BANK OF RUSSIA
RECOMMENDATIONS ON STANDARDISATION

RS BR IBBS-2.2-2009

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

METHODOLOGY FOR ASSESSING THE RISKS OF INFORMATION SECURITY BREACH*

Effective date: 2010-01-01

Moscow
2009

Foreword

1. Adopted and enacted by Bank of Russia Directive No. R-1190, dated 11 November 2009.
2. ENACTED FOR THE FIRST TIME

Table of Contents

Introduction

To establish and maintain the Information Security Maintenance System (IS Maintenance System) of organisations of the Banking System (BS) of the Russian Federation (RF) at the appropriate level, the current standard of the Bank of Russia "Maintenance of Information Security of the Russian Banking System Organisations. General Provisions" (hereinafter – "STO BR IBBS-1.0") defines the requirement for assessing the risk of information security (IS) breaches.

This methodology establishes the recommended methods and procedures for assessing the risk of IS breaches in a RF BS organisation, given that such assessment is an integral part of the IS Management System (IS Management System) in RF BS organisations.

The provisions of this methodology can be used for the purpose of internal controls in RF BS organisations.

A RF BS organisation shall independently establish the frequency for assessing IS breach risks with reference to the provisions of this methodology.

BANK OF RUSSIA RECOMMENDATIONS ON STANDARDISATION

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

METHODOLOGY FOR ASSESSING THE RISKS OF INFORMATION SECURITY BREACHES

Effective date: 2010-01-01

1. Scope of Application

This methodology applies to RF BS organisations that are assessing IS breach risks as part of building/improving their Information Security Maintenance System (IS Maintenance System) in accordance with the requirements of STO BR IBBS-1.0.

It is recommended that the provisions of this methodology be used when assessing IS breach risks and in operations in the wake of the assessment of IS risks, and may also be used as a reference and/or its provisions may be directly employed in the internal documents of RF BS organisations.

Other methodologies can be used by a RF BS organisation to assess IS breach risks. The use of this methodology and other methodologies for assessing the risks of IS breaches have equal importance when building IS Maintenance System in a RF BS organisation.

2. Regulatory References

This methodology uses the regulatory references to STO BR IBBS-1.0.

3. Terms and Definitions

This methodology uses terms from STO BR IBBS-1.0, including the following terms (in alphabetical order) with corresponding definitions:

3.1. **"A Priori Protection Measures":** protection measures that are used to reduce in a qualitative and quantitative manner any existing vulnerabilities in objects pertaining to information asset protection, thereby reducing the probability of corresponding IS threats materialising (for example, security tools to safeguard against unauthorised access).

3.2 **"A Posteriori Protection Measures":** protection measures used to reduce the severity of consequences resulting from a breach affecting information assets (e.g., information backup and recovery tools).

3.3. **"Acceptable Risk of Information Security Breaches":** the level of potential damage from an IS breach that is acceptable to a RF BS organisation at a given time and in a given situation.

3.4. **"Information Asset":** information that is identifiable through requisite details and which is of value to the RF BS organisation; furthermore, this is information held by the RF BS organisation and is produced on any physical storage device in a manner suitable for its processing, storage or transmission.

3.5. **"Source of Information Security Threat"; "Source of IS threat":** an object or entity causing the IS threats by impacting objects in the information asset environment of a RF BS organisation.

3.6. **"Model of Information Security Threats"; "Model of IS threats":** the description of sources of IS threats; methods of executing IS threats; objects suitable for manifesting IS threats; vulnerabilities exploited by sources of IS threats; types of potential losses (e.g., the unavailability of information, or breaches in the integrity or confidentiality of information assets); scale of potential damage.

3.7. **"Handling the Risk of Information Security Breach":** the process of selecting and implementing protection measures to reduce IS breach risks, or measures to transfer, accept or avoid these risks.

3.8. **"Object related to Information Assets":** a physical object intended for the use and/or operation of an information asset (storage object, transmission object, processing object, destruction object, etc.)

3.9. **"Residual Risk of Information Security Breach":** the risk remaining after handling the risk of IS breaches.

3.10. **"Assessing the Risks of Information Security Breach":** the systematic and documented process of identifying, collecting, using and analysing information to assess the risk of IS breaches related to the use of information assets of a RF BS organisation at all stages of their life cycle.

3.11. **"Risk":** a measure that takes into account the probability of a threat and the amount of losses (damage) should this threat materialise.

3.12. **"Risk of Information Security Breach"; "IS Breach Risks"[1]:** the risk associated with the IS threat.

3.13. **"Information Security Threat"; "IS Threat":** the threat of violating such properties of IS as the availability, integrity or confidentiality of the information assets of a RF BS organisation.

3.14. **"Damage":** loss of assets, damage (loss of properties) of assets and/or infrastructure of the organisation, or other damage to assets and/or the infrastructure of a RF BS organisation occurring as a result of IS threats executed through IS vulnerabilities.

4. General Approach to Assessing IS Breach Risks

4.1. The information assets of a RF BS organisation are viewed in aggregate with the objects associated with them. In this, IS properties are provided to information assets by ensuring that the objects associated with them are completely secure.

4.2. IS threats are generated at their sources (IS Threat Sources), which may affect the objects associated with information assets within a RF BS organisation. If an IS threat successfully materialises, the information assets lose some or all of their IS properties.

4.3. The risks of IS breaches are assessed for the types of information assets (types of information) included in a pre-defined area of assessment. The following is pre-defined and documented in order to assess the risks of IS breaches:

- A complete list of information asset types contained in the assessment area;
- A complete list of the objects and their types associated with each type of information asset in the assessment area;
- A model of IS threats describing the IS threats for all types of associated objects selected in a RF BS organisation at all levels of the information infrastructure hierarchy of the RF BS organisation.

The list of threat sources and threat models should take into account the provisions of STO BR IBBS-1.0, as well as the list of the main sources of IS threats provided in Annex 1.

4.4. The list of information asset types is based on the results obtained from classifying the information assets of a RF BS organisation. The list of information asset types (classification of information) shall not contradict the provisions of Russian legislation, including the regulatory acts of the Bank of Russia.

[1] IS breach risks threaten the loss of the properties of information assets secured by IS as a result of the manifestation of IS threats that may result in damages incurred by a RF BS organisation.

The following list of information asset types in a RF BS organisation is used as an example:

- Restricted access information:
  - Information containing details that constitute a banking secret:
  - Payment information (information intended for settlement, cash and other banking and accounting operations);
  - Information containing details that constitute a trade secret:
  - Personal data;
  - Data used in the operation of payment, information and telecommunications systems (data used for the technical configuration of software and hardware systems for processing, storing and transmitting information);
- Open (public) information.

An RF BS organisation can modify this list in accordance with the approaches it has adopted to classify information assets and the level of detail it has established for types of information assets when assessing IS breach risks.

4.5. The lists of associated object types are generated in accordance with the hierarchy of information infrastructure levels in a RF BS organisation, as defined in STO BR IBBS-1.0. In particular, these lists might include the following types of associated objects:

- Communication lines and data networks;
- Network software and hardware, including network servers;
- Data files, databases, data warehouses;
- Information media, including paper media;
- Application software and system software;
- Software and hardware components to automated systems;
- Premises, buildings, and constructions;
- Payment and information processes.

4.6. IS breach risks are determined in accordance with qualitative assessments of:

- The probability of IS threats materialising (hereinafter, "PISM") as a result of identified and/or anticipated sources of IS threats subsequent to their impact on objects associated with the information asset types under examination;
- The severity of consequences from the loss of the IS properties of these information asset types (hereinafter, "SCLIS").

4.7. The assessment of PISM and SCLIS is based on an expert review performed by the IS service personnel within a RF BS organisation with the assistance of IT personnel. In addition, the assessment of SCLIS necessitates the input of those employees from the specialised units who use the information asset types under examination. The collaboration of the employees of these units is provided within the framework of a permanent work group, or an ad hoc work group established for the duration of the IS data breach risk assessment.

4.8. The expert review of PISM and SCLIS requires the assistance of employees of the RF BS organisation with the proper knowledge, education and experience.

4.8.1. The experts engaged for the assessment of PISM and SCLIS from among the employees of IS service or IT unit of RF BS organisation should possess the following:

Knowledge of the laws of the Russian Federation in the area of information security; knowledge of international and national standards in the area of information security;

Knowledge of regulatory acts and instructions issued by regulatory and supervisory authorities in the area of information security;

Knowledge of the internal documents of RF BS organisation regulating activities in the area of information security;

Knowledge of modern computing and telecommunication equipment, operating systems, database management systems, as well as a comprehension of specific methods for ensuring information security for such equipment and systems;

Knowledge of potential sources of IS threats, the methods used for implementing IS threats, and how often IS threats have materialised in the past;

Knowledge of methods used to provide information security to payment, information and telecommunication systems within a RF BS organisation;

An understanding of various approaches to information security, and knowledge of protection measures, and their inherent limits.

4.8.2. The experts engaged for the assessment of SCLIS from among the employees of specialised units should possess the following:

Knowledge of the laws of the Russian Federation in the area of their professional activities; knowledge of regulatory acts and instructions issued by regulatory and supervisory authorities in the area of their professional activities;

Knowledge of the internal documents of a RF BS organisation regulating their professional activities;

Knowledge of business processes in a RF BS organisation, as well as the arrangement of payment, information and technological processes in the area of their professional activities;

An understanding of the impact from potential IS incidents on the functioning of business processes in a RF BS organisation in the area of their professional activities;

Knowledge of the payment, information and telecommunication systems in a RF BS organisation in the area of their professional activities.

4.8.3. Each expert involved in assessing IS breach risks should possess the following qualifications:

Higher education;

Four years of continuous experience in his/her professional field; continuing education and maintenance of his/her knowledge base;

The ability to identify personnel in the RF BS organisation who can provide pertinent information as it is needed;

Business and management communication skills.

4.8.4. If the personnel in the RF BS organisation do not possess the necessary knowledge and experience to assess PISM, outside consultants or experts should then be engaged.

5. Procedures for Assessing the IS Data Breach Risks

5.1. The information defined in section 4.4 of this methodology represents baseline data for assessing IS breach risks.

5.2. The following procedures are performed to assess IS breach risks.

Procedure 1. List the types of information assets which require assessment of IS breach risks (hereinafter, the "Area requiring IS risk assessment").

Procedure 2. List the types of associated objects for each information asset type in the area requiring IS risk assessment.

Procedure 3. Identify the sources of threats for each object type defined in procedure 2.

Procedure 4. Define PISM for the associated object types defined in procedure 2.3

Procedure 5. Define SCLIS for the information asset types in the area requiring IS risk assessment.

Procedure 6. Assessing the risks of IS breaches.

5.3. **Procedure 1.** The area requiring IS risk assessment can be defined as:

– the complete list of information asset types within the RF BS organisation;

– the list of information asset types within a unit in the RF BS organisation;

– the list of information asset types corresponding to individual processes employed in the RF BS organisation as a whole, or within a unit in the RF BS organisation.

5.3.1. For each information asset type, define the list of essential IS properties which must be supported to ensure the information security maintenance system (IS Maintenance System) in a RF BS organisation.

For the purposes of this methodology, the key IS properties are as follows:

– Confidentiality;

– Integrity;

– Availability.

If necessary, other (additional) IS properties can be defined for specific types of information assets in a RF BS organisation.

5.3.2. The sample form provided in Annex 2 should be used to list the information asset types and their IS properties in the area requiring IS risk assessment.

5.4. **Procedure 2.** For each information assets type selected under procedure 1, prepare the list of associated object types. When preparing this list, categorize the associated object types by their level in the information infrastructure of the RF BS organisation.

The sample form provided in Annex 3 should be used to list the associated object types.

5.5. **Procedure 3.** For each associated object type defined in the procedure 2, list the sources of threats that can lead to the loss of IS properties in corresponding information asset types. The associated object types and their identified sources of threats must match each other within the hierarchy of information infrastructure in a RF BS organisation.

The list of threat sources is generated based on the model of threats for the RF BS organisation. The initial list of threat sources recorded in the model of threats for the RF BS organisation (or additional partitions from compilations of new threat models for some of the delineated associated object types or specific associated objects) can be expanded.

When generating the list of threat sources, consideration should be made of the variations as regards their potential impact on the associated objects, which may result in the loss of IS properties in the corresponding information asset types (the ways in which IS threats are manifested). The RF BS organisation defines the level of detail and order of grouping to be used when determining the ways in which IS threats are manifested.

5.5.1. The sample form for documenting the data and results of PISM assessment provided in Annex 4 should be used to document the results of procedure 3 (complete the fields Information asset type, Associated object type, Source of IS threats, IS properties of information asset type, Method of is threats materialising).

5.6. **Procedure 4.** To assess PISM, use the results of procedures 1, 2, 3 of this methodology and analyse the potential loss of each IS property for each information asset type from the impact of the selected threat sources on the corresponding associated object types.

5.6.1. The key factors for assessing PISM are as follows:

– Information on relevant models of threats, in particular:

– Location of the threat source relative to the corresponding associated object type;

– Information on the motivation of the threat source (for threat sources of an anthropogenic nature);

– Assumptions concerning the abilities and/or resources of the threat source;

– Statistics on the frequency of the threat generating from the source in the past;

– Information on methods used for generating IS threats;

– Information on the complexity of detecting threats generating from the given source;

– Information on the organisational, technical and other a priori security measures possessed by the associated object types.

5.6.2. To assess PISM, use the following qualitative degree scale:

– Null;

– Minimum;

– Medium;

– High;

– Critical.

When engaging several experts to assess PISM and obtain various expert assessments, the final, summary assessment of PISM should be equal to the expert assessment defining the highest degree of PISM.

5.6.3. The data used as a basis for assessing PISM and its results should be documented by using the sample form for documenting the data and results of PISM assessment provided in Annex 4 (complete the fields "The priori protection measures that are used", "Other data to determine PISM, PISM assessment").

5.7. **Procedure 5.** To assess SCLIS, use the results of procedures 1, 2, 3 of this methodology and analyse the potential loss of each IS property for each information asset type from the impact of the selected threat sources on corresponding associated object types.

5.7.1. The key factors for assessing SCLIS are as follows:

– Degree of impact on the business continuity of a RF BS organisation;

– Degree of impact on business reputation;

– Amount of financial and material losses;

– Amount of financial and material costs required to restore IS properties for the type of information asset under consideration and to eliminate the consequences of the IS breach;

– The human resources required to restore IS properties to the type of information assets under consideration and to eliminate the consequences of the IS breach;

– The time required to restore IS properties to the type of information assets under consideration and to eliminate the consequences of the IS breach;

– The extent to which the legal requirements and/or contractual obligations of a RF BS organisation have been violated;

– The extent to which the requirements of regulatory and controlling (supervisory) authorities in the area of IS, as well as the requirements of the regulatory acts of the Bank of Russia have been violated;

– The quantity of stored, transmitted, processed, and destroyed information corresponding to the given associated object type;

– Information on the organisational, technical and other a posteriori protection measures contained in the given associated object type.

5.7.2. To assess SCLIS, use the following qualitative degree scale:

– Minimum;

– Medium;

– High;

– Critical.

When engaging several experts for assessing SCLIS and obtaining various expert assessments, the final, summary assessment of SCLIS should be equal to the expert assessment defining the highest SCLIS.

5.7.3. The data used as a basis for assessing SCLIS and its results should be documented by using the sample form for documenting the data and results of SCLIS assessment provided in Annex 5.

5.8. **Procedure 6.** The risks of IS breaches are assessed by comparing the assessments of PISM and SCLIS of the eventual manifestation of corresponding IS threats.

The risks are assessed for all the IS properties of the selected information asset types and all the corresponding combinations of associated object types, along with the sources of threats that affect them.

To assess the risks of IS breaches, use the results of procedures 4 and 5 of this methodology.

5.8.1. To assess the risks of IS breaches, use the following qualitative degree scale:

– Acceptable;

– Unacceptable.

5.8.2. To compare the assessments of PISM and SCLIS, complete the table of acceptable/unacceptable risks of IS breaches. An example of how to complete the table is provided in Table 1. The risks of IS breaches are assessed based on the information in the table.

Table 1. Acceptable/Unacceptable Risks of Information Security Breaches

PISM	**SCLIS**			
	Minimum	**Medium**	**High**	**Critical**
Null	Acceptable	Acceptable	Acceptable	Acceptable
Minimum	Acceptable	Acceptable	Acceptable	Unacceptable
Medium	Acceptable	Acceptable	Unacceptable	Unacceptable
High	Acceptable	Unacceptable	Unacceptable	Unacceptable
Critical	Unacceptable	Unacceptable	Unacceptable	Unacceptable

5.8.3. The results of assessing the risks of IS breaches should be documented by using the sample form provided in Annex 6.

6. The Quantitative Assessment of the Risks of IS Data Breaches

6.1. The risks of IS breaches can be assessed in monetary terms. The quantitative, or monetary assessment of the risks of IS breaches is made to establish the recommended reserves for possible losses associated with IS incidents, and is determined by a quantitative assessment of the following:

– PISM expressed in quantitative form (percentage) (hereinafter, "$PISM_Q$");

– SCLIS expressed in quantitative (monetary) form (hereinafter, "$SCLIS_Q$").

6.2. The assessments of $PISM_Q$ are prepared by an expert translation of the qualitative assessments of PISM obtained in procedure 4 to their quantitative equivalent in accordance with the following recommended scale:

Table 2. Recommended Matching Scale of PISM and $PISM_Q$

PISM	$PISM_Q$
Null	0 %
Minimum	1 – 20 %
Medium	21 – 50 %
High	51 – 100 %
Critical	100 %

6.3. The data used as a basis for assessing $PISM_Q$ and its results should be documented using the sample form for documenting the data and results of $PISM_Q$ assessment provided in Annex 7.

6.4. The assessments of $SCLIS_Q$ are prepared by experts via the translation of the qualitative assessments of SCLIS obtained in procedure 5 to their quantitative equivalent in accordance with the following recommended scale:

Table 3. Recommended Matching Scale of SCLIS and $SCLIS_Q$

SCLIS	$SCLIS_Q$
Minimum	Up to 0.5 % of the capital of the RF BS organisation
Medium	From 0.5 % to 1.5 % of the capital of the RF BS organisation
High	From 1.5 % to 3.0 % of the capital of the RF BS organisation
Critical	More than 3.0 % of the capital of the RF BS organisation

6.5. The data used as a basis for assessing $SCLIS_Q$ and its results should be documented using the sample form for documenting the data and results of $SCLIS_Q$ assessment provided in Annex 8.

6.6. The quantitative assessments of IS breach risks are calculated for all IS properties of the selected information asset types and all the corresponding combinations of environmental objects and their threat sources by multiplying the $PISM_Q$ assessments by the $SCLIS_Q$ assessments.

6.7. The results of the quantitative assessment of IS breach risks should be documented using the sample form provided in Annex 9.

6.8. The total quantitative assessment of IS breaches in a RF BS organisation is calculated as the sum of quantitative assessments covering all individual risks of IS breaches. A reserve should be established for possible losses related to IS incidents in an amount equal to the total quantitative assessment of IS breach risks.

RS BR IBBS-2.2-2009

Annex 1
Recommended List of Classes, Main Sources of IS Threats and Their Description

Source of IS Threats	Description
Class 1: Sources of IS threats associated with adverse events of a natural, technological or social character	
Fire	Uncontrolled combustion process accompanied by destruction of property and posing a danger to human life. Possible causes: arson, spontaneous combustion, natural phenomena
Natural disasters, emergencies and calamities	Destructive natural phenomena (floods, earthquakes, volcanic eruptions, hurricanes, tornadoes, typhoons, tsunamis, etc.)
Man-made disasters	Destructive processes that develop as a result of a disruption in the normal interaction of technological objects with each other or with the components of the environment leading to a loss of life, destruction of or damage to facilities and environmental components
Disruption of indoor climate conditions	Adverse changes in the climate inside the premises hosting the hardware and/or personnel: considerable changes in temperature and humidity, increased levels of carbon dioxide, dust, etc. Possible consequences: disruptions, hardware failures and accidents, decreased performance and damage to personnel health, disruptions to process continuity, reductions in the quality of information services
Power failure	Disruption or a reduction in the power supply. Possible causes: man-made disaster, natural disaster, natural phenomenon, a terrorist act, fire, etc. Possible consequences: faults and failures in equipment
Malfunctions in life-support systems	Failures and accidents in water supply, sewage, and heating systems
Threats to the health of personnel	Threats to the health of personnel resulting from radiation, biological, mechanical, thermal, chemical and other impacts from the environment, engineering infrastructure facilities, hardware, food poisoning, industrial injuries. Possible causes: man-made or natural disasters, accidents in objects belonging to engineering infrastructure, equipment malfunctions, failures to comply with safety regulations and labour safety, health regulations, etc. Possible consequences: staff shortages, cash payouts, litigation
Class 2: Sources of IS threats associated with the activities of terrorists, criminals and lawlessness	
Public disorder, vandalism, riots, political instability	Destruction of or damage to the property of a RF BS organisation
Terrorist acts	Explosions, arson or other acts aimed at intimidating the public and endangering the lives of people resulting in significant property damage or other serious consequences, aimed at influencing the decisions adopted by the RF BS organisation, as well as threats to commit such acts for the same purposes
Industrial espionage	The transmission, collection, theft or storage of the information assets of a RF BS organisation with the aim of inflicting damage on the RF BS organisation
Intimidation and blackmail	Forcing the personnel of a RF BS organisation to perform unauthorised actions by blackmail, physical violence or violence against relatives
Social engineering	Deliberate actions of third parties for fraudulent purposes and implemented by way of deception, misrepresentation aimed at employees of a RF BS organisation. Possible consequences: employee errors, disruption of property, loss of information assets, breach of process continuity, a drop in the quality of information services
Class 3: Sources of IS threats associated with the activities of suppliers / service providers / partners	
Dependence on partners/customers	Dependence on partners forces the organisation to rely on their information security, and so the organisation must be confident that the partner is able to ensure adequate security, or else take into account this source of threats
Errors made at the conclusion of contracts with providers of	Inaccuracies and uncertainties in the contract with the provider of external

Source of IS Threats	Description
external services	services which can create problems in the customer's business operations
Breaches of contractual obligations by third parties	Failure by third parties to perform their obligations for quality, composition, content, and/or the provision of services, supplying products, etc. For example, failure of developers, suppliers of software, hardware and services or external users to comply with requirements
Errors in ensuring the security of information systems at various stages of their life cycle	Errors in ensuring safety during the development, operation, follow-up and decommissioning of information systems
Development and use of low-quality documentation	Poorly documented descriptions of the procedures for processing, storage, data transmission, manuals for personnel involved in these processes, as well as inadequate descriptions of IS tools and poorly-written user manuals
The employment of software tools and information lacking source guarantees	The use of unverified data or unlicensed software in the organisation's information system
Class 4: Sources of IS threats associated with faults, failures, destruction/damage of software and hardware	
Excessive loads	Unintentionally excessive load on the computing and network resources of the system. Employees performing more operations than allowed by psycho-physiological standards. Possible causes: inadequate computing and/or throughput capacity, poor management of business processes. Possible consequences: hardware faults and failures, disruption of hardware availability, human error, damage to health
Destruction/damage, breakdowns in hardware and communication channels	Physical destruction/damage of hardware (communication channel), or certain combination of failures of its elements resulting in malfunctions associated with particularly significant technical losses, which make it impossible to operate the hardware (communication channel) as a whole over a considerable period of time. Possible causes: the impact of external (physical unauthorised access, terrorist act, man-made disaster, natural disaster, natural phenomena, riots) and/or internal (significant failures in hardware elements) factors. Possible consequences: breach of information asset properties, their loss, disruption of process continuity, a drop in the quality of information services
Faults and failures in hardware	Software malfunctions Possible causes: invalid change to parameters or properties of software due to internal processes (errors) and/or external impact from malicious software, agency, and hardware. Possible consequences: breach of information asset properties, disruption of process continuity, a drop in the quality of information services
Faults and failures in hardware and communication channels	Interruption in the availability of hardware or its failure to perform its functions within the predefined range. Possible causes: invalid change in the characteristics of hardware impacted by internal processes, the complexity of hardware, staff shortages, inadequate maintenance. Possible consequences: faults, software failures, system crashes, disruption in availability of information assets, disruption of process continuity, a drop in the quality of information services
Breaches in the functionality of the cryptographic system	Accidental or intentional mismanagement of cryptographic keys, cryptographic protocols and algorithms, software and hardware used for cryptographic information protection systems that leads to a loss in the confidentiality, integrity and availability of information, a disruption in the failure-free reception and transmission of information, the blocking of payment and information management systems in the RF BS organisation
Breaches in the functionality of the archiving system	Breach in the confidentiality and integrity of archived data and/or failure in the services of the archiving system (breach in availability) resulting from accidental user errors or mismanagement of the archiving system, and also as a result of physical impacts on the components of the archiving system

Class 5: Sources of IS threats associated with the activities of internal violators of IS	
Bad-faith performance of duties	Deliberate failure of employees to perform some of their duties or negligent performance of such duties
Negligence	Failure to perform or improper performance by an person of responsibility of his/her duties as a result of bad-faith or a negligent attitude
Damage to property	Intentional damage to information assets by personnel. Primarily, the sabotage may be directed against hardware and software, as well as against information assets. Possible consequences: damage caused by the breach of the asset's properties, including their corruption and destruction
Human error	Any actions by personnel that do not comply with the established rules or personnel practices that are committed without malice. Possible causes: insufficiently defined responsibilities, negligence, lack of training or unqualified personnel. Errors are facilitated by the lack of a disciplinary process and documenting of processes, provision of unwarranted authority, the deliberate use of social engineering methods with regard to personnel Possible consequences: breach in confidentiality and integrity of information, loss of information assets, disruption of process continuity, a drop in the quality of information services, hardware and software faults and failures
Theft	Illegal uncompensated seizure and/or use of the property of a RF BS organisation committed for mercenary purposes and causing damage to the owner or other holder of such property
Execution of malicious software	Introducing and executing malicious software in the system: software back doors, Trojans, software viruses and worms, etc. Possible causes: carelessness, negligence, unqualified personnel (users), vulnerabilities in software tools. Possible consequences: unauthorised access to information assets, breaches of their properties, faults, failures and destruction of software, disruption of process continuity, a drop in the quality of information services
Use of information assets other than for their intended purpose	Intentional use of information assets of an organisation for purposes other than those established by the organisation. Possible causes: lack of supervision over personnel. Possible consequences: lack of computing, networking, or human resources, direct damage to the organisation
Violations of IS arrangements by personnel	Failure of personnel to comply with the requirements of internal documents regulating IS activities
Errors in personnel management	Errors in personnel management include hiring unskilled employees, dismissal/transfer of employees without corresponding IS procedures, failure to conduct or sporadic conduction of training and personnel checks
Class 6: Sources of IS threats associated with the activities of external violators of IS	
Actions by an unauthorised entity	Deliberate actions on the part of the entity acting from an environment that is outside the IS area. Possible consequences: corruption and destruction of hardware and software, introduction and execution of malicious software, breach of properties, loss of information assets and services
False report about a threat	False report about a threat, such as a fire, terrorist act, man-made disaster, civil riots, etc. Possible consequences: breach of information asset properties, their loss, disruption of process continuity, a drop in the quality of information services
Uncontrolled destruction of the information asset	Unintentional destruction of information assets. Possible causes: equipment failures, natural factors and technogenic disasters. Possible consequences: direct damage to the organisation
Uncontrolled modification of the information asset	Unintentional changes made to information assets. Possible causes: equipment failures, natural factors and technogenic disasters. Possible consequences: disruption of process continuity, direct damage to the organisation
Unauthorised logical access	Unauthorised logical access by unauthorised entities to components of the unit and information assets. Possible causes: password compromises, allowing

	users/administrators excessive access rights, shortcomings (lack) of mechanisms for user and administrator authentication, administrative errors, unattended software and hardware. One method of gaining unauthorised access to the system is through the deliberate introduction of malicious software to steal passwords for logging into the system or to acquire access rights. Possible consequences: breach of information asset properties, faults, failures and breakdowns in software and hardware, disruption of process continuity and/or a drop in the quality of information services
Unauthorised physical access	Unauthorised physical access by unauthorised parties to controlled areas hosting the hardware and/or information assets. Possible causes: potentially through bypassing physical access control or by using lost/stolen access tools. Possible consequences: corruption and destruction of hardware and software, breach of the information asset's confidentiality, integrity, and availability, disruption of process continuity and/or a drop in the quality of information services
Class 7: Sources of IS threats associated with non-compliance with the requirements of supervisory and regulatory authorities, applicable laws	
Non-compliance of internal documents with the applicable laws	Non-compliance of activities may lead to administrative and criminal sanctions imposed by judicial, supervisory and regulatory authorities on the unit's responsible parties, and the cessation of certain types of activities
Variation and inconsistency in the requirements established by supervisory and regulatory authorities, higher authorities	Instability, differences and conflicts in the content of requirements and/or procedures established for complying with such requirements can upset the activities of the unit or its individual services, reduce their efficiency and quality, and sometimes impede their performance. This contributes to "blurring" or overlaps in the areas of responsibility established for employees and services, the juggling by officials and services of rights and obligations to the detriment of general activities. It leads to a redistribution of resources in favour of that activity (which is often not the key activity) which is the most sensitive for the organisation (the administrator) in terms of the punishment for non-compliance

Annex 2
Sample Form for Documenting the List of Information Asset Types and Their IS Properties in the IS Risk Assessment Area

Example of completion:

Information asset type – "Restricted Access Information" (hereinafter, "Restricted Information")

Information asset type	Information security properties			
	Confidentiality	Integrity	Availability	Other IS properties (if required)
"Restricted Information"	+	+	+	–
…				
…				

Note:

IS properties that must be supported as part of the IS Maintenance System of the RF BS organisation for the information asset type are marked by a "+" sign; the other IS properties are marked by the "-" sign.

Annex 3
Sample Form for Documenting the List of Associated Object Types

Example of completion:

Information asset type – "Restricted Information"

Information asset type	Levels of information infrastructure hierarchy	Associated object types
"Restricted Information"	Physical level	Communication lines, hardware and technical equipment, physical media
	Network level	Routers, switches, hubs
	Network application and service level	Software components for data transmission over computer networks (network services)
	Operating system level	Data files with "Restricted Information"
	Database management system level	Databases with "Restricted Information"
	Banking process application and service level	Application to access and process "Restricted Information", paper media

Annex 4
Sample Form for Documenting the Data and Results of PISM Assessment

Example of completion:

Information asset type – "Restricted Information"
IS property – "Confidentiality";
Method of threat materialising – "Unauthorised copying";
Associated object type – "Data Files with Restricted Information";
Threat sources - "Internal Violator" and "External Violator".

Information asset type	Associated object type	Source of IS Threats	IS properties of an information asset	Method used for executing IS threats[1]	Used a priori protection measures	Other data defining PISM	PISM assessment
"Restricted Information"	Data files with "Restricted Information"	Internal violator	Confidentiality	Unauthorised copying	Personnel management. Monitoring and logging access to data files. Using antivirus protection	User with access rights to data files can commit illegal acts	**High**
		...					
		External violator	Confidentiality	Unauthorised copying	Controlling and logging access to data files. Arranging physical security for buildings and premises. Using antivirus protection	No data	**Minimum**

Note:
In the "PISM assessment" cells, specify a value from the following list: Null; Minimum; Medium; High; Critical.

[1] The level of detail and grouping procedure for considering the methods of IS threat materialising are defined by the RF BS organisation.

Annex 5
Sample Form for Documenting the Data and Results of an SCLIS Assessment

Example of completion:

Information asset type – "Restricted Information"
Associated object type – "Data Files with Restricted Information";
Threat sources - "Internal Violator" and "External Violator"

Information asset type	Associated object type	Source of IS Threats	IS properties of information asset	Used a posteriori protection measures	Other data defining SCLIS	SCLIS assessment
"Restricted Information"	Data files with "Restricted Information"	Internal violator	Confidentiality	Not used	No data	**High**
			Integrity	Backup and checksumming of data files	No data	**Medium**
			Availability	Backup of data files	No data	**Medium**
			Other IS properties (if required)			
		…				
		External violator	Confidentiality	Not used	No data	**High**
			Integrity	Backup and checksumming of data files	No data	**Medium**
			Availability	Backup of data files	No data	**Minimum**
			Other IS properties (if required)			

Note:
In the "SCLIS assessment" cells, specify a value from the following list: Minimum; Medium; High; Critical.

Annex 6
Sample Form for Documenting the Data and Results of the Assessment of the Risk of IS Breaches

Example of completion:

Information asset type – "Restricted Information"
IS property – "Confidentiality";
Method of threat materialising – "Unauthorised copying";
Associated object type – "Data Files with Restricted Information";
Threat sources – "Internal Violator" and "External Violator"

Information asset type	Associated object type	Source of IS Threats	IS properties of information asset	Method of IS threat materialising	PISM assessment	SCLIS assessment	Assessment of the risks of IS breaches
"Restricted Information"	Data files with "Restricted Information"	Internal violator	Confidentiality	Unauthorised copying	High	High	**Unacceptable**
		…					
		External violator	Confidentiality	Unauthorised copying	Minimum	High	**Acceptable**

Note:
In the "Assessment of the risk of IS breaches" cells, specify a value from the following list: Acceptable; Unacceptable.

Annex 7
Sample Form for Documenting Data and Results of $PISM_Q$ Assessment

Example of completion:

Information asset type – "Restricted Information"
IS property – "Confidentiality";
Method of threat materialising – "Unauthorised copying";
Associated object type – "Data Files with Restricted Information";
Threat sources – "Internal Violator" and "External Violator"

Information asset type	Associated object type	Source of IS Threats	IS properties of information asset	Method of IS threat materialising	Used a priori protection measures	Other data defining $PISM_Q$	$PISM_Q$ assessment
"Restricted Information"	Data files with "Restricted Information"	Internal violator	Confidentiality	Unauthorised copying	Personnel management. Monitoring and logging the access to data files. Using antivirus protection	User with the right to access the data files can commit an illegal act	**56 %**
		…					
		External violator	Confidentiality	Unauthorised copying	Controlling and logging access to data files. Arranging physical security for buildings and premises. Using antivirus protection	No data	**15 %**

Annex 8
Sample Form for Documenting Data and Results of $SCLIS_Q$ Assessment

Example of completion:

Information asset type – "Restricted Information"
Associated object type – "Data Files with Restricted Information";
Threat sources – "Internal Violator" and "External Violator"

Information asset type	Associated object type	Source of IS Threats	IS properties of the information asset	Used a posteriori protection measures	Other data defining $SCLIS_Q$	$SCLIS_Q$ assessment (RUB)
"Restricted Information"	Data files with "Restricted Information"	Internal violator	Confidentiality	Not used	No data	**7 million**
			Integrity	Backup and checksumming of data files	No data	**4 million**
			Availability	Backup of data files	No data	**3 million**
			Other IS properties (if required)			
		…				
		External violator	Confidentiality	Not used	No data	**9 million**
			Integrity	Backup and checksumming of data files	No data	**4 million**
			Availability	Backup of data files	No data	**0.5 million**

Annex 9
Sample Form for Documenting Data and Results of Quantitative Assessment of the Risks of IS Breaches

Example of completion:

Information asset type – "Restricted Information"
IS property – "Confidentiality";
Method of threat materialising – "Unauthorised copying";
Associated object type – "Data Files with Restricted Information";
Threat sources – "Internal Violator" and "External Violator"

Information asset type	Associated object type	Source of IS Threats	IS properties of information asset	Method of IS threat materialising	$SCLIS_Q$ assessment (RUB)	$PISM_Q$ assessment	Assessment of the risks of IS breaches
"Restricted Information"	Data files with "Restricted Information"	Internal violator	Confidentiality	Unauthorised copying	**7 million**	**56 %**	**3.92 million**
		…					
		External violator	Confidentiality	Unauthorised copying	**9 million**	**15 %**	**1.35 million**

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