BANK OF RUSSIA RECOMMENDATIONS ON STANDARDISATION

RS BR IBBS-2.5-2014

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

MANAGEMENT OF INFORMATION SECURITY INCIDENTS*

Effective date: 2014-06-01

Official publication

Moscow
2014

Foreword

1. ADOPTED AND ENACTED by Bank of Russia Directive No. R-400 of 17 May 2014.

Table of Contents

Introduction

The purpose of the current Bank of Russia standard, "Maintenance of Information Security of the Russian Banking System Organisations. General Provisions" (hereinafter "STO BR IBBS-1.0") is to create and satisfactory maintain an Information Security Maintenance System (hereinafter "IS Maintenance System") for the Russian Federation (hereinafter "RF") Banking System (hereinafter "BS") organisations and to reduce the severity of repercussions from IS violations per the organisation's requirements for detecting and responding to Information Security (hereinafter "IS") incidents.

The Bank of Russia Recommendations on Standardisation establish a strategy for implementing an incident detection and response process for Russian banking system organisations, which is an integral part of their IS management system (IS Management System).

BANK OF RUSSIA RECOMMENDATIONS ON STANDARDISATION

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

MANAGEMENT OF INFORMATION SECURITY INCIDENTS

Effective date: 2014-06-01

1. Scope of Application

These Bank of Russia Recommendations on Standardisation apply to RF BS organisations that detect and respond to IS incidents in accordance with the requirements of STO BR IBBS-1.0.

These Bank of Russia Recommendations on Standardisation should be applied by directly using the provisions set forth herein, in detecting and responding to IS incidents, and by including references hereto and (or) directly using the provisions contained herein, in the internal documents of a RF BS organisation.

The provisions of these Bank of Russia Recommendations on Standardisation are optional. To detect and respond to IS incidents, a RF BS organisation may use other guidelines and (or) requirements.

2. Regulatory References

These Bank of Russia Recommendations on Standardisation include regulatory references to STO BR IBBS-1.0.

3. Terms and Definitions

These Bank of Russia Recommendations on Standardisation use the terms and definitions set forth by STO BR IBBS-1.0, and also the following terms and their respective definitions:

3.1. **IS Incident**: an IS event or a combination of IS events indicating a past, present or future IS threat resulting in:

- Failure of the IS Maintenance System of a RF BS organisation, including the failure of its information security facilities;
- Failure of a RF BS organisation to meet the requirements of Russian law, the rules and regulations of regulatory and supervisory authorities and RF BS internal documents regarding information security, or a violation of the IS Management System processes by a RF BS organisation;
- Failure of a RF BS organisation to carry out operational procedures;
- Damage incurred by a RF BS organisation and (or) its clients.

3.2. **IS Event**: a change in the status of an IS monitoring object or area, and the actions of the RF BS organisation's employees and (or) other persons who indicate a potential IS incident.

3.3. **IS Event Log**: an electronic log containing records of IS events, including the actions of users and personnel operating the automated banking system (ABS).

3.4. **IS Incident Management**: the timely detection of IS incidents and an adequate response to them which aims to minimise and (or) eliminate adverse consequences for the RF BS organisation and (or) its clients.

3.5. **IS Incident Closure**: actions taken by RF BS organisations' employees in response to IS incidents, which result in:

- The elimination of IS Maintenance System threats to a RF BS organisation caused by an IS incident;
- The elimination of the consequences of IS threats realised as part of an IS incident;
- The causes of atypical organisational behaviour by RF BS organisation employees and (or) other persons, abnormal operation of ABS or other facilities that are part of the information assets of the RF BS organisation, or atypical events in its banking operations.

3.6. **IS Incident Response Group** (hereinafter "ISIRG"): a permanent group of employees belonging to an RF BS organisation that respond to IS incidents per its procedure.

3.7. **IS Incident Classifier**: a document designating the methods for describing IS incidents, which utilises a set of IS incident parameter attributes.

3.8. **IS Incident Record**: an element of the centralised database for IS incidents containing a description of a specific IS incident in accordance with the IS incident classifier.

3.9. **IS Administrator**: an employee of an RF BS organisation responsible for IS monitoring and control of ABS security measures, auditing privileges and controlling the actions of ABS users and operating personnel.

3.10. **Information Asset Access Administrator**: the head of a structural unit or employee of an RF BS organisation responsible for providing access to information assets within the scope of powers granted by said organisation.

4. Designations and Abbreviations

ABS — Automated banking system;
RF BS — Russian Federation Banking System;
ISIRG — IS Incident Response Group;
IS — Information security;
IS Maintenance System — Information security maintenance system;
IS Management System — Information security management system;

5. General Provisions

5.1. In order to properly implement, operate, control and maintain IS incident management, it is recommended that the RF BS organisation introduce a number of IS incident management processes grouped in the form of the Deming cycle model: plan - do - check - act - plan...".

5.2. Planning in the IS incident management system involves the following measures:

– Development and documentation of the RF BS organisation's IS incident management policy;
– Determination of the organisational structure and roles of IS incident response processes;
– Establishment and documentation of IS incident detection and response rules;
– Selection of technical means, including information security facilities, to be used in the IS incident detection and response processes, and stipulation of the procedures for using such technical means, in the internal documents of the RF BS organisation;
– Determination of the control procedures for the IS incident detection and response processes.

5.3. Implementation of the IS incident management system includes the following core measures:

– Allocation of required resources and assignment of roles to perform the IS incident response processes;
– Training and raising the awareness RF BS organisations' employees, representatives of external organisations and clients of RF BS organisations who use its information infrastructure in detecting and responding to IS incidents;
– Carrying out IS incident detection and response activities.

5.4. IS incident management system analysis involves the following core measures:

– Analysing the actions of RF BS organisations' employees while fulfilling IS incident response processes;
– Determining areas and protocols of RF BS organisations' IS Maintenance System which may be refined, based on the results of its IS incident management processes;
– Determining areas and protocols of the IS incident management processes which may be improved.

5.5. Refining the IS incident management system involves the following core measures:

– Making decisions and initiating the improvement of IS incident management processes;
– Making decisions and initiating the improvement of RF BS organisations' IS Maintenance System. Direct implementation of IS incident management processes is carried out by planning and implementation within the scope of the IS incident management system.

Decisions on the improvement of RF BS organisations' IS Maintenance System are fulfilled as part of tactical and strategic improvements, which are set forth by the requirements of STO BR IBBS-1.0.

6. Recommendations for Planning IS Incident Management Systems

6.1. Recommendations for Developing and Documenting IS RF BS Organisations' Incident Management Policy

6.1.1 The IS incident management policy of RF BS organisations is set forth in the principles and key provisions stipulated in its internal documentation.

IS incident management policy is developed by the RF BS organisation's IS Service together and (or) with consultation of its IT department, legal department, subdivisions responsible for ensuring continuity of the organisation's banking processes, and its HR department, and is approved by the management of the said RF BS organisation.

6.1.2 The following provisions are recommended for IS incident management policy of RF BS organisations

1. Goals and objectives of IS incident management.

The main goals of IS incident management established by the RF BS organisation's policy should designate:

- The creation of conditions for the timely detection and prompt response to IS incidents, including their closing;
- The prevention and (or) mitigation of adverse effects on the banking operations of RF BS organisations and (or) their clients caused by IS incidents;
- Prompt improvement of RF BS organisations' IS Maintenance System.

The main objectives set by RF BS organisations' IS incident management policy and addressed by the management of security incidents should ensure the attainment of its stated objectives through:

- Timely detection of IS incidents;
- Prompt response to IS incidents in accordance with Russian law, Bank of Russia regulations, and regulations established by the internal documents of RF BS organisations;
- Coordination of actions taken by employees of RF BS organisations' structural units in the course of IS incident response processes, including the closing thereof;
- Maintaining a database of registered IS events and detected IS incidents;
- Accumulation and reuse of expertise in IS incident detection and response;
- Analysis, efficiency evaluation and improvement of RF BS organisations' IS incident management processes;
- Providing the management of RF BS organisations with information and reports on IS incident management processes, including information about IS incident detection and the results of the response on them.

2. General description of IS events and criteria for classifying IS events as IS incidents. IS events should be described by forming a list of IS event types for each level of RF BS organisations' information infrastructure as specified by STO BR IBBS-1.0.

3. General description of IS incident detection and response stages, the roles of RF BS organisations' employees who are involved in the stages of IS incident response, and organisational specifications of units of RF BS organisations' employees who are assigned the said roles.

It is recommended to consider the following stages of IS incident detection and response:

- The stages of detection, notification, and evaluation at which an IS incident is identified by an RF BS organisation analysing the said IS event and the criteria established by authorised employees of the RF BS organisation giving notification regarding an evaluation of the IS incident and decisions made on further response to the IS incident;
- The collection and documentation stage of IS incident-related information;
- The IS incident closing stage, including its localisation (prevention of its distribution) and the return of ordinary banking operations of the RF BS organisation, which had been negatively effected by the IS incident (if any) that was eliminated;
- The analysis stage of the collected IS incident-related information and the adoption of administrative decisions based on the results of IS incident response.

The stages of collection and documentation of information, IS incident closing, analysis of information, and adoption of administrative decisions in these recommendations are combined into a common term "IS incident response".

4. General description of the organisational structure of the IS incident response processes, specifying:

- The composition of RF BS organisations' subdivisions and employees which are assigned roles related to IS incident response;
- ISIRG requirements, including for the composition of its members;
- Roles of participants responding to security incidents;

– The principles and methods of interaction between the ISIRG and employees of RF BS organisations, within the framework of the IS incident response process.

6.2. Recommendations for Determining the Organisational Structure of IS Incident Response

6.2.1. The organisational structure of IS incident response should ensure all structural units of RF BS organisations achieve IS incident management goals and objectives To that end, a two-level organisational structure at central and branch (regional) levels is recommended for IS incident response.

6.2.2. The following tasks are implemented at the central level of IS incident response:

– Planning of RF BS organisations' IS incident response processes;
– Establishment of IS incident response rules;
– Control over RF BS organisations' IS incident response processes;
– Planning, control and coordination of joint ISIRG operations at various levels;
– General analysis of the results of IS incident response;
– Development of proposals for the adoption administrative decisions based on the results of IS incident response;
– Development of proposals for the improvement and control over the improvement of IS incident management processes;
– Detection and response to IS incidents at the head (central) structural unit of RF BS organisations, and response to IS incidents that have escalated from the regional level in accordance with the criteria established by the RF BS organisation.

6.2.3. The following care tasks are fulfilled at the branch (regional) level of IS incident response:

– Planning of IS incident response measures at the branch (regional) level;
– Control over compliance with the established IS incident response rules at the branch (regional) level;
– Detection and response to IS incidents at the branch (regional) level, and escalation of IS incidents to the central level in accordance with the criteria established by the RF BS organisation.

ISIRG establishes the basis of the organisational structure for IS incident response at each of the levels.

6.2.4. Central level ISIRGs coordinate and respond to incidents at the RF BS organisations' head (central) structural subunits, coordinates and controls responses to IS incidents at the regional level, in the event that they escalate to the central level. The core of central level ISIRGs should be formed from IS Service representatives and IT subunits of the RF BS organisation that has the powers required to allocate the employees of these departments to respond to IS incidents. It is recommended that the organisational structure, composition, obligations and powers of central level ISIRGs be determined by the Policy on ISIRG.

6.2.5. Branch (regional) level ISIRGs coordinate and respond to IS incidents within the scope of the relevant branch (region), and, if IS incidents cannot be processed through their own resources and the criteria specified by the RF BS organisation that escalates them to the central level ISIRG. The core of ISIRGs at the regional level should be formed from among IS Service representatives and IT departments having the necessary competences to respond to IS incidents.

The standard organisational structure, composition, obligations and powers of regional level ISIRGs should be determined at the central level based on a standard Policy on regional ISIRG.

6.3. Recommendations for Determining the Roles of the IS Incident Response Process

6.3.1 It is recommended to designate the roles of employees in connection with IS incident response and to appoint persons responsible for their performance in RF BS organisations. Among other things, it is recommended to identify the roles associated with the implementation of activities in the following stages:

– Notification and evaluation stage;
– Collection and documentation of information stage;
– IS incident closing stage;
– Analysis and adoption of administrative decisions based on the results of IS incident response.

6.3.2. It is recommended that persons responsible for implementation of the roles when responding to IS incidents are included in ISIRGs. If necessary, ISIRGs may be supplemented with outside experts that are hired on a temporary basis.

The actions of ISIRG members during IS incident processing should be determined by corresponding IS incident response rules.

6.3.3. It is recommended to establish the following ISIRG roles:

1. The role of the ISIRG Administrator is to organise and supervise IS incident response processes and ISIRG operations, and also to provide supervisory control over the competence and timeliness of RF BS organisations' response to IS incidents.

Among other things, the ISIRG Administrator shall:

– Initiate administrative decisions based on the results of IS incident response;

– Inform the management of RF BS organisations about detected IS incidents and the outcome of the response to them;
– Make decisions on conducting investigations based on the facts surrounding IS incidents, as well as the need to interact with external organisations and law enforcement agencies in the investigation of security incidents.

It is recommended that ISIRG Administrators are appointed from among the RF BS organisations' leadership.

2. ISIRG supervisors roles are to ensure day-to-day management of IS incident response.

ISIRG supervisors should be vested with administrative powers enabling him or her to manage and coordinate the participants of the IS incident processes in accordance with the established procedures. ISIRG supervisors duties include:

– Initialise IS incident response in ISIRG;
– Appoint a person within ISIRG to be responsible for responding to the detected and registered IS incidents;
– Coordinate the activities of ISIRG members responding to IS incidents;
– Attract the required skill sets within ISIRG to respond to IS incidents;
– Monitor compliance with regulatory documents while responding to IS incidents;
– Make decisions on whether IS incidents may be closed;
– Provide consultation and recommendations to the participants of the IS incident response process.

Moreover, the obligations of the ISIRG supervisor should include drawing up proposals for the improvement of IS incident response processes and revision of the respective rules.

ISIRG managers are the chief responsible parties for fulfilling IS incident response processes and their outcomes.

It is recommended that ISIRG supervisors are appointed from among RF BS organisations' leadership.

3. ISIRG dispatch operators act as a single entry point ensuring the collection of information about IS events and IS incidents that have been detected and (or) have taken place in RF BS organisations.

ISIRG dispatch operators must:

– Track (monitor) IS events using IS monitoring technology;
– Collect information about IS and (or) non-standard events that are potentially related to IS from employees of RF BS organisations;
– Conduct an initial evaluation of IS events to determine whether an IS event is an IS incident;
– Ensure and control the recording of IS events;
– If IS events are classified as IS incidents, they must be registered as such and the supervisors and (or) members of ISIRG must be informed.

4. ISIRG analysts with the required qualifications are responsible for responding to detected and registered IS incidents.

ISIRG analysts perform the following core functions:

– Secondary evaluation of IS events in order to confirm that the said IS events are indeed IS incidents and, if so, to respond to and investigate the IS incidents, including the collection and documentation of information, and the coordination and monitoring of the closing of the IS incidents;
– Alert RF BS organisation employees of IS incidents in accordance with the established rules;
– Interact with ISIRG dispatch operators and the ISIRG supervisors on issues regarding IS incident response;
– Propose the need for cooperation in the investigation of IS incidents with outside organisations and law enforcement agencies;
– Advancement of proposals based on the results of IS incident response, including proposals on the improvement of the RF BS organisations' IS Maintenance System, IS incident management processes, IS incident response rules, and internal documents relating to IS incidents.

It is recommended to combine ISIRG analysts into functional groups to meet the challenges of responding to specific types of IS incidents, for example IS incidents related to the impact of a malicious code or IS incidents occurring during remote banking operations.

It is recommended to appoint ISIRG analysts from among the employees of the IS Services or the RF BS organisations' IT Department.

5. ISIRG secretaries main task is to collect and analyse information in order to make and submit analytical reports of materials to the ISIRG supervisor and ISIRG Administrator, including:

– Collection and summarising of information about IS incidents, including IS events mistakenly recognised as IS incidents;
– Preparation of reports on recorded IS incidents, including IS events mistakenly recognised as IS incidents;
– Preparation of reports on the results of IS incident response and IS incident investigation.

There are no restrictions on assigning several ISIRG duties to one employee, however, it is not recommended to combine ISIRG positions for the development, modernisation and immediate operation of the ABS.

6.3.4. It is recommended to include representatives of the following RF BS organisations' structural units when assembling the ISIRG, and recruiting temporary IS incident response staff:

– Members of RF BS organisations' IS Service, which take part in all stages of IS incident response;
– Members of the IT Departments are recommended, in order to evaluate the effect (impact) of IS incidents on RF BS organisations' IT services and to develop solutions for the support and recovery of the same during an IS incident response;
– Members of the Legal Department should be added if there are grounds to believe that an IS incident may have legal consequences, including participation while gathering evidence, preparation of materials for law enforcement authorities or for the submission thereof to the court;
– Members of the PR and Media Relations Department should be added, if there are grounds to believe that it will be necessary to inform the media and public;
– Units of RF BS organisations that are able to ensure the continuity of banking operations, and employees who must be made aware of IS incidents and their consequences Moreover, the qualifications of employees from these units in mitigating compromises to banking operations of RF BS organisations in various circumstances should be considered when planning IS incident response. It is recommended that the rules for IS incident response and the recovery of banking operations in RF BS organisations are approved and allow for the possibility of employees from these units in the response to IS incidents;
– Members of subunits responsible for ensuring physical safety and access to the buildings and premises of RF BS organisations, should be included if there are grounds to believe that physical safety was infringed or that an IS incident involves coordinated unauthorised actions for logical and physical access to protected resources. Moreover, in the course of the IS incident response procedures, ISIRG members might require access to the buildings and premises for which an individual access mode is established;
– Members of RF BS organisations' HR Departments should be included if there are grounds to believe that response to an IS incident will require disciplinary measures to be imposed on employees whose actions led to the incident.

6.4. Guidelines for Establishing and Documenting the Rules for IS Detection and Response

6.4.1 RF BS organisations should establish and document operational rules at the following stages:

– Detection and notification of IS events;
– Evaluation of IS events, and detection and notification of IS incidents;
– Collection and documentation of information about IS incidents;
– IS incident closing.

The said rules are to be developed by the RF BS organisations' IS Service together and (or) by agreement with the IT Department, Legal Department, and subunits that are qualified to ensure the continuity of the RF BS organisation's business processes and HR department, and which is approved by the management of the RF BS organisation (for example, the ISIRG Administrator).

6.4.2 Regulations for the detection and notification of IS events are to include:

– A detailed list of IS events. Upon detection of the said events, the employees of the RF BS organisation shall notify a ISIRG dispatch operator;
– A detailed description of methods for initially documenting information about IS events by the employees of the RF BS organisation who identified them;
– A detailed description of the procedures for notifying and transferring documents containing information about the detected IS events to a ISIRG dispatch operator;
– A detailed description of the registration procedures for information about the detected IS event, that are to be used by ISIRG dispatch operators;
– A description of the procedures for storing the information about IS events, including in electronic form.

6.4.3 When compiling lists of IS events, it is recommended that they be grouped according to RF BS organisations' information infrastructure.

The main sources of IS events are:

– Hardware and software for monitoring the IS and controlling operation over the applied protective measures;
– Employees of RF BS organisations identifying IS events;
– Clients and partners of RF BS organisations (including employees of third party organisations) who have access to the information assets controlled (accessed) by RF BS organisations.

6.4.4 The recommended sources of information on RF BS organisations' IS events formed by IS monitoring of hardware and software facilities and on control over the applied protective measures are:

– IS management, control and IS monitoring journals;
– Operating system logs;
– Database management system logs;

– Application logs;
– Active network equipment logs;
– Registration logs of the information security facilities used, including facilities for protecting information from unauthorised access, malware protection facilities, monitoring journals from specialised software and hardware facilities designed for the detection of intrusions and network attacks, as well as software for verifying file integrity;
– Information on special physical access control devices, including closed circuit television systems, control, access management and security alarm systems;

6.4.5 A list of IS events identified by RF BS organisations' employees, clients and partners shall be compiled by experts and shall be regularly reviewed and updated, including the possible emergence of new threats to information security, information assets, various activities.

To determine the list of IS events, an approximate list of IS event types may be used as provided in Appendix 1 hereto, which is to be adjusted in accordance with the specifics of the activity of specific RF BS organisations.

6.4.6 Methods for the primary documentation of information about IS events must ensure the legal significance of collected information based on the following principles:

– Information collected about IS events is to be stored safely on read-only media;
– At least two persons are to be present when collecting information about IS events and their actions must be monitored;
– A description of service commands used to collect information about IS events is to be documented and stored together with the collected information;
– It is advisable to collect and analyse dated related to ABSs, services and (or) networks, for example network equipment and firewalls.

6.4.7 It is recommended to determine a single entry point for information about IS events occurring in the RF BS organisation which is the ISIRG dispatch operator.

All RF BS organisations' employees must be familiar with the IS events notification procedure. Moreover, RF BS organisations must define and implement procedures to inform clients and partners about the notification methods it uses when ID events relating to the RF BS organisation's activities are detected.

It is recommended to assign each IS events identified by RF BS organisations' employees, clients or partners, a unique identification number.

6.4.8 It is recommended to store information about detected IS events for the following periods of time:

– At least 5 years for IS events detected in the course of bank payment operations;
– At least 3 years for other IS events.

6.4.9 Regulations for evaluating IS events, detecting IS incidents and providing notification about IS incidents should include:

– Initial evaluation procedures and criteria for classifying IS events as IS incidents;
– The procedure for using the IS incidents classifier and initial classifications of IS incidents;
– Procedures for notifying managers and members of the ISIRG about detected IS incidents;
– Procedures and criteria necessary for escalating IS incidents to the central IS incident response level.

6.4.10 Initial evaluations of IS events and their classification as IS incidents are made by competent ISIRG dispatch operators who use their own judgement and criteria established by RF BS organisations to make their decisions.

It is recommended to classify IS events as IS incidents in the following cases:

– There is evidence that IS events violated Russian law, Bank of Russia regulations, payment system regulations, or internal documents of RF BS organisations;
– IS events indicate unauthorised and (or) unregulated actions with respect to the information assets of RF BS organisations;
– IS events indicate possible irregularities of RF BS organisations' banking operations;
– IS events indicate possible theft and (or) unauthorised transfer of monetary funds.

6.4.11 A single classification system for all IS incidents should be determined and used in responding to IS incidents. If an IS event is classified as an IS incident, its attributes are to be determined and recorded, and used to manage and control IS incident response processes The procedure for determining the attributes of IS incidents must be described in documents regulating the use of incident classifiers.

6.4.12. Detailed and specific instructions should be developed for ISIRG dispatch operators, regarding the notification of ISIRG managers and members about detected IS incidents and escalating IS incidents to the central IS incident response level.

6.4.13. When regulating actions, it is expedient to appoint members of the ISIRG to be responsible at all times for the corresponding IS indecent response operations.

6.4.14 It is recommended that regulations for the collection and documentation of information about IS incidents include:

– A detailed description of the sources that are to be used to collect information about the IS incident;
– A procedure for ISIRG members to use IS incident classifiers;

– A detailed description of methods for ISIRG members to document and store information about IS incidents.

6.4.15 It is recommended that a description of the sources of information about IS incidents are given for each level of RF BS organisations' information infrastructure, based on the list of IS incident sources, which are set forth by subclauses 6.4.3 and 6.4.4 hereof.

6.4.16 The protocol for documenting information about IS incidents must ensure the legal value of collected information based on the principles set forth by subclause 6.4.5 hereof.

The recommended retention period for information about IS incidents is set forth by subclause 6.4.7 hereof.

6.4.17 It is recommended that rules for IS incident closing include:

– The procedure and conditions for the functional escalation of security incidents and (or) recruitment of additional skill sets;
– Liaison protocol for ISIRG members and persons involved in IS incident closing;
– A detailed description of the protocol for documenting and storing IS incident response information, including IS incident closing, as well as the analysis of the causes of the IS incident;
– Protocol for notifying the management of RF BS organisations about the results of the IS incident analysis;
– procedures for preparing and sending information about IS incidents involving monetary transfers, to payment system operators, in accordance with the rules of said payment systems, and to the Bank of Russia, in accordance with Bank of Russia regulations.

6.5 Guidelines for Choosing IS Incident Detection and Response Equipment and Determining the Procedure for its Operation

6.5.1 The hardware (including software) used in detecting and responding to IS incidents (hereinafter the "Equipment") should include:

– Technical equipment used to generate data, which are sources of information about IS events and IS incidents as recommended by subclause 6.4.4 hereof;
– Technical equipment used for the centralised collection of information about IS events, correlating information about IS events, and detecting IS incidents based on established IS incident regulations (hereinafter "IS monitoring facilities");
– Technical equipment used for controlling the security measures applied by RF BS organisations;
– Technical equipment for the automation of IS response processes, including storage of information about IS events and IS incidents.

6.5.2 Equipment for monitoring and controlling IS protective measures must comply with the following basic functions:

– Tracking and registration of IS events to detect IS incidents;
– Aggregation of information obtained about IS events, correlation of information about IS events, detection of IS incidents based on the criteria and rules established by RF BS organisations;
– Monitoring of the information security equipment and detection of any deviations in their regular operation;
– Monitoring of users' and operating personnel's activities and identification of any violations in the operation of hardware.

6.5.3 It is expedient to establish requirements for the IS monitoring and safeguard control infrastructure that is used for reporting IS events by RF BS organisations, at their creation and (or) modernisation.

Using compensatory functions for generating information about IS events realised by other components of RF BS organisations' information infrastructure (for example by operating systems or database management systems) is encouraged in instances when applied software bought by a RF BS organisation does not have the functional capabilities of maintaining IS event registration logs and making adaptations.

6.5.4 Technical equipment for the automation of IS incident response processes must include the following functions:

– Storage and protection of information about IS events and IS incidents;
– Classification of IS incidents and determination of IS incident attributes in accordance with the IS incident classifiers used by RF BS organisations;
– Implementation of role-based access to information on IS security incidents by ISIRG members in accordance with the roles established for them within the ISIRG;
– Monitoring and control of IS incident response stages and control of compliance by the ISIRG members, per the established regulations for IS incident response.

6.5.5 The operating procedures for the hardware must allow for:

– A description of the hardware, including its composition (number), installation locations, and settings;
– A description of the hardware and the organisational measures required to ensure its operation;
– Operating instructions for the hardware, including those for updating its software, and for monitoring and controlling its settings;
– A description of the roles and functions of the personnel responsible for the operation of the hardware and for those exercising control over operations;

– Instructions for users and operating personnel, including the personnel responsible for control over the hardware's operation;
– Rules and procedures for controlling the operating personnel's access to the hardware;
– Requirements for the composition and content of the organisational and administrative documents necessary for the operation of hardware;
– Requirements for the organisational measures required to ensure the operation of the hardware, including measures for assigning the roles of the operating personnel, training, notification and raising the awareness of the operating personnel and users;
– A description of the rules and procedures for ensuring the information security when decommissioning ABS or upon completion of information processing.

6.5.6 It is recommended that RF BS organisations implement procedures to ensure the hardware settings comply with the operational documentation. It is not recommended that gatekeepers have sole and uncontrolled capabilities to change the hardware settings. All changes to the hardware settings should be controlled and performed under the control of the IS Service employees in accordance with the pre-approved program.

Access to information protocol configuration changes of hardware may only be accessed by the operating personnel (read-only), IS administrators and (or) employees of the IS Service.

6.5.7 It is recommended for RF BS organisations to implement procedures ensuring control of access to logs that contain information about IS events and IS incidents used in accordance with the recommendations set forth by subclause 6.4.4 hereof. Such logs are to be managed by authorised employees of the IS Service.

6.5.8 It is recommended for RF BS organisations to implement procedures ensuring the integrity of logs containing the information about IS events and IS incidents used in accordance with the recommendations set forth by subclause 6.4.4 hereof in the event of possible hardware and (or) software malfunctions or failures.

6.5.9 Full access to the data of the IS monitoring facilities is only provided to authorised ISIRG members and (or) IS Service employees.

6.5.10 In order to ensure information security when using hardware, the following are recommended:
– Prohibit unauthorised access to hardware;
– Protect against unauthorised deactivation of hardware;
– Protect against unauthorised changes to the list of IS events subject to registration;
– Retain an archive of files with IS monitoring data records and IS event registration logs;
– Protect against unauthorised editing or deletion of files with IS monitoring data records and IS event registration logs.

Frequent archiving and backup should be established by RF BS organisations' IS Services in consultation with its IT department.

6.5.11 The responsibilities for the operation and control of hardware should be reflected in the job descriptions of the RF BS organisations.

6.6 Guidelines for Defining Control Procedures over IS Incident Detection and Response Processes

6.6.1 It is recommended that RF BS organisations establish regulations for periodic monitoring in the following areas:
– Monitoring of compliance with the procedures for detection and timely notification of IS events;
– Monitor if the list of IS events is up to date;
– Monitor compliance of regulations on the initial documentation of information about IS events;
– Monitor the timely evaluation, classification, and notification of IS incidents;
– Monitor the use of IS incident classifiers;
– Monitor compliance with regulations for collecting and recording information about IS incidents;
– Monitoring the timeliness of measures to close security incidents, including their temporary escalation, and (or) the use of additional skill sets;
– Monitor the knowledgeability of RF BS organisations' IS incident detection and response employees, and ISIRG members;
– Monitoring of hardware operation.

6.6.2 It is recommended that organisation of the monitoring of compliance with IS incident detection and response processes is vested in the ISIRG Administrator, and the immediate performance of control measures should be conducted by the IS Service, with the involvement of RF BS organisations' employees, who are ISIRG members.

7. Recommendations for Implementing IS Incident Management Systems

7.1 Recommendations for allocating required resources and assigning IS incident response process roles

7.1.1 The following roles must be assigned within RF BS organisations:

– Central Level IS incident response roles;
– Regional level IS incident response roles;
– ISIRG members' roles;
– Roles of RF BS organisations' employees involved in closing IS incidents;
– Roles of RF BS organisations' employees operating hardware;
– Roles ensuring control over IS incident detection and response processes.

7.1.2 The ISIRG administrator should be in control of role assignment for IS incident response processes.

7.1.3 In order to provide more efficient use of personnel, less qualified staff should be used to identify and filter false alarms while more qualified employees should be assigned to processes requiring their skills, but only at process stages where their assistance is required.

7.1.4 These roles are to be provided with all the necessary resources that are required in order for them to fulfil their duties, including:

– Regulations for conducting corresponding activities;
– Required hardware;
– Time and material resources, including premises, office equipment, and work places.

7.1.5 It is recommended that role assignments and authority to perform the roles should be assigned by administrative acts of RF BS organisations, while the ABS access privileges, necessary for the implementation of roles should be provided based on requests that are subject to the approval of the corresponding administrators of the information assets.

7.1.6 When responding to IS incidents, the structural units of the RF BS organisations interact by including their representatives in ISIRG, and involving them in the IS incident response process. The procedure for enlisting RF BS organisation employees for the IS incident response process, including their powers, must be regulated.

7.1.7 The interaction of the RF BS organisations' structural units during the processing and investigation of IS incidents is organised by authorised ISIRG administrators.

7.2. Recommendations for Training and Raising Awareness about IS Incident Detection and Response

7.2.1 It is recommended that RF BS organisations implement a program that conducts regular training and raises awareness in the following key areas:

– Raise awareness of RF BS organisation employees about implementing regulations on the detection and notification of IS events, including the composition of IS events;
– Raise awareness about the order and procedures for notifying RF BS organisations of detected IS incidents, among the representatives of external organisations and clients who use its information infrastructure;
– Conduct training and raise the awareness about the collection, recording, and documentation of information about IS incidents and the use of the IS incident classifier, for ISIRG members and RF BS organisation employees who are involved in responding to IS incidents;
– Conduct training and raise the awareness of ISIRG members and the employees of RF BS organisations who are involved in responding to IS incidents, in order to help them acquire knowledge about the technical operation of RF BS organisations' information structure and enabling them to close IS incidents in a prompt manner;
– Provide employee training on the operation of hardware for subdivisions of RF BS organisations' IT Departments;
– Provide employee training on the control of hardware operations for RF BS organisations' IS Service.

7.2.2. It is recommended that RF BS organisations acquaint employees with the IS event notification procedure and the need to immediately notify the ISIRG dispatch operator about detected IS events. Employees should become acquainted with the following:

– A list or description of IS events, which must be reported;
– The notification format for IS events, including details essential for classifying IS incidents, and a description of response actions (for example, about the type of irregularities or violations, malfunctions, screen messages, or abnormal behaviour);
– Methods for initial documentation of information about IS events;

– Recommended actions in the event of clear IS violations, for example performance or, on the contrary, the prohibition of any actions other than the immediate notification of the ISIRG dispatch operator.

7.3. Recommendations for Carrying out IS Incident Detection and Response Activities

7.3.1 It is recommended to organise IS incident detection and response activities in accordance with the following general algorithm:

– Detection of IS events by employees of RF BS organisations and (or) hardware. Employees of RF BS organisations perform the initial documentation of information about detected IS events and notify ISIRG dispatch operators in accordance with the established procedure. Employees of RF BS organisations use a list of IS events supplied to them, to identify IS events. The hardware is used in accordance with the documentation agreed upon by the IS Services of RF BS organisations. Information about IS events that have been identified by clients and partners of RF BS organisations should also be submitted to ISIRG dispatch operators;
– This includes registration of information about IS events (including the collection of information related to IS events), and initial evaluations of the collected information performed by the ISIRG dispatch operators. The main objective of the initial evaluation is to determine whether an IS event is an IS incident, and, specifically, whether there has been an infringement of the IS or IS requirements established for the RF BS organisation. IS monitoring hardware is recommended to automatically detect IS incidents from the of information flow about IS events in accordance with the established rules of IS event correlation;
– And to provide notification of ISIRG members and (or) ISIRG supervisors about IS incidents executed by the ISIRG dispatch operator. Specific ISIRG analysts, and ISIRG functional group supervisors and (or) ISIRG supervisors are to be notified, depending on the character of the IS incident, which is based on criteria established by the operating procedures for ISIRG dispatch operators;
– Secondary evaluations of IS incidents are performed by ISIRG analysts to confirm or disprove that detected IS events are IS incidents;
– If a detected IS event is confirmed to be an IS incident, specific measures are taken for closing the IS incident, which may including the decision to escalate the IS incident, eliminate irregularities in the IS Maintenance System of the RF BS organisation, terminate the impact of the IS threat(s) that have been discovered, and the recovery of the RF BS organisation's banking operations;
– Escalation of IS incidents and the use of additional skill sets for its processing The necessity of escalation is determined by the ISIRG supervisor who, if necessary, appeals to the ISIRG administrator. Escalation may be hierarchical, if the powers of the ISIRG supervisor are not adequate to take the responsive actions to IS incidents that he/she deems necessary (for example, termination of certain banking operations), or functional, if specialists outside the ISIRG need to be involved. Hierarchical escalation also includes applying to Central Level ISIRG if an IS incident cannot be closed by an RF BS organisation’s branch-level ISIRG or, in other circumstances, for example if a branch-level ISIRG cannot close an IS incident within the established time limits;
– If an IS incident may lead to judicial proceedings against a person or organisation, or for a RF BS organisation to take disciplinary measures, all information pertaining to the IS incident is to be gathered, preserved, and presented for further analysis and possible acceptance by the court as evidence. Depending on the nature of IS incidents, it is desirable that IS event and incident logs are completely duplicated, provided that this may also be done after the IS incident is closed;
– A decision to close incidents must be approved by a ISIRG supervisor and only implemented after a full recovery of violations in the IS Maintenance System of the RF BS organisation, restoration of the RF BS organisation's banking operations, determination of the security implications and causation of all abnormalities in the RF BS organisation's business processes or unusual behaviour of its employees.

7.3.2 IS incident response is managed and information is recorded during IS incident response using the IS incident classifier. The IS incident classifier is used by RF BS organisations' employees who are involved in responding to IS incidents, so as to determine and record information about IS incidents (IS incident attributes) identified in the IS incident response process.

7.3.3 The IS incident classifier is used to formalise the archiving of IS incidents in the centralised IS Incidents Database (determining IS incident attributes) at the various stages of IS incident detection and response, as well as during implementation of the following activities:

– Initial processing of IS incidents carried out by a determination the values of selected IS incident attributes/signs (the values of these attributes are to be included in the IS incident record that was created);
– Management of the notification process for specific ISIRG members and managers, depending on selected IS incident attributes;
– Making a decision on the escalation of IS incidents, based on specific attributes of the IS incidents;
– Determining the values of the IS incident attributes by employees of RF BS organisations when responding to the IS incidents;

– Determining the values of the IS incident attributes based on the results of closing the IS incidents;
– Recording an incorrect (false) classification of an IS event as an IS incident.

7.3.4 When regulating the actions of ISIRG members and other employees of RF BS organisations responding to IS incidents, it is recommended to coordinate these activities with the recorded values of individual IS incident attributes, and to provide records of IS incidents in accordance with current security incident classifiers.

8. Recommendations for Conducting Analysis when Implementing IS Incident Management Systems

8.1 It is recommended that RF BS organisations establish and comply with the procedures for analysing IS incident detection and response processes. The above procedures should be performed by the employees of the RF BS organisation's IS Service under the general supervision of the ISIRG Administrator.

8.2 The analysis procedures are to be performed based on:
– Monitoring of IS incident detection and response processes;
– Analysis of statistical reports on IS incident detection and response;
– Analysis of IS incident records containing information about IS violations, the information assets affected by the IS incident, ABS, and the severity of consequences of the detected IS incidents.

8.3 As a result of the analysis, it is recommended to determine the most vulnerable segments and components of the RF BS organisation's information infrastructure from the point of view of IS incident exposure, the most significant IS vulnerabilities and deficiencies, and to evaluate the sufficiency of measures taken and resources allocated for IS incident response.

Moreover, it is recommended to analyse the tendencies that may indicate the necessity to improve the RF BS organisation' IS Maintenance System.

8.4 The actions taken by RF BS organisations' employees in response to IS incidents are subject to additional analysis. The purpose of the analysis is to make (initiate) improvements in terms of:
– Making corrections to the established IS incident detection and response procedures;
– Changing the composition of the ISIRG membership and adjusting the persons involved in IS incident response;
– Changing the requirements for the qualification of ISIRG members;
– Adjusting the procedure for interaction between the persons responding to IS incidents;
– Adjusting the hardware operation procedure.

8.5 It is expedient to use the results of the IS incident detection and response analysis as the basis for initiating and implementing tactical and strategic improvements of RF BS organisations' IS Maintenance System requirements, which are set by STO BR IBBS-1.0.

8.6 To determine the areas and methods of improving the IS incident management processes, it is recommended, after reviewing the documents and reports on IS incidents, to analyse the efficiency of the applied IS incident detection and response procedures, in particular:
– Evaluate the adequacy of the current composition of registered IS events and the necessity to correct it;
– Evaluate the adequacy of the applied IS incident classifier and the necessity to correct it;
– Evaluate the efficiency of the applied IS monitoring procedures;
– Evaluate the adequacy of IS incident response rules.

8.7 When developing proposals for improving the IS incident management processes, it is recommended to take into account:
– The available information about the relevant experience of third party organisations;
– Changes in Russian laws, the Bank of Russia regulations, payment system rules, and RF BS organisations' internal documents.

8.8 It is recommended that RF BS organisations establish procedures for informing their management about results from analysing IS incident management processes and of any significant IS incidents having substantially negative effects on RF BS organisations' business processes.

9. Guidelines for Classifying IS Incidents and Using IS Incident Classifiers in Their Processing

9.1 The main purpose of IS incident classification is to enhance consistency and to minimise subjectivity in implementing IS incident response processes by determining and recording the attributes of each IS incident for further use in the course of IS incident response and in analysing the IS incident management system.

9.2 When classifying IS incidents, it is recommended to describe IS incidents using a pre-established number of signs (attributes), while the attribute values must be specified as specific to certain rules.

9.3 The IS incident classifier used by RF BS organisations should allow adaptation, additions, and extensions for which the structure of the IS incident classifier is to ensure:

– Input of additional attributes or attribute values;
– Classification of newly detected IS incidents without breaking the integrity or changing the established classification processes.

9.4 Classification of IS incidents is required in order to define a set of attributes characterising IS incidents, and the values that each value can take.

The IS incident classification procedure involves assigning corresponding values to the classification attributes of specific IS incidents. In this case, not all attributes may be used for a specific IS incident or the values of some IS incident attributes may be determined gradually as incident response proceeds.

9.5 A set of attribute values for specific IS incidents is a record of the IS incidents that is entered in a centralised database of IS incidents. It is recommended to form and update a centralised database of IS incidents with a record format that is based on IS incident classifiers.

9.6 The roles for classifying IS incidents are assigned to ISIRG members and employees involved in responding to IS incidents.

9.7 It is recommended to classify IS incidents based on the following signs:

– Severity of consequences for RF BS organisations' operations (in money terms and point scale);
– Probability of a repeated IS incident;
– Types of sources of IS threats causing IS incidents;
– Character of IS incident occurrence (accidental, deliberate, erroneous);
– Types of information infrastructure objects involved (affected) in IS incident implementation;
– Information infrastructure level at which IS incident occurs;
– Information security properties that were compromised (confidentiality, integrity, availability);
– Types of IS incidents (completed IS incident, attempted IS incident, suspected IS incident);
– Area and effect of IS incident distribution (within the scope of one ABS, within an individual structural subdivision of a RF BS organisation, within a whole RF BS organisation, extending outside of a RF BS organisation);
– Complexity of IS incident identification;
– Complexity of IS incident closing;
– Other signs established by RF BS organisations.

9.8 The signs of IS incident classification should be determined subject to reporting forms that were created based on the results of IS incident classifications and provided by RF BS organisations per Russian law, Bank of Russia regulations, and payment system rules.

9.9 It is recommended to use IS incident classifiers at all stages of IS incident detection and response. It is recommended to establish a configuration of IS incident attributes that can be completed at each stage of IS incident response.

9.10 Appendix 2 hereto contains a sample IS incident classifier.

Appendix 1. Sample List of IS Event Types

Physical level of the information infrastructure:

- Physical access to the RF BS organisation's buildings and premises by employees and other persons;
- Physical access to and use of the RF BS organisation's computer equipment by employees and other persons;
- Use of copying and multifunctional devices by the RF BS organisation's employees and other persons;
- Use of facsimile devices by the RF BS organisation's employees and other persons;
- Changes in computer and telecommunication equipment settings;
- Changes in settings of computer equipment;
- Failures or breakdowns of computer and telecommunications equipment;
- Failures or breakdowns of computer equipment;
- Failures or breakdowns of information security equipment;
- Failures or breakdowns of the telephone communication network;
- Failures of data transmission networks;
- Physical impact on computer, telecommunication, and information security equipment or data transmission networks;
- Changes in the climatic conditions of premises in which the computer and telecommunication equipment are located;
- Changes in the operation parameters of data transmission networks;
- Replacement and/or modification of software and/or hardware of computer or telecommunication equipment;
- Actions with information media, including taking information media outside the RF BS organisation's facilities;
- Taking of portable computer equipment outside the RF BS organisation;
- Use of portable computer equipment within the territory of the RF BS organisation;
- Transfer of computer equipment among the RF BS organisation's divisions;
- Transfer of computer equipment to external organisations;
- Photo and/or video recording of RF BS organisation's premises by employees and other persons;
- Taking measures ensuring access to television security surveillance systems, security alarms, and access control and management systems;
- Events generated by television security surveillance systems, security alarms, and access control and management systems;
- Actions with information media and systems enabling physical access to the RF BS organisation's buildings and premises.

Level of network equipment:

- Changes in the settings of the network equipment and the software of the network equipment;
- Change of the composition and version of the network equipment software;
- Identification of abnormal network activity;
- Authentication and session termination on the network equipment;
- Identification of malicious code and its manifestations;
- Changes in the computer network topology;
- Connection of the equipment to computer networks;
- Failures of the network equipment software;
- Update of the network equipment software;
- Perform maintenance operations on the network equipment;
- Use vulnerability analysis tools to analyse the network equipment;
- Shutdown/reboot network equipment;
- Detection of "denial of service" attacks;
- Change and/or compromise of authentication data used to access network equipment;
- Failures of information security products;
- Changes in the operation parameters of information security products;
- Computer network launch analysis tools.

Level of network applications and services:

– Session identification, authentication, authorisation and termination for RF BS organisations' employees and other persons;
– Changes in software settings, composition and versions;
– Identification of malicious code and its manifestations;
– Set-up of connections and the processing of requests (including remote requests) at the level of network applications and services;
– Faults and failures in network applications and services;
– Perform operations related to the use and administration of network applications and services;
– Identification of atypical (abnormal) requests at the level of network applications and services;
– Shutdown/reboot or suspension of network applications and services;
– Operations for providing access to network applications and services, including email and Internet;
– Operations for achieving network applications and services data, including email data;
– Operations for the exchange of messages, including the exchange of payment messages;
– Failures in the exchange of messages, including in the exchange of payment messages;
– Distortion or modification of messages, including payment messages;
– Authentication of messages, including payment messages;
– Authentication of work stations participating in the exchange of messages, including payment messages;
– Termination/suspension of network applications and services by mistake;
– Distribution and/or collection of information using network applications and services;
– Perform operations with mailing lists and address books;
– Vesting the RF BS organisation's employees and/or other persons with user rights for a certain package of services, including Internet services and resources;
– Use of analysis tools to analyse the vulnerabilities of network applications and services;
– Change and/or compromise of authentication data used to access network applications and services;
– Failures of information security products;
– Redirection of messages, including payment messages;
– Distribution of information urging the client to provide information required to perform the actions on his or her behalf;
– External impacts from the Internet, including network attacks;
– Operations with data and key information encryption tools.

Operating system level:

– Authentication and termination of work of the RF BS organisation's employees and other persons, including at the levels of system software, database management systems and applied software, as well as ABS software (hereinafter the "operating system level software");
– Changes in the parameters of the configuration, composition and versions of the operating system level software;
– Start-up, stopping and (or) shutdown/reloading of the operating system level software;
– Identification of malicious code and its manifestations;
– Establishing connections and query processing using software-level operating systems;
– Failures of the operating system level software;
– Operations related to the use and administration of the operating system level software;
– Identification of non-typical requests using the operating system level software;
– Failures or breakdowns of information security equipment;
– Changes in the configuration parameters of information security facilities;
– Operations for providing access to the operating system level software and information resources processed using the operating system level software;
– Operations for archiving, backup, and recovery of information;
– Termination/suspension of the operating system level software by mistake;
– Use of analysis tools to analyse the vulnerabilities of the operating system level software;
– Change and/or compromise of authentication data used to access the operating system level software and information resources processed using the operating system level software;
– Changes in the configuration parameters of information security facilities;

– External impacts on the operating system level software from the Internet;
– Creation, authorisation, destruction or change of payment information;
– Creation, destruction or change of information resources, databases and/or other arrays of information;
– Compromise of authentication data and key information;
– Operations with data and key information encryption tools.

The level of a RF BS organisation's technical operations and applications, and business processes:

– Individual operations or procedures within the scope of the banking payment processes and information operations;
– Control of operations or procedures within the scope of the banking payment processes and information operations;
– Operations or procedures within the scope of banking payment processes and information operations using data encryption tools;
– Implementation of individual stages of the ABS lifecycle;
– Control over the fulfilment of individual stages of the ABS lifecycle;
– Allocation and assignment of roles, including roles for ensuring information security.

Appendix 2. Sample IS Incident Classifiers

IS incident attribute	Description of IS incident attribute values
Group 1. Registration attributes	
1.1 Unique IS incident identifier	Number or another identifier to refer to the IS incident
1.2 Date and time of IS incident detection	
1.3 Source of IS incident information	RF BS organisation's employee or hardware
1.4 Full name of the RF BS organisation's employee who identified the IS incident	
1.5 Subdivision of the RF BS organisation's employee who identified the IS incident	
1.6 Title of the RF BS organisation's employee who identified the IS incident	
1.7 Role of the RF BS organisation's employee who identified the IS incident	(user, ABS administrator, IS administrator, IS Service employee)
1.8 Contact information of the RF BS organisation's employee who identified the IS incident	employee's contact data
1.9 Hardware facility by means of which the IS incident was detected	
1.10 IS incident description	Message from the employee or information provided by TS
Group 2. Attributes describing the contents of the IS incident	
2.1 Non-compliance with IS requirements	- "no" - "document details, document clause"
2.2 Data about the person violating the IS requirements	- "no" - "Full name and title of the offender"
2.3. Malfunction of information security facilities (ISF)	- "no" - "IFS breakdown" - "ISF failure" - "unavailability of information critical for ISF functions (for example, breakdown of key information media)" - "ISF software integrity violation" - "deviation of ISF settings" - "deterioration in ISF functionality (parameters)"
2.4 IS threat realisation	- "no" - "identifier of the source of the threat based on the threat model or the current list of actual IS threats"

2.5. Violation of the security properties	- "no" - "Confidentiality" - "Integrity" - "Availability" - "Other properties"
2.6 Non-standard (unauthorised) behaviour	- "no" - "violation of the established order or day schedule"; - "deviation from the current order or the mode of use of information resources"
2.7 Character of IS incident	- "accidental" - "deliberate" - "erroneous"
2.8 Type of IS incident	- "completed IS incident" - "attempted IS incident" - "suspected IS incident"
2.9. Difficulty of detection IS incident detection	- "Ordinary" - "High"

IS incident attribute	Description of IS incident attribute values
Group 3. Attributes describing the impact on information infrastructure facilities	
3.1 Type of information assets affected by the IS incident	- "none" (information assets not affected); - "payment information" - "financial and analytical information" - "service information" - "management information (general and special purpose" - "reference information" - "Information and telecommunication operating environment"
3.2. Affected information infrastructure facilities	- "none" - "data transmission lines and networks" - "network software and hardware facilities" - "other hardware" - "data files, databases" - "information media (including paper media)" - "Applications and system-wide software" - "Software and hardware components of automated systems" - "premises, buildings, structures, utility lines and systems" - "work stations"
3.3 Characteristics of banking operations	- "none" (no information or operations affected by the IS incident) - "payment operations" - "information operations"
3.4 IS incident level	- "physical" - "network" - "operating system" - "database management systems" - "banking operations and applications" - "organisation's business processes"
3.5. Severity of consequences	- "none" - "minimum" - "medium" - "high" - "critical"

Probability of a repeated IS incident	- "none" - "minimum" - "medium" - "high" - "critical"
3.7. Scope of IS incident distribution and effect	- "within one ABS" - "within an individual structural subdivision of the RF BS organisation" - "within the whole RF BS organisation" - "beyond the RF BS organisation"
Group 4. Attributes reflecting the significance of the IS incident	
4.1 IS incident priority	- "0 (Highest)" - "1 (High)" - "2 (Increased)" - "3 (Medium)" - "4 (Low)" - "5 (Minimum)"
4.2. IS incident response time	- "Ordinary" - "High"
Group 5. Attributes related to IS incident response	
5.1. Report on IS incident occurrence	- "none" - "time of report and addressee"
5.2. IS incident elimination report	- "none" - "time of report and addressee"
5.3 IS incident escalation	- "no" - "yes"
5.4. Functional group	- "no" - "name of the functional group of specialists entrusted with responding to the IS incident"

IS incident attribute	Description of IS incident attribute values
5.5. Time of functional group appointment	- "no" - "appointment time of the functional group responsible for IS incident response"
5.6. Appointment of a specialist who is an ISIRG member	- "no" - "surname of the specialist responsible for IS incident response"
5.7 IS incident status	- "Registered" - "Assigned" - "In process" - "Closed"
5.8. IS incident response stage	
5.9. Established period for IS incident closure	- "no" - "established period for IS incident closure"
5.10. Other measures:	- "no" - "description of measures for IS incident closure"
5.11. Necessity to inform the RF BS organisation's structural subdivision about the IS incident.	- "no" - "list of units"
Group 6. Attributes related to IS incident closure	
6.1 Date and time of IS incident closure	- "no" - date and time
6.2. Consequences of (damage from) IS incident for the RF BS organisation	- "none" - "description of damage (consequences) in text form"
6.3. Complexity of IS incident closure	- "Ordinary" - "High"
6.4. Necessity of informing RF BS organisations' structural subunits of IS incident closure.	- "no" - "list of subunits"

Bibliography

1. Bank of Russia Standardisation Guidelines RS BR IBBS-2.2-2009 “Maintenance of Information Security of the Russian Banking System Organisations. Methodology for Assessing the Risks of Information Security Violations".
2. GOST R ISO/IEC 18044-2007 “Information Technology. Security Methods and Techniques. Information Security Incident Management".

Key words: Banking system of the Russian Federation, information security management system, information security policy, information security incidents, and information security incident management.

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