BANK OF RUSSIA STANDARD

STO BR IBBS-1.1-2007

INFORMATION SECURITY OF RUSSIAN BANKING INSTITUTIONS

INFORMATION SECURITY AUDIT*

Date enacted: 1 May 2007

Moscow
2007

Foreword

1. ADOPTED AND ENACTED by Bank of Russia Directive No. R-345, dated 28 April 2007.
2. ENACTED FOR THE FIRST TIME.

This standard may not be fully or partially reproduced, duplicated or distributed as an official publication without Bank of Russia permission.

Table of Contents

Introduction

One of the prerequisites for achieving the goals of Russian banking institutions (RBIs) is maintaining a necessary and sufficient level of their information security (IS).

An IS audit is the main type of inspection used to check the IS level in RBIs. Global experience in IS defines an IS audit as a key process in the continuous cycle of IS management in an organisation.

The Bank of Russia is a proponent of regular IS audits conducted in RBIs.

The main goals of the IS audit of RBIs are as follows:

- Increasing confidence in RBIs;
- Assessing the compliance of IS in RBIs with IS audit criteria established in accordance with requirements of Bank of Russia Standard STO BR IBBS-1.0 "Information Security of Russian Banking Institutions. General Provisions" (hereinafter STO BR IBBS-1.0).

BANK OF RUSSIA STANDARD

INFORMATION SECURITY OF RUSSIAN BANKING INSTITUTIONS

INFORMATION SECURITY AUDIT

Date enacted: 1 May 2007

1. Scope of Application

This standard applies to RBIs, as well as to organisations that conduct the IS audit of RBIs, and establishes the requirements for conducting the external IS audit of RBIs.

It is recommended that this standard be used by making references to it and/or using its provisions and requirements directly in the development of IS audit programmes, as well as in drafting other RBI regulations on IS.

The provisions of this standard shall apply on a voluntary basis, unless some specific provisions are made binding by applicable legislation, a Bank of Russia regulation or the terms of a contract.

2. Regulatory References

This standard contains references to the following standards: GOST R 1.4-2004 Standardisation in the Russian Federation. Standards of Organisations. General Provisions

STO BR IBBS-1.0

3. Terms and Definitions

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

3.1 **The external information security audit of a Russian banking institution; an information security audit:** A systematic, independent and documented process for obtaining audit evidence of the IS activities of a RBI and for establishing the degree of compliance by RBI with IS audit criteria, conducted by an independent auditing firm which is external to an audited organisation.

3.2 **An auditor (expert):** A person with competence to conduct an information security audit.

3.3 **An audit team:** One or more auditors conducting an information security audit with the support, if necessary, of technical experts.

3.4 **The findings of an information security audit; IS audit findings**: The results of an assessment of collected information security audit evidence in terms of its compliance with information security audit criteria.

Note: The findings of an information security audit indicate the degree of compliance of RBI's IS with IS audit criteria.

3.5 **An information security audit client; an IS audit client**: An organisation or a person who ordered an information security audit.

Note: A client may be an audited organisation or any other organisation that has a legal right to request an information security audit.

3.6 **An opinion on information security audit results (an auditor's opinion); a opinion on IS audit results**: Qualitative and/or quantitative assessments of the degree of compliance with information security audit criteria presented by an audit team after reviewing all the findings of an information security audit in accordance with the goals of an information security audit.

3.7 **Information security audit (self-assessment) criteria; IS audit (self-assessment) criteria:** A set of requirements for information security defined in accordance with the provisions of STO BR IBBS-1.0, or part thereof that describes a certain level of information security.

Note: Information security audit (self-assessment) criteria are used for comparison with information security audit (self-assessment) evidence.

3.8 **A scope of an information security audit; an IS audit scope:** The content and limits of an information security audit.

Note: The scope of an information security audit typically includes the location, the organisational structure, types of the activities of an audited organisation and processes subject to the information security audit, as well as a covered period.

3.9 **An audited organisation**: A Russian banking institution where an information security audit is conducted.

3.10 **An auditing firm:** An organisation that conducts an information security audit.

3.11 **An information security audit programme; an IS audit programme:** A plan for conducting one or more information security audits (and other information security checks) planned for a specific period and aimed at achieving a specific goal.

Note: An information security audit programme includes all activities necessary for planning, conducting, exercising control, analysing and improving information security audits (and other information security checks).

3.12 **Information security audit (self-assessment) evidence; IS audit (self-assessment) evidence:** Records, a statement of facts or other information that are relevant to information security audit (self-assessment) criteria and can be verified.

Note: Information security audit (self-assessment) evidence can be qualitative or quantitative.

3.13 **The information security self-assessment of a Russian banking institution; an IS self-assessment:** A systematic and documented process for obtaining self-assessment evidence in RBI's IS activities and establishing the degree of compliance by the RBI with IS self-assessment criteria. An IS self-assessment is conducted independently by RBI employees.

3.14 **A technical expert:** A person providing his/her knowledge and/or experience on specific issues to an audit team.

4. An Initial Conceptual Scheme (a Paradigm) for the Information Security Audit of Russian Banking Institutions

4.1 The initial conceptual scheme of the IS audit of RBIs is based, on the one hand, on the desire of an owner to prove that a RBI has achieved a high standard of IS and thereby to increase confidence in that organisation, and, on the other hand, it is based on the efforts of auditors to determine, by conducting an independent and competent assessment, the true (within the capabilities of the IS audit) level of IS activities and the degree of compliance of RBI's IS with established requirements (audit criteria).

4.2 The IS level in a RBI is considered high if the processes of the IS system are consciously based on forecasting, monitoring and analysing the internal and external environment and on developing and changing the business goals of the RBI.

4.3 Potential changes in the RBI external business environment or a change in or growth of IS risks as a result of natural and/or intentional changes in the RBI external and internal environment serve as a reason for regular IS audits of the RBI, making it possible to adopt timely measures for maintaining IS at the required level.

4.4 The compliance of RBI's IS with IS audit criteria is assessed in accordance with IS documents and facts confirming the performance, partial performance or failure to perform the established IS requirements.

5. Main Principles of the Information Security Audit of Russian Banking Institutions

5.1 **IS audit independence**. Auditors are independent in their activities and not responsible for activities that are subject to an IS audit. The independence forms the grounds for impartiality during the IS audit and objectivity in making an opinion based on the findings of the IS audit.

5.2 **IS audit completeness.** The IS audit should cover all areas in accordance with an audit engagement. In addition, the completeness of the IS audit is determined by the adequacy of requested and provided materials and documents and their level of conformity to tasks at hand. The completeness of an IS audit is a prerequisite for making objective opinions based on findings following the IS audit.

5.3 **An assessment based on IS audit evidence.** In the case of periodic IS audits, an assessment based on IS audit evidence is the only way to obtain a regular opinion on the results of the IS audit, which increases confidence in the opinion. To obtain a regular opinion, IS audit evidence should be verifiable.

5.4 **The reliability of IS audit evidence.** Auditors shall be confident in the reliability of IS audit evidence. Confidence in documentary IS audit evidence is increased when its reliability is confirmed by a third party or the RBI management. Trust in the facts obtained during interviews with the employees of an audited organisation is increased when such facts are confirmed by different sources. Confidence in the facts obtained by monitoring the IS activities of the audited organisation is higher if they are obtained directly during audited procedures or processes.

5.5 **Competence.** Confidence in the process and results of an IS audit depends on the competence of those who perform the IS audit and their ethical conduct. Competence is based on the auditor's ability to apply his/her knowledge and skills.

5.6 **An ethical conduct.** An ethical conduct implies responsibility, personal integrity, the ability to keep confidentiality, and impartiality.

6. The Management of an Information Security Audit Programme

6.1 An IS audit programme includes the activities necessary for planning and arranging a certain number of IS audits, their control, analysis and improvement, and providing them with the resources necessary to efficiently conduct IS audits within the established periods.

The IS audit programme is developed by a RBI. Several IS audit programmes may be developed in general.

The recommended sequence of processes for the management of an IS audit programme is shown in Figure 1. (The sequence of processes for the management of audit programmes is harmonised with the IS management model defined in section 5 of STO BR IBBS-1.0 and the provisions of the international standard [1].

6.2 The RBI management shall allocate authority and responsibility for managing the IS audit programme.

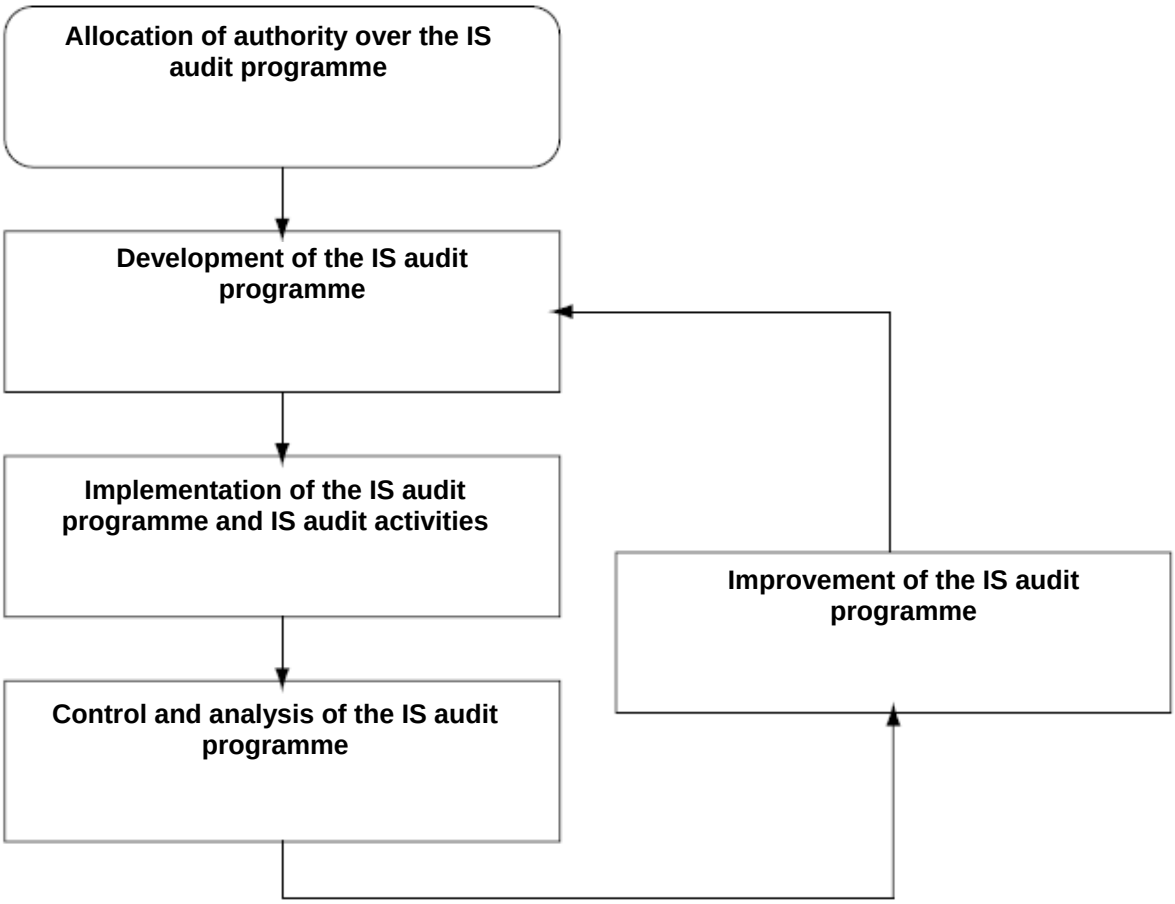
The persons responsible for managing the IS audit programme shall have an understanding of IS audit principles, the competence of auditors, and the stages of an IS audit, and also possess IS knowledge.

The persons responsible for managing the IS audit programme shall:

- develop, implement, control, analyse and improve the IS audit programme;
- determine the resource needs of the IS audit programme;
- promote decisions on providing the IS audit programme with necessary resources.

6.3 The development of an IS audit programme shall include the determination of goals and the scope of the programme, as well as financial, information and human resources necessary for its implementation.

Figure 1. The Sequence of Processes for Managing an IS Audit Programme



The purpose of an IS audit programme is to assess the compliance of RBI's IS with audit criteria and, when necessary, to contribute to raising the IS level in a RBI.

The scope of an IS audit programme is influenced by the size and complexity of the RBI organisational structure, the scope of each IS audit and the frequency of IS audits.

6.4 The implementation of an IS audit programme shall include the following:

- Communication of the IS audit programme to the parties participating in its implementation;
- Planning of IS audits;
- Determination of auditing firms to be engaged and the resources to be provided for conducting IS audits;
- Conducting of IS audits in accordance with the IS audit programme;
- Analysis and approval of reports on the results of IS audits;
- Determination of actions to be taken based on the results of IS audits.

6.5. The RBI shall control the implementation of the IS audit programme, analyse the achievement of goals set for the IS audit programme and identify opportunities for improving it. The RBI management shall be informed of the results of the analysis.

The control and analysis of an IS audit programme shall include the following:

- Verification of the abilities of audit teams, services or individuals to implement the IS audit. Details on the education and experience of the members of an audit team or certificates confirming their qualifications of members may prove the ability to implement an audit;
- Analysis of the achievement of IS audit goals and the IS audit programme on the whole;
- Analysis of reports and auditor's reports.

6.6. The improvement of an IS audit programme consists of determining corrective and preventive actions for improving the IS audit programme, including the review and adjustment of periods established for IS audits and the necessary resources, and improving methods for preparing IS audit evidence.

7. Conducting an Information Security Audit

7.1. Requirements for the Relationship between the Representatives of an Auditing Firm and the Representatives of an Audited Organisation

7.1.1. In the process of communication, the representatives of an auditing firm and the representatives of an audited organisation shall, at all stages of an IS audit, demonstrate honesty, openness, and willingness to discuss, and, whenever possible, resolve any disagreements.

The auditing firm shall inform the audited organisation on all steps taken as part of the audit.

The audited organisation shall ensure that the auditing firm is provided with all information necessary for conducting the IS audit.

7.1.2. The engagement for conducting an IS audit shall be documented by a contract in accordance with the requirements of Russian legislation.

Good practices are as follows:

- Submission of a formal proposal to an auditing firm by an audited organisation or an audit client, such as a government supervisory body, to conclude a contract for an IS audit;
- Sending of a letter on conducting an IS audit by an auditing firm to the management of an audited organisation before the contract is concluded in order to agree on the terms of the upcoming contract.

The contract for an IS audit shall specify IS audit criteria in accordance to which the auditing firm shall express its opinion.

7.1.3. When preparing for an IS audit and during the auditing process, an audit team may independently make decisions on sources, methods of acquisition and reliability of IS audit evidence (see point 7.2.10) needed to make its opinion on the results of the IS audit, unless otherwise specified in the contract for the IS audit.

7.1.4. During the IS audit process, the leader of an audit team shall periodically bring information on the progress of the IS audit and any problems encountered to the attention of the audited organisation and the audit client. Evidence gathered during the IS audit which identifies vulnerabilities which are critical to the IS of the audited organisation (in the opinion of the audit team leader) shall be immediately brought to the attention of the audited organisation and, if necessary, the IS audit client.

If the available IS audit evidence (or lack thereof) indicates that the goal of the IS audit is unattainable, the leader of the audit team shall communicate the reasons to the IS audit client and the audited organisation in order to determine further actions. These actions may include either a change in the goal or scope of the IS audit or termination of the IS audit.

7.1.5. The auditing firm is responsible for the following:

- The reliability of an opinion based on the results of the IS audit;
- The confidentiality of information and documents received and drafted in the course of auditing the organisation (except in cases specified by Russian legislation). If necessary, requirements for using the documents of the audited organisation and the IS audit report shall be defined by the contract for the IS audit.

7.1.6. The management of the audited organisation is responsible for the following:

- The reliability and completeness of information provided to an auditing firm;
- Any restrictions on the ability of the auditing firm to meet its obligations.

7.1.7. Any failure to comply with the requirements specified by point 7.1.5 thereof shall be reported to the authorities overseeing the activities of auditing firms and to the IS audit client.

Any failure to comply with the requirements stipulated by point 7.1.6 shall be specified in the IS audit report and may serve as grounds for terminating the IS audit process.

7.2. Requirements for the Stages of the Information Security Audit of Russian Banking Institutions

7.1.2. The IS audit of RBIs shall include the following stages:

- Preparing for the IS audit;
- Analysing documents;
- Conducting an on-site IS audit;
- Preparing, approving and distributing an IS audit report;
- Completing the IS audit.

7.2.2. The preparation for an IS audit shall start by determining the possibility of conducting an IS audit, as well as negotiating and concluding a contract for the IS audit (see point 7.1.2) between the RBI and the auditing firm. The subsequent preparation of the auditing firm for the IS audit shall include forming an audit team, appointing its leader and establishing a contact between the leader of the audit team and an audited organisation.

The contract for an IS audit may have special features, but, as a rule, it should specify the following:

- The scope of an IS audit;

- The responsibility of the management of an audited organisation to prepare and provide the necessary IS audit evidence;
- The requirements for an IS audit report;
- The procedure for interaction between the representatives of the auditing firm and the audited organisation;
- The procedure for collecting the necessary audit evidence;
- The price of the IS audit;
- The procedure for engaging other auditing firms and/or technical experts to work on any IS audit issues;
- The necessary liability restrictions of the auditing firm.

7.2.3. An auditing firm shall determine the feasibility of an IS audit based on the willingness of an audited organisation to cooperate and the availability of time and relevant resources.

If conducting an IS audit is considered infeasible, then an alternative (postponing the audit, engaging another auditing firm for the IS audit) shall be offered to the audit client based on consultations with the audited organisation.

7.2.4. An audit team shall be formed by an auditing firm to conduct an IS audit. An audit team leader who will be responsible for conducting the IS audit of a RBI shall be appointed by the management of the auditing firm.

The competence of the audit team based on the qualification level of its members shall be considered first and foremost when determining the size and composition of the audit team.

If the auditors on the audit team do not possess the necessary knowledge and experience on specific issues, the team shall include technical experts. The technical experts shall work under the guidance of auditors.

7.2.5. The leader of an audit team shall, in accordance with an audit contract, establish contacts with an audited organisation, primarily in order to establish ways for sharing information with the representatives of the audited organisation in order to confirm authority for an IS audit and request access to the necessary documents of the audited organisation.

7.2.6. Prior to conducting an on-site IS audit, the audit team shall analyse the required documentation of the audited organisation to determine the compliance of provisions in documents to IS audit criteria.

If the documents are found to be inadequate, then the leader of the audit team shall inform the IS audit client and the audited organisation. The audit team shall decide whether the IS audit can be continued or whether it shall be suspended until all issues with regard to the documentation are resolved.

7.2.7. If the audit team decides to continue the IS audit, the leader of the audit team shall prepare an on-site IS audit plan and coordinate it with the audit client and the audited organisation.

The on-site IS audit plan shall include the following:

- The goal of the IS audit;
- IS audit criteria;
- The scope of the IS audit;
- The date and duration of the on-site IS audit;
- The roles of audit team members and accompanying persons from the audited organisation;
- The results of analysis of documents provided by the audited organisation for the IS audit and an assessment of IS audit evidence;
- A description of activities and measures for the on-site IS audit;
- The allocation of resources during the audit.

The plan agreed upon shall be provided to the audited organisation before starting the on-site IS audit.

7.2.8. The on-site IS audit shall include the following activities:

- Holding an introductory meeting;
- Collecting additional IS audit evidence;
- Assessing the IS audit evidence;
- Making an opinion based on the results of the IS audit;
- Holding a final meeting.

7.2.9. The introductory meeting between the audit team and persons responsible for the divisions or processes to be audited shall be held in order to describe the actions planned for the IS audit and confirm the methods of sharing information between the audit team and representatives of the audited organisation. The meeting shall be chaired by the leader of the audit team.

The description of actions planned for the IS audit primarily involves reviewing issues regarding audit procedures and the sources, methods of preparation and reliability of IS audit evidence necessary for making an opinion on the IS audit results.

7.2.10 The main sources of IS audit evidence shall be as follows:

- IS documents of the audited organisation and third parties;
- Oral statements and written responses given by the employees of the audited organisation during conducted interviews;
- Results of auditors' oversight of the audited organisation’s IS activities.

The main methods used for obtaining IS audit evidence shall be as follows:

- Auditing and analysing documents related to the organisation’s IS;
- The oversight of the audited organisation’s IS activities;
- Interviewing the employees of the audited organisation and an independent (third) party.

IS audit evidence shall be categorized by degree of reliability (from highest to lowest) as follows:

- Evidence obtained from a third party in writing;
- Evidence obtained from an audited organisation and confirmed by a third party in writing;
- Evidence obtained during audit procedures (overseeing activities, analysing data from the IS monitoring system, etc.);
- Evidence obtained in the form of documents;
- Evidence obtained in the form of oral statements.

7.2.11. When collecting IS audit evidence, auditors shall assume that the IS activities of an audited organisation are carried out in accordance with audit criteria, if this is supported by evidence. The auditors shall exercise a reasonable degree of professional scepticism with regard to collected IS audit evidence by taking into account the possibility of various IS breaches in the audited organisation.

The examination and analysis of documents may be carried out at all stages of the audit. The examination and analysis of documents allow the auditor to obtain IS audit evidence which is maximally complete and easy to comprehend and use as compared to other methods for obtaining IS audit evidence. However, this IS audit evidence has varying degrees of reliability, depending on its nature and source, as well as on the efficiency of the organisation's internal control over the preparation and processing of the documents provided.

Oral interviews may be conducted at all stages of the audit. The results of oral interviews shall be recorded in the form of minutes or as a short summary, which shall include the full name of the employee of an auditing firm who conducted the interview, the full name of the interviewee, and their signatures. Forms with lists of questions of interest may be prepared for conducting standard interviews. Written information based on oral interviews shall be attached by the auditing firm to other working documents of the audit. However, the results of oral interviews need to be verified, as the interviewee may express his/her subjective opinion. A good practice is to conduct cross-check interviews of employees in an organisation (i.e., interviews of different persons). An oversight is an auditor's monitoring of procedures or processes performed in the audited organisation by other persons (including the personnel of organisation). Information shall be deemed reliable only if it is obtained directly at the time the audited procedures are performed or during the processes.

7.2.12. IS audit evidence shall be assessed in terms of audit criteria for the preparation of IS audit findings. The findings of an IS audit indicate the degree of compliance of RBI’s IS to IS audit criteria.

The assessment of the compliance of RBI’s IS with IS audit criteria is based on the documents and methods adopted by the RBI.

7.2.13 The IS audit findings and the IS audit evidence that confirms them shall be reviewed and analysed by the auditors together with a representative of the audited organisation in order to obtain confirmation that the IS audit evidence is true and clear. Any unresolved issues shall be registered in the minutes of meetings and reflected in an IS audit report.

7.2.14. Based on IS audit results, the audit team shall make an auditor’s opinion.

If the restriction of the IS audit scope is so material and deep that the auditor is unable to assess the compliance of IS in the audited organisation with IS audit criteria, then the audit team shall refrain from making an opinion.

A knowingly false auditor’s opinion may be made as a result of an IS audit. If any stakeholder in RBI activities detects any fact confirming a knowingly false auditor’s opinion, the stakeholder has the right to seek the retraction of the opinion. An auditor’s opinion may be recognised as knowingly false only in accordance with the procedure established by the authorities overseeing the activities of auditing firms.

7.2.15. A final meeting involving the representatives of an auditing firm, audited organisation and IS audit client and chaired by the leader of an audit team shall be held following the end of the IS audit.

At the meeting, IS audit findings and an opinion on IS audit results shall be presented in such a way as to make them clear and recognised by the audited organisation. Any disagreements arising between the audit team and the audited organisation on the findings and/or the opinion on IS audit results shall be discussed and resolved if possible. If the parties fail to come to a consensus, this shall be documented.

Recommendations on improving the IS level in the audited organisation may be presented at the meeting.

7.2.16. The audit team shall prepare a report on the results of the IS audit. The leader of the audit team is responsible for the preparation and content of the report on the results of the IS audit.

The report shall provide complete, accurate, clear and adequate records on the IS audit and shall include the following:

- Information on an auditing firm;
- Information on the leader and members of an audit team;
- Information on an audited organisation;
- Information on an IS audit client;
- The goal of an IS audit;
- The scope of the IS audit, in particular, information on audited organisational and functional units or processes and the covered period;
- The period over which the IS audit was conducted;
- An on-site IS audit plan;
- A documented set of questionnaires containing IS audit criteria and IS audit findings made for each of the IS audit criteria considered;
- An opinion on the results of the IS audit;
- A list of representatives from the audited organisation who accompanied and were interviewed by the audit team during the IS audit;

- A summary of the IS audit process, including any element of uncertainty and/or problems that could affect the reliability of an opinion on the results of the IS audit;
- A confirmation that the goal of the IS audit has been achieved in accordance with the IS audit plan;
- Any areas within the IS audit scope which were not covered;
- Any unresolved disagreement between the audit team and the audited organisation;
- A statement on the confidential nature of the report's content;
- A distribution list for the report on the results of the IS audit.

The report on the results of the IS audit shall be released within the period agreed upon, approved by the head of the auditing firm and sent to the recipients specified by the IS audit client.

The report on the results of the IS audit is the property of the IS audit client. The members of the audit team and all recipients of the report shall maintain the confidentiality of its content, except for cases specified by applicable Russian legislation.

8. Conducting an Information Security Self-Assessment

8.1. An IS self-assessment is a good practice for checking the RBI's IS level and preparation for an IS audit. The IS self-assessment is conducted based on documents and methods adopted by the RBI.

Using an IS self-assessment, RBIs can independently assess the compliance of their IS with audit criteria and analyse the deficiencies of their IS systems.

The results of the IS self-assessment may serve as a basis for eliminating the deficiencies identified in the IS system before an IS audit is conducted in the RBI.

8.2. An IS self-assessment may be conducted as part of an IS audit programme developed by a RBI.

8.3. The results of an IS self-assessment cannot serve as a statement of compliance with IS audit criteria.

8.4. An IS self-assessment in RBIs shall include the following stages:

- Forming groups for organising an IS self-assessment and collecting and analysing IS self-assessment data;
- Conducting the IS self-assessment;
- Making IS self-assessment results and informing the RBI management on IS self-assessment results.

8.5. The IS self-assessment shall be conducted by the employees of the RBI who are directly involved in IS activities. As a rule, these should be IS service employees.

8.6. The results of the self-assessment shall be analysed by the RBI management in order to understand IS problems existing in the RBI and define measures to resolve them.

Bibliography

[1] ISO/IEC 27001:2005(E) Information technology — Security techniques — Information security management systems — Requirements

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