

# Information Security Regulations in Finance BRICS e-Booklet

India | 2021

BRICS Rapid Information Security Channel



BRICS  
INDIA 2021

.....

.....

---

## Contents

Introduction	2
Brazil	3
Russia	7
India	15
China	25
South Africa	29
Appendix	36
Annex	37

---

## 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 recognised 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 defences against cyber risks. Many countries and international bodies have formulated cybersecurity regulations and legislations to effectively manage the cybersecurity-related risks responsibly. However, constant up-gradation 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 five 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 publication of this e-booklet would not have been possible without the valuable inputs given by the BRISC members; whose comprehensive research helped in the compilation of this document. The editorial team played a significant role by providing their comments and revisions at all stages. 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.

```
0100010  
10010010001  
1000100100100  
010010001001001  
10010010001001  
0001001001000  
1000100100  
0010001  
0010010  
0010010  
0100010  
01000100  
01001001  
10001001  
10010001  
10010010  
100010010  
100100010  
100100100
```

## A. Regulations

Resolution 4658 provides for the cyber security policy and is closely related to cyber risk management. It is important to highlight that, in the Brazilian regulatory framework, Resolution 4658 is usually applied together with Resolution 2554 and Resolution 4557, which provides for the risk management framework, including the management of operational risk (Articles 32 and 33 provide for IT risk management structure). Finally, the Guide to Supervision Practices brings a set of practices that Supervision expects to find in financial institutions, according to the institution's risk exposure and the size and complexity of its operations.

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 A<sup>1</sup>

### 1. Resolution 2554 of September 24, 1998

Provides for the establishment and implementation of internal controls system. Financial institutions and other institutions authorized by the Brazilian Central Bank (BCB) should establish and implement internal controls for their activities and financial, operational, and managerial information systems, and to ensure compliance with the applicable legal rules and regulations.

The internal controls, regardless of the size of the institution, should be effective and consistent with the nature, complexity, and risk of the institution's operations.

### 2. Resolution 4557 of February 23, 2017

Provides for the structure for risk management and the structure for capital management.

### 3. Resolution CMN 4893 of February 26, 2021

Provides for the cyber security policy and the requirements for contracting services of data processing, data storage and cloud computing to be observed by financial institutions and other institutions licensed by the BCB.

### 4. Resolution BCB 85 of April 08, 2021

Provides for the cyber security policy and the requirements for contracting services of processing, data storage and cloud computing to be observed by payment institutions licensed by the BCB.

### 5. Guide to Supervision Practices (GSP)

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).

## B. Functional Categorisation

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<sup>2</sup>:

<sup>1</sup> The titles of the regulations are hyperlinked to the translated regulation in Appendix.

<sup>2</sup> Financial Stability Report, October 2020 - <https://www.bcb.gov.br/en/publications/financialstabilityreport>

---

## Identify

Resolution CMN 4893 and Resolution BCB 85

- Sharing relevant incident information.
- 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 detection tests.

Resolution CMN 4557 and Resolution CMN 2554

- 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

- Existence of an information governance system.
- Alignment between security strategy and business strategy.
- Implementation of vulnerability analysis.

## Protect

Resolution CMN 4893 and Resolution BCB 85

- 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.

Resolution CMN 4557 and Resolution CMN 2554

- Establishment of strategies to ensure continuity of activities and limit losses arising from 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 security system information.
- 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

Resolution CMN 4893 and Resolution BCB 85

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

Resolution CMN 4557 and Resolution CMN 2554

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

Guide to Supervision Practices

- Monitoring and attack prevention.

## Respond

Resolution CMN 4893 and Resolution BCB 85

- 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

Resolution CMN 4893 and Resolution BCB 85

- 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.

Resolution CMN 4557 and Resolution CMN 2554

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

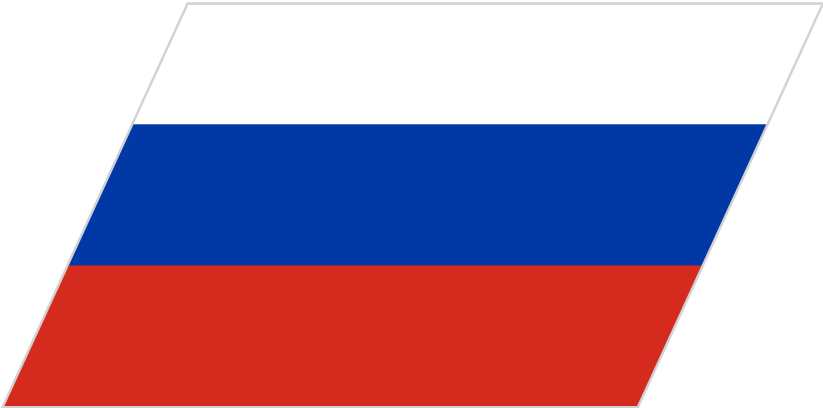
Guide to Supervision Practices

- Establishment of business continuity plans.



---

# Russia



The cyber security framework encompasses the technological aspects of processing protected information; software of automated systems and infrastructures.

```
0100010  
10010010001  
1000100100100  
010010001001001  
10010010001001  
0001001001000  
1000100100  
0010001  
0010010  
0010010  
0100010  
01001000  
01001001  
10001001  
01001001  
010010010  
100010010  
100100010  
100100100
```

To counter unauthorised funds transfers and other illicit financial operations, the Bank of Russia has established regulations under the framework comprised of three main groups:

- information security requirements covering the technological aspects of processing protected information (technological information security safeguards);
- information security requirements covering applicable software of automated systems and applications;
- information security requirements covering information technology infrastructures.

The regulations under this framework are:

- for national payment system participants, including participants of the Bank of Russia Payment System, concerning funds transfers (Bank of Russia Regulations No. 719-P and No. 747-P);
- for credit institutions concerning banking activities (Bank of Russia Regulation No. 683-P);
- for non-credit financial institutions concerning financial market activities (Bank of Russia Regulation No. 757-P).

## A. Regulations

The translated version of the regulations mentioned below is given in Appendix.

**1. Bank of Russia Regulation No. 719-P, dated 4 June 2020, “On the requirements for ensuring information security when executing money transfers and on the procedure for monitoring the compliance with information security requirements when executing money transfers”**

Source: <https://www.cbr.ru/Queries/UniDbQuery/File/90134/1119>

The Regulation establishes requirements for ensuring by money transfer operators, bank payment agents (subagents), information exchange service operators, payment application providers, payment system operators, payment infrastructure service operators the protection of information in the process of money transfers, as well as the procedure of control by the Bank of Russia over compliance with information protection requirements in the process of money transfers within the framework of the Bank of Russia.

The Regulation will enter into force from January 1, 2022, except for specific provisions for which other terms are stipulated and will replace the Regulation of the Bank of Russia dated June 9, 2012 No 382-P “On Requirements for Ensuring Protection of Information in money transfers and on the Procedure of Control by the Bank of Russia over Compliance with Requirements for Ensuring Protection of Information in money transfers.”

The Regulation will also apply to operators of information exchange services and providers of payment applications.

**2. Bank of Russia Regulation No. 747-P, dated 23 December 2020, “On the Requirements regarding Data Protection within the Bank of Russia Payment System”**

Source: <https://www.cbr.ru/Queries/UniDbQuery/File/90134/1243>

This Regulation establishes the requirements regarding the data protection in the Bank of Russia payment system. These requirements are obligatory for the Bank of Russia payment system participants that are credit institutions (their branches), as well as operations

centres or payment clearing centres of other payment systems when providing operational services and payment clearing services during funds transfers using the Faster Payments System. These requirements cover automated systems, software, and computer and telecommunications equipment used for processing protected data.

The Regulation also stipulates that basic set of organisational and technical measures” should be applied to data infrastructure facilities used for connecting to the Bank of Russia payment system, while ensuring the required level of conformity to the requirements of the standard (maturity level).

In addition, the Regulation determines the procedure for ensuring cryptographic protection of data in business applications and processes, the requirements concerning the use of identification and strict authentication procedures regarding the parties involved, and measures to counter unauthorized transactions. Moreover, the Regulation establishes the procedure for submitting reports to the Bank of Russia, the payment system’s operator, by the payment system participants.

### **3. 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 Unauthorized Funds Transfers”**

Source: <https://www.cbr.ru/Queries/UniDbQuery/File/90134/812>

Regulation No. 683-P sets mandatory requirements for credit institutions concerning ensuring data protection in banking to counter unauthorised funds transfers. These requirements cover data infrastructure facilities, applied software of automated systems and applications, and protected data processing technology. The requirements are applied to protect the data that is prepared, processed and stored in the automated systems forming part of data infrastructure facilities and used in banking operations related to funds transfers.

National Standard of the Russian Federation GOST R 57580.1-2017 “Security of financial (banking) operations-Protection of financial institutions’ information” envisages that the technologies used to process protected data in accordance with Regulation No. 683-P should be regulated and their compliance with the requirements should be monitored; they should ensure integrity and reliability of protected data and feature a developed system for recording actions taken in respect of access to protected data and results of such activities, during all technological stages of the process, including recording actions performed both by employees and clients using automated systems and software.

Other requirements concern identifying incidents related to violations of data protection requirements in banking and communicating with the Bank of Russia (Financial CERT) to exchange information on security incidents and results of investigation thereof, as well as response measures taken in their regard.

### **4. Bank of Russia Regulation No. 757-P, dated 20 April 2021, “On establishing mandatory requirements for non-credit financial institutions concerning ensuring information protection when performing activities in the financial markets to counter illegal financial transactions”**

Source: <https://www.cbr.ru/Queries/UniDbQuery/File/90134/2334>

The Bank of Russia has set mandatory requirements for non-bank financial institutions (NFIs) concerning data protection to prevent illegal financial transactions. The require-

ments are mainly similar to those for credit institutions established by Regulation 683-P. The document also contains the list of protected information types, data protection requirements for data infrastructure facilities, software, and technologies for processing protected data. The requirements are differentiated depending on the data protection level applicable to the particular NFI.

## Standards

### 5. National Standard of the Russian Federation GOST R 57580.1-2017 “Security of Financial (Banking) Operations. Information Security of Financial Institutions. Basic Set of Organisational and Technical Measures”

Source: <http://protect.gost.ru/document1.aspx?control=31&baseC=6&page=0&month=7&year=2021&search=57580&id=230678>

This standard establishes the information security levels and the respective requirements for the basic set of information security measures to be applied by financial institutions to comply with the information security requirements prescribed by Bank of Russia regulations. The provisions of this standard must be used by credit institutions, non-bank financial institutions and national payment system participants. The basic set of information security measures defined by this standard applies to all information systems, including automated systems (AS) used by financial institutions to perform business processes and/or technical processes related to the provision of financial services, banking services or money transfer services.

### 6. 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.”

Source: <http://protect.gost.ru/document1.aspx?control=31&baseC=6&page=0&month=7&year=2021&search=%D0%93%D0%9E%D0%A1%D0%A2%20%D0%A0%20%D0%98%D0%A1%D0%9E/%D0%9C%D0%AD%D0%9A%2015408-3-2013&id=184748>

### 7. Bank of Russia Standard STO BR BFBO-1.5-2018 “On the forms and timeframes for the Bank of Russia’s interaction with information exchange participants when detecting incidents related to the violations of information protection requirements”

Source: <http://cbr.ru/statichtml/file/59420/st-15-18.pdf>

This standard establishes how the Bank of Russia interacts with credit institutions, non-credit financial institutions, and national payment system entities in identifying violations of information protection requirements. The forms of requests and the submission of information are provided.

### 8. National Standard of the Russian Federation GOST R 57580.2-2018 “Security of Financial (Banking) Operations. Information Protection of Financial Organizations. Conformity Assessment Methods”

<http://protect.gost.ru/document1.aspx?control=31&baseC=6&page=0&month=7&year=2021&search=57580.2&id=230678>

This standard stipulates the requirements for the methodology and recording of results of the evaluation of data protection conformance in a financial institution when choosing and im-

<sup>1</sup> The standard is identical to international standard ISO/IEC 15408-3:2008 “Information technology - Security techniques - Evaluation criteria for IT security - Part 3. Security assurance components”.

plementing organisational and technical data protection measures by the requirements of GOST R 57580.1 applied by financial institutions to comply with the data protection requirements established by Bank of Russia regulations.

**9. Standard of the bank of Russia STO BR IBBS-1.0-2014 “Information security maintenance of organizations in the banking system of the Russian federation”**

[https://www.cbr.ru/Content/Document/File/51217/st-10-14\\_en.pdf](https://www.cbr.ru/Content/Document/File/51217/st-10-14_en.pdf)

This standard applies to the Bank of Russia, credit institutions and representative offices of foreign banks. In order to manage information security risks, each institution creates an authorized body – its information security service, which could be a separate unit or persons responsible for ensuring information security. Thus, an information security policy is developed, along with models of threats and violators and the respective procedures. Besides, general requirements are set for ensuring information security through antivirus tools, banking payments and IT processes when using the Internet and cryptographic means of data protection. Special attention is paid to processing personal data. Information security management system is described in detail. The procedure for developing internal documents concerning information security is established, and the general procedure for conducting self-assessment and audit with regard to information security.

## Guidelines

**10. Bank of Russia Guidelines for the Advancement of Information Security in the Financial Sector for 2019–2021**

[http://www.cbr.ru/content/document/file/83253/onrib\\_2021.pdf](http://www.cbr.ru/content/document/file/83253/onrib_2021.pdf)

The Guidelines for the Advancement of Information Security in the Financial Sector for 2019–2021 set priority goals and objectives for improving information security and cyber resilience, including the following:

- information security and cyber resilience that would enhance the financial stability of each financial market institution;
- operational reliability and business continuity of credit and financial institutions;
- countering cyber-attacks, including with the use of innovative financial technologies;
- protecting the rights of financial services consumers.

The Guidelines describe the prerequisites for and trends in the development of information security in the credit and financial sector in the Russian Federation, the Bank of Russia's objectives and priority activities in the sphere of information security and cyber resilience, as well as measures to be taken in this area. The measures stipulated in the Guidelines were developed, among other purposes, to implement a range of objectives as part of federal projects under the “Digital Economy in the Russian Federation” national programme.

## B. Functional Categorisation

Please find below a detailed description of information security requirements with regard to the information technology infrastructures stipulated by National Standard of the Russian Federation GOST R 57580.1-2017, as well as various Bank of Russia regulations, with a breakdown for the *Identify, Protect, Detect, Respond* and *Recovery* functions.

---

## Identify

Bank of Russia regulations establishing information security requirements determine the list of protected information types to which those requirements apply. It is implied that financial institutions identify such information for the purposes of compliance with Bank of Russia requirements when compiling, processing and storing it in automated systems.

According to GOST R 57580.1-2017, to manage the operational risk related to information security, financial institutions have to take measures to identify, classify and keep record of IT systems, including automated systems.

When identifying and keeping record of IT systems, financial institutions must account for the basic levels of information infrastructure, including but not limited to the following:

a) system levels:

- hardware level;
- networking hardware level;
- level of network applications and services;
- level of server virtualisation components and software infrastructure services;
- level of operation systems, database management systems, and application servers;

b) level of automated systems and applications used to render financial services as part of the financial institutions' business or technological processes.

To ensure that the organisational and technical information protection measures used are adequate, financial institutions are required to develop a threat model and an information security violator model. Recommendations on the basic outlines for these models are provided in the Annex to GOST R 57580.1-2017.

## Protect

List of technological information protection measures:

- verifying (double-checking) the correctness of compiling (preparing) electronic messages;
- verifying the correctness of completing electronic message fields and electronic signature holder's rights (input check);
- monitoring of electronic message duplication;
- monitoring the structure of electronic messages;
- protection of protected information when transferring it via communication channels;
- ensuring that clients sign electronic messages through a method that ensures the message's integrity and confirms that the authorised person indeed compiled the message in question;
- receiving confirmation from clients that financial (banking) operations have been completed;
- comparative verification of outgoing electronic messages and respective incoming electronic messages;
- comparative verification of the results of financial banking operations and information contained in electronic messages;
- sending notifications to clients with regard to completion of banking operations if

such notifications are stipulated by Russian law or respective contracts.

Information protection requirements covering applicable software of automated systems and applications oblige financial institutions to use the Internet to execute:

- certification pursuant to the requirements established by the authorised executive body of the Russian Federation, or
- evaluation of compliance with the requirements to the estimated trust level set out by National Standard of the Russian Federation GOST R ISO/IEC 15408-3-2013 concerning applicable software of automated systems and applications distributed by credit institutions among their clients and software that processes protected information in the sections used for receiving electronic messages.

To enforce the information security requirements for IT infrastructures, National Standard of the Russian Federation GOST R ISO/IEC 15408-3-2013 stipulates the following information protection processes that implement the Protect function:

1. Process "Information security in access administration", including the following sub-processes:
  - administering accounts and rights of logical access subjects;
  - identification, authentication, authorisation (discriminate access) in logical access;
  - information protection in physical access;
  - identification, classification and accounting of resources and access objects.
2. Process "Protection of computer networks", including the following sub-processes:
  - segments and firewalls in computer networks;
  - protection of information transferred via computer networks;
  - protection of wireless networks.
3. Process "Protection from malicious code".
4. Process "Prevention of information leaks".
5. Process "Protection of virtualisation environments".
6. Process "Protection of information in cases of remote logical access via mobile devices".

The description of information protection processes in the National Standard of the Russian Federation GOST R 57580.1-2017 includes measures grouped according to the requirements for information protection processes that they help implement.

## Detect

Bank of Russia regulations make it obligatory to register any incidents related to violation of information security requirements, including incidents that have resulted or may result in unauthorised banking operations or failure to provide services, in particular those on the list of incident types (the "information protection incidents"). This list is provided in Bank of Russia Standard STO BR BFBO-1.5-2018.

In order to enforce the information security requirements for IT infrastructures, National Standard of the Russian Federation GOST R 57580.1-2017 stipulates the following information protection processes (and sub-processes) that implement the Detect function:

1. Identification of network breaches and attacks, which should provide:
  - monitoring of network traffic content;



- registration of information protection events related to the results of monitoring network traffic content.

2. Verification of integrity and security of IT infrastructures, which should provide:

- monitoring of occurrence of any known (described) information protection vulnerabilities of IT systems;
- organising and monitoring of placement, storage and updates of IT infrastructure software;
- monitoring the content and integrity of IT infrastructure software;
- registering information protection events related to the results of monitoring the integrity and protection of information infrastructure.

## Respond

Bank of Russia regulations oblige financial institutions to inform the Bank of Russia about information protection incidents. Besides, forms and timeframes established by Bank of Russia Standard STO BR BFBO-1.5-2018 provide for detailed and extensive data to be submitted on information protection incidents, including the date and time of the incident's registration, incident type, the object for which the threat materialised, and information on whether the financial institution requires the Bank of Russia's assistance.

To enforce the information security requirements for IT infrastructures, National Standard of the Russian Federation GOST R 57580.1-2017 stipulates the following information protection processes (and sub-processes) that implement the Respond function:

1. Monitoring and analysis of information protection that should provide for:

- monitoring of registration data on information protection events accumulated by information protection tools and systems, as well as IT systems, in particular, under the requirements for the basic setup of information protection methods;
- collection, protection and storage of registration data on information protection events;
- analysis of registration data on information protection events;
- registration of information protection events related to the processing of registration data on information protection events.

2. Detection of and response to information protection incidents, providing for:

- detection and registration of information protection incidents;
- response to information protection incidents;
- storage and protection of information on information protection incidents;
- registration of information protection events related to the results of identifying and responding to information protection incidents.

## Recovery

Bank of Russia Standard STO BR BFBO-1.5-2018 allows financial institutions to inform the Bank of Russia about the actions taken in order to eliminate the information protection incident, while also allowing the Bank of Russia to provide recommendations on possible actions with regard to the incident.



---

# India



CERT-In and CSIRT-Fin respond to incidents, issue alerts, guidelines and directions for mitigation. In addition, the CSITE in RBI issues cyber-security directions and guidelines and also supervises through onsite and offsite surveillance mechanisms.

```
0100010
,10010010001
,1000100100100
}10010001001001
}1001001000100}
?001001001000
^1000100100
0010001
0010010
0010010
0100010
}01001000
}01001001
}10001001
}10010001
}10010010
100010010
100100010
100100100
```

In India, the Indian Computer Emergency Response Team (CERT-In) under Ministry of Electronics and Information Technology (MeitY), Government of India is the national nodal agency for responding to computer 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. CERT-In provides the requisite leadership for the CSIRT-Fin (Computer Security Incident Response Team-Finance Sector) operations under its umbrella for responding to, containment and mitigation of cyber security incidents reported from the financial sector.

The Cyber Security and Information Technology Examination Group (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>)
- Cyber Security Framework in Banks dated June 02, 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 June 08, 2017 (<https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD53E0706201769D6B56245D7457395560CFE72517E0C.PDF>)
- Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) dated October 19, 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 December 31, 2019 (<https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOT1129BB26DEA3F5C54198BF24774E1222E61A.PDF>)
- Cyber Security controls for Third party ATM Switch Application Service Providers dated December 31, 2019 (<https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT13060CC89309DEC4BFB8B7CBC33FAA05FE5.PDF>)
- The Master Direction on Digital Payment Security Controls dated February 18, 2021 (<https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF>)

## B. Functional Categorisation

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

### 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/unauthorised 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 organisation 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.
- 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.
- 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.
- Appoint/designate Chief Information Security Officer (CISO) in the bank to apply security best practices and strengthen security of IT infrastructure
- Regularly carry out security audit of IT infrastructure, web applications and websites on periodic basis to check resilience of cyber assets against malicious attacks
- 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.
- 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.
- Background checks, non-disclosure and security policy compliance agreements shall be mandated for all third-party service providers
- 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
- Put in place a fully effective Incident Response programme with due approval of the Board / Top Management.
- 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.
- Entities shall 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.

- 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.
- 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.
- Develop a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.

## Protect

- Appropriately manage and provide protection within and outside organisation 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
-



have an escrow arrangement for the source code for ensuring continuity of services in case the vendor defaults or is unable to provide services.

- 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.

## 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.
- 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.

## 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.

- 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
- 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 cyber-attacks/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.

---

# China



The main cybersecurity regulation issued by the PBoC defines the cyber incidents and the key elements, process as well as timelines of incident reporting.

```
0100010  
10010010001  
1000100100100  
010010001001001  
10010010001001  
0001001001000  
1000100100  
0010001  
0010010  
0010010  
0100010  
01001000  
01001001  
10001001  
10010001  
10010010  
100010010  
100100010  
100100100
```

## A. Regulations

The main cybersecurity regulation issued by the PBC 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 which 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://www.cfstc.org/bzgg/gk/view/bzxq.jsp?i\\_id=1909](https://www.cfstc.org/bzgg/gk/view/bzxq.jsp?i_id=1909))
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://www.cfstc.org/bzgg/gk/view/bzxq.jsp?i\\_id=1885](https://www.cfstc.org/bzgg/gk/view/bzxq.jsp?i_id=1885))

## B. Functional Categorisation

### Identify

- Computer security incidents of banks shall include:
  - (1) hardware and software failure of the information system;
  - (2) failure of the network communication system;
  - (3) failure of the power supply system;
  - (4) the infection of the system with a computer virus;
  - (5) the flood, fire, and lightning suffered by the data processing center;
  - (6) invasion or attack of the bank network;
  - (7) the disclosure of sensitive data in the information system;
  - (8) the data theft from the information system; and
  - (9) the theft of the bank data processing equipment.
- A computer security incident that meets any of the following requirements must be reported:
  - (1) Interruption or abnormal operation of the computer information system for more than four hours.
  - (2) Causing a direct economic loss of more than RMB1 million.

- 
- (3) Seriously threatening the security of bank funds.
  - (4) Causing the bank to be unable to operate normally, and affecting more than one county-level administrative region.

## Protect

1. 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, fire-fighting facilities, and access control systems in the server room. Video records and server room access records should be kept for at least 3 months.
2. 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.
3. FIs should use validation technology to ensure the integrity of data in the process of network communication as well as transmission and storage.
4. Access and data flow across the boundaries should be communicated through a controlled interface provided by network boundary control devices.
5. 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.
6. Encryption or other protective measures should be employed to ensure the confidentiality of authentication information during the transmission and storage process.
7. 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

1. FIs should be able to detect intrusions into critical nodes and provide alerts in the event of a serious intrusion.
2. FIs should be able to detect possible known vulnerabilities and patch them in a timely manner after adequate testing and evaluation.
3. 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 PBC, and send a copy thereof to the computer security department.
- The report on a computer security incident shall include:
  - (1) when and where the computer security incident occurs, the entity and its person in charge and his or her contact information;

- (2) the category of the computer security incident, the software and hardware systems involved, and the cause of the incident;
- (3) the consequences and coverage of the computer security incident;
- (4) the reasons for the occurrence of the computer security incident;
- (5) the liable persons or the persons involved in the case; and
- (6) 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 PBC. 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 PBC.
- After receiving the report on a computer security incident from the banking system, the branch or sub-branch of the PBC shall, within 12 hours, report it to the computer security departments of the branches and operation offices of the PBC, and central sub-branches of the PBC in capital cities of provinces (autonomous regions). The branches, operation offices, and central sub-branches of the PBC 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 PBC.
- Any entity or individual shall have the right to report to the local branch or sub-branch of the PBC the hidden dangers of computer security existing in the bank. The relevant department of the PBC 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<sup>1</sup>, 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.

## Recover

-NIL-

<sup>1</sup> Implementation guidelines for classified protection of cybersecurity of financial industry—Part 1: Fundamentals and vocabulary (JR/T 0071.1—2020)

---

# South Africa



The Prudential Authority develops various regulations, guidance and supervisory practices for the financial sector addressing cybersecurity.

```
0100010  
10010010001  
1000100100100  
010010001001001  
10010010001001  
0001001001000  
1000100100  
0010001  
0010010  
0010010  
0100010  
01001000  
01001001  
10001001  
01001001  
010010010  
100010010  
100100010  
100100100
```

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 financial sector level.

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

## A. Regulations

### 1. **Guidance Note 5 of 2014: Outsourcing of functions within banks**

Published Date: 2014-07-11

Last Modified Date: 2020-10-01

<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, 09:30 PM

<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

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

### 4. **Prudential Standards: Governance and Operational standards for Insurers (GOI)**

[Governance and Operational Standards for Insurers 5](#)

[Governance and Operational Standards for Insurers 3.2](#)

Date: July 1, 2018

[https://www.resbank.co.za/en/home/publications/prudential-authority/pa-insurance/pa-post-insurance/Draft\\_Prudential\\_Standards\\_-\\_9\\_March\\_2018](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: Flavour of the year**

Published Date: 2016-02-09

Last Modified Date: 2020-10-01

<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: Flavour of the year**

Published Date: 2021-02-12

Last Modified Date: 2021-02-22

<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>



## B. Functional Categorisation

The broad categorisation of regulatory instruments and practices under five NIST category are given below:

### **Issued Regulatory Instruments**

#### **1. Guidance Note 5 of 2014**

*(Identify, Protect, Detect and Respond)*

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.

#### **Identify**

- Paragraph 5.1 (b) states that a bank must plan for outsourcing activities, including performing risk assessments surrounding the outsourcing of material business activities and functions.
- Paragraph 5.1 (c) states that a bank must have due diligence processes in place for the selection of service providers.

#### **Protect**

- Paragraph 5.1 (d) states that a bank must have a legal contract in place for all outsourcing of material business activities and functions with third parties.
- Paragraph 5.1 (h) states that a bank must have administrative measures and reporting in place that facilitate oversight, accountability, monitoring and risk management.

#### **Detect**

- Paragraph 5.1 (e) states that a bank must have a monitoring process in place to manage outsourced material business activities and functions.

#### **Respond**

- Paragraph 5.1 (g) states that a bank must develop viable contingency and business continuity plans.

#### **2. Directive 2 of 2019**

*(Respond and Recover)*

Issued to banks to formally report all material IT and/or cyber incidents to the PA.

#### **Respond**

- Paragraph 2.1.3 states that banks must implement a sufficiently robust incident management framework to manage and report IT and cyber incidents.

#### **Recover**

- Paragraph 2.1.6 states that banks must submit a root cause and impact analysis report, with available information to the PA within 14 calendar days from the date of notification.

### 3. **Guidance Note 4 of 2017**

*(Identify and Protect)*

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.

#### **Identify**

- Paragraph 2.3.4 states that with regards to security testing, specifically also referring to penetration testing, when using third parties banks are required to make use of reputable external service providers for such testing which may, for instance, be evidenced through certification or accreditation.

#### **Protect**

- Paragraph 2.3.3 states that the recovery time objectives for a bank should be based on a thorough business impact assessment and take all other relevant legislative and regulatory requirements into consideration. In addition, high availability and failover should be taken into account when designing resilience principles to minimise the impact on customers.
- Paragraph 2.3.5 states that the PA does not require banks to join specific information sharing initiatives. However, the bank's situational awareness must include cyber threat intelligence which is applicable to the local market and its operations in South Africa. Participation in a banking sector computer security incident response team is strongly encouraged.

### 4. **Governance and Operational Standards for Insurers 5**

*(Identify, Protect, Detect and Respond)*

Issued to insurers for outsourcing of material business activities and also addresses confidentiality, privacy and the security of information related to outsourcing.

Issued to insurers to address the appropriateness, effectiveness, efficiency, integrity, confidentiality and reliability of the information technology and data quality systems.

#### **Identify**

- Paragraph 4.3 states that an insurer must, when outsourcing any business activity or function, identify and manage all risks introduced by the outsourcing arrangement.
- Paragraph 7.2 (a) states that the insurer must demonstrate that it has assessed the costs and benefits and potential risk to its insurance business inherent in the proposed outsourcing.
- Paragraph 7.2 (b) states that the insurer must demonstrate that it has identified potential service providers to undertake.

#### **Protect**

- Paragraph 4.2 states that an insurer must have a board-approved policy and related procedures for assessing the risks involved with outsourcing, which policy and related procedures must be consistent with this Standard.
- Paragraph 4.5 states that an insurer must when outsourcing any function or activity avoid, and where this is not possible mitigate, any conflicts of interest between the insurance business of the insurer, the interests of policyholders or the business of the other person that performs the outsourcing.

- Paragraph 6.3 states that the Prudential Authority may object to any arrangement to outsource a material business activity if it is convinced that the proposed outsource is inconsistent with this Standard.

#### **Detect**

- Paragraph 7.1 states that prior to entering into any such arrangement, an insurer must notify the Prudential Authority of a proposed outsourcing of a material business activity.
- Paragraph 7.2 (g) states that the insurer must demonstrate that it has assessed the service provider's governance, risk management, and internal controls and its ability to comply with applicable laws.

#### **Respond**

- Paragraph 7.2 (g) states that the insurer must demonstrate that it assessed whether the service provider's operational capability or financial position pose a material risk to the service provider's ability to deliver the proposed outsourced function or activity.
- Paragraph 7.2 (i) states that the insurer must demonstrate that it developed appropriate contingency plans to ensure the continuous functioning of the insurance business of the insurer in the event that the outsourcing arrangement is terminated or found to be ineffective.

### **5. Governance and Operational Standards for Insurers 3.2**

*(Respond)*

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.

#### **Respond**

- Paragraph 10.1 states that an insurer must notify the Prudential Authority as soon as possible, but no later than 24 hours, after experiencing a major disruption that has the potential to have a material impact on the insurer's risk profile, or affect its financial soundness. The insurer must explain to the Prudential Authority the nature of the disruption, the action being taken, the likely effect and the timeframe for returning to normal operations. The insurer must notify the Prudential Authority when normal operations resume.

### **6. 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. *(Respond)*

#### **Respond**

- Section 6(3)(d) of the Financial Markets Act, 2012, requires that all licensed market MIs to report all significant events to the Registrar without delay and within 48 hours of becoming aware of the significant event.

## **Draft Regulatory Instruments**

### **7. Information Technology (IT) Risk Joint Standard**

*(Identify, Protect, Detect, Respond and Recover)*

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.

### **8. Cyber Security Joint Standard:**

*(Identify, Protect, Detect, Respond and Recover)*

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.

## **Issued Practices**

### **9. Guidance Note 2 of 2016**

*(Identify, Protect, Detect and Respond)*

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**

- Paragraph 4.2 (a) relates to how the board ensures that it has the necessary awareness, knowledge and understanding in order to be able to provide oversight of cyber security and any possible impact on strategy.
- Paragraph 4.2 (c) relates to the bank's approach to managing cyber security and its inclusion and integration in the bank's enterprise risk management framework.

#### **Protect**

- Paragraph 4.2 (d) relates an overview of the bank's primary cyber security governance structures.
- Paragraph 4.2 (f) relates to the bank's approach in addressing the shortage of cyber security skills, creating awareness with customers and employees and the availability of an adequate budget.

#### **Detect**

- Paragraph 4.2 (e) relates to the recent initiatives to bolster cyber defences and future plans.

#### **Respond**

- Paragraph 4.2 (g) relates to how the board is addressing the legal implications of cyber risks and what considerations have been made with regard to cyber insurance.
- Paragraph 4.2 (h) relates the bank's approach to managing cyber risks that are

---

introduced through outsourcing and third party service provider arrangements.

- Paragraph 4.2 (i) relates to the bank's approach in sharing of threat intelligence within the banking industry as well as the board's views in terms of the interaction with the proposed government cyber structures, such as the Cyber Hub.

#### 10. Letters

*(Identify, Protect, Detect, Respond and Recover)*

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.

#### 11. Guidance Note 2 of 2021

*(Identify, Protect, Detect, Respond and Recover)*

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.

#### 12. IT Risk Questionnaire

*(Identify, Protect, Detect, Respond and Recover)*

An annual questionnaire was developed and issued to the industry in 2020 in order to obtain insights related to the IT risk posture within the financial institution (FI), industry and sector.

#### 13. Survey

*(Identify, Protect, Detect, Respond and Recover)*

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

### **Draft Practices**

#### 14. Cybersecurity Questionnaire

*(Identify, Protect, Detect, Respond and Recover)*






An annual questionnaire is being developed to obtain insights related to the cyber security posture within the Financial Institution (FI), industry and sector.

---

# Appendix

## Translated Regulation

### A. List of Translation Regulation: Brazil

1. [Brazil - Resolution 2554 of September 24, 1998](#) 
2. [Brazil - Resolution 4557 of February 23, 2017](#) 
3. [Resolution CMN 4893 of February 26, 2021](#) 
4. [Resolution BCB 85 of April 08, 2021](#) 
5. [Brazil - Guide to Supervision Practices \(GSP\)](#) 

### B. List of Translation Regulation: Russia

1. Bank of Russia Regulation No. 719-P, dated 4 June 2020 
2. Bank of Russia Regulation No. 747-P, dated 23 December 2020 
3. [Bank of Russia Regulation No. 683-P, dated 17 April 2019](#) 
4. Bank of Russia Regulation No. 757-P, dated 20 April 2021 
5. [National Standard of the Russian Federation GOST R 57580.1-2017](#) 
6. National Standard of the Russian Federation GOST R ISO/IEC 15408-3-2013  
<https://www.iso.org/ru/standard/46413.html>
7. Bank of Russia Standard STO BR BFBO-1.5-2018  
(*Translation awaited*)
8. [National Standard of the Russian Federation GOST R 57580.2-2018](#) 
9. [Standard of the bank of Russia STO BR IBBS-1.0-2014](#) 
10. [Bank of Russia Guidelines for the Advancement of Information Security in the Financial Sector for 2019–2021.](#) 

## Annex

### BRICS Rapid Information Security Channel (BRISC) Members

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

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



**BRISC - Editorial Team**

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

**Disclaimer:** Information for this document have been gathered from a substantial number of sources. While every reasonable effort has been made to verify the source and accuracy of the data collected, the editorial team cannot exclude potential errors and omissions. This report should not be considered to provide legal or investment advice. This document has been produced and disseminated for general information purpose.





Published by



Reserve Bank of India