БАНК РОССИИ

BANK OF RUSSIA STANDARD

STO BR IBBS-1.0-2014

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

GENERAL PROVISIONS*

Date enacted: 1 June 2014

Official Edition

Moscow
2014

Foreword

1. ADOPTED AND ENACTED by Bank of Russia Directive No. P-399 dated 17 May 2014.

2. TO SUPERSEDE STO BR IBBS-1.0-2010.

Contents

Introduction

The Banking System (BS) of the Russian Federation (RF) comprises the Bank of Russia, lending institutions and representative offices of foreign banks [1]. The activities of the Bank of Russia are aimed at developing and strengthening the RF BS and maintaining the stability and development of the National Payment System [2]. The most important prerequisite for achieving these objectives is maintaining a necessary and sufficient level of information security (IS) of RF BS organisations and their assets (including information), which is to a large extent determined by the level of IS of bank processes (payment processes, information processes, etc.) and computerized banking systems operated by RF BS organisations.

The nature of the RF BS is such that the negative consequences of an operational failure in individual organisations could lead to the rapid development of a systemic crisis of the RF Payment System and cause damage to the interests of both owners and clients. When IS incidents occur, composite risk and potential damage to RF BS organisations increase significantly. That is why IS threats present a significant hazard to RF BS organisations.

In order to counteract such threats and ensure the effectiveness of actions taken to mitigate the unfavourable consequences of IS incidents (their influence on operational risk, reputation risk, strategic risk and other risks), a sufficient IS level must be maintained in RF BS organisations. This level must also be preserved for a prolonged period. IS maintenance is, therefore, a fundamental aspect of a RF BS organisation's activities.

Activities associated with IS maintenance shall be monitored. In connection with this, the Bank of Russia is a proponent of regular IS level assessments in RF BS organisations, assessment of IS breach risk level and taking the actions required to manage such risk.

Accordingly, this standard on IS maintenance for RF BS organisations has been developed; it forms the basis for a set of standardisation documents for development and maintenance of the standard which together make up a package of standardisation documents for IS maintenance in RF BS organisations.

The main aims of the standardisation of IS maintenance in RF BS organisations include:

- To develop and strengthen the RF BS;
- To increase confidence in the RF BS;
- To maintain the stability of RF BS organisations and thereby the stability of the RF BS as a whole;
- To achieve adequacy of protective measures to actual IS threats;
- To prevent and/or reduce damage from IS incidents.

The main objectives of standardisation for IS provision for RF BS organisations include:

- To establish uniform requirements for IS maintenance in RF BS organisations;
- To improve the effectiveness of IS maintenance and support measures in RF BS organisations.

BANK OF RUSSIA STANDARD

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

GENERAL PROVISIONS

Date enacted: 1 June 2014

1. Scope

This standard applies to RF BS organisations and establishes provisions for IS maintenance in RF BS organisations.

It is recommended that this standard be used by including references to it and/or using its provisions directly in internal documents of RF BS organisations and in agreements.

The provisions of this standard shall apply on a voluntary basis, unless the application of specific provisions is made binding by Russian legislation or other regulations, including Bank of Russia regulations.

The application of this standard may be made binding by agreements concluded by RF BS organisations or the decision of a RF BS organisation to accede to the standard. In such cases, requirements of this standard containing 'must' provisions are obligatory, while recommendations are to be applied as decided by the RF BS organisation.

2. Normative References

This standard includes normative references to the following standards:

Bank of Russia Standard STO BR IBBS-1.2 ‘Maintenance of Information Security of the Russian Banking System Organisations. Assessment Method for Compliance of Information Security of the Russian Banking System Organisations with Requirements of STO BR IBBS-1.0’.

Bank of Russia Recommendations on Standardisation RS BR IBBS-2.0 ‘Maintenance of Information Security of the Russian Banking System Organisations. Recommended Practices for Documentation Related to Information Security Maintenance in Accordance with STO BR IBBS-1.0’

Bank of Russia Recommendations on Standardisation RS BR IBBS-2.1 ‘Maintenance of Information Security of the Russian Banking System Organisations. Guidelines for Self-Assessment of Conformity of Information Security of the Russian Banking System Organisations to Requirements of STO BR IBBS-1.0’.

3. Terms and Definitions

The terms specified herein are to be applied in documents of any type and in all activities related to IS maintenance within the framework of the BR IBBS Package (see 3.4).

3.1**. Banking System of the Russian Federation:** The Bank of Russia, lending institutions and representative offices of foreign banks [1].

3.2. **Standard:** A document that, for the purpose of voluntary repeated use, specifies product characteristics, rules of execution and specifications for engineering processes (including surveys), manufacture, construction, installation, set-up, operation, storage, transportation, distribution and disposal and for work or service performance [3].

Note:

The standard may also contain rules and methods for research (testing) and measurements, sampling rules, requirements for terms, symbols, packaging, marking or labels and rules for their application.

3.3. **Recommendations on standardisation:** A document containing organisational and methodological advice concerning standardisation activities which facilitate the application of the fundamental standard.

3.4. **BR IBBS Package:** An interrelated set of documents on Bank of Russia standardisation ‘Maintenance of Information Security of the Russian Banking System Organisations’.

3.5. **Management:** Coordinated activities related to governance and administration.

3.6. **System:** a set (complex) of tangible objects (elements) of any nature, including any physical nature, and information objects that interact to achieve a common goal; this complex must have a systemic property or properties.

Note:

A systemic property (or properties) is a property which none of the elements or subsets of elements possesses when any method of division is used. A systemic property is not directly inferable from the properties of the elements and parts.

3.7. **Information:** Messages or data, whatever the form of their presentation [4].

3.8. **Infrastructure:** A set of interconnected servicing structures forming the basis for solving a problem or task.

3.9. **Information infrastructure:** A system of organisational structures for ensuring the operation and development of the information environment and means of information interaction.

Note:

Information infrastructure:

comprises a combination of information centres, data banks, knowledge bases and communication systems and ensures consumer access to information resources.

3.10. **Document:** Information recorded on a tangible carrier with details for its identification.

[GOST R 52069.0-2003]

Note:

A tangible carrier means a product or material used to record information and enabling the preservation and copying of such information (e.g. paper, magnetic tape or card, magnetic or laser disk, photographic film, etc.).

3.11. **Process:** A set of interrelated activities which transforms inputs into outputs.

3.12. **Technology:** A set of interconnected methods, means and techniques for specific activities.

3.13. **Technological process:** A process for implementing a particular technology.

3.14. **Automated system:** A system consisting of personnel and a package of tools for automating personnel activity which implements the information technology of executing specified functions.

[GOST 34.003-90]

3.15. **Authorisation:** Granting of access rights.

3.16. **Identification:** The process of assigning an identifier (a unique name) and comparing a presented identifier with the list of identifiers assigned.

3.17. **Authentication:** Checking that a presented identifier belongs to the access subject (verification of authenticity).

3.18. **Registration:** Recording of data concerning actions (or events) completed.

3.19. **Role:** A predetermined set of rules establishing allowable interaction between the subject and the object.

Notes:

1. Subjects include persons from amongst the managers, personnel or clients of an organisation in the Banking System of the Russian Federation, or processes for performing actions with objects initiated on their behalf.

2. Objects may be hardware, software, firmware, an information resource, a service, a process or a system with which an action is performed.

3.20. **Threat:** A hazard which could entail possible losses or damage.

3.21. **Risk:** A metric which factors the likelihood of a threat occurring and the magnitude of losses or damage which would result from the occurrence of this threat.

3.22. **Asset:** Anything that is valuable to the RF BS organisation and is at its disposal.

Note:

Assets of a RF BS organisation may include:

Employees (personnel), financial (monetary) resources, computer equipment, telecommunication equipment, etc.;

Various types of bank information, such as payment information, financial analysis data, service information, management data, personal data, etc.;

Bank processes (bank payment processes, bank information processes);

Bank products and services provided to clients.

3.23. **Information asset:** Information, along with details making it possible to identify it, that is valuable to a RF BS organisation, is at the disposal of the RF BS organisation, and is presented on any tangible carrier in a form suitable for processing, storage or transfer.

3.24. **Classification of information assets:** The division of the existing information assets of a RF BS organisation by type according to the severity of consequences from loss of their significant IS properties.

3.25. **Object related to Information asset:** A tangible object of the information asset use and/or operation environment (a storage, transfer, processing or destruction object, etc.).

3.26. **Resource:** An asset of a RF BS organisation which is used or consumed during the performance of a certain activity.

3.27. **Banking process:** A technological process which changes and/or determines the state of assets of a RF BS organisation which are used during operations or necessary for the performance of bank services.

Notes:

1. Operations with assets of a RF BS organisation may be carried out manually or automatically (e.g. through computerized bank systems).

2. Depending on the type of activity, bank payment processes, bank information processes, etc. are distinguished.

3.28. **Bank payment process:** A part of the bank process during which actions with information associated with funds transfer, payment clearing and settlement and actions with archives of such information are carried out.

3.29. **Bank information process:** A part of the bank process during which actions with information that are necessary for a RF BS organisation to fulfil its functions but which are not bank payment processes are carried out.

3.30. **Payment information:** Information based on which operations associated with funds transfer are performed.

3.31. **Non-payment information:** Information required for the operation of a RF BS organisation, other than payment information, which may comprise, for instance, data on statistical accounting and internal activities, analytical, financial and reference information.

3.32. **Automated banking system:** An automated system which implements the banking process.

3.33. **Automation technology complex of the automated banking system:** The set of all components of the automated banking system of a RF BS organisation, except people.

3.34. **Security:** A state of protection of the interests or goals of a RF BS organisation in threat conditions.

3.35. **Information security, IS:** Security associated with threats in the field of information.

Notes:

1. Protection is achieved by maintaining a set of IS properties: availability, integrity and confidentiality of information assets. The priority of IS properties is determined by the value of the given assets for the interests or goals of the RF BS organisation.

2. The field of information is the sum of information; information infrastructure; subjects which collect, generate, distribute, store and use information; and the system that governs the resulting relations.

3.36. **Availability of information assets:** An IS property of a RF BS organisation consisting in the fact that information assets are provided to an authorised user in the form and in the location required by the user, and at the time when they are needed by such user.

3.37. **Integrity of information assets:** An IS property of a RF BS organisation consisting in maintaining its information assets unchanged or correcting changes identified in information assets.

3.38. **Confidentiality of information assets:** An IS property of a RF BS organisation consisting in the fact that processing, storage and transfer of information assets are carried out such that information assets are available only to authorised users, system objects or processes.

3.39. **Information Security System; ISS:** A set of safeguards, protective measures and their operating processes, including resource and administrative (organisational) support.

3.40. **Information Security Management System; IS Management System:** Part of the management of a RF BS organisation intended to create, implement, operate, monitor, analyse, maintain and improve the IS maintenance system.

3.41. **Information Security Provision System; IS Maintenance System:** The combination of the ISS and the IS Management System of a RF BS organisation.

3.42. **Scope of application of the Information Security Provision System; scope of application of IS Maintenance System:** The sum of the information assets and elements of information infrastructure of a RF BS organisation.

3.43**. Awareness of the necessity of information security maintenance; IS awareness:** The understanding by the management of a RF BS of the necessity to make a forecast of IS maintenance results, independently and based on the values adopted by the organisation and accumulated knowledge, and to consider it within the framework of the main activities or business, and to support these activities appropriately in light of the forecast.

Note:

IS awareness is an internal motivation for the management of a RF BS organisation to initiate and maintain IS maintenance activities, as opposed to motivation or compulsion where the decision to initiate and maintain IS maintenance activities is determined either by the emergence of problems in the organisation or by external factors (e.g. statutory requirements), respectively.

3.44**. Safeguard:** An existing practice, procedure or arrangement used to mitigate the risk associated with an IS breach with a RF BS organisation.

3.45**. Information security threat; IS threat:** The threat of a breach of IS properties, such as the availability, integrity or confidentiality of information assets of the RF BS organisation.

3.46**. Information security vulnerability; IS vulnerability:** A weak spot in the infrastructure of a RF BS organisation, including the IS Maintenance System, which may be used to implement or facilitate implementation of an IS threat.

3.47. **Damage:** The loss of assets, deterioration (loss of use) of the assets and/or infrastructure of an organisation or any other harm to the assets and/or infrastructure of a RF BS organisation resulting from the implementation of an IS threat through IS vulnerability.

3.48. **Information security incident; IS incident:** A single event or a series of events indicating that an IS threat has occurred, is being undertaken or is probable, the result of which is:

– Malfunction or possible malfunction of information security equipment which forms part of the IS Maintenance System of the RF BS organisation;

– Violation or possible violation of the requirements set out in the legislation of the Russian Federation, regulations and instructions of regulatory or oversight authorities, internal documents of the RF BS organisation related to IS maintenance, disturbance or possible disturbance in the performance of IS Maintenance System processes of the RF BS organisation;

– A breakdown or possible breakdown in the performance of the banking processes of the RF BS organisation;

– Infliction or possible infliction of damage to the RF BS organisation and/or its clients.

3.49. **Information security violator; IS violator:** A party which implements IS threats against a RF BS organisation, violating the authority provided to him/her to access the assets of the RF BS organisation or to dispose of them.

3.50. **Information security violator model; IS violator model:** A description and classification of IS violators, including a description of their experience, knowledge, available resources required for threat implementation, possible motivation for their activities, and ways such violators could implement IS threats.

3.51. **Information security threat model; IS threat model:** A description of sources of IS threats relevant to RF BS organisation; methods of IS threat implementation; suitable objects for IS threat implementation; vulnerabilities used by sources of IS threats; types of possible losses (e.g. breakdowns in the availability, integrity or confidentiality of information assets); and the range of potential damage.

3.52. **Risk of information security breach; risk of IS breach:** The risk associated with an IS threat.

3.53. **Assessing the risk of information security breach:** A systematic and documented process of identification, collection, use and analysis of information that makes it possible to assess the risks of IS breach associated with the use of information assets of a RF BS organisation in all phases of their life cycle.

3.54. **Handling the risk of information security breach:** The process of selecting and executing safeguards which reduce the risk of IS breach or measures for transfer, acceptance or avoidance of risk.

3.55. **Residual risk of information security breach:** Risk remaining after IS breach risk handling.

3.56. **Acceptable risk of information security breach:** A risk of IS breach the expected damage from which a RF BS organisation is ready to accept for the time being in the given situation.

3.57. **Documentation:** A set of interrelated documents with a common aim.

3.58. **Information security maintenance plan:** A document listing work or measures planned for the maintenance of IS in a RF BS organisation, their sequence, scope (in one form or another), execution period, responsible persons and the specific persons who are to perform them.

3.59. **Information security maintenance evidence:** A document or part of a document containing the results achieved (interim or final) with regard to IS maintenance in a RF BS organisation.

3.60. **Information security policy; IS policy:** Documentation specifying the high-level aims, scope and main areas of IS maintenance activities, intended for the RF BS organisation in general.

3.61. **Individual information security policy; individual IS policy:** Documentation presenting the details of IS policy applicable to one or more IS areas or types and technologies of RF BS activity.

3.62. **IS monitoring:** Constant observation of objects and parties affecting the IS of a RF BS organisation, as well as the collection, analysis and summarising of observation results.

3.63. **Information security conformity assessment; IS conformity assessment:** The systematic and documented process of obtaining evidence of a RF BS organisation's activities related to the implementation of IS requirements, and establishing the degree to which IS assessment (audit) criteria have been met within the RF BS organisation.

3.64. **Information security audit; IS audit:** An independent assessment of IS conformity carried out by employees of an organisation that is external to the RF BS organisation, enabling a professional audit judgement to be made concerning the state of IS in the RF BS organisation.

3.65. **Information security self-assessment; IS self-assessment:** An information security conformity assessment performed by employees of a RF BS organisation.

3.66. **Information security assessment (audit) criteria; IS assessment (audit) criteria:** The sum of IS maintenance requirements as specified in the Bank of Russia Standard STO BR IBBS-1.0 ‘Maintenance of Information Security of the Russian Banking System Organisations. General Provisions’, or part thereof.

3.67. **Assessment (audit) evidence of conformity of information security to specified criteria; IS conformity assessment (audit) evidence:** Records, a statement of facts or other information that are related to the criteria for IS conformity assessment (conformity self-assessment, audit) and can be verified.

Note:

IS conformity assessment (conformity self-assessment, audit) evidence may be qualitative or quantitative.

3.68. **Information security audit findings; IS audit findings:** The result of assessment of collected IS audit evidence.

3.69. **Opinion on information security audit results (auditor opinion); opinion on IS audit results:** Qualitative or quantitative assessment of conformity to IS audit criteria established, presented by the audit team after reviewing all the findings of an IS audit in accordance with the goals of the IS audit.

3.70. **Information security audit scope; IS audit scope:** The content and range of an IS audit.

Note:

IS audit scope usually typically includes the location, the organisational structure and the nature of the activities of the audited organisation and the processes subject to the IS audit, as well as the covered period.

3.71. **Information security audit programme; IS audit programme:**

A plan for conducting one or more IS audits (and other IS checks) planned for a specific period and aimed at achieving a specific goal.

Note:

The IS audit programme includes all activities necessary for planning, conducting, overseeing, analysing and improving IS audits (and other IS checks).

4. Designations and Abbreviations

ABS = Automated Banking System

BS = Banking system

LC = Life cycle

IS = Information security
ISPD = Information system of personal data
UA = Unauthorised access
URA = Unregulated activities within the delegated authority
RF = Russian Federation
DET= Data encryption tool
IS Management System = Information Security Management System
ISS = Information Security System
IS Maintenance System = Information Security Maintenance System
ECM= Electronic computing machine (computer)

5. Initial Conceptual Scheme (Paradigm) for Information Security Maintenance in the Russian Banking System Organisations

5.1. The essence of business consists in involving an asset possessed by the owner (a RF BS organisation) in the business process. This activity is always subject to risk, since both the asset and the business process may be subjected to various threats.

Threats are implemented through their sources and have a corresponding probability of implementation.

Sources of threats may be natural, technogenic or anthropogenic. Sources of anthropogenic threats may be either malicious or non-malicious.

5.2. The initial conceptual scheme of IS of RF BS organisations is based on the adversarial relationship between the owner[1] and the violator[2] in order to gain control over information assets. However, other non-malicious actions or sources of threats are also within the scope of consideration of this standard.

If the violator succeeds in establishing such control, both the RF BS organisation and clients who have entrusted their assets to the organisation suffer damage.

5.3. The RF BS organisation's management must know what is to be protected. To this end, it is necessary to define and protect all information assets or resources, with regard to which implementation of threats could result in damage to the RF BS organisation.

5.4. RF BS organisation's own personnel have the greatest opportunity to cause damage to the organisation. In such a case, the substance of the violator's activities is the direct unauthorised use of asset control granted to the violator for the fulfilment of work duties or unregulated activity for gaining asset control. The violator will strive to conceal the traces of his/her actions.

An external violator usually has an associate (or associates) within the RF BS organisation.

Non-malicious actions of the organisation's own employees create either IS vulnerabilities or incidents which affect the properties of availability, integrity and confidentiality of an information asset or the parameters of the system supporting this asset.

5.5. An imminent attack is hardly ever known of in advance; as a rule, it is unexpected. Attacks are usually local and specific in location, purpose and time.

5.6. As a rule, the violator analyses the object of attack both theoretically (without showing himself/herself) and practically (by identifying IS vulnerabilities). The violator searches for or creates IS vulnerabilities to work out the most effective method of attacking or gaining asset control.

In order to manage the risk of IS breach, the owner establishes an authorised body, its own IS service (a unit or persons in the RF BS organisation in charge of IS maintenance), and arranges for the creation and operation of an IS Maintenance System, as well as arranging for the operation of the ABS in accordance with the rules and requirements set by the IS Maintenance System. One of the goals of the IS service is to identify traces of violator activity.

5.7. One of the main IS maintenance tools the owner has is a forecast based on experience (making a threat model and violator model)[3].

[1] The owner here means an economic organisation entitled to possess, dispose of or use assets, which is interested in or obliged (in accordance with statutory requirements or other legislative or regulatory legal acts) to ensure the protection of assets against threats that may deteriorate their value or cause damage to the owner.

[2] The violator here means a person who is performing or has performed a premeditated action and is aware of its hazardous consequences, or who did not foresee these consequences, but should have and could have foreseen that such consequences might occur (adapted from Article 27 of the Criminal Code of the Russian Federation).

[3] Models of IS (threats and violators) are designed to reflect the future; therefore, they are of a predictive nature. IS models are based on previous facts and experience, but they are focused on the future. Models and forecasts are developed using available experience and knowledge; therefore, the higher the level of knowledge, the more accurate the forecast is.

The sounder and more accurate the forecast is with respect to IS breach risks relevant for the RF BS organisation, the more appropriate and efficient the actions planned and undertaken to provide the necessary IS level will be. It should be considered that threats, their sources and risks may change. Therefore, models should be revised from time to time.

5.8. The most correct and effective method of preventing unacceptable risks of IS breach in a RF BS organisation's activities consists in developing an IS policy for the RF BS organisation and implementing, operating and improving the IS Maintenance System of the RF BS organisation in accordance with it.

5.9. The IS policy of RF BS organisations is based on the IS maintenance experience accumulated within the RF BS organisation, the results of identification of assets to be protected, the results of risk assessment based on the features of the business and technologies, the requirements of the legislation of the Russian Federation, Bank of Russia regulations and the interests and business goals of a particular RF BS organisation.

5.10. Compliance with IS policy is, to a considerable extent, an element of corporate ethics; thus, the IS level is affected greatly by relations both within the staff and between the staff and the owner of the RF BS organisation or the management representing interests of the owner. Therefore, these relations should be managed. Realizing that personnel are the most critical element of security in a RF BS organisation, the owner must encourage the interest and awareness of the personnel in resolving IS-related problems.

5.11. By no means every RF BS organisation has the capability for creating threat and violator models and IS policy on its own. In this case, external organisations must be involved in creating these documents.

Threat and violator models shall account for the requirements of the legislation of the Russian Federation related to IS, the research of leading banking system specialists and international experience in this sphere.

5.12. When threat and violator models are developed, it should be considered that the violator will most probably choose, out of all possible attack objects, those that are monitored worst of all, where his/her action will remain undetected for as long as possible. Therefore, all operations in bank processes where personnel interact with automation tools and systems shall be monitored very carefully.

5.13. Thus, the IS maintenance strategy for RF BS organisations lies both in the effective use of previously developed IS maintenance measures in accordance with the current plan to counteract violator attacks and in the regular revision of IS models and policies and adjustment of the IS Maintenance System. In the case that a threat is implemented, an additional (dedicated) plan of action shall be used to minimise potential losses and to restore the IS Maintenance System.

5.14. Risks are characteristic of any purposeful activity or business. This is an objective reality, and risks may be reduced only to a certain residual level. The remaining (residual) risk, determined, among other things, by factors of the business environment of the RF BS organisation, shall be recognized as acceptable and be accepted or rejected. In this case, risk should be avoided (by changing the business environment) or transferred to someone (e.g. through insurance). Thus, the level of protection of the interests or goals of a RF BS organisation is determined, firstly, by the magnitude of the residual risks accepted and, secondly, by the efficiency of activities for maintaining risks at an allowable low (residual) level.

5.15. The risks of IS breach shall be harmonized and connected hierarchically with the risks of the main (business) activity of the RF BS organisation through potential damage.

Information security risks can be assessed as part of operational risks to make an integrated risk map and to assess the cost of damage for the entire organisation.

The risks of IS breach are expressed in the potential loss of protection of the interests or goals of the RF BS organisation in the information environment and damage to the business of the RF BS organisation or losses.

Loss of protection of the interests or goals of the RF BS organisation in the information environment lies in the loss of the properties of availability, integrity or confidentiality of information assets or the loss of parameters set by business aims or the availability of services of the RF BS organisation infrastructure.

5.16. IS vulnerability creates the prerequisites for threat implementation through that vulnerability (an IS incident). The implementation of an IS breach threat involves the loss of the protection of interests or goals of a RF BS organisation in the information environment, as a result of which damage is done to the RF BS organisation. The severity of the damage and the probability of an IS incident which could cause such damage determine the risk magnitude.

5.17. Constant analysis and study of the infrastructure of a RF BS organisation to identify and eliminate IS vulnerabilities is the basis for the efficient operation of the IS Maintenance System.

5.18. The identification, analysis and assessment of the risks of IS breach shall be based on the identification of assets of the RF BS organisation, their value for the aims and objectives of the RF BS organisation and the IS threat and violator models of the RF BS organisation.

5.19. When it is decided to implement safeguards to counteract identified threats (risks), it should be taken into account that the complexity of the IS Maintenance System of the RF BS organisation may increase at the same time, which, in turn, usually creates new risks. Therefore, when a decision to implement safeguards for handling of existing risks is made, issues concerning the operation of the safeguards and their influence on the overall structure of organisation risks must be considered.

5.20. A RF BS organisation carries out its activity by implementing a set of processes, among which the following groups may be specified:

- Main processes for ensuring the achievement of the aims and objectives of the RF BS organisation;
- Auxiliary processes for ensuring quality, including IS maintenance for the RF BS organisation;
- Management (administrative) processes for maintaining the parameters of both main and auxiliary processes within a predetermined range and adjusting them when external or internal conditions change.

Such a division of processes is conventional, as the main and auxiliary processes frequently make up an integrated whole. For instance, operation of safeguards forms part of the group of main processes. At the same time, management processes are separated from main and auxiliary processes, which are management objects.

5.21. A combination of safeguards making it possible to maintain IS in a RF BS organisation and the processes of their operation, including resource and administrative (organisational) support, make up the ISS of the RF BS organisation.

The sum of IS management processes, including resource and administrative (organisational) support of these processes, make up the IS Management System of the RF BS organisation. The combination of the ISS and the IS Management System make up the IS Maintenance System of the RF BS organisation.

5.22. Safeguard operation processes are performed on a real-time basis. Safeguards and their operation processes must provide the IS level currently required under normal operating conditions, as well as in the case of implementation of threats taken into account in the models of the RF BS organisation and involving:

- Local IS incidents;
- Large-scale disasters and accidents of any nature, the consequences of which may be related to the IS of the RF BS organisation.

5.23. The IS Maintenance System must be defined, planned and regulated within the RF BS organisation. However, even correctly built processes and used safeguards tend to eventually become less effective due to objective reasons. This inevitably leads to degradation of the protection system and an increase in the risks of IS breach.

In order to maintain the protection system at the appropriate level, monitoring of events and incidents in the ISS is used as an operational measure. Management of events and security incidents detected as a result of IS monitoring makes it possible to avoid degradation and to ensure the required asset security level.

To assess the IS of a protected asset and to identify signs of degradation of safeguards used, assessment (or self-assessment) of the system's conformity to the requirements of this standard is performed.

5.24. In order to implement and maintain IS within the RF BS organisation, four groups of processes should be implemented:

- Planning of the IS Maintenance System of the RF BS organisation ('Plan');
- Implementation of the IS Maintenance System of the RF BS organisation ('Do');
- Monitoring and analysis of the IS Maintenance System of the RF BS organisation ('Check');
- Maintenance and improvement of the IS Maintenance System of the RF BS organisation ('Act').

The above groups of processes make up the IS Management System of the RF BS organisation.

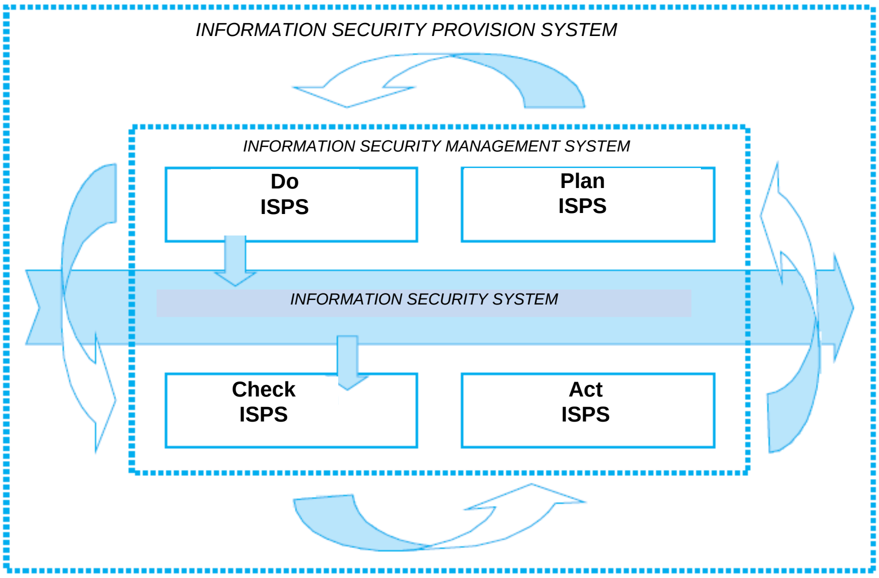
5.25. IS management is a part of the overall corporate management of a RF BS organisation that is focused on facilitating the achievement of the organisation's aims by maintaining the security of its information environment.

The process groups of the IS Management System of the RF BS organisation should be arranged in the form of the Deming Cycle Model " ... — Plan — Do — Check — Act — Plan — ... ", which is the basis of the management model in the quality standards GOST R ISO 9001 [5] and IB ISO/IEC IS 27001-2005 [6]. Organisation and performance of IS Management System processes are required to ensure that the good practical experience of the RF BS organisation is documented and becomes mandatory and that the IS Maintenance System is updated.

5.26. The building of the IS Maintenance System of a RF BS organisation is based on the requirements of the legislation of the Russian Federation, Bank of Russia regulations, the contractual requirements of the RF BS organisation, and the conditions of conduct of business based on the identification of assets of the RF BS organisation and of threat and violator modelling.

5.27. Figure 1 shows the interrelation of the ISS, the IS Management System and the IS Maintenance System of a RF BS organisation.

Fig. 1. The IS Maintenance System of a RF BS organisation


INFORMATION SECURITY PROVISION SYSTEM
INFORMATION SECURITY MANAGEMENT SYSTEM
Do
ISPS
Plan
ISPS
INFORMATION SECURITY SYSTEM
Check
ISPS
Act
ISPS

5.28. The management of a RF BS organisation should initiate, maintain and oversee performance of IS Maintenance System processes. The degree of execution of these activities by the organisation management is determined by awareness of the necessity of maintaining IS in the RF BS organisation. Awareness of the necessity of maintaining IS for a RF BS organisation is manifested in the RF BS organisation's management using the business advantages of IS maintenance, which contribute to the creation of conditions for further development of the organisation's business with allowable risks.

5.29. Awareness of the necessity of IS maintenance is an internal motivation for the management of a RF BS organisation to initiate, maintain, analyse and oversee IS Maintenance System continuously, as opposed to a situation when the decision to carry out such activities is either made as a result of emerging problems or is determined by external factors.

5.30. Awareness of the necessity of IS maintenance in a RF BS organisation is expressed in the execution by the management of activities aimed at initiating, maintaining, analysing and overseeing the IS Maintenance System of the RF BS organisation within the framework of the IS Management System.

6. Information Security Threat and Violator Models in Organisations of the Banking System of the Russian Federation

6.1. Threat and violator models should be a RF BS organisation's main tool for the deployment, maintenance and improvement of the IS Maintenance System.

6.2. The activities of the RF BS organisation are supported by the information infrastructure forming a part of it, which ensures the implementation of bank technologies and may be represented as a hierarchy of the following main levels:

- Physical (communications lines, hardware, etc.);
- Network equipment (routers, switches, multiplexers, etc.);
- Network applications and services;
- Operating systems (OS);
- Database Management Systems (DBMS);
- Bank processes and applications;
- Business processes of the organisation.

6.3. Threats and their sources (including violators), protection methods and safeguards, and approaches to assessing effectiveness vary at each of the levels.

6.4. The main goal of a violator is to gain control over information assets at the business process level. Direct attack at the business process level, e.g. by discovering confidential bank analytical information, is more effective for the violator and more hazardous for the owner than attack through other levels, which requires specific experience, knowledge and resources (including time resources) and therefore is less effective with regard to the cost-benefit ratio.

The violator may aim to disrupt the functioning of the business processes of the RF BS organisation (e.g. through distribution of malicious programs or breach of the rules of operation of computers or their networks).

6.5. The organisation shall define the specific objects related to information assets at each of the information infrastructure levels.

6.6. The main sources of IS threats include:

- Unfavourable natural, technogenic and social events;
- Terrorists and criminal elements;
- Dependence on suppliers/providers/partners/clients;
- Malfunctions, failures, destruction/damage of software and hardware;
- Employees of the RF BS organisation implementing IS threats using the rights and powers legally provided to them (internal IS violators);
- Employees of the RF BS organisation implementing IS threats outside of the rights and powers legally provided to them, as well as parties other than employees of the RF BS organisation who attempt to use UA and URA (external IS violators);
- Failure to comply with the requirements of regulatory or oversight authorities or effective legislation.

6.7. The most relevant sources of threats at the physical level, the level of network equipment and the level of network applications include:

- External IS violators: persons who develop/distribute viruses and other malicious program codes; persons arranging DoS, DDoS and other attacks; persons attempting to use UA and URA;
- Internal IS violators: personnel having access to hardware (including network equipment), administrators of servers, network applications, etc.;
- Combined sources of threats: external and internal IS violators acting jointly and/or in coordination;
- Malfunctions, failures or destruction/damage of software and hardware.

6.8. The most relevant sources of threats at levels of operating systems, database management systems and bank processes include:

- Internal IS violators: OS administrators, DBMS administrators, users of bank applications and technologies, IS administrators, etc.;
- Combined sources of threats: External and internal IS violators acting in collusion[1].

6.9. The most relevant sources of threats at the business process level include:

- Internal IS violators: authorised users and ABS operators, representatives of the organisation's management, etc.;
- Combined sources of threats: external IS violators (e.g. competitors) and internal violators acting in collusion;
- Failure to comply with the requirements of regulatory or oversight authorities or effective legislation.

6.10. Sources of threats are used to implement an IS vulnerability threat.

6.11. It is good practice in RF BS organisations to develop IS threat and violator models for the organisation as a whole and, if necessary, for its individual bank processes.

The level of detail in the parameters of IS threat and violator models may vary and is determined by the actual needs for each separate organisation.

6.12. A RF BS organisation should establish appropriate procedures for regular analysis of the need to revise the IS threat and violator model.

7. The Information Security System of Organisations in the Banking System of the Russian Federation

7.1. General Provisions

7.1.1. The fulfilment of the requirements for the ISS of a RF BS organisation is the basis for maintaining an appropriate IS level. The requirements for the ISS of a RF BS organisation shall be based on:

- The provisions of this section of the standard;
- Performance of activities within the framework of the IS Management System of the RF BS organisation as specified in Section 8 of this standard (in particular, activities related to the development of IS breach risk handling plans).

The requirements for the ISS of a RF BS organisation shall be documented in accordance with the Standardisation Recommendations of the Bank of Russia RS BR IBBS-2.0 ‘Maintenance of Information Security of the Russian Banking System Organisations. Recommended Practices for Documentation Related to Information Security Maintenance in Accordance with STO BR IBBS-1.0’.

7.1.2. The provisions set out in subsections 7.2 to 7.11 of this standard form a basic set of ISS requirements that is applicable to most RF BS organisations. In accordance with the peculiarities of a specific RF BS

[1] Implementation of threats at these levels and the business process level by external IS violators acting independently, with no participation of internal violators, is almost impossible.

organisation, this basic set of requirements may be expanded through activities within the framework of processes of the IS Management System of the RF BS organisation (e.g. determining the scope of the IS Maintenance System of the RF BS organisation, analysis and assessment of the risks of IS breach).

7.1.3. ISS requirements shall be composed for the following areas:

– Assignment and distribution of roles and maintenance of trust in personnel;
– IS maintenance in the phases of the ABS LC;
– Protection against UA and URA, access control and registration of all actions in the ABS, telecommunications equipment, automatic telephone systems, etc.;
– Virus protection;
– Use of Internet resources;
– Use of data encryption tools;
– Protection of bank payment and information processes, including banking processes, within the framework of which personal data is processed.

ISS requirements within a specific RF BS organisation may also be made for other areas and fields of activities.

7.1.4. When rights to access the information assets of the RF BS organisation are distributed to employees and clients, the following principles should be followed:

– Know Your Customer[1];
– Know Your Employee[2];
– Need to Know[3];

the use of the Dual Control principle[4] is advisable as well.

7.1.5. Role formation shall be based on the existing business processes of the RF BS organisation and shall be carried out in order to exclude any concentration of powers and to reduce the risk of IS incidents associated with the loss of the properties of availability, integrity or confidentiality of information assets.

Roles shall not be formed by recording the actual rights and powers of RF BS organisation personnel.

7.1.6. Roles associated with IS maintenance shall be specified for the purpose of IS maintenance and oversight of IS maintenance quality within the RF BS organisation. The management of the RF BS organisation shall coordinate the timeliness and quality of the execution of roles associated with IS maintenance.

7.1.7. ABS IS shall be maintained in all phases of the ABS LC which automate bank processes, taking into account the interests of all parties involved in LC processes (developers, clients, product and service suppliers, operating and supervising units of the RF BS organisation).

7.1.8. If the management of a RF BS organisation decides to use the Internet, and when documents regulating the procedure for Internet use and other documents associated with IS maintenance during Internet use are composed, the following points should be considered:

– The Internet lacks a single management body (except for a name and address space management service), and it is not a legal organisation with which a contract (or agreement) could be entered into. Internet providers (intermediaries) may provide only services implemented directly by them;
– There exists a likelihood of unauthorised access to or loss or distortion of information transmitted via Internet;
– Equipment, software and information resources connected/available from the Internet may be attacked by violators;
– IS maintenance is not guaranteed by any body/institution/organisation when the Internet is used.

7.1.9. Within the framework of bank payment processes, the following should be considered as first-priority assets for protection:

– The bank payment process;
– Payment information;
– Information considered sensitive information in accordance with Clause 2.1 of Bank of Russia Regulation *On Information Security Requirements When Transferring Funds and the Bank of Russia's Procedure for Oversight of Compliance with Information Security Requirements When Transferring Funds* No. 382-P dated 09/06/2012, as amended by Bank of Russia Ordinance No. 3007-U dated 05/06/2013 [7].

[1] Know Your Customer: A principle used by regulatory authorities to express an attitude toward financial institutions in terms of knowledge of customer activities.

[2] Know Your Employee: A principle demonstrating an organization's concern about employees' attitude toward their job duties and potential problems, such as improper use of property, fraud or financial difficulties that could lead to security problems.

[3] Need to Know: A principle limiting access to information and resources for information processing to the minimum level required for the performance of specific duties.

[4] Dual Control: Principle of maintaining process integrity and fighting against distortion of system functions, which requires duplication (algorithmic, time, resource or other) of actions prior to completion of certain transactions.

7.2. General Requirements for Information Security when Assigning and Distributing Roles and Ensuring Trust toward Personnel

7.2.1. Roles shall be specified for personnel of a RF BS organisation.

The creation of roles associated with IS maintenance should be based, among other things, on the requirements set out in Section 7 and Section 8 of this standard.

The creation and assignment of roles for employees of a RF BS organisation should be based on the principle of providing the minimum rights and powers required for fulfilment of job duties.

7.2.2. Roles should be personalised and responsibility for their fulfilment should be specified. Responsibility should be recorded (e.g. in job descriptions or organisational and management documents of the RF BS organisation.

7.2.3. In order to prevent the occurrence of IS breach risk and to reduce such risks, the following functions shall not be combined within a single role: development and maintenance of the ABS/software, their development and operation, maintenance and operation, system administrator and IS administrator, performance of operations in the ABS and oversight of their performance.

7.2.4. A RF BS organisation shall specify, execute and record activity oversight procedures for employees with a package of powers determined by their roles which allows them to gain control over a protected information asset of the RF BS organisation.

7.2.5. A RF BS organisation shall specify, execute and record hiring procedures for jobs which affect IS maintenance, including:

- Checking the authenticity of provided documents and stated qualifications and the accuracy and completeness of biographical information;
- Checking professional skills and assessing occupational fitness. The above procedures must provide for the recording of the results of the checks conducted.

7.2.6. It is recommended that procedures for regular checks of professional skills and assessment of occupational fitness of employees be defined, executed and registered with recording of results, as well as unscheduled checks in the case of detection of inappropriate behaviour, involvement in IS incidents or suspicion of such behaviour or involvement.

7.2.7. All employees of the RF BS organisation shall undertake in writing to maintain confidentiality and to be committed to the rules of corporate ethics, including requirements for preventing any conflict of interests.

In the case of interaction with external organisations and clients, IS maintenance requirements shall be governed by provisions included in contracts or agreements with such external organisations and clients.

7.2.8. Personnel obligations concerning the fulfilment of IS maintenance requirements shall be included in employment contracts (agreements) and/or job descriptions.

Failure by RF BS organisation employees to meet IS maintenance requirements shall be made equivalent to non-performance of job duties and shall result in disciplinary liability at the least.

7.3. General Requirements for the Information Security of Computerized Bank Systems in Life Cycle Phases

7.3.1. With regard to IS maintenance issues, the following general phases of the ABS LC model should be considered:

1. Development of Terms of Reference.
2. Engineering.
3. Creation and Testing.
4. Acceptance and Commissioning.
5. Operation.
6. Maintenance and Upgrading.
7. Decommissioning.

In case of independent ABS development within the RF BS organisation, all phases of the ABS LC should be considered, and if prefabricated ABSs are acquired, phases 4 to 7 of the ABS LC should be considered.

7.3.2. Work performed in all phases of the ABS life cycle related to IS maintenance issues shall be coordinated and monitored by the IS service.

7.3.3. Organisations contracted for IS maintenance in the ABS LC phases shall be licensed to provide technical protection of confidential information in accordance with the legislation of the Russian Federation.

7.3.4. Terms of Reference for ABS development or upgrading should include information security requirements established and used by the RF BS organisation to provide IS within the framework of the process flows of the RF BS organisation which are implemented by means of the ABS being created or upgraded.

7.3.5. In the phases of creating and testing ABSs and/or their components, a RF BS organisation is to ensure the prohibition of using protected information as test data, data anonymity and monitoring of the appropriateness of access provision and delimitation.

7.3.6. ABSs and/or their components in operation shall be provided with documentation containing a description of the safeguards implemented in the ABS, including a description of the scope and requirements for implementation of organisational safeguards and the scope and requirements for technical safeguard operation.

The RF BS organisation should analyse the adoption of safeguards designed to ensure safe ABS development and delivery by the ABS developer.

7.3.7. A contract (agreement) related to ABS development or delivery of prefabricated ABSs and their components to RF BS organisations shall include provisions on maintenance of products supplied throughout their service life. Should it be impossible to include the said provisions in the contract (agreement), a full package of documents making it possible to maintain the ABSs and their components without the involvement of the developer shall be acquired. If both of the specified options are unacceptable (e.g. due to high cost or the position of the supplier (developer), the management of the RF BS organisation shall assess and record the tolerability of the IS breach risk which would arise if it were impossible to maintain the ABSs and their components.

7.3.8. When terms of reference are developed for remote banking service systems, it should be taken into account that data protection must be maintained in the following circumstances:

- Attempts to use unauthorised access to information by anonymous or unauthorised violators through the public network;
- Possible errors of authorised system users;
- Possible unintentional or inappropriate use of protected information by authorised users.

7.3.9. The following procedures shall be specified, executed and recorded in the ABS operation phase:

- Monitoring of the operability (functioning, effectiveness) of safeguards implemented in the ABS, including monitoring of the implementation of organisational safeguards and monitoring of the scope and settings parameters for technical safeguards applied;
- Monitoring of the absence of vulnerabilities in ABS equipment and software;
- Monitoring of changes in ABS settings parameters and technical safeguards applied;
- Monitoring of required ABS software updates, including of technical safeguard software.

7.3.10. During the ABS operation phase, the procedures required to ensure recovery of all IS maintenance functions implemented shall be specified, executed, recorded and monitored.

7.3.11. During the ABS operation phase, the procedures for monitoring the configuration of ABS software installed and/or used shall be specified, executed and recorded.

7.3.12. A RF BS organisation shall specify and assign roles associated with the operation and monitoring of ABS operation and the technical safeguards used, including changes in their settings parameters.

Operation monitoring procedures shall be defined and executed for all ABSs by the IS service. ABS operation monitoring measures and their results shall be recorded.

7.3.13. During the ABS operation phase, the procedures required to ensure the integrity of media for protected information shall be defined, executed and monitored.

7.3.14. During the maintenance (upgrading) phase, monitoring procedures shall be defined, executed and recorded which provide protection against:

- Intentional unauthorised disclosure, modification or destruction of information;
- Unintentional modification, disclosure or destruction of information;
- Refusal or deterioration of service.

7.3.15. During the maintenance (upgrading) phase, the following procedures shall be defined, executed and recorded for ABSs considered by the RF BS organisation to be critical ones, including ABSs involved in the implementation of the bank payment process and in ISPDs:

- Recording of changes made;
- Checking of the functionality of ABSs, including information protection measures applied after changes have been made.

7.3.16. During the decommissioning phase, procedures shall be defined, executed and recorded to ensure deletion of information from the fixed memory of ABSs and external media using algorithms and/or methods which make it impossible to recover deleted information whose unauthorised use could cause damage to the business activity of the organisation, and information used by technical safeguards, except for archives of electronic documents and electronic interface protocols which are to be maintained and kept for a certain period in accordance with the legislation of the Russian Federation, Bank of Russia regulations and/or contractual documents.

7.4. General Requirements for Information Security in Access and Log-In Control

7.4.1. Procedures for identification, registration and classification (categorising as one of the types) of information assets of a RF BS organisation shall be defined, executed, recorded and monitored. Access rights of RF BS organisation employees and clients to information assets and/or their types shall be registered and recorded.

7.4.2. The ABS configuration shall include integrated safeguards against UA and URA, and information security tools certified in accordance with information security requirements may also be used.

Safeguards against UA shall ensure that authentication data entered by access subjects is hidden on information display devices. The placement of ABS information display devices shall prevent unauthorised viewing of information.

7.4.3. A RF BS organisation shall define, execute, record and monitor the following rules and procedures:

– Identification, authentication and authorisation of access subjects, including external access subjects that are not employees of the RF BS organisation and software processes (or services);
– Delimitation of access to information assets based on the role method and determination of rights of access to information assets for each role;
– Management of granting/withdrawal and locking of access, including access through external information and telecommunication networks;
– Recording of access subject actions and monitoring of registration data integrity and protection;
– Management of identification data, authentication data and means of authentication;
– Management of access subject accounts;
– Detection and blocking of unsuccessful access attempts;
– Access session locking upon expiration of the predetermined idle time or as requested by an access subject that requires repeated authentication and authorisation to continue working;
– Restriction of user actions related to changing the settings of users' workstations (use of restrictions on BIOS change);
– Management of the scope of permitted actions prior to identification and authentication;
– Restriction of user actions related to changing ABS settings parameters and monitoring of actions performed by operating personnel to change ABS settings parameters;
– Detection and blocking of unauthorised movement (copying) of information, including databases, file resources and virtual machines;
– Use of wireless information access technologies, if any are used, and protection of internal wireless connections;
– Use of mobile devices to gain access to information, if any are used. Access control procedures shall exclude 'self-authorisation'.

7.4.4. A RF BS organisation shall define, execute, record and monitor the rules and procedures of IS monitoring, analysis and storage of data on actions and operations that make it possible to detect illegal or suspicious operations and transactions; for which it is necessary, among other things, to:

– Define the actions and operations to be registered;
– Determine the scope and content of data on actions and operations to be registered and its storage period;
– Provide backing up of the necessary memory capacity for data recording;
– Respond to failures during the recording of actions and operations, including hardware and software errors and failures, in technical information collection systems;
– Generate time marks for recorded actions and operations and synchronise system time on technical systems used for IS monitoring, data analysis and storage.

A RF BS organisation shall maintain logs of actions and operations for workstations, server and network equipment, firewalls and ABSs to be used in response to IS incidents.

Data on actions and operations shall be stored for three years at least and data resulting from performance of the bank payment process shall be stored for five years at least, unless otherwise established by the legislation of the Russian Federation or Bank of Russia regulations.

In order to carry out IS monitoring and analysis of data on actions and operations, dedicated software and/or hardware should be used.

IS monitoring and analysis of data on actions and operations shall use fixed criteria for detection of illegal or suspect actions and operations. The IS monitoring and analysis procedures specified shall be applied regularly (e.g. every day) to all actions and operations (transactions) completed.

7.4.5. A RF BS organisation should define and monitor the fulfilment of requirements for:

– Segmentation of computer networks, including those created using virtualization technology;
– Firewall provision;
– Information interaction between segments of computer networks. Computer networks should be segmented to ensure independent execution of bank payment processes of the RF BS organisation and bank information processes of the RF BS organisation with various degrees of criticality, including bank information processes within the framework of which personal data in an ISPD is processed.

RF BS documents shall regulate and monitor the procedure for making changes to network equipment configuration, which provides for the coordination of changes introduced with the IS service. It is recommended that IS service employees provide access to network equipment configuration without the possibility of making changes.

7.4.6. The procedure for access to objects related to information asset, including access to premises where objects related to information asset are located, shall be defined, executed, recorded and monitored.

7.4.7. ABSs used within a RF BS organisation, including remote banking service systems, shall provide, among other things, for the possibility of recording:

– Operations with client account data, including opening, modification and closing of client accounts;
– Performed transactions with financial implications;
– Operations associated with the assignment and distribution of user rights.

7.4.8. A RF BS organisation shall define, execute and monitor the procedure for using removable data media.

7.4.9. Remote banking service systems shall provide for the implementation of safeguards ensuring non-repudiation of operations or transactions carried out by clients.

Protocols of operations performed by means of remote banking service systems should be attributed with legal relevance (e.g. by introducing relevant provisions in remote banking service contracts).

7.4.10. When contracts are concluded with external organisations, the necessary level of interaction should be provided for in case an IS incident spreads beyond a particular RF BS organisation. An example of such interaction may be suspension of a transaction distributed between more than one organisation if available IS monitoring data and operations protocol analysis indicate that performance of that transaction forms part of violator plans.

7.4.11. Procedures specifying actions to be taken in the case that information required for identification, authentication and/or authorisation of employees or clients, including compromise for which they are at fault, and information about techniques to identify such cases should be defined and communicated to employees and clients of the RF BS organisation.

These procedures shall provide for the recording of all actions of both employees and clients and their results.

7.4.12. Remote banking service systems shall contain mechanisms for notification (regular, continuous or as required) of clients of any operations performed under their name.

7.4.13. A RF BS organisation shall apply measures intended to ensure protection against UA and damage or disturbance of the integrity of data on actions and operations, as well as measures used to protect information required for identification, authentication and/or authorisation of clients and employees of the RF BS organisation. Any attempts to gain UA to such information shall be recorded. Access to data on actions and operations is provided only for the fulfilment of job duties.

In the case of dismissal or changes in the job duties of RF BS organisation employees having access to the above-mentioned data, specified procedures for access right revision should be carried out.

7.4.14. In the case of access within the area of telecommunication channels and communication links, including wireless ones which are not monitored by the RF BS organisation, network protocols providing protection of the network connection, monitoring of network interface integrity and bidirectional authentication technology implementation shall be used.

7.4.15. Protected data shall be transmitted via communication links going out of the zone under control of the RF BS organisation only provided that it is protected against disclosure and modification.

7.4.16. All employees and clients of a RF BS organisation shall have unique and personified accounts in ABSs.

7.5. General Requirements for Information Security Maintenance by Means of Virus Protection

7.5.1. Any workstations and ABS servers of a RF BS organisation shall have means of virus protection unless otherwise provided for in process flow implementation.

The RF BS organisation shall define, execute, record and monitor procedures for installation and regular updating of virus protection (versions and databases) at workstations and ABS servers.

7.5.2. It is recommended that continuous virus protection in the automatic mode and automatic installation of updates of virus protection software and its databases be put in place.

7.5.3. Prior to connecting removable data media to computer equipment involved in bank processes, it is advisable to carry out a virus check on them using a dedicated self-contained computer.

7.5.4. Instructions and recommendations for virus protection taking bank process features into consideration shall be developed and enforced.

7.5.5. A RF BS organisation shall arrange for virus filtration of all e-mail traffic.

7.5.6. A RF BS organisation shall arrange for a layered and centralized virus protection system providing for the use of virus protection tools from various manufacturers on:

– Workstations;
– Server equipment, including e-mail servers;
– Firewalls.

7.5.7. Procedures for preliminary virus checking of installed or modified software shall be defined, executed, recorded and monitored. Virus checking shall be carried out after software installation or modification.

7.5.8. Procedures performed in the case of computer virus detection shall be defined, executed, recorded and monitored; in particular, these should contain:

– Measures necessary for responding to and eliminating the consequences of the virus attack;
– Procedure for official notification of management;

- Procedure for work suspension, if necessary (until the virus attack consequences have been eliminated).

7.5.9. Procedures for control of the disconnection and updating of antivirus tools on all ABS equipment shall be defined, executed and recorded.

7.5.10. The head of the functional division of a RF BS organisation shall be responsible for meeting virus protection requirements, and responsibility for the performance of prescribed virus protection measures shall be placed on each employee of the organisation who has access to the computer and/or ABS.

7.6. General Requirements for Information Security when Using Internet Resources

7.6.1. The decision to use the Internet for production and/or business activities shall be taken by the management of a RF BS organisation. The aims of Internet use shall be listed expressly and recorded; for example, the Internet may be used for the following purposes in a RF BS organisation:

- Maintaining remote banking services;
- Obtaining and distributing information associated with bank activities (e.g. by creating information websites for the RF BS organisation);
- Performing information analysis in the interests of the organisation;
- Exchanging electronic messages between RF BS organisations and other subjects of the national payment system;
- Exchanging electronic messages (e.g. e-mail).

The Internet shall not be used for purposes not specified.

In order to restrict Internet use for non-specified purposes, the RF BS organisation should allocate a limited number of packages containing the services and Internet resources available to users. The granting of user rights for a specific package to RF BS organisation employees shall be recorded and executed in accordance with the person's job duties (in particular, in accordance with roles assigned to him/her).

7.6.2. Procedures for connection and use of Internet resources shall be defined, executed, recorded and monitored.

7.6.3. Protected data shall be transmitted via Internet only if such data is protected against disclosure and modification.

7.6.4. Due to increased risks associated with IS breach during interaction with the Internet, RF BS organisations shall use safeguards, including firewalls, antivirus tools, intrusion detectors and data encryption tools, which provide, among other things, information acceptance and transmission only in a set format and only for a certain technology.

Instructions and recommendations for Internet use which take bank process features into account shall be developed and enforced.

Procedures for recording Internet resource visits by RF BS organisation employees shall be defined and executed. Data on Internet resources visited by RF BS organisation employees shall be available to the IS service staff.

7.6.5. It is recommended that computers through which direct interaction with the Internet is carried out be physically isolated from internal networks.

7.6.6. During performance of remote banking services, appropriate safeguards shall be applied to prevent authorised client substitution by a violator within a working session. Any attempt at such substitution shall be recorded as established by the RF BS organisation.

7.6.7. Any operations performed by clients during a working session with remote banking service systems, including operations related to funds transfer, shall be carried out only upon identification, authentication and authorisation. If the connection is disrupted or broken, the current session should be closed, and procedures for identification, authentication and authorisation should be repeated.

Customized client software should be used to provide user access to remote banking service systems.

7.6.8. The scope and procedure for application of safeguards used to arrange for mail exchange via Internet shall be specified.

It is recommended that mail exchange via Internet be arranged for through a limited number of points, consisting of the external mail server (connected to the Internet) and the internal mail server (connected to internal networks of the organisation) with a safe system of mail message replication between them (Internet kiosks).

7.6.9. E-mails shall be archived. The aims of the creation of E-mail archives are:

- To monitor information flows, including for the purpose of preventing information leakage;
- To use the archives in proceedings related to information leakage.

Rules and procedures for access to and changing of archived information which provide IS service staff with access to the archived information shall be specified, executed, recorded and monitored.

7.6.10. It is advisable to abstain from the practice of storing and processing bank information (including public information) on computers connected immediately to the Internet. The availability of bank information on such computers shall be determined by the business goals of the RF BS organisation and authorised by the organisation management.

7.6.11. The scope and procedure of application for safeguards used when interacting with the Internet and making it possible to counteract violator attacks and spam[1] distribution shall be defined.

7.7. General Requirements for Information Security when Using Data Encryption Tools

7.7.1. Data encryption tools or (hereafter, DETs) are designed to protect information during its processing, storage and transmission by communication links.

The necessity of using DETs is determined by a RF BS organisation independently unless otherwise provided for by the legislation of the Russian Federation.

7.7.2. DETs shall be used in a RF BS organisation in accordance with the IS threat model and IS violator model adopted by the RF BS organisation. It is advisable to approve a special IS policy concerning the use of DETs within the RF BS organisation.

7.7.3. DETs used to protect personal data shall be Class KC2 at least.

7.7.4. Information security provided using DETs shall be consistent with the legislation of the Russian Federation and normative documents regulating DET operation issues, technical documentation for DETs and licensing requirements of the Federal Security Service of Russia.

7.7.5. To maintain security DETs should be used which:

- Allow for incorporation into processes for electronic message processing, ensure interaction with application software at the level of processing of requests for cryptographic transformation and result delivery;
- Have a full package of operational documents provided by the DET developer, including a description of the key system, rules for its operation and substantiation of the necessary organisation and staff support;
- Are certified by a governmental authority or permitted by the Federal Security Service of Russia.

7.7.6. Installation and commissioning, as well as DET operation, shall be carried out in accordance with operational and technical documentation related to these tools.

7.7.7. When DETs are used, the continuity of the processes of logging of DET operation in accordance with the technical documentation for DETs and maintenance of the integrity of software for the DET operation environment, which is a set of hardware and software with which DETs are normally operated and which may affect the fulfilment of requirements specified for DETs, shall be maintained.

7.7.8. IS of DET cryptographic key making shall be provided by a package of process, organisational, technical and software safeguards and means of protection mentioned in the technical documentation for DETs.

7.7.9. In order to improve the level of security when operating DETs and their key systems, IS monitoring procedures should be implemented to record all significant events occurring during exchange of cryptographically protected data and all IS incidents.

7.7.10 The DET implementation procedure is determined by the management of the RF BS organisation based on the documents mentioned above in this section, and it shall comprise:

- Commissioning procedure, including the procedure for incorporating the DET into the ABS;
- Operation procedure;
- Procedure for restoring operationality in emergencies;
- Changing procedure;
- Decommissioning procedure;
- Key system management procedure;
- Procedure for handling media with key information, including actions associated with change and compromise of keys.

7.7.11. Cryptographic keys may be made by RF BS organisations and/or by the client of the RF BS organisation independently. Relations between RF BS organisations and their clients are governed by concluded contracts.

7.8. General Requirements for Information Security of Bank Payment Processes

7.8.1. The ISS of the bank payment process shall comply with requirements set out in Clauses 7.2 to 7.7 and 7.8 of this standard.

7.8.2. The bank payment process shall be regulated (described) within the RF BS organisation.

7.8.3. The procedure for payment information exchange shall be recorded in contracts between participants exchanging payment information.

7.8.4. Employees of the RF BS organisation, including administrators of automated systems and information protection tools shall not be authorised for the unsupervised creation, authorisation, destruction and modification of payment information or for unauthorised operations for changing the status of bank accounts.

[1] Spam is a general name for electronic messages and advertising letters that are not solicited by users and are sent by Internet to user addresses which have become known to the distributing party.

7.8.5. The results of technological operations for payment information processing shall be monitored (checked) and certified by persons/automated processes.

It is recommended that payment information and result monitoring (checking) be processed by different employees/automated processes.

7.8.6. The set of safeguards for the bank payment process shall provide for the following:

- Protection of payment information against distortion, falsification, redirection, unauthorised destruction and false authorisation of electronic payment messages;
- Access by RF BS organisation employees only to those resources of the bank payment process necessary to such employees for the fulfilment of job duties or the exercise of rights provided for by the payment information processing technology;
- Oversight (or monitoring) of the performance of preparation, processing, transmission and storage of payment information;
- Authentication of incoming electronic payment messages;
- Bidirectional authentication of automated workstations and servers and parties exchanging electronic payment messages;
- The possibility to enter payment information into the ABS only for authorised users;
- Monitoring aimed at excluding any malicious actions (in particular double entry), reconciliation and setting restrictions depending on the amount of operations performed;
- Recovery of payment information in case of its intentional or accidental destruction or distortion or the breakdown of computer equipment;
- Reconciliation of outgoing electronic payment messages with relevant incoming and processed electronic payment messages in interbank settlements;
- Possibility to block acceptance of client instructions for execution;
- Delivery of electronic payment messages to exchange parties.

Moreover, the RF BS organisation should arrange for authorised entry of payment information in ABS by two employees to be followed by software reconciliation of entry results to verify agreement (Dual Control principle).

7.8.7 For remote banking service systems, safeguarding mechanisms to be applied shall provide:

- Reduction of the probability of performance of unintentional or accidental operations or transactions by authorised clients;
- Notification of clients of potential risks associated with the performance of operations or transactions.

Clients of remote banking service systems shall be provided with detailed instructions describing procedures for carrying out operations or transactions.

7.8.8. Procedures for servicing computer equipment used in the bank payment process, including replacement of their software and/or hardware parts, shall be defined, executed, recorded and monitored.

7.8.9. Procedures for the regular monitoring of all payment information security maintenance functions (requirements) implemented through safeguards shall be specified, executed and recorded.

7.8.10. Procedures for monitoring the absence of specialized tools for unauthorised information retrieval on devices involved in the bank payment process which are located in public places beyond the area under constant monitoring of the RF BS organisation, including cash machines and payment terminals, shall be defined, executed and recorded.

7.8.11. Procedures for recovery of all payment information security maintenance functions implemented by means of software and hardware shall be defined, executed, recorded and monitored.

7.9. General Requirements for Information Security of Bank Information Processes

7.9.1. The ISS of the bank information process shall comply with the requirements set out in Clauses 7.2. to 7.7 and 7.9 of this standard.

7.9.2. Information in a RF BS organisation which is not related to payments shall be categorized, and a list of its types shall be defined.

Information not related to payments should be classified in accordance with the severity of consequences from loss of IS properties (in particular, the properties of availability, integrity and confidentiality).

7.9.3. A set of security requirements shall be documented for each of the types of information not related to payment resulting from classification.

7.9.4. Bank information processes shall be regulated (described) within the RF BS organisation. The above-mentioned processes shall be implemented within the framework of ABSs created for these purposes. Servers, computers and other equipment that do not form part of such ABSs should be isolated from the ABSs at the level of local computer networks in a manner coordinated with the IS service.

7.9.5. Requirements for information security during interaction of RF BS organisation ABSs with information systems of external organisations (external information systems) shall be defined, executed and monitored.

7.10. General Requirements for Personal Data Processing in an Organisation of the Banking System of the Russian Federation

7.10.1 The management of a RF BS organisation shall specify the aims of personal data (hereafter, PD) processing.

7.10.2 The RF BS organisation shall determine the necessity of notifying the authority for protection of the rights of PD subjects of PD processing and arrange for the sending of such notification in good time in accordance with the Federal Law *On Personal Data* [8] as required.

7.10.3 The RF BS organisation shall establish criteria for categorising a ABS as an ISPD.

7.10.4 A RF BS organisation shall define, execute, record and monitor procedures for PD resource[1] accounting, including ISPD accounting.

7.10.4.1 The following shall be done for each PD resource:

- Establishing the purpose of PD processing;
- Setting and observation of PD storage time and the conditions for discontinuing their processing;
- Determining the list and categories of PD processed (special PD categories, biometric PD, PD obtained from public sources or other PD);
- Performing accounting of the number of PD subjects, including PD subjects who are not employees of the RF BS organisation;
- Satisfying the PD processing restriction by achieving the purpose of PD processing;
- Compliance of the scope and volume of PD processed with established processing purposes;
- Accuracy, sufficiency and relevance of PD, including with regard to PD processing purposes;
- Executing established procedures to obtain the consent of PD subjects (or their legal representatives) to process their PD if such consent is required under the Federal Law *On Personal Data*;
- Executing established procedures to obtain the consent of PD subjects to assign processing of their PD to third parties if such consent is required under the Federal Law *On Personal Data*;
- Discontinuing PD processing and destruction or depersonalization of PD when processing purposes have been achieved or when requested by the PD subject in cases provided by the Federal Law *On Personal Data*, including withdrawal of consent to PD processing by the PD subject.

7.10.4.2 The RF BS organisation shall define, execute, record and monitor procedures for discontinuing PD processing and destruction or depersonalization of PD within the time established by the Federal Law *On Personal Data* in the following cases:

- Upon achievement of the purpose of PD processing (unless otherwise provided for by a contract to which the PD subject is a party, beneficiary or guarantor or by any other agreement between the RF BS organisation and the PD subject);
- Withdrawal of consent for PD processing by the PD subject and if PD storage is no longer needed for PD processing purposes (unless otherwise provided for by a contract to which the PD subject is a party, beneficiary or guarantor or by any other agreement between the RF BS organisation and the PD subject);
- If the PD has been obtained illegally or is not required for the processing purpose specified;
- Detection of illegal PD processing by a RF BS organisation or processor acting on the instructions of such an organisation, if it is impossible to ensure the legality of PD processing;
- Detection of illegal PD processing without PD subject consent.

7.10.4.3. Where it is impossible to destroy or depersonalize PD within the time established by the Federal Law *On Personal Data*, the RF BS organisation is to block and subsequently destroy the PD. PD shall be destroyed within six months of blocking.

7.10.5. The RF BS organisation shall define, execute and monitor the PD processing policy and, if necessary, shall specify PD processing procedures for individual PD resources. For PD resources processed in ABSs of a RF BS organisation, including ISPDs, the PD processing procedure may form part of the operational documentation for the ABS, and is developed during ABS creation or upgrading.

7.10.5.1 The above documents:

- Define the procedures for providing access to PD;
- Define the procedures for changing PD to ensure PD accuracy, reliability and relevance, including with regard to PD processing purposes;
- Define the procedures for PD destruction, depersonalization or blocking where such procedures need to be carried out;
- Define the procedures for processing applications of PD subjects or their legal representatives in cases provided for by the Federal Law *On Personal Data*, in particular, the procedure for of preparing information about the availability of PD related to a certain PD subject, information required to make it possible for PD subjects (or their legal representatives) to familiarize themselves with their PD, and procedures of processing applications on PD clarification, blocking or destruction if PD is incomplete, outdated, inaccurate, obtained illegally or is not required to fulfil the established purpose of processing;

[1] A PD resource is a package of PD being processed in the RF BS organisation with or without the use of automation tools and ABSs, including ISPDs united by common processing purposes.

- Define procedures for processing a request made by an authority for the protection of the rights of PD subjects;
- Define procedures for obtaining PD subject consent for PD processing and PD processing assignment to third parties;
- Define procedures for transmission of PD between users of a PD resource which provides for PD communication only between employees of the RF BS organisation who have access to PD;
- Define procedures for transmission of PD to third parties;
- Define procedures for handling of tangible PD media;
- Define procedures required for notifying an authority for the protection of the rights of PD subjects of PD processing within the time established by the Federal Law *On Personal Data*;
- Define whether it is necessary to apply standard forms of documents for PD processing and PD handling procedures. The standard form of a document means a template, blank form of a document or any other standardized form of a document used by a RF BS organisation to gather PD.

7.10.5.2. A RF BS organisation shall publish or otherwise provide unrestricted access to the document defining its PD processing policy and to information concerning personal data security requirements implemented.

7.10.6. A RF BS organisation shall determine in which cases PD subject consent is required; both the form and procedure of obtaining PD subject consent shall be regulated.

7.10.7. A RF BS organisation shall define, execute, record and monitor procedures for registration of persons having access to PD.

The document listing persons having access to PD is to be approved by the head of the RF BS organisation.

Employees of the RF BS organisation shall engage in PD processing only for the purpose of fulfilling their job duties.

A RF BS organisation shall define, execute, record and monitor procedures for familiarizing employees of the RF BS organisation involved immediately in PD processing with provisions of the legislation of the Russian Federation and internal documents of the RF BS organisation that contain requirements for PD processing and security to the extent that they relate to their job duties. The RF BS organisation may familiarize employees as stated above during training or awareness improvement.

7.10.8. A RF BS organisation shall define, execute, record and monitor procedures for registration of PD processing premises and access by employees of the RF BS organisation or others to the PD processing premises.

7.10.9. The following shall be provided for when tangible PD media are handled:

- Separation of PD from any other information (in particular, by recording such PD on individual removable PD media or in dedicated sections or fields of document forms (when processing PD on paper);
- Registration of removable PD media;
- Establishment, execution and monitoring of execution of the procedure related to the storage of and access to removable PD media, including machine-readable media;
- Storage of PD whose processing is known to have incompatible purposes on separate removable media;
- Recording and accounting of locations where tangible PD media are kept, and recording of the category of personal data processed (special PD categories, biometric PD, PD obtained from public sources or other PD), including separate storage of PD resources processed for various purposes;
- Appointing employees responsible for providing storage of tangible PD media;
- Establishing and executing the procedure for destruction (erasure) of information on machine-readable PD media.

PD shall be stored in a form which makes it possible to identify the PD subject for as long as required by PD processing purposes, unless a PD storage period is established by federal law or a contract to which the PD subject is a party, beneficiary or guarantor.

7.10.10. Public PD sources are to be created and published by a RF BS organisation only to fulfil requirements set out in the legislation of the Russian Federation. The RF BS organisation shall define, execute, record and monitor procedures for publication of PD in public PD sources.

7.10.11. Assignment of PD processing to any third party (hereafter, processor) shall be made on a contractual basis. The above-mentioned contract shall contain a list of actions or operations with PD to be performed by the processor and the purposes of processing, and shall specify that the processor must provide PD security (including PD confidentiality) when processing the PD and disclose and distribute PD only with the consent of the PD subject, unless otherwise provided for by federal law, and PD security requirements shall be specified. In the event that personal data processing is assigned to a processor, the RF BS organisation shall obtain the consent of the PD subject unless otherwise provided for by the legislation of the Russian Federation.

7.10.12. A RF BS organisation shall define, execute, record and monitor procedures to be performed when cross-border transmission of PD is required.

7.10.13. A RF BS organisation shall appoint a person responsible for PD processing management. The powers of the person responsible for PD processing management, as well as the rights and obligations of that person, shall be specified by the management of the RF BS organisation.

7.11. General Requirements for Information Security of Bank Processes within the Framework of which Personal Data is Processed

7.11.1. The ISS of a bank payment process within the framework of which personal data is processed shall meet the requirements set out in Clause 7.8 of this standard.

The ISS of a bank information process within the framework of which personal data is processed shall meet requirements set out in Clauses 7.9 and 7.11 of this standard.

7.11.2. IS provision requirements specified in Section 7 and Section 8 of this standard should be implemented to ensure that personal data security requirements are met for PD security levels 3 and 4 when they are processed in ISPDs established by Russian Government Resolution *On Approval of Security Requirements for Personal Data Processed in Personal Data Systems* No. 1119 dated 1 November 2012 [9].

7.11.3. Information security requirements established in Section 7 and Section 8 of this standard are intended to neutralize relevant[1] (as applied to most RF BS organisations) threats related to personal data security.

7.11.4. Considering the specific features of personal data processing and security in RF BS organisations, threats of personal data leakage through technical channels and threats associated with the presence of undocumented (undeclared) capabilities in the system and application software used in ISPDs should be recognized as irrelevant to RF BS organisations.

7.11.5. The result of assessment of personal data security breach risks is a Personal Data Threat Model containing personal data security threats relevant to the RF BS organisation, based on which requirements accounting for the peculiarities of personal data processing in a particular RF BS organisation and expanding the requirements set out in Section 7 and Section 8 of this standard are to be developed.

7.11.6. In order to meet the requirements for personal data security for PD security level 2 when PD is processed in an ISPD established by Russian Government Resolution *On Approval of Security Requirements for Personal Data Processed in Personal Data Systems* No. 1119 dated 1 November 2012, the following measures should be taken:

With regard to ABS IS provision in life cycle phases:

- Defining, executing and recording procedures for monitoring the integrity and provision of trusted software loading (including software for technical safeguards) on computer equipment incorporated into an ISPD;
- Defining, executing, recording and monitoring procedures for access to operational documentation and archive files containing parameters of ISPD settings, including settings for applicable technical safeguards;
- Defining, executing, recording and monitoring procedures for backup and provision of possible recovery of PD;
- Defining, executing, recording and monitoring procedures for backup and provision of possible recovery of software (including software for technical safeguards) that is incorporated into an ISPD;

With regard to IS maintenance in access and log-in control:

- Identifying and authenticating devices used for access;
- Locating facilities designed for ISPD administration, user workstations and ISPD server components in separate segments of computer networks;
- Network traffic monitoring, detection of intrusions and network attacks and response to them;
- Defining, executing, recording and monitoring procedures for updating of signature bases for technical safeguards, network traffic monitoring and identification of intrusions and network attacks;

With regard to IS maintenance for bank information processes:

- Defining, executing, recording and monitoring procedures for use of communication ports, information input/output devices, removable machine-readable media and external information storage media;
- Defining, executing, recording and monitoring procedures for access to PD archives.

7.11.7. A RF BS organisation shall provide protection of computer network segment perimeters within which ISPDs are located and monitoring of information interaction between computer network segments.

The RF BS organisation shall define and monitor rules for information interaction of ISPDs with other ABSs.

7.11.8. Information protection tools certified under information security requirements shall be used in ISPDs in accordance with requirements set out in Federal Service for Technical and Export Control Order *On Approval of the Scope and Content of Organisational and Technical Measures to Ensure Security of Personal Data Processed in Information Systems with Personal Data* No. 21 dated 18 February 2013 [10].

7.11.9. A RF BS organisation employee responsible for personal data security in an ISPD shall be appointed for each ISPD.

8. The Information Security Management System of Organisations of the Banking System of the Russian Federation

[1] Relevant threats are those threats for which the risk of implementation in the RF BS organisation is unacceptable.

8.1. General Provisions

8.1.1. In order to implement, operate, monitor and maintain the IS Maintenance System at the appropriate level, a number of IS Management System processes should be implemented; these should be arranged into groups in the form of a cyclic Deming model: *“ ... — Plan — Do — Check — Act — Plan —... “*

8.1.2. The aim of performance within the Plan group of processes is to start up the IS Management System cycle by defining initial plans related to IS Maintenance System creation, commissioning and control, and defining plans for IS Maintenance System upgrading based on decisions made in the Act phase. Performance in the Plan phase consists in defining/adjusting the IS Maintenance System scope, formalisation of the approach to IS risk assessment and resource distribution, conducting of IS risk assessment and defining/adjusting handling plans for such risks. It is important to ensure that all decisions to implement/adjust the IS Maintenance System are made by the management of the RF BS organisation (hereafter, the management).

8.1.3. The Do phase is carried out based on the results of the Plan and/or Act phases, and consists in executing all plans associated with IS Maintenance System creation, commissioning and upgrading as specified in the Plan phase and/or implementing solutions that were defined in the Act phase and do not require planning of relevant improvements. Among other things, it is important to arrange for IS training and awareness improvement, implementation of IS incident identification and response, and continuity of the business of the RF BS organisation.

A RF BS organisation shall choose safeguards appropriate to threat and violator models, taking into consideration the costs of implementing such safeguards and the scope of potential losses caused by threats. A RF BS organisation shall apply only those safeguards that can be checked for operation validity; the RF BS organisation shall regularly assess the appropriateness of safeguards and the effectiveness of their implementation based on the safeguards' influence on the business goals of the organisation.

8.1.4. The aim of performance within the Check group of processes is to ensure sufficient confidence in the fact that the IS Maintenance System (including safeguards) is operating properly and is appropriate to the existing IS threats and internal and/or external operational IS conditions of the RF BS organisation. Moreover, any changes in assumptions or risk assessment should be considered. This activity may be performed at any time and frequency, depending on what is suitable for a given situation. The following shall be done in the Check phase: IS monitoring and oversight of safeguards used; carrying out regular self-assessment to check whether the IS of the RF BS organisation meets the requirements of this standard and conducting IS audit; analysis of IS Maintenance System operation on the whole, including on the part of the management.

A RF BS organisation shall detect in good time problems related to IS directly or indirectly which may affect its business goals. The cause-and-effect relation of possible problems should be identified to use it as basis for forecasting their development.

The result of performance in the Check phase is the basis for IS Maintenance System improvement.

8.1.5. The Act group of processes comprises making decisions on tactical and/or strategic improvements of the IS Maintenance System. This activity, i.e. transition to the Act phase, is performed only when the result of Check processes requires IS Maintenance System upgrading. The actual upgrading of the IS Maintenance System shall be carried out within the Do group of processes, and the Plan group if necessary. An example of the first situation is putting the existing business continuity plan into execution, since the necessity of doing so was determined in the Check phase. An example of the second situation is new threat identification and subsequent updating of risk assessment in the Plan phase. It is important to ensure that all stakeholders are notified immediately of IS Maintenance System improvements made and that relevant training is provided as required.

A RF BS organisation shall accumulate, generalize and use both its experience and the experience of other organisations at all levels of decision making and performance.

8.1.6. The following sets of requirements should be fulfilled to ensure successful IS Management System operation in a RF BS organisation:

- Requirements for organisation and operation of the IS service of the RF BS organisation;
- Requirements for defining/adjusting the IS Maintenance System scope;
- Requirements for selecting/ adjusting the approach to IS breach risk assessment and the performance of such assessment;
- Requirements for development of IS breach risk handling plans;
- Requirements for development/adjustment of internal documents used to control IS maintenance activities;
- Requirements for decision making by the management of the RF BS organisation on IS Maintenance System implementation and operation;
- Requirements for managing implementation of IS breach risk handling plans;
- Requirements for the development and execution of training and awareness improvement programmes in the field of IS;
- Requirements for management of security incident detection and response;
- Requirements for arranging business continuity and restoration after interruptions;
- Requirements for IS Maintenance System monitoring and safeguards oversight;

- IS self-assessment requirements;
- IS audit requirements;
- IS Maintenance System operation analysis requirements;
- Requirements for IS Maintenance System analysis by the management of the RF BS organisation;
- Requirements for decision making on tactical IS Maintenance System improvements;
- Requirements for decision making on strategic IS Maintenance System improvements.

8.2. Requirements for Arrangement and Operation of the Information Security Service of an Organisation in the Banking System of the Russian Federation

8.2.1. In order to implement, operate, monitor and maintain the IS Maintenance System at the proper level, the management should set up an IS service consisting of at least two members (appoint authorised persons), and approve goals and tasks associated with its activity.

The IS service shall have powers and resources approved by the management which are required to fulfil the specified aims and objectives, as well as a supervisor appointed from amongst the management. The IS service and the computerisation (automation) service shall not have the same supervisor.

The IS service should be provided with its own budget.

RF BS organisations having a network of affiliates or regional representative offices should be provided with relevant IS units (authorised persons) on site to be given necessary resources and a regulatory framework.

8.2.2. The IS service shall be vested with the following minimum powers:

- Managing the preparation and monitoring the performance of all IS maintenance plans of the RF BS organisation;
- Developing and proposing changes in the IS policies of the organisation;
- Managing changes in existing internal documents and adoption by the management of new internal documents regulating IS maintenance activities within the RF BS organisation;
- Defining requirements for IS maintenance measures within the RF BS organisation;
- Supervising employees of the RF BS organisation to ensure that they meet the requirements of internal documents regulating IS maintenance activities, especially employees who have access rights to protected information assets;
- Monitoring events associated with IS maintenance;
- Participating in the investigation of events associated with IS incidents and, if necessary, proposing sanctions against persons using UA and URA (e.g. those who have violated the requirements of instructions, manuals, etc., on IS maintenance within the RF BS organisation);
- Participating in restoration of ABS operability after failures and accidents;
- Monitoring IS maintenance in ABS LC phases, including testing and commissioning of IS subsystems of the ABS of the RF BS organisation;
- Participating in the creation, maintenance, operation and improvement of the IS Maintenance System of the RF BS organisation.

8.3. Requirements for Definition/Adjustment of the Scope of the Information Security Provision System

8.3.1. Procedures for accounting of protected information assets by classes (types) shall be defined, executed, recorded and monitored. Classification of information assets should be based on assessments of the information asset's value for the interests (or goals) of the RF BS organisation (e.g. in accordance with the severity of consequences from loss of IS properties of information assets).

8.3.2. A RF BS organisation shall have criteria for placing certain information assets into one or more categories of information assets.

8.3.3. Procedures for accounting of assiciated objects for each information asset and/or type of information asset which cover all levels of the information infrastructure of the RF BS organisation determined in Section 6 of this standard shall be defined, executed, recorded and monitored.

8.3.4. A RF BS organisation shall define roles for information asset accounting and accounting of associated objects, and persons responsible for the performance of these roles shall be appointed.

8.4. Requirements for Selection/Adjustment of the Approach to Information Security Breach Risk Assessment and Performance of Information Security Breach Risk Assessment

8.4.1. A RF BS organisation shall adopt/adjust a methodology of IS breach risk assessment/an approach to IS breach risk assessment.

8.4.2. The RF BS organisation shall have criteria specified for IS breach risk acceptance and the level of allowable IS breach risk.

8.4.3. The IS breach risk assessment methodology/approach to IS breach risk assessment for a RF BS organisation shall specify the method and procedure for qualitative or quantitative assessment of IS breach risk based on the following assessments:

- The probability of IS threat materialisation by sources of IS threats identified and/or assumed, which are recorded in threat and violator models, where such threats affect objects related to information assets of the RF BS organisation (or types of information assets);
- The severity of consequences from the loss of IS properties (in particular, the properties of availability, integrity and confidentiality) for the information assets (types of information assets) considered.

The procedure of IS breach risk assessment shall contain necessary IS breach risk assessment processes and the sequence of their performance.

8.4.4. The risks of IS breach are assessed for the IS properties of all information assets (or types of information assets) of the IS Maintenance System scope.

8.4.5. Risk magnitudes resulting from IS breach risk assessment shall be correlated with the level of the allowable risk accepted within the RF BS organisation. The result of performance of this procedure is a recorded list of unacceptable risks of IS breach.

8.4.6. A RF BS organisation shall define roles associated with defining/adjustment of the IS breach risk assessment methodology/approach to IS breach risk assessment, and persons responsible for the performance of these roles shall be appointed.

8.4.7. A RF BS organisation shall define roles for IS breach risk assessment, and persons responsible for the performance of these roles shall be appointed.

8.5. Requirements for Development of Information Security Breach Risk Handling Plans

8.5.1. For each unacceptable IS breach risk a plan specifying one of the possible handling techniques shall be determined:

- Transfer of risk to external organisations (e.g. through insurance against such risk);
- Avoidance of the risk (e.g. by forgoing the activity causing risk occurrence);
- Conscious risk acceptance;
- Creating IS maintenance requirements which reduce the IS breach risk to a tolerable level, and making plans for their implementation.

8.5.2. IS breach risk handling plans shall be coordinated with the head of the IS service or with the person in charge of IS maintenance within the RF BS organisation and approved by the management.

8.5.3. Plans for implementation of IS maintenance requirements shall contain a sequence of safeguards (organisational, technical, etc.) and time frames for their implementation.

8.5.4. A RF BS organisation shall define roles for the development of IS breach risk handling plans, and persons responsible for the performance of these roles shall be appointed.

8.6. Requirements for Development/Adjustment of Internal Documents Regulating Information Security Maintenance Activities

8.6.1. Development/adjustment of internal documents regulating information security maintenance activities within a RF BS organisation should be based on Bank of Russia Standardisation Recommendations RS BR IBBS-2.0 ‘Maintenance of Information Security of the Russian Banking System Organisations. Recommended Practices for Documentation Related to Information Security Maintenance in Accordance with STO BR IBBS-1.0’.

8.6.2. A RF BS organisation shall develop/adjust the following internal documents:

- The IS policy of the RF BS organisation;
- Special IS policies of the RF BS organisation;
- Documents regulating the procedures for performance of certain types of activities associated with IS maintenance within the RF BS organisation.

Moreover, the list and forms of documents testifying to the performance of IS maintenance activities within the RF BS organisation shall be defined.

The IS policy of the RF BS organisation shall be approved by the management.

8.6.3. The following shall be defined/adjusted in the IS policy (in special policies):

- Aims and objectives of IS maintenance;
- Main areas of IS maintenance;
- Main types of information assets protected;
- Threat and violator models;
- A set of rules, requirements and guiding principles related to IS;
- Basic requirements for IS maintenance;
- Principles for counteracting IS threats against the main types of information assets protected;
- Basic principles for improvement of IS knowledge and awareness;
- Principles for implementation and monitoring of the performance of IS policy requirements.

8.6.4. Development/adjustment of internal documents regulating IS provision activities shall be based on:

- The legislation of the Russian Federation;
- The BR BSIS package, in particular, the requirements of Section 7 and Section 8 of this standard;
- Regulations and instructions of regulatory or oversight authorities;
- Contractual requirements of the RF BS organisation with external organisations;
- Results of risk assessment providing an itemisation of information assets or types of information assets under consideration consistent with the level of the document being developed.

8.6.5. The set of internal documents regulating IS maintenance activities shall contain IS maintenance requirements for all the information assets or types of information assets identified which are within the scope of the IS Maintenance System of the RF BS organisation.

8.6.6. Documents regulating procedures for certain types of activities associated with IS maintenance shall elaborate on the provisions of the IS policy (or special policies) and shall not contradict them.

8.6.7. If units of a RF BS organisation have employees responsible for IS maintenance, a procedure for interaction or coordinated work between the IS service and these employees shall be approved by the management within the RF BS organisation.

8.6.8. Internal documents regulating IS maintenance activities should contain:

- A list of evidence of activity performance;
- The responsibility of RF BS organisation employees for the performance of such activities.

8.6.9. Procedures for assignment and distribution of IS maintenance roles shall be defined.

8.6.10. The procedure for development, maintenance, revision and monitoring of performance of internal documents regulating IS maintenance activities within a RF BS organisation shall be determined.

8.6.11. A RF BS organisation shall define roles for development, maintenance, revision and monitoring of execution of internal documents regulating IS maintenance activities, and persons responsible for the performance of these roles shall be appointed.

8.7. Requirements for Decision Making by the Management of an Organisation of the Banking System of the Russian Federation to Implement and Operate an Information Security Provision System

8.7.1. Decisions on IS Maintenance System implementation and operation shall be approved by the management of a RF BS organisation. In particular, the RF BS organisation shall record decisions made by the management:

- On analysis and acceptance of residual risk of IS breach;
- On planning of IS Maintenance System implementation phases (in particular, the IS provision requirements set out in Section 7 and Section 8 of this standard);
- On the distribution of roles related to IS maintenance within the RF BS organisation;
- On the adoption of safeguard implementation plans by the management which are designed to fulfil the requirements specified in Section 7 and Section 8 of this standard and to reduce IS risks;
- On allocation of resources required for IS Maintenance System implementation and operation.

8.7.2. All IS Maintenance System implementation plans, in particular, plans for fulfilling the requirements of Section 7 and Section 8 of this standard and plans for IS breach risk handling and safeguards implementation, shall be approved by the management. The above-mentioned plans shall specify:

- The sequence of performance of measures within the framework of the above-mentioned plans;
- Time frames for the start and end of the planned measures;
- Officials (of the unit) who are responsible for the performance of each of the above-mentioned measures.

8.7.3. The procedure for development, revision and monitoring of performance of IS maintenance plans for a RF BS organisation shall be defined.

8.7.4. The RF BS organisation shall have recorded decisions made by the management with regard to role assignment and distribution for all units in accordance with the provisions of internal documents regulating IS maintenance activities within the RF BS organisation.

8.8. Requirements for Managing the Execution of Information Security System Implementation Plans

8.8.1. Procedures for engineering/acquisition/deployment, implementation, operation, monitoring and support of operations of safeguards (the ISS) that are provided for by plans for the fulfilment of IS maintenance requirements shall be defined, executed, recorded and monitored.

8.8.2. In order to build ISS elements related to a certain area or sphere of activity of the RF BS organisation, specific safeguards applicable to associated objects shall be implemented in accordance with the existing IS maintenance requirements of the RF BS organisation stated in the IS policy and other internal documents of the RF BS organisation.

8.8.3. A RF BS organisation shall define roles associated with the execution of IS breach risk handling plans and implementation of required safeguards, and persons responsible for the performance of these roles shall be appointed.

8.9. Requirements for the Development and Execution of Training and Awareness Improvement Programmes in the Field of Information Security

8.9.1. Work with personnel and clients in the field of IS awareness improvement and training authorised by the management of the RF BS organisation shall be arranged.

8.9.2. IS training and awareness improvement plans and programmes shall be developed. Knowledge obtained as a result of executing these plans shall be verified.

8.9.3. Training and awareness improvement plans shall specify requirements for the frequency of training and awareness improvement.

8.9.4. Training and awareness improvement programmes shall be developed for various groups of employees based on their job duties and roles performed; they shall include information concerning:

- Existing IS policies;
- Safeguards applied within the RF BS organisation;
- Correct use of safeguards in accordance with internal documents of the RF BS organisation;
- The relevance and importance of activities performed by employees for IS maintenance within the RF BS organisation.

8.9.5. The RF BS organisation shall define a list of evidence of execution of IS training and awareness improvement programmes. In particular, such evidence may be:

- Documents (logs) testifying to the IS training of both managers and employees of the RF BS organisation and indicating the level of education, skills, experience and expertise of trainees;
- Documents containing the results of verification of training of RF BS organisation employees;
- Documents containing results of verification of IS awareness within the RF BS organisation.

8.9.6. An employee assigned a new role shall be provided with IS training or briefing consistent with the role assigned.

8.9.7. A RF BS organisation shall define roles for the development and execution of IS training and awareness improvement plans and programmes and for monitoring of results, and persons responsible for the performance of these roles shall be appointed.

8.10. Requirements for Management of Information Security Incident Detection and Response

8.10.1. Procedures for incident handling shall be defined, executed, recorded and monitored; these include:

- Procedures for IS incident detection;
- Procedures for notification about incidents, including notification of the IS service;
- Procedures for classification of incidents and assessment of damage caused by an IS incident;
- Procedures for response to an incident;
- Procedures for analysis of IS incident causes and assessment of the results of response to IS incidents (with the participation of external IS experts, if necessary).

8.10.2. Procedures for storage and distribution of information about IS incidents, IS incident analysis practices and results of response to IS incidents shall be defined, executed, recorded and monitored.

8.10.3. Actions of RF BS organisation employees when abnormal IS events are identified and such events are communicated shall be defined, executed, recorded and monitored. Employees of the organisation shall be notified of the established procedures.

8.10.4. Procedures for IS incident investigation shall take into account the legislation of the Russian Federation, IS-related provisions of Bank of Russia regulations and internal documents of the RF BS organisation.

8.10.5. RF BS organisations shall make, record and execute decisions on any IS incidents detected.

8.10.6. A RF BS organisation shall define roles for the detection, classification, response, analysis and investigation of IS incidents, and persons responsible for the performance of these roles shall be appointed.

8.11. Requirements for Managing Business Continuity and Restoration after Interruptions

8.11.1. Procedures for accounting of information assets or types of information assets that are significant to ensuring continuity of the RF BS organisation's business shall be defined, executed, recorded and monitored.

8.11.2. A RF BS organisation shall have IS provision requirements which regulate business continuity and restoration after interruption, including requirements for events related to the restoration of necessary information, software, facilities and communication links.

8.11.3. A plan for providing business continuity and restoration after potential interruption shall be defined. The plan shall contain instructions and business restoration procedures for RF BS organisation employees. In particular, the plan shall comprise:

- Conditions for plan activation;
- Actions to be undertaken after an IS incident;
- Restoration procedure;

- Plan testing and checking procedures;
- A training and awareness improvement plan for RF BS organisation employees;
- Obligations of organisation employees specifying persons responsible for execution of each of the plan provisions.

8.11.4. Plans for providing business continuity and restoration after interruption shall be developed on the basis of results of assessment of IS breach risks within the RF BS organisation with regard to information assets that are significant for ensuring business continuity and restoration after interruption.

8.11.5. A RF BS organisation shall use safeguards to provide business continuity with regard to information assets that are significant to ensuring business continuity and restoration after interruption.

Application of safeguards to ensure business continuity and restoration after interruption shall be based on relevant IS maintenance requirements.

8.11.6. The plan for ensuring business continuity and restoration after interruption shall be coordinated with existing IS incident development procedures within the organisation.

8.11.7. Procedures for regular testing of the plan for ensuring business continuity and restoration after interruption shall be defined, executed, recorded and monitored. Based on testing, the plan is to be adjusted appropriately as needed. The testing scenario shall be based on the threat and violator model existing within the RF BS organisation and on risk assessment results.

8.11.8. A training and awareness improvement programme for employees with regard to ensuring business continuity and restoration after interruptions shall be implemented within the RF BS organisation.

8.11.9. A RF BS organisation shall define roles for the development of the plan to ensure business continuity and restoration after interruption, and persons responsible for the performance of these roles shall be appointed.

8.12. Requirements for Information Security Monitoring and Safeguard Oversight

8.12.1. Procedures for IS monitoring and oversight of safeguards, including monitoring of configuration parameters and settings of protection tools and mechanisms shall be defined, executed and recorded. Performance of the above procedures shall be managed by the IS service and shall cover all safeguards included in the ISS which have been implemented and are in operation.

8.12.2. Procedures for gathering and storage of information about actions of RF BS organisation employees, events and parameters related to safeguard operation shall be specified, executed, recorded and monitored.

8.12.3. Information about all incidents detected during IS monitoring and safeguard oversight shall be considered within the framework of performance of IS incident information storage procedures.

8.12.4. Procedures for IS monitoring and safeguard control shall be subject to regular, recorded revisions due to changes in the scope and methods of safeguard application and identification of new IS threats and vulnerabilities and on the basis of data on IS incidents.

8.12.5. A RF BS organisation shall define roles associated with the performance of procedures for IS monitoring and safeguard oversight and revision of these procedures, and persons responsible for the performance of these roles shall be appointed.

8.13. Requirements for Information Security Self-Assessment

8.13.1. IS self-assessment is carried out by the organisation's own personnel and on the initiative of the management of the RF BS organisation.

8.13.2. IS self-assessment shall be consistent with Bank of Russia Standard STO BR IBBS-1.2 ‘Maintenance of Information Security of the Russian Banking System Organisations. Assessment Method for Compliance of Information Security of the Russian Banking System Organisations with Requirements of STO BR IBBS-1.0’. IS self-assessment should be organised in accordance with Bank of Russia Recommendations on Standardisation RS BR IBBS-2.1 ‘Maintenance of Information Security of the Russian Banking System Organisations. Guidelines for Self-Assessment of Conformity of the Information Security of the Russian Banking System Organisations with Requirements of STO BR IBBS-1.0’.

8.13.3. The IS self-assessment programme to be established and implemented shall contain information necessary for IS self-assessment planning and management and the monitoring, analysis and improvement of these processes; as well as provision of resources required for conducting effective and successful IS self-assessments within the predetermined time frame.

8.13.4. The following procedures shall be defined, executed, recorded and monitored:

- Generation, collection and storage of IS self-assessment evidence;
- Observation of the frequency of IS self-assessment;
- Storage and distribution of IS self-assessment results.

8.13.5. A self-assessment plan shall be established for each IS self-assessment carried out within the RF BS organisation; it shall specify:

- The purpose of IS self-assessment;
- Objects and activities subject to IS self-assessment;

- Procedure and time frames for IS self-assessment measures;
- Distribution of roles among BS organisation employees in connection with IS self-assessment.

8.13.6. Reports shall be prepared based on IS self-assessments. IS self-assessment results and relevant reports shall be submitted to the management of the RF BS organisation.

8.13.7. A RF BS organisation shall define roles associated with the execution of the IS self-assessment programme, and persons responsible for the performance of these roles shall be appointed.

8.14. Requirements for Information Security Audit

8.14.1. IS audit within a RF BS organisation shall be consistent with the following Bank of Russia standards: STO BR IBBS-1.1 ‘Maintenance of Information Security of the Russian Banking System Organisations. Information Security Audit’ and STO BR IBBS-1.2 ‘Maintenance of Information Security of the Russian Banking System Organisations. Assessment Method for Compliance of Information Security of the Russian Banking System Organisations with Requirements of STO BR IBBS-1.0’.

8.14.2. The IS audit programme to be established and implemented shall contain information necessary for IS audit planning and management and the monitoring, analysis and improvement of these processes; as well as provision of resources required for conducting effective and successful IS audits within the predetermined time frame.

8.14.3. An audit plan shall be established for each IS audit carried out within the RF BS organisation; it shall specify:

- The purpose of the IS audit;
- IS audit criteria;
- The scope of the IS audit;
- The date and duration of the IS audit;
- Audit team members;
- A description of audit activities and events;
- Allocation of resources during the audit.

8.14.4. A RF BS organisation shall conclude contracts with auditing organisations, and procedures shall be established for:

- Storage, access and use of materials obtained during the IS audit;
- Interaction with the auditing organisation during the IS audit;
- Interaction between the audit team and the management, enabling audit team representatives to contact the management directly as needed;
- Arrangement of employee interviews;
- Arrangement of observation of activities performed by RF BS organisation employees by representatives of the auditing organisation.

8.14.5. Reports shall be prepared based on the audit. Audit results and relevant reports shall be submitted to the management.

8.14.6. Procedures for storage, access and use of materials obtained during audits (in particular, audit reports) shall be defined, executed, recorded and monitored.

8.14.7. A RF BS organisation shall define roles associated with the management of execution of audit programmes and plans for individual audits, and persons responsible for the performance of these roles shall be appointed.

8.15. Requirements for Analysis of the Operation of the Information Security Provision System

8.15.1. Procedures for IS Maintenance System operation analysis shall be specified, executed, recorded and monitored using:

- Results of IS monitoring and safeguard oversight;
- Information about IS incidents;
- Results of IS audits and IS self-assessments;
- Data on threats, potential violators and IS vulnerabilities;
- Data on changes within the RF BS organisation (e.g. data on changes in processes and technologies implemented within the framework of the main process flow; changes in internal documents of the RF BS organisation);
- Data on changes outside the RF BS organisation (e.g. data on changes in the legislation of the Russian Federation; changes in requirements of the BSIS BR package; or changes in the contractual obligations of the organisation).

8.15.2. IS Maintenance System operation analysis shall include:

- Analysis of compliance of the package of internal documents regulating IS maintenance activities within the RF BS organisation with the requirements of the legislation of the Russian Federation, requirements of Bank of Russia standards (in particular, the requirements of this standard) and contractual requirements of the organisation;

- Analysis of compliance of internal documents of low hierarchy levels which regulate IS maintenance activities within the RF BS organisation to the requirements of the IS policies of the RF BS organisation;
- Evaluation of the IS risks of the organisation, including assessment of the level of residual and allowable risk and assessment of the appropriateness of the threat model of the RF BS organisation to existing IS threats;
- Checking the conformity of applied safeguards to requirements set out in internal documents of the RF BS organisation and risk assessment results;
- Analysis of the absence of discontinuities in IS maintenance processes and lack of coordination in the use of safeguards.

8.15.3. A RF BS organisation shall define roles associated with procedures for IS Maintenance System operation analysis, and persons responsible for the performance of these roles shall be appointed.

8.16. Requirements for Analysis of the Information Security Provision System by the Management of an Organisation in the Banking System of the Russian Federation

8.16.1. A RF BS organisation shall define a list of documents or data required for preparation of information provided to the management for conducting of IS Maintenance System analysis. In particular, this list shall include:

- Reports on results of IS monitoring and safeguard oversight;
- Reports on results of IS Maintenance System operation analysis;
- Reports on results of IS audits;
- Reports on results of IS self-assessments;
- Documents containing information about ways and methods of protection, safeguards or procedures for their application which could be used to improve IS Maintenance System operation;
- Documents containing information about both new and detected IS vulnerabilities and threats;
- Documents containing information about actions taken based on previous IS Maintenance System analyses performed by the management;
- Documents containing information about changes that could affect the organisation of the IS Maintenance System (e.g. changes in the legislation of the Russian Federation and/or in provisions of Bank of Russia standards;
- Documents containing information about detected IS incidents;
- Documents confirming the performance of required IS maintenance activities (e.g. execution of risk handling plans);
- Documents confirming the fulfilment of requirements related to business continuity and restoration after interruption.

8.16.2. A RF BS organisation shall have an IS Maintenance System monitoring and analysis plan. In particular, this plan shall contain provisions on meetings at the management level during which IS problems affecting the business of the RF BS organisation are sought out and analysed.

8.16.3. A RF BS organisation shall define roles associated with the preparation of information required for IS Maintenance System analysis by the management, and persons responsible for the performance of these roles shall be appointed.

8.17. Requirements for Decision Making on Tactical Improvements of the Information Security Provision System[1]

8.17.1. In order to make decisions associated with tactical IS Maintenance System improvements, the following results should be considered, among others:

- IS audits;
- IS self-assessments;
- IS monitoring and safeguard oversight;
- IS Maintenance System operation analysis;
- IS incident handling;
- Detection of new IS threats and vulnerabilities;
- Risk assessment;
- Analysis of the list of safeguards that may be applied;
- Strategic IS Maintenance System improvements;

[1] Tactical IS Maintenance System improvements should include corrective or preventive actions associated with the revision of certain procedures of IS Maintenance System-related activity performance within the RF BS organisation, and which do not require any revision of the IS policy or special IS policies of the RF BS organisation. As a rule, tactical IS Maintenance System improvements do not require any activity to be performed within the framework of the IS Management System Plan phase.

- IS Maintenance System analysis by the management;
- Analysis of successful IS practices (the organisation's own or those of other organisations).

8.17.2. Decisions on tactical IS Maintenance System improvements shall be recorded and either shall contain conclusions concerning lack of necessity for tactical IS Maintenance System improvements, or areas of tactical IS Maintenance System improvements shall be specified in the form of corrective or preventive actions, e.g.:

- Revision of procedures for performance of certain types of IS provision activities;
- Revision of procedures for operation of certain types of safeguards;
- Revision of procedures for incident detection and handling;
- Updating of the list of information assets;
- Revision of the personnel training and awareness improvement programme;
- Revision of the plan for ensuring business continuity and restoration after interruption;
- Revision of risk handling plans;
- Imposition of sanctions against personnel;
- Revision of procedures for IS monitoring and safeguard oversight;
- Revision of audit programmes;
- Adjustment of relevant internal documents regulating procedures for performance of IS maintenance activities and safeguard operation;
- Introduction of new safeguards or replacement of safeguards used.

8.17.3. Activities associated with the implementation of tactical improvements shall be recorded. Tactical IS Maintenance System improvement implementation plans and documents containing the results of the execution of such plans shall be established.

8.17.4. Activities associated with the implementation of IS Maintenance System improvements shall be authorised and monitored by the management of the IS service of a RF BS organisation.

8.17.5. Procedures for coordination and notification of stakeholders regarding tactical IS Maintenance System improvements (in particular, changes related to IS maintenance, responsibility in the field of IS and IS maintenance requirements) shall be defined, executed, recorded and monitored.

8.17.6. When decisions are made regarding tactical IS Maintenance System improvements, roles shall be defined, and persons responsible for the performance of these roles shall be appointed.

8.18. Requirements for Decision Making on Strategic Improvements of the Information Security Provision System[1]

8.18.1. In order to make decisions associated with strategic IS Maintenance System improvements, the following results should be considered, among others:

- IS audits;
- IS self-assessments;
- IS monitoring and safeguard oversight;
- IS Maintenance System operation analysis;
- IS incident handling;
- Identification of new information assets of the RF BS organisation or their types;
- Detection of new IS threats and vulnerabilities;
- Risk assessment;
- Revision of basic IS risks;
- IS Maintenance System analysis by the management;
- Analysis of successful IS practices (the organisation's own or those of other organisations);
  as well as changes:
- In the legislation of the Russian Federation;
- In Bank of Russia regulations (in particular, the requirements of this standard);
- The business interests, aims and objectives of the RF BS organisation;
- Contractual obligations of the RF BS organisation.

8.18.2. Decisions on strategic IS Maintenance System improvements shall be recorded and either shall contain conclusions concerning lack of necessity for strategic IS Maintenance System improvements, or areas of strategic IS Maintenance System improvements shall be specified in the form of corrective or preventive actions, e.g.:

[1] Strategic IS Maintenance System improvements include corrective or preventive actions associated with the revision of the IS policy and special IS policies of the RF BS organisation, to be followed by relevant tactical IS Maintenance System improvements. Strategic IS Maintenance System improvements always require performance of activities within the framework of the IS Management System Plan phase.

- Updating/revision of the aims and objectives of IS maintenance defined within the framework of the IS policy or special IS policies of the RF BS organisation;
- Change in the scope of the IS Maintenance System;
- Revision of threat and violator models;
- Change of approaches to IS risk assessment and criteria for IS risk acceptance.

8.18.3. Any activities related to the implementation of strategic improvements shall be recorded. Strategic IS Maintenance System improvement implementation plans and documents containing the results of the execution of such plans shall be established.

8.18.4. Activities associated with the implementation of strategic IS Maintenance System improvements shall be coordinated by the IS service and authorised and monitored by the management of the RF BS organisation.

8.18.5. In the case of strategic IS Maintenance System improvements, corresponding tactical IS Maintenance System improvements shall be implemented for all required IS maintenance procedures, safeguards used and relevant internal documents. In particular, the following shall be done:

- Development of tactical IS Maintenance System improvement plans;
- Updating of risk handling plans;
- Updating of the safeguards implementation programme;
- Updating of procedures for use of safeguards.

8.18.6. Procedures for coordination and notification of stakeholders regarding strategic IS Maintenance System improvements (in particular, changes related to IS maintenance, responsibility in the field of IS and IS maintenance requirements) shall be defined, executed, recorded and monitored.

8.18.7. When decisions are made regarding strategic IS Maintenance System improvements, roles shall be defined, and persons responsible for the performance of these roles shall be appointed.

9. Checking and Assessment of the Information Security of Organisations in the Banking System of the Russian Federation

9.1. IS within RF BS organisations is to be checked and assessed through the following processes:

- IS monitoring and safeguard oversight;
- IS self-assessment;
- IS audit;
- IS Maintenance System operation analysis (including that conducted by the management).

The above processes form part of the IS Management System Check group of processes; the requirements for such processes are specified in Section 8 of this standard.

9.2. The main objectives of IS monitoring and safeguard oversight within the RF BS organisation are: effective and continuous observation; and gathering, analysis and processing of data based on predetermined aims. Such analysis aims may include:

- monitoring of implementation of provisions concerning IS maintenance within the RF BS organisation;
- identification of inappropriate (including malicious) actions in the ABS of the organisation;
- IS incident detection.

Safeguards are monitored and controlled by RF BS organisation personnel in charge of IS.

Requirements for safeguard monitoring and oversight within the RF BS organisation are specified in subsection 8.12 of this standard.

9.3. IS self-assessment is recommended when preparing for an IS audit.

9.4. IS audit carried out by independent auditing organisations external to the RF BS organisation is one form of checking and assessment (or monitoring) of how the RF BS organisation is fulfilling the requirements of this standard.

IS audit is performed both for the RF BS organisation's own purposes and to enhance confidence in the RF BS organisation from other organisations.

Organisations qualified and experienced in the assessment of IS conformity with the requirements of this standard should be brought in as auditing organisations.

9.5. IS Maintenance System operation is analysed by RF BS organisation personnel in charge of IS provision and by the management, including on the basis of documents or data prepared for the management.

The main objectives of IS Maintenance System operation analysis are:

- Assessment of IS Maintenance System effectiveness;
- Assessment of IS Maintenance System conformity with requirements set out in the legislation of the Russian Federation and Bank of Russia standards;
- Assessment of IS Maintenance System conformity with both existing and potential IS threats;
- Assessment of adherence to IS principles and fulfilment of IS maintenance requirements stated in the IS policy of the RF BS organisation and in other internal documents of the RF BS organisation.

Results obtained during IS Maintenance System operation analysis are, among other things, the basis for IS Maintenance System improvement.

9.6. This standard does not require the obtaining of a license for technical protection of confidential information (restricted access information) when conducting security maintenance measures in special ISPDs for the in-house needs of RF BS organisations, nor does it require ISPD certification. Where the standard is put into force in a RF BS organisation, the said requirements are not mandatory when a package of measures is conducted to ensure the security of personal data in ISPD of RF BS organisations.

9.7. A license of the Federal Security Service of Russia is obtained by a RF BS organisation in accordance with the requirements set out in the legislation of the Russian Federation.

9.8. IS conformity assessment in the form of an IS audit or IS self-assessment is to be carried out by a RF BS organisation at least once every two years.

References

1. Federal Law *On Banks and Banking Activities* No. 395-1 dated 1 December 1990.
2. Federal Law *On the Central Bank of the Russian Federation (Bank of Russia)* No. 86-FZ dated 10 July 2002.
3. Federal Law *On Technical Regulation* No. 184-FZ dated 27 December 2002.
4. Federal Law *On Information, Information Technologies and Information Protection* No. 149-FZ dated 27 July 2006.
5. GOST R ISO 9001-2008 *Quality Management System. Requirements.*
6. ISO/IEC IS 27001:2013 *Information Technology. Security Techniques. Information Security Management Systems. Requirements.*
7. Bank of Russia Regulation *On Information Security Requirements for Funds Transfers and on the Bank of Russia's Procedure for Monitoring Compliance with Information Security Requirements for Funds Transfers* No. 382-P dated 9 June 2012, as amended by Bank of Russia Ordinance No. 3007-U dated 5 June 2013.
8. Federal Law *On Personal Data* No. 152-FZ dated 27 July 2006.
9. Resolution of the Government of the Russian Federation *On the Approval of Requirements for Protection of Personal Data Processed in Information Systems with Personal Data* No. 1119 dated 1 November 2012.
10. Federal Service for Technical and Export Control Order *On Approval of the Scope and Content of Organisational and Technical Measures to Ensure Security of Personal Data Processed in Information Systems with Personal Data* No. 21 dated 18 February 2013.

Key words: banking system of the Russian Federation, Information Security Management System, information security policy

*In case of any translation ambiguity the Russian version shall prevail.