operational Standards for Insurers 3.2
Date: July 1, 2018
Link: https://www.resbank.co.za/en/home/publications/prudential-authority/pa-insurance/pa-post-insurance/Draft_Prudential_Standards_-_9_March_2018

5. **Guidance Note 2 of 2016: Meetings to be held during the 2016 calendar year with the boards of directors of banks and controlling companies**
Published Date: 2016-02-09
Last Modified Date: 2020-10-01

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

6. **Guidance Note 2 of 2021**
Published Date: 2021-02-12
Last Modified Date: 2021-02-22
Link: https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-guidance-notes/2021/G2-2021-Flavour-of-the-year-topics

7. **IT Governance and Risk Management Standard**
Published Date: 2023-11-10
Last Modified Date: 2023-11-10
Link: https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-public-awareness/Communication/2023/Joint-Communication-4-of-2023-Publication-of-the-Joint-Standard-IT-Gov-and-Risk

8. **Cybersecurity and Cyber Resilience Standard**
Published Date: 2024-05-17
Last Modified Date: 2024-05-17
Link: https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-public-awareness/Communication/2024/Joint-Communication-2-of-2024-Publication-of-the-Joint-Standard-Cybersecurity-and-cyber-resilience

9. **Joint Standard on Outsourcing for Insurers**
Published Date: 2024-05-17
Last Modified Date: 2024-05-17
https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-public-awareness/Communication/2024/Joint-Communication-1-of-2024-Outsourcing-by-Insurers

OVERARCHING REGULATION AND PRACTISE

- **IT Governance and Risk Management Joint Standard:** The PA and the FSCA are in the process of developing this standard which sets out the principles for IT risk management that financial institutions must comply with, in line with sound practices and processes in managing IT. The standard also incorporates elements of cyber and information security and will be released for public consultation. **(Identify, Protect, Detect, Respond and Recover)**
- **Cybersecurity and Cyber Resilience Joint Standard:** The PA and the FSCA are in the process of developing this standard, which sets out the principles for cyber security, resilience, and practices that financial institutions must comply with to maintain operational resilience while managing cyber risks. **(Identify, Protect, Detect, Respond and Recover)**

DRAFT REGULATIONS AND PRACTICES

- **Draft standard on Operational Resilience:** The PA is in the process of drafting an Operational Risk and Resilience standard that will be applicable to all regulated industries. This is dependent on the work coming out of the IAIS and other regulatory setting bodies.
- **Draft Third Party Risk Management Joint Standard:** The PA is in the process of drafting a joint standard on Third Party Risk Management with the FSCA.

Below is a list of the regulatory instruments and practices classified according to the five NIST categories:

IDENTIFY

Issued Regulatory Instruments

- Guidance Note 5 of 2014: Issued to banks to conduct supplier risk assessments, due diligence as well as monitoring and reporting prior to engagements in any outsourced arrangements with third parties. This includes an assessment of the cyber resilience of suppliers.
- Guidance Note 4 of 2017: Refers to cyber resilience for financial market infrastructures and was issued to banks. The PA is of the view that the principles applied in the risk management categories and overarching components as set out by the CPMI and IOSCO are also applicable to the banking industry. This regulatory instrument will be repealed once the Cybersecurity and Cyber resilience standard comes into effect.
- Governance and Operational Standards for Insurers 5: Issued to insurers for outsourcing of material business activities and also addresses confidentiality, privacy and the security of information related to outsourcing.
- Governance and Operational Standards for Insurers 5: Issued to insurers to address the appropriateness, effectiveness, efficiency, integrity, confidentiality and reliability of the information technology and data quality systems.
- Joint Standard on Outsourcing for Insurers: Issued to insurers for outsourcing of material business activities and also addresses conduct issues, confidentiality, privacy and the security of information related to outsourcing.

Issued Practices

- Guidance Note 2 of 2016: Flavour of the year issued to banks with the objective to have discussions with Board of directors (Boards) of FIs to determine the exposure and impact of cyber and information security.
- Letters: Issued to MIs in 2019 for the Flavour of the year with the objective to have discussions with Boards of MIs to determine the exposure and impact of cyber and information security.
- Guidance Note 2 of 2021: Flavour of the year issued to banks with the objective to have discussions with Boards of FIs to determine the exposure and impact of new technologies including cyber and information security.
- IT Risk Questionnaire: An annual questionnaire was developed in 2020 and issued to the industry in order to obtain insights related to the IT risk posture within the financial institution (FI), industry and sector. This questionnaire was subsequently updated each year since 2020 and issued annually to the financial sector.

- Cybersecurity and Cyber resilience Questionnaire: An annual questionnaire was developed in 2022 and issued to the industry in order to obtain insights related to the cybersecurity and cyber resilience posture within the financial institution (FI), industry, and sector. This questionnaire was subsequently updated each year since 2022 and issued annually to the financial sector.
- Survey: Issued to insurers and market infrastructures in 2021 to determine the exposure and impact of new technologies including cyber and information security.

PROTECT

Issued Regulatory Instruments

- Guidance Note 5 of 2014: Issued to banks to conduct supplier risk assessments, due diligence as well as monitoring and reporting prior to engagements in any outsourced arrangements with third parties. This includes an assessment of the cyber resilience of suppliers.
  - Guidance Note 4 of 2017: Refers to cyber resilience for financial market infrastructures and was issued to banks. The PA is of the view that the principles applied in the risk management categories and overarching components as set out by the CPMI and IOSCO are also applicable to the banking industry. This regulatory instrument will be repealed once the Cybersecurity and Cyber Resilience Standard comes into effect.
- Governance and Operational Standards for Insurers 5: Issued to insurers for outsourcing of material business activities and also addresses confidentiality, privacy and the security of information related to outsourcing.
- Governance and Operational Standards for Insurers 5: Issued to insurers to address the appropriateness, effectiveness, efficiency, integrity, confidentiality and reliability of the information technology and data quality systems.
- Joint Standard on Outsourcing for Insurers: Issued to insurers for outsourcing of material business activities and also addresses conduct issues, confidentiality, privacy and the security of information related to outsourcing.

Issued Practices

- Guidance Note 2 of 2016: Flavour of the year issued to banks with the objective to have discussions with Board of directors (Boards) of FIs to determine the exposure and impact of cyber and information security.
- Letters: Issued to MIs in 2019 for the Flavour of the year with the objective to have discussions with Boards of MIs to determine the exposure and impact of cyber and information security.
- Guidance Note 2 of 2021: Flavour of the year issued to banks with the objective to have discussions with Boards of FIs to determine the exposure and impact of new technologies including cyber and information security.
- IT Risk Questionnaire: An annual questionnaire was developed in 2020 and issued to the industry in order to obtain insights related to the IT risk posture within the financial institution (FI), industry and sector. This questionnaire was subsequently updated each year since 2020 and issued annually to the financial sector.
  - Cybersecurity and Cyber resilience Questionnaire: An annual questionnaire was developed in 2022 and issued to the industry in order to obtain insights related to the cybersecurity and cyber resilience posture within the financial institution (FI), industry, and sector.

This questionnaire was subsequently updated each year since 2022 and issued annually to the financial sector.

- Survey: Issued to insurers and market infrastructures in 2021 to determine the exposure and impact of new technologies including cyber and information security.

DETECT

Issued Regulatory Instruments

- Guidance Note 5 of 2014: Issued to banks to conduct supplier risk assessments, due diligence as well as monitoring and reporting prior to engagements in any outsourced arrangements with third parties. This includes an assessment of the cyber resilience of suppliers.
- Guidance Note 4 of 2017: Refers to cyber resilience for financial market infrastructures and was issued to banks. The PA is of the view that the principles applied in the risk management categories and overarching components as set out by the CPMI and IOSCO are also applicable to the banking industry. This regulatory instrument will be repealed once the Cybersecurity and Cyber Resilience standard comes into effect.
- Governance and Operational Standards for Insurers 5: Issued to insurers for outsourcing of material business activities and also addresses confidentiality, privacy and the security of information related to outsourcing.
- Governance and Operational Standards for Insurers 5: Issued to insurers to address the appropriateness, effectiveness, efficiency, integrity, confidentiality and reliability of the information technology and data quality systems.

Issued Practices

- Guidance Note 2 of 2016: Flavour of the year issued to banks with the objective to have discussions with Board of directors (Boards) of FIs to determine the exposure and impact of cyber and information security.
- Letters: Issued to MIs in 2019 for the Flavour of the year with the objective to have discussions with Boards of MIs to determine the exposure and impact of cyber and information security.
- Guidance Note 2 of 2021: Flavour of the year issued to banks with the objective to have discussions with Boards of FIs to determine the exposure and impact of new technologies including cyber and information security.
- IT Risk Questionnaire: An annual questionnaire was developed in 2020 and issued to the industry in order to obtain insights related to the IT risk posture within the financial institution (FI), industry and sector. This questionnaire was subsequently updated each year since 2020 and issued annually to the financial sector.
- Cybersecurity and Cyber resilience Questionnaire: An annual questionnaire was developed in 2022 and issued to the industry in order to obtain insights related to the cybersecurity and cyber resilience posture within the financial institution (FI), industry, and sector. This questionnaire was subsequently updated each year since 2022 and issued annually to the financial sector.
- Survey: Issued to insurers and market infrastructures in 2021 to determine the exposure and impact of new technologies including cyber and information security.

RESPOND

Issued Regulatory Instruments

- Directive 2 of 2019: Issued to banks to formally report all material IT and/or cyber incidents to the PA.
  - Guidance Note 4 of 2017: Refers to cyber resilience for financial market infrastructures and was issued to banks. The PA is of the view that the principles applied in the risk management categories and overarching components as set out by the CPMI and IOSCO are also applicable to the banking industry. This regulatory instrument will be repealed once the Cybersecurity and Cyber Resilience standard comes into effect.
- Governance and Operational Standards for Insurers 3.2: Requires insurers to notify the PA of major disruptions that has a potential to have a material impact on their risk profile or effect its financial soundness or security requirements.
- The Financial Sector Conduct Authority (FSCA), previously known as the Financial Services Board, issued a notice in terms of Section 6(3)(d) of the Financial Markets Act, 2012, to all licensed market infrastructures (MIs) to report all significant events to the Registrar without delay and within 48 hours of becoming aware of the significant event. The notice requires MIs to report to the FSCA, however, there is an informal agreement to notify the PA as well.

Issued Practices

- Guidance Note 2 of 2016: Flavour of the year issued to banks with the objective to have discussions with Board of directors (Boards) of FIs to determine the exposure and impact of cyber and information security. (Identify, Protect, Detect, Respond and Recover)
- Letters: Issued to MIs in 2019 for the Flavour of the year with the objective to have discussions with Boards of MIs to determine the exposure and impact of cyber and information security. (Identify, Protect, Detect, Respond and Recover)
- Guidance Note 2 of 2021: Flavour of the year issued to banks with the objective to have discussions with Boards of FIs to determine the exposure and impact of new technologies including cyber and information security. (Identify, Protect, Detect, Respond and Recover)
- IT Risk Questionnaire: An annual questionnaire was developed in 2020 and issued to the industry in order to obtain insights related to the IT risk posture within the financial institution (FI), industry and sector. This questionnaire was subsequently updated each year since 2020 and issued annually to the financial sector.
- Cybersecurity and Cyber resilience Questionnaire: An annual questionnaire was developed in 2022 and issued to the industry in order to obtain insights related to the cybersecurity and cyber resilience posture within the financial institution (FI), industry, and sector. This questionnaire was subsequently updated each year since 2022 and issued annually to the financial sector.
  - Survey: Issued to insurers and market infrastructures in 2021 to determine the exposure and impact of new technologies including cyber and information security. (Identify, Protect, Detect, Respond and Recover)

RECOVER

Issued Regulatory Instruments

- Guidance Note 4 of 2017: Refers to cyber resilience for financial market infrastructures and was issued to banks. The PA is of the view that the principles applied in the risk management categories and overarching components as set out by the CPMI and IOSCO are also applicable to the banking industry.
- Governance and Operational Standards for Insurers 3.2: Requires insurers to notify the PA of major disruptions that has a potential to have a material impact on their risk profile or effect its financial soundness or security requirements.
- The Financial Sector Conduct Authority (FSCA), previously known as the Financial Services Board, issued a notice in terms of Section 6(3)(d) of the Financial Markets Act, 2012, to all licensed market infrastructures (MIs) to report all significant events to the Registrar without delay and within 48 hours of becoming aware of the significant event. The notice requires MIs to report to the FSCA, however, there is an informal agreement to notify the PA as well.

Issued Practices

- Guidance Note 2 of 2016: Flavour of the year issued to banks with the objective to have discussions with Board of directors (Boards) of FIs to determine the exposure and impact of cyber and information security.
- Letters: Issued to MIs in 2019 for the Flavour of the year with the objective to have discussions with Boards of MIs to determine the exposure and impact of cyber and information security.
- Guidance Note 2 of 2021: Flavour of the year issued to banks with the objective to have discussions with Boards of FIs to determine the exposure and impact of new technologies including cyber and information security.
- IT Risk Questionnaire: An annual questionnaire was developed in 2020 and issued to the industry in order to obtain insights related to the IT risk posture within the financial institution (FI), industry and sector. This questionnaire was subsequently updated each year since 2020 and issued annually to the financial sector.
- Cybersecurity and Cyber resilience Questionnaire: An annual questionnaire was developed in 2022 and issued to the industry in order to obtain insights related to the cybersecurity and cyber resilience posture within the financial institution (FI), industry, and sector. This questionnaire was subsequently updated each year since 2022 and issued annually to the financial sector.
- Survey: Issued to insurers and market infrastructures in 2021 to determine the exposure and impact of new technologies including cyber and information security.

UAE

UAE has developed a National Cyber Security Strategy with a vision to create safe and resilient cyber infrastructure that enables citizens to fulfil their aspirations and empowers business to thrive, this vision is to impact all segments of the society.

At the helm of the vision is to have robust cyber security laws and Regulations that would address all types of cybercrimes, secure existing and emerging technologies, support protection of all Businesses etc.

A. REGULATIONS

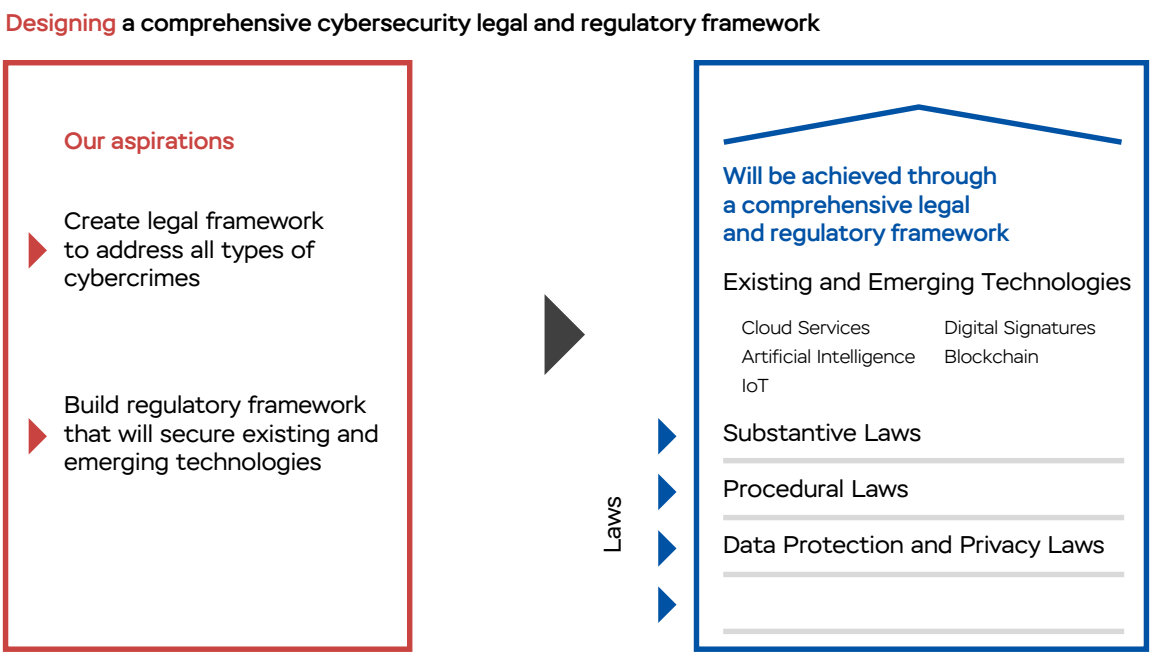
Cyber Laws, below identifies the laws and regulations relating to cyber security:

- Cyber Security Council Policies
- UAE Information Assurance Regulation
- Federal Law by Decree No. 3 of 2003 as amended Regarding the Organization of Telecommunications Sector
- Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes
- Federal Decree by Law No. 45 of 2021 Concerning the Protection of Personal Data
- Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services
- Regulation of Using Social Media by the Employees of Federal Entities as Approved by the Cabinet Resolution No. 73/3/ & 1 of 2014 (PDF, 1 MB)
- Ministerial Resolution No. 1 of 2008 Regarding the issuance of Certification Service Provider Regulations (PDF, 1 MB)
- Law No. 26 of 2015 Regulating Data Dissemination and Exchange in the emirate of Dubai (PDF, 1 MB)

In November 2020, the UAE Cabinet agreed to establish the UAE Cybersecurity Council with the aim of developing a comprehensive cybersecurity strategy and creating a safe and strong cyber infrastructure in the UAE.

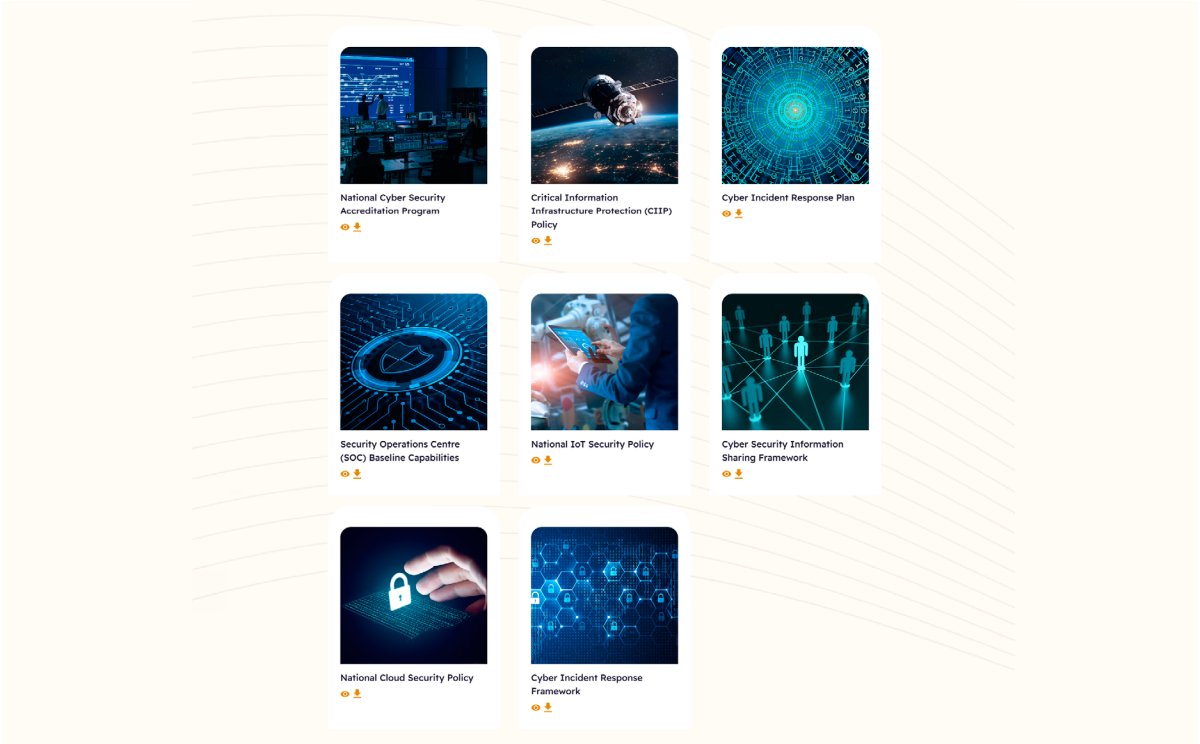
The council is chaired by the Head of Cyber Security for the UAE Government and contributes to creating a legal and regulatory framework that covers all types of cybercrimes, securing existing and emerging technologies and establishing a robust “National Cyber Incident Response Plan” to enable swift and coordinated response to cyber incidents in the country.

Below diagram shows the design process for cybersecurity legal and regulatory framework:



The CBUAE aligns with the overall National Cyber Security Strategy and Regulations through working closely with regulatory stake holders and cyber security council towards promoting financial and monetary stability, efficiency and resilience in the financial system, and consumer protection.

The Cyber Security Council has developed set of cyber security policies as shown below available from the URL (https://csc.gov.ae/en/policies) with comprehensive controls to be applied across the UAE.



B. FUNCTIONAL CATEGORIZATION

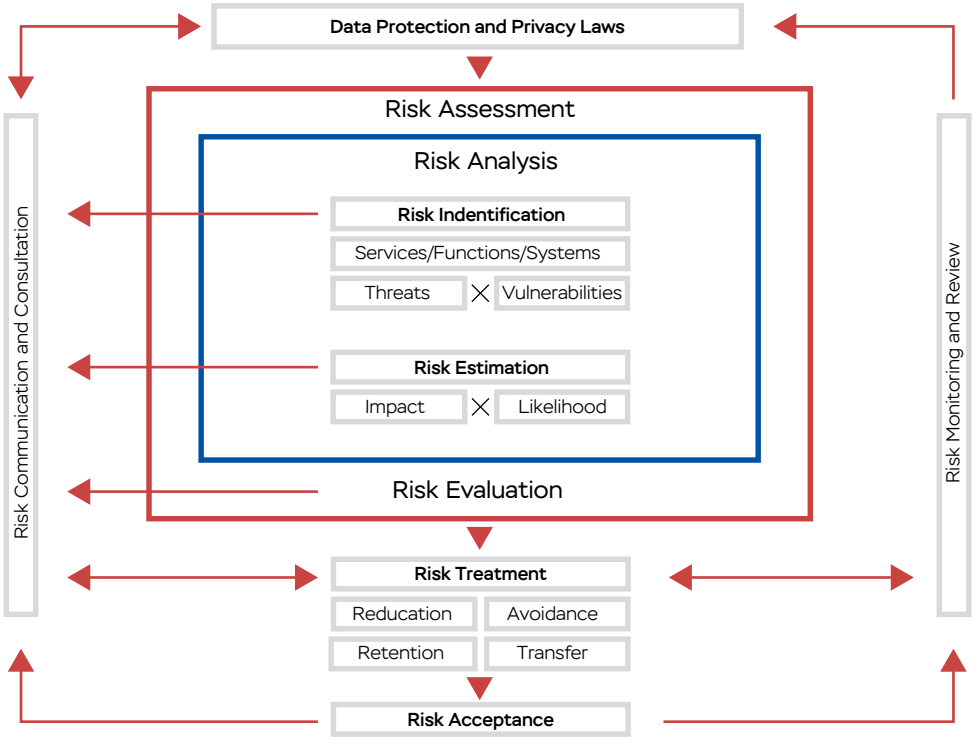
The applicable regulations are reflected in each separate standards, directives as well as laws. The below identifies various requirements within different regulations into the five areas of the NIST framework.

For detailed listing of appropriate controls please refer to the above shared references/ URLs, the below provides briefing of requirements across multiple functions.

IDENTIFY

- Defining the Management and Technical controls to be implemented against cyber threats in addition to roles and responsibilities.
- Having Cyber Security Framework in place as per best practices to govern digital related processes and operations.
- Developing applicable policies and standards for the financial system's digital infrastructure.
- Defining the protection of personal data with roles and responsibilities of all involved towards collecting, storing and processing of personal data.
- Identifying applicable controls and prioritisation towards controls implementation.
- Identifying risks related to third parties with cyber security vetting process in place to vet for qualified service providers as well as the services being obtained.
- Defining and developing Third-party Access Policy to ensure secure access is in place at all times.
- Having a programme in place to regularly identify system weaknesses/vulnerabilities with remediation process.
- Defining information security strategy together with the operating model to adhere to the strategy.
- Developing information security plans for each major service to identify and mitigate the risks corresponding to each service.
- Defining Information Security Risk Management process to conduct risk assessments, statements of applicability, security testing and evaluations of information security controls on applicable services.
- Identifying and documenting key success factors for the information security programme.

Below Diagram presents the Risk-Based Identification Approach.



PROTECT

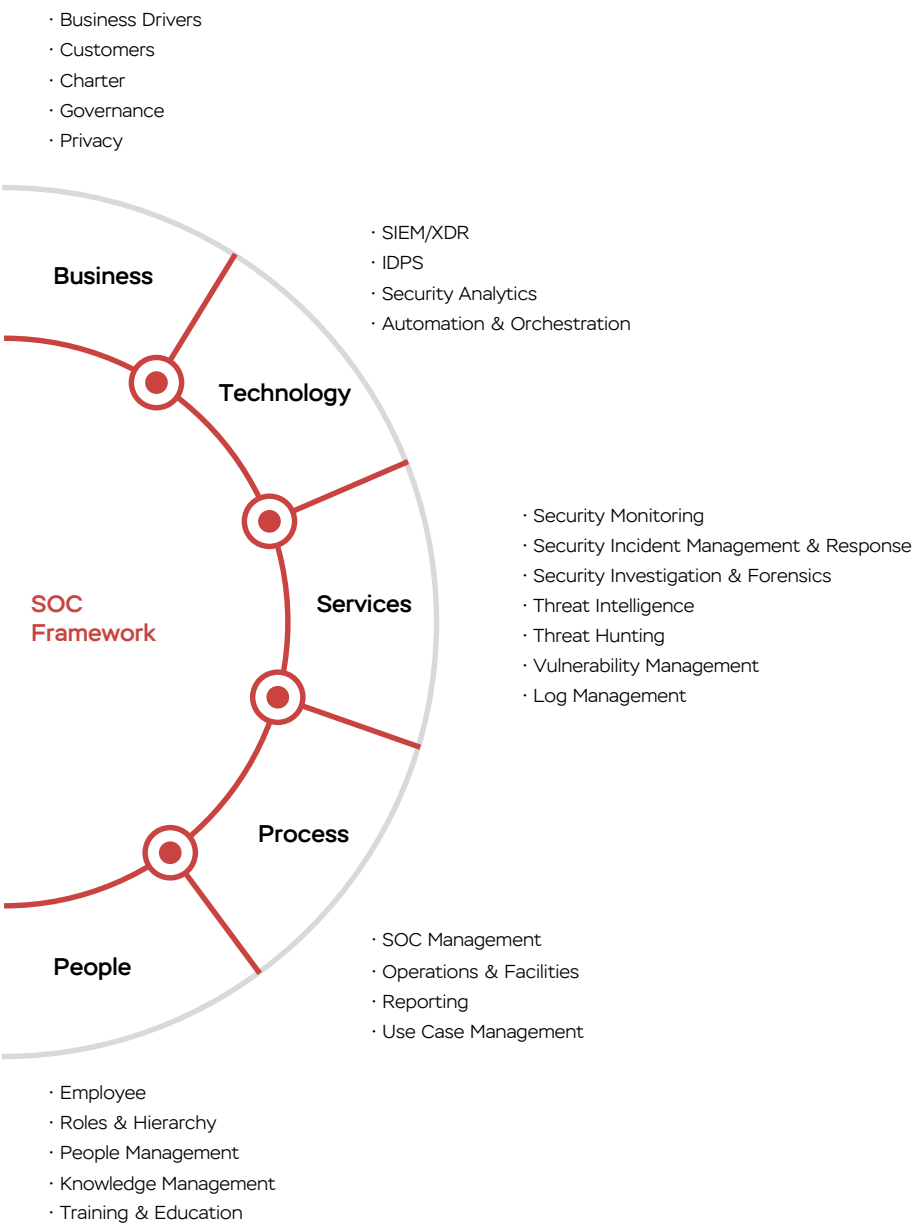
- Adopting a risk-based approach to protect the digital systems.
- Implementing appropriate technical controls to protect the digital ecosystem.
- Assets shall be managed and information shall be classified and labelled to ensure that assets including information receives an appropriate level of information security controls.
- Operational procedures and responsibilities shall be developed, to ensure an adequate level of information security. In addition, backup, media handling, e-services security and monitoring shall be addressed to ensure protection against malicious code and spyware.
- Access control processes shall be developed to control access to information, manage user access, control access to both internal and external network services, control access to operating systems, control access to applications and to apply appropriate protection when using mobile computing and teleworking services.
- An information systems acquisition, development and maintenance process shall be implemented to prevent unauthorised modification or misuse of information in applications, ensure that a cryptographic control policy is in place, to maintain security in development and support processes and manage technical vulnerabilities.
- Third party security shall be managed to ensure that they implement and maintain the appropriate level of information security and service delivery, and information stored, processed, and retrieved, including via cloud services.
- Organization to have in place a management authorisation process for new information systems.

DETECT

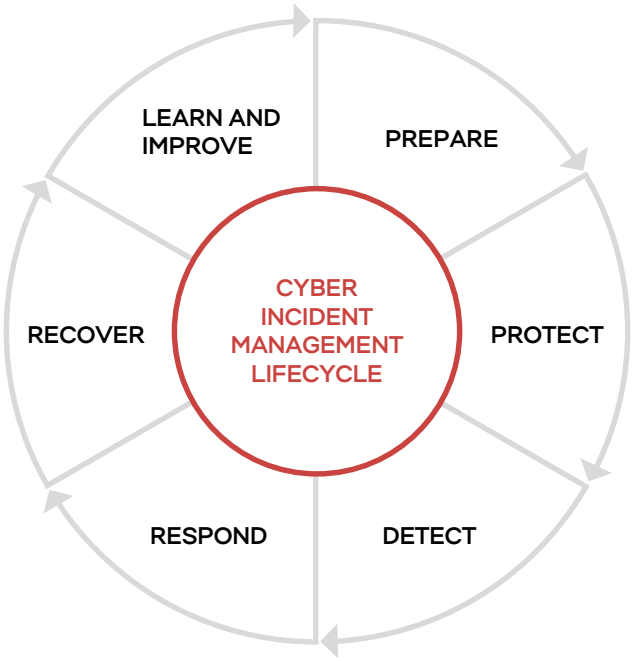
- Information security events and weaknesses shall be reported and evidence of security incidents shall be collected and analysed to ensure that they are properly communicated and security incidents adequately managed.
- Monitoring external party access to Organization's information and its systems.
- Having robust incident management in place to provide 24x7 threat monitoring and alerting.

- Ensuring information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
- Having in place threat intelligence mechanism for receiving known threats with a platform to share with wider financial community.
- Instituting threat hunting capabilities with related processes and procedures to identify underlying threats.

Below Diagram shows SOC Framework for Incident Management Capability.



Below diagram shows the incident management lifecycle implemented:



Further details on the above diagrams description can be found on the shared URLs.

RESPOND

- Maintaining appropriate contacts with relevant special interest groups in case of required urgent collaboration such as with law enforcement agencies, courts etc.
- Having incident response plan to capture various aspects of known security threats and potentially not previously discovered threats.
- Developing and Maintaining operational management policy to provide guidance on the operational requirements of information assets.
- Maintaining an information security incident management policy to cover the information security incident procedures including the detection, reporting and treatment of incidents.
- Providing incident response training in a regular manner to ensure appropriate staff are equipped to handle cyber incidents.
- Reporting information security events through appropriate management channels.

RECOVER

- Implementing business continuity management process to counteract interruptions to business activities and to protect critical business processes from failures of information systems.
- Ensuring information security events and weaknesses associated with information systems are communicated in a manner that allows timely corrective action to be taken.
- Maintaining an information continuity management policy to cover the continuity and redundancy of information based on their level of criticality.
- Establishing an information systems continuity planning policy.
- Counteracting interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
- Developing Information Systems Continuity Plans with regular testing to ensure adequate proactive mechanism is always in place to be invoked when required.

CENTRAL BANK OF UAE (CBUAE)

The CBUAE is the Supervisory and regulatory authority of the banking and insurance sector, it promotes financial and monetary stability, efficiency and resilience in the financial system, and the protection of consumers through effective supervision that supports economic growth for the benefit of the UAE and its people.

CBUAE plays pivotal role towards championing cybersecurity objectives across the UAE financial sector whilst maintaining strong collaboration with various institutional stake holders both nationally and international.

CBUAE regularly promotes nationally coordinated cyber activities across the financial sector as well as other stake holders from different sectors to participate or observe in such as wargaming cyber simulations to improve on overall cyber readiness.

It maintains cyber security centre of excellence (COE) with a vision to have a secure UAE Financial sector infrastructure that inspires technological innovation and supports economic growth.

ANNEX

BRICS RAPID INFORMATION SECURITY CHANNEL (BRISC) MEMBERS

Members	Position, Organization
Central Bank of the Russian Federation (as the chair)	
Mr. Maxim Leonov	BRICS Coordinator, Consultant, Department for Cooperation with International Organizations
Ms. Evgeniya Molotova	BRICS Coordinator, Chief Economist, Department for Cooperation with International Organizations
Mr. Kirill Shumei	BRICS Coordinator, Lead Economist, Department for Cooperation with International Organizations
Mr. Andrey Vybornov	Deputy Director, Information Security Department, Ph.D. in Technology
Mr. Grigory Tsarev	Deputy Head of the Financial CERT
Mr. Alexander Chuburkov	Consultant, Information Security Department
Mr. Alexei Kudrin	Chief Engineer, Information Security Department
South African Reserve Bank	
Ms. Samantha Springfield	Head, IERPD
Ms. Philadelphia Makhanya	Manager, IERPD
Mr. Gerhard Cronjé	Divisional Head, Cyber and Information Security, Business Systems and Technology Department
Ms. Yolande Poley	BRICS Coordinator, International Economic Relations and Policy Department (IERPD)
Ms. Motshidisi Mokoena	Senior Economic Policy Analyst, IERPD
Mr. Jacques Théron	Financial Sector Cyber Security Consultant, Business Solutions and Technology Department
Central Bank of the United Arab Emirates	
Mr. Thabet Bakheet Khamis	Chief Risk Officer
Mr. Hamed Obaid Areidat	Senior Director – IT Operations
Mr. Bader Ali Murad Mohammed	Team Lead – Information Security
Central Bank of Brazil	
Ms. Veruska Rocha de Aragão	Deputy Head, Information Technology Department
Mr. Marcio Rodrigues Alves dos Santos	Head of Division, Information Technology Department

Members	Position, Organization
Mr. Jefferson Umebara Pelegrini	Head of Division, Strategic Management and Specialized Supervision Department
Mr. Estenio do Nascimento Cabral	Advisor, Information Technology Department
Mr. Alexander Bulbow	Coordinator, Strategic Management and Specialized Supervision Department
Mr. Ricardo Terranova Favalli	Coordinator, Strategic Management and Specialized Supervision Department
Mr. Carlos Eduardo Gomes Marins	Coordinator, Information Technology Department
Mr. Nilton de Almeida Naretto	Analyst, International Affairs Department
Ms. Paula Castello Branco Teklenburg	Analyst, International Affairs Department
People's Bank of China	
Mr. Shen Xiaoyan	Division Chief, Technology Department
Ms. Cai Xiaoli	Deputy Division Chief, International Department
Mr. Wang Tao	Level IV Division Rank Official, Technology Department
Mr. Tan Leiyu	Staff, Technology Department
Ms. LV Leyan	Staff, International Department
Mr. Dai Chen	Staff, Technology Division, PBOC Jiangsu Branch
Central Bank of Egypt	
Dr. Sherif Hazem	CBE Sub-Governor and Cyber Security Sector Head
Dr. Ibrahim Mostafa	CBE Assistant Sub-Governor and EG-FinCIRT Director
Eng. Karim Wahba	Cyber Intelligence and Vulnerability Handling Head – EG-FinCIRT
Eng. Mahmoud Abdelbary	R&D Team Leader – EG-FinCIRT
Eng. Sherif Embaby	Cyber Intelligence Team Leader – EG-FinCIRT
National Bank of Ethiopia	
Mr. Windewosen Tsegaw Feleke	Director, Information System Management Directorate, National Bank of Ethiopia
Reserve Bank of India	
Dr. Sanjay Bahl	Director General, CERT-In
Mr. T. K. Rajan	Chief General Manager-in-Charge, Department of Supervision, RBI
Mr. Noorul Ameen	Scientist "E", CERT-In

Members	Position, Organization
Mr. Vinod Kumar Chouhan	Scientist, Ministry of Electronics & Information Technology
Ms. Darshana S Kulkarni	General Manager, Department of Information Technology, Reserve Bank of India
Mr. Sreejith S	Assistant Manager, International Department, RBI
Central Bank of the Islamic Republic of Iran	
Mr. Najmeh Ramouz	Head of Group, International Strategic Cooperation, Central Bank of the Islamic Republic of Iran

BRICS RAPID INFORMATION SECURITY CHANNEL (BRISC) EDITORIAL TEAM

Members	Position, Organisation
Central Bank of the Russian Federation (as the chair)	
Mr. Alexander Chuburkov	Editor-in-Chief, Consultant, Information Security Department, GOST R expert
Mr. Konstantin Starodubov	Co-Editor, Consultant, Information Security Department, Ph.D. in Technology
Mr. Igor Litvinov	Contributor, Chief Engineer, Information Security Department
Mr. Dmitry Nikitin	Contributor, Chief Engineer of the Information Security and Cyber Resilience Sector of the Bank of Russia's Siberian Main Directorate
Mr. Oleg Savva	Contributor, Head of the Information Security and Cyber Resilience Sector of the Bank of Russia's Siberian Main Directorate
Mr. Viktor Kuchin	Linguistic Support, Head of Unit, Department for Cooperation with International Organizations
Mr. Mikhail Godunov	Linguistic Support, Consultant, Department for Cooperation with International Organizations
Ms. Lidia Yarina	Linguistic Support, Consultant, Department for Cooperation with International Organizations
Ms. Alexandra Marsova	Linguistic Support, Lead Expert, Department for Cooperation with International Organizations
Ms. Tatiana Shevlyakova	Linguistic Support, 1st cat. Expert, Department for Cooperation with International Organizations
South African Reserve Bank	
Mr. Gerhard Cronjé	Head of Cyber and Information Security Unit
Mr. Jacques Théron	Financial Sector Cybersecurity Consultant
Central Bank of the United Arab Emirates	
Mr. Thabet Bakheet Khamis	Chief Risk Officer
Mr. Hamed Obaid Areidat	Senior Director – IT Operations
Mr. Bader Ali Murad Mohammed	Team Lead – Information Security
Central Bank of Brazil	
Mr. Alexander Bulbow	Coordinator, Strategic Management and Specialized Supervision Department

Members	Position, Organisation
Mr. Estenio do Nascimento Cabral	Advisor, Information Technology Department
People's Bank of China	
Mr. Shen Xiaoyan	Division Chief, Technology Department
Ms. Cai Xiaoli	Deputy Division Chief, International Department
Mr. Wang Tao	Level IV Division Rank Official, Technology Department
Mr. Tan Leiyu	Staff, Technology Department
Ms. LV Leyan	Staff, International Department
Mr. Dai Chen	Staff, Technology Division, PBOC Jiangsu Branch
Central Bank of Egypt	
Dr. Mohamed Shishtawy	Head of Cybersecurity Readiness – Cyber Security Sector
Eng. Ahmed Diaa	Cyber Security Readiness Assessor – Cyber Security Sector
National Bank of Ethiopia	
Mr. Windewosen Tsegaw Feleke	Director, Information System Management Directorate, National Bank of Ethiopia
CERT-In and Reserve Bank of India	
Mr. Pradeep Raj Singh	General Manager, Department of Supervision, RBI
Mr. Ashutosh Bahuguna	Scientist "E", CERT-In
Mr. Devender Yadav	Officer on Special Duty, CSIRT-Fin, CERT-In
Mr. Shashank Gupta	Scientist "C", CERT-In
Mr. Saikrishna Medishetti	Manager, Department of Supervision, RBI
Central Bank of the Islamic Republic of Iran	
Mr. Najmeh Ramouz	Head of Group, International Strategic Cooperation, Central Bank of the Islamic Republic of Iran