BANK OF RUSSIA RECOMMENDATIONS
ON STANDARDISATION

RS BR IBBS-2.1-2007

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

GUIDELINES FOR SELF-ASSESSMENT OF CONFORMITY OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS TO REQUIREMENTS OF STO BR IBBS-1.0*

Effective date: 1 May 2007

Moscow
2007

Foreword

1. ADOPTED AND ENACTED by Bank of Russia Directive No. R-347 of 28 April 2007.
2. ENACTED FOR THE FIRST TIME.

Table of Contents

Introduction

In order to inspect the level of information security (IS) both for the Bank of Russia and for the Russian banking system (BS) organisations, the Bank of Russia Standard STO BR IBBS-1.0.2006 'Maintenance of Information Security of the Russian Banking System Organisations. General Provisions' (hereinafter – "STO BR IBBS-1.0") provides for regular IS self-assessment.

RF BS organisations self-assess their information security compliance in accordance with the Bank of Russia Standard STO BR IBBS-1.2 'Maintenance of Information Security of the Russian Banking System Organisations. Assessment Method for Compliance of Information Security of the Russian Banking System Organisations with Requirements of STO BR IBBS 1.0-2006'.

BANK OF RUSSIA RECOMMENDATIONS ON STANDARDISATION

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

GUIDELINES FOR SELF-ASSESSMENT OF CONFORMITY OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS TO REQUIREMENTS OF STO BR IBBS-1.0

Effective date: 1 May 2007

1. Scope of Application

These guidelines apply to Russian banking system organisations that perform self-assessment of their information security (IS) compliance with the requirements of STO BR IBBS-1.0 and determine the approaches to such self-assessment.

These guidelines are recommended to be applied by RF BS organisations by directly using the provisions set forth herein in their IS self-assessment. Organisations perform IS self-assessment through their own effects and at the initiative of their executives.

The provisions hereof are optional, unless certain provisions are bound by the Russian laws, Bank of Russia regulations or contractual terms.

2. Regulatory References

These guidelines include regulatory references to the following standards: STO BR IBBS-1.0

STO BR IBBS-1.1.-2007 ‘Maintenance of Information Security of Russian Banking System Organisations. Information Security Audit’

STO BR IBBS-1.2.-2007 ‘Maintenance of Information Security of Russian Banking System Organisations. Methodology for Assessing the Compliance of the Information Security of Russian Banking System Organisations with STO BR IBBS 1.0-2006’.

3. Terms and Definitions

These guidelines include the terms used in STO BR IBBS-1.0 and STO BR IBBS-1.1 ‘Information Security of Russian Banking System Organisations. Information Security Audit’ and STO BR IBBS-1.2 ‘Information Security of Russian Banking System Organisations. Assessment Method for Compliance of Information Security of the Russian Banking System Organisations with Requirements of STO BR IBBS 1.0-2006’ (hereinafter the "Methodology").

4. Self-Assessment by Russian Banking System Organisations of their Information Security Compliance with STO BR IBBS-1.0

4.1. RF BS organisations self-assess their IS compliance with STO BR IBBS-1.0 pursuant to the Methodology in the following assessment areas:

- The organisation's current IS level;
- The organisation's IS management;
- IS awareness within the organisation.

4.2. When RF BS organisations are conducting self-assessment of their IS compliance with STO BR IBBS-1.0, it is essential to:

- Review the Methodology, in particular the set of individual and group IS indicators, the assessment areas, the method for calculating group IS indicators, the methods of evaluation within the areas and a RF BS organisation's final IS compliance level with the STO BR IBBS-1.0 requirements;
- Determine a set of individual IS indicators covered by self-assessment;
- Assess required individual IS indicators;
- Calculate the assessment values for group IS indicators, the assessment values within the areas and the final IS compliance level.

4.3. All individual IS indicators per the Methodology are to be assessed. However, before assessing individual IS indicators an analysis is to be made of whether the IS requirements inspected by individual IS indicators per the Methodology are relevant for the RF BS organisation's primary and auxiliary activities. An IS requirement may only be considered irrelevant if the organisation does not carry out the activities covered by said IS requirement. In this case, the respective individual indicators are determined as non-assessable and are not taken into account in forming further self-assessment results.

4.4. An individual indicator may be determined non-assessable by eliminating it from those subject to assessment, in which case the relevance coefficients must be recalculated for the remaining individual IS indicators within the limits of the group IS indicator, while preserving the level of their relevance for the calculated value of the group IS indicator.

If an individual IS indicator is determined as non-assessable, the irrelevance of this individual IS indicator for the RF BS organisation's activities must be substantiated and documented.

4.5. The value of an individual IS indicator is formed based on the identified compliance level with the inspected requirement through expert assessment. The Methodology establishes the following compliance scale with the inspected requirements:

- "no" - an assessment assigned a zero value;
- "partially" - the assessment is assigned the value of 0.25, 0.5 or 0.75;
- "yes" - the assessment is assigned the value of 1.

4.6. Individual IS indicator assessment must be based on self-assessment evidence, the recommended primary sources of which are:

- Regulatory documents maintained by the inspected RF BS organisation and, where necessary, third parties' documents regarding IS within the RF BS organisation;
- Oral statements of the inspected RF BS organisation's employees during interviews;
- The auditors' observations over IS activities performed by the RF BS organisation's employees.

Based on verbal interviews of the RF BS organisation's employees and observations of their activities, the inspection group members are to make a conclusion on the level of compliance for such assessed activities with the requirements of the inspected RF BS organisation's regulatory documents.

The IS self-assessment evidence that was obtained and its sources must be documented by filling out IS self-assessment evidence sheets, an example of which is given Appendix A. When filling out these IS self-assessment evidence sheets, references are to be given to the respective regulatory documents of the inspected RF BS organisation, the interviews with its employees and the inspection group's observations. The interviews and observations must be signed by the interviewed employees of the RF BS organisation or the inspection group member, respectively.

4.7. The following approach is recommended when determining the level of IS security compliance in the assessment of individual indicators:

Table 1. Recommended criteria for evaluating individual IS indicators

Individual IS indicator values	Criteria for evaluating individual IS indicators
0	Compliance requirements for individual IS indicators that are not set in the inspected RF BS organisation's internal regulatory documents and are not evaluated
0	Compliance requirements for individual IS indicators that are partially set in the inspected RF

	BS organisation's internal regulatory documents, but are not evaluated
0.25	Compliance requirements for individual IS indicators that are entirely set in the inspected RF BS organisation's internal regulatory documents, but are not evaluated
0.25	Compliance requirements for individual IS indicators that are not set in the inspected RF BS organisation's internal regulatory documents and are not completely evaluated
0.25	Compliance requirements for individual IS indicators that are partially set in the inspected RF BS organisation's internal regulatory documents and are not completely evaluated
0.5	Compliance requirements for individual IS indicators that are completely set in the inspected RF BS organisation's internal regulatory documents and are not completely evaluated
0.5	Compliance requirements for individual IS indicators that are not set in the inspected RF BS organisation's internal regulatory documents but are completely evaluated
0.75	Compliance requirements for individual IS indicators that are partially set in the inspected RF BS organisation's internal regulatory documents but are completely evaluated
1	Compliance requirements for individual IS indicators that are completely set in the inspected RF BS organisation's internal regulatory documents and are completely evaluated

4.8. If all individual IS indicators are excluded within a certain group IS indicator, the IS indicator group is to be excluded from the indicators that form the value for the area, and the evaluation formula given in the Methodology for the area is to be adjusted.

4.9. To perform self-assessment of IS compliance, it is recommended to use the automated system for self-assessment of IS compliance with STO BR IBBS-1.0, to which should be familiar with the recommended Bank of Russia documents containing a general description and user guide for the systems that are to be reviewed.

4.10. Following self-assessment, a report is made, containing:

– Completed assessment forms of group IS indicators;
– Documents justifying the exclusion of specific self-assessment indicators;
– Completed self-assessment evidence sheets confirming the values of individual IS indicators;
– Documents with the outcomes of IS compliance self-assessment in the assessment areas and the final level of the RF BS organisation's IS compliance with STO BR IBBS-1.0, as well as a circular assessment chart for group IS indicators as determined and described in the Methodology.

4.11. The Bank of Russia recommends that the value for the final level of the RF BS organisation's IS compliance with STO BR IBBS-1.0 is from 0.85 to 1 inclusively.

5. Procedure for Self-Assessment by Russian Banking System Organisations of their Information Security Compliance

It is recommended that the scope of work for IS self-assessment by RF BS organisations include the following stages:

- Preparation for IS self-assessment;
- Analysis of documents;
- On-site IS self-assessment;
- Preparing and distributing an IS self-assessment report.

5.1. Preparing for Information Security Self-Assessment

5.1.1. When preparing for IS self-assessment, it is recommended to:

- Form a group to conduct self-assessment from among the employees of the RF BS organisation's IS department;
- Appoint a leader of the inspection group;
- Make an IS self-assessment plan;
- Assign roles and obligations for performing IS self-assessment and using its results;
- Determine the form of the IS self-assessment report.

5.1.2. When determining the size and members of the group responsible for IS self-assessment (inspection group) the competence of the inspection group should be measured, based on the qualifications of its members. If the inspection group members do not have the required knowledge and expertise on specific issues, the group must include technical experts. Technical experts should be supervised by the inspection group members.

5.1.3. If any material discrepancies between the expert opinion and information (documents) of the inspected units are identified when analysing the performance of the technical experts or if the inspection group considers the expert's opinions to be unfounded, the inspection group shall conduct additional procedures for verifying the validity of the expert's opinion or appoint another expert.

5.1.4. The technical expert's opinion should be included in the inspection group's working documentation. If in an exceptional case, the technical expert provides verbal explanations, the inspection group must include these explanations in its working documentation.

5.1.5. Using the technical expert's work in IS self-assessments does not relieve the inspection group members from responsibility for the conclusion.

5.1.6. It is recommended the IS self-assessment plan include at least the following information:

- The purpose of IS self-assessment;
- Facilities and activities subject to IS self-assessment;
- The date and duration of the IS self-assessment;
- Distribution of roles among the inspection group members for analysing documents, conducting on-site self-assessment, and preparing and distributing the self-assessment report;
- The procedure and period for analysing the documents;
- The procedure and period of on-site IS self-assessment;
- The procedure and period for preparing and distributing the IS self-assessment report.

It is recommended that the self-assessment plan is agreed upon by all stakeholders and approved by the person responsible for IS self-assessment (from among the RF BS organisation's senior management).

5.1.7. The inspection group members must prepare the working documentation required to register the IS self-assessment results. The working documentation must be kept at least until the IS self-assessment is completed. The documents containing confidential or proprietary information must be stored in compliance to the relevant security requirements.

Appendix A provides the recommended form of IS self-assessment evidence sheets. The sheets are to contain the information obtained by the auditors in the course of IS self-assessment using various methods of IS self-assessment evidence collection (interview, observation of the activities and analysis of identified regulatory documents).

5.1.8. The RF BS organisation's executives must establish and provide resources to support IS self-assessment, including identification of those responsible for all aspects of IS self-assessment aspects, and the appropriate financial and infrastructural support for the required IS self-assessment functions, such as collection, analysis, storage, communication and distribution of data.

5.1.9. It is recommended the RF BS organisation's leadership appoint a person responsible for the IS self-assessment process (from among its senior management), and to approve the self-assessment rules determining:

- The procedure for generating, collecting and storing self-assessment evidence;
- The frequency of IS self-assessment;
- The procedure for storing and distributing the results of the IS self-assessment.

5.1.10. It is recommended to determine the following obligations for the person in charge of the IS self-assessment process:

- Interact with the heads of the inspected units to assist in IS self-assessment;
- Ensure the possibilities of data collection for IS self-assessment;
- Appoint qualified personnel to develop and implement an IS self-assessment plan;
- Ensure a single IS self-assessment process is used throughout the entire organisation.

5.1.11. It is recommended that IS self-assessment be preceded by an introductory meeting. This meeting, should be attended by the inspection group members and the persons responsible for the inspected units, and carried out in order to present the operations for IS self-assessment and to approve the methods of exchanging information between the inspection group and the representatives of the inspected units. The meeting is to be chaired by the head of the inspection group.

Description of actions for IS self-assessment primarily involves considering the sources, methods of collection, and validity of IS self-assessment evidence required to assess individual indicators of the Methodology.

5.1.12. In some cases, the introductory meeting may simply be in the form of an IS self-assessment notice and explanations regarding its character.

In other cases, it is recommended the meeting include:

- Introducing the inspection group members, and specifying their roles;
- Approving the self-assessment schedule;
- Reviewing the methods and procedures used in IS self-assessment;
- Approving the methods of exchanging information between the inspection group and the inspected units of the RF BS organisation;
- Ensuring the availability of resources and equipment that may be required by the inspection group;
- Approving the confidentiality principles;
- Becoming acquainted with the IS self-assessment report form;
- Providing information about procedure for handling the comments provided by the RF BS organisation's inspected units with respect to IS self-assessment or its outcome.

5.2. Analysing the Documents

5.2.1. Before on-site self-assessment, it is recommended that the inspection group analyses the relevant documents regulating IS in the inspected units of the RF BS organisation to determine the conformity of the provisions contained in such documents with the requirements of STO BR IBBS-1.0.

5.2.2. The documents are analysed within the scope of self-assessment in order to collect self-assessment evidence making it possible to evaluate individual IS indicators per the Methodology.

The recommended list of documents required by the inspection group members to analyse the RF BS organisation's IS compliance with STO BR IBBS-1.0 is provided in Appendix B.

5.2.3. In addition to the documents listed in Appendix B, other documents containing evidence of IS activities may be received at the analysis stage. These documents may include:

- Registries and inventories;
- Registration logs;
- Protocols;
- Orders and directives;
- Acts;
- Agreements;
- Reports.

5.3. On-Site Self-Assessment of Information Security

5.3.1. On-site IS self-assessment involves:

- Collecting additional IS self-assessment evidence;
- Evaluating individual IS indicators per the Methodology;
- Holding the final meeting.

5.3.2. The main sources of IS self-assessment evidence during on-site IS self-assessment are:

- Documents that for some reasons were not identified at the document analysis stage and contain the required IS self-assessment evidence;
- Verbal statements of employees from the inspected units;

– Observations of inspection group members regarding activities for ensuring compliance with the regulatory IS documents.

5.3.3. Auditors evaluate individual indicators of the Methodology based on the self-assessment evidence that was documented in the self-assessment evidence forms.

5.3.4. After completing on-site IS self-assessment, it is recommended to hold a final meeting with representatives of the inspection group and the inspected units, chaired by the head of the inspection group.

At the meeting, the evaluation results for each of the individual indicators per the Methodology are to be presented in such a way that they are clear and accepted by all interested parties and units of the RF BS organisation. Any discrepancies in the evaluated individual indicators per the Methodology must be discussed and settled, if possible. Failure to reach a consensus is to be documented.

At the meeting, recommendations may be provided on enhancing the IS level.

5.4. Preparing and Distributing an Information Security Self-Assessment Report

5.4.1. Following the assessment of individual IS indicators under the Methodology, the inspection group evaluates the level of the RF BS organisation's IS compliance with the requirements of STO BR IBBS-1.0 and prepares an IS self-assessment report. In accordance with the documents determined by Clause 4.10 hereof, the IS self-assessment report is to include:

– Information about the RF BS organisation that performed the IS self-assessment;
– Information about the leadership and members of the inspection group;
– The time period of the self-assessment;
– A summary of the self-assessment process;
– Any unsettled discrepancies;
– A statement about the confidential nature of the IS self-assessment report;
– A distribution list for the IS self-assessment report.

The IS self-assessment report must be approved by the person responsible for the IS self-assessment process (from among the RF BS organisation's senior management).

5.4.2. The reviewed and finalised IS self-assessment report may be distributed to all participants, including the head of the RF BS organisation, heads and employees of the information security department, and other interested parties.

Members of the RF BS organisation must have access to the IS self-assessment report on a need to know basis and in accordance with their rights.

It may be necessary to distribute the IS self-assessment outcomes among third party stakeholders, including regulatory authorities, shareholders, customers and suppliers.

Appendix A
Information Security Self-Assessment Evidence Form

Group IS indicator_____

Individual IS indicator	Evidence sources and IS self-assessment evidence (documents, interviews, or observations)	IS self-assessment evidence provided by	Employee/supervisor signature	Date

_____
(signature)

_____
(signature)

_____
(signature)

Appendix B
Documents recommended as sources of evidence for information security self-assessment by RF BS organisations

1. The organisation's IS policy and individual IS policies, including:

a) Individual policy for bank payment system IS;
b) Individual policy for bank information system IS;
c) Individual policy for bank telecommunication system IS.

2. Documents (regulations, guidelines, instructions) regulating the activities and/or containing evidence of the activities for:

a) Assignment and distribution of roles within the organisation;
b) Personnel management, including documents determining the RF BS organisation's internal requirements for:
   – Hiring of personnel;
   – Maintaining confidentiality of information by the organisation's employees;
   – Compliance by the organisation's employees with its corporate ethics;
   – Preventing conflicts of interests;
   – Conducting training, notifying personnel, and testing of IS skills.
c) Ensuring IS of automated banking systems throughout their life cycle, including the requirements for:
   – Raising technical requirements, development of requirements specifications, design, creation, testing and acceptance of IS tools for automated banking systems;
   – Commissioning, operation, maintenance and decommissioning of automated banking systems.
d) Managing access to the RF BS organisation's computer resources, local area networks, and automated banking systems;
e) Virus protection;
f) Using Internet resources;
g) Using cryptographic data protection facilities;
h) Ensuring IS of the RF BS organisation's bank payment operations;
i) Ensuring IS of the RF BS organisation's bank information operations.

3. Documents (regulations, guidelines, instructions, etc.) regulating the activities and/or containing evidence of the activities within the scope of the RF BS organisation's information security management system (IS Management System):

a) Determining/ specifying the scope of IS Management System application and selecting the approach to IS risk assessment. Such documents may include:
   – A document determining the selected approach to and methods of IS risk assessment;
   – A document describing the scope of IS Management System.
b) Analysing and assessing IS risks, and selecting the IS risk processing options. These documents may include:
   – Documents reflecting the results of IS risk analysis and assessment;
   – Documents containing IS risk-processing options.
c) Determining/specifying the organisation's IS policies;
d) Determining/specifying IS goals and protective measures. These documents may include:
   – Documents containing the protective measures selected (specified);
   – Documents with the organisation's selected (specified) IS goals.
e) Acceptance of residual risks and making decisions on IS Management System implementation and operation/improvement by the organisation's management. These documents may include:
   – Resolutions on IS Management System implementation and operation (improvements);
   – Documents governing IS Service activities;
   – Documents reflecting the organisation's senior management's acceptance of residual IS risks;
   – Documents defining IS roles.
f) Development of a plan for processing IS risks. This may include documentation defining the IS risk processing plan;
g) Fulfilling the IS risk processing plan, implementing protective measures, and managing the work and resources related to IS Management System implementation. These documents may include:
   – Evidence of implementing protective measures;
   – Evidence of implementing an IS risk processing plan;
   – IS training programmes and notifications;
   – Documents determining the composition and the procedure for managing the RF BS organisation's IS documentation.
h) Implementing IS training programmes and notifications. These documents may include:
   – Evidence of implemented IS training programmes;
   – Evidence of implemented IS notification programmes.
i) Detecting and responding to security incidents. These documents may include:

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

- Documents that determine the procedures for detecting and informing about IS incidents;
- Documents that determine the procedures for evaluating and making decisions on IS events / incidents;
- Documents determining IS incident response procedures.

j) Provision of business continuity and recovery after interruptions. These documents may include:
- Business continuity policy;
- Plan for recovering the business after interruptions;
- Documents that defining the procedure for periodic testing of the plan for recovering the business after interruptions;
- Training programme and notifications about business process recovery after interruptions.

k) Monitoring and control over protective measures, including registration of IS Management System-related actions and events. These documents may include:
- Reports on prompt IS assessment;
- Documentation that determines the monitoring and control procedures.

l) Analysis of IS Management System efficiency, including residual and acceptable IS risk levels. These documents may include:
- Reports on IS risk revaluation and analysis of residual and acceptable IS risk levels;
- Documents that determining the procedure for analysing the IS Management System performance.

m) Internal IS audit. These documents may include:
- Documents determining the procedure for internal IS audit;
- IS audit programme;
- Documents with the outcomes of internal IS audits and propositions for IS development.

n) IS Management System analysis by the senior management. These documents may include:
- Documents on the outcomes of IS Management System analysis by the senior management;
- Documents with a list of documents to be submitted to the senior management for analysis.

o) External IS audit. These documents may include:
- IS audit programme, including a description of the activities required for planning, organising, conducting and improving the external IS audit;
- Audit reports.

p) Implementation of tactical IS Management System improvements. This may include documentation describing the actions to improve IS Management System.

q) Implementation of strategic IS Management System improvements and the use of experience. These documents may include:
- Documents describing changes (in IS policies, IS risk processing plans, etc.);
- Documents containing the management's resolutions on corrective and preventive actions to IS Management System.

r) Information about changes and their approval by interested parties. These documents may include:
- Documents determining the procedure for notifying the interested parties about IS changes;
- Documents determining the procedure for the approval of IS changes by the interested parties;
- Documents determining the procedure for making amendments to contracts (agreements) for interaction with third parties.

s) Evaluation of the attainment of the set goals. This may include documentation approved by the management after analysing the reasons for irregularities in IS Management System implementation and/or operation, pertaining to the specification of IS policies and IS goals.

4. Documents (regulations, guidelines, instructions, etc.) regulating the activities and/or containing evidence of the activities for implementing general information security principles by RF BS organisations:

a) Timely detection and forecast of IS problems and development and evaluation of their effect on the organisation's business goals. These documents may include:
- Documents reflecting the classification of resources according to their criticality for business continuity;
- Documents containing threats models and models of violators;
- Documents with the requirements for IS incident processing procedures;
- Documents containing evidence of analysis activities and processing of IS incidents;
- Documents containing evidence of IS risk management activities.

b) Definition of objectives, validity of protective measures selected, their efficiency and controllability. These documents may include:
- Documents determining the RF BS organisation's IS goals and objectives;
- Documents containing evidence of the RF BS organisation's specified/revised IS goals and objectives;
- Documents substantiating the protective measures selected;
- Documents containing the plan for protective measures;
- Documents containing evidence of control over the correct implementation and use of protective measures;
- Documents determining the procedure for testing the applied protective measures;
- Documents containing evidence of the testing of the applied protective measures;

- Documents on controlling compliance with current IS regulations and requirements.

c) Continuity of information security and the use of experience in making and implementing decisions. These documents may include:
   - Documents regulating the activities of the RF BS organisation's IS Service;
   - Documents determining IS roles within RF BS organisations;
   - Evidence of activities performed to analyse and improve RF BS organisations;
   - Documents defining a plan for business continuity and business recovery after interruptions;
   - Documents containing evidence of the implementation of procedures for periodic testing of the plan to recover business processes after interruption.

d) Knowledge of its customers and employees, and the personification of an adequate separation of roles and responsibilities and satisfactory role functions and procedures. These documents may include:
   - Documents regulating the procedures for hiring and selection of job applicants;
   - Agreements of RF BS organisations with its clients;
   - Documents determining IS roles within RF BS organisations.

e) Availability of services, visibility and accessibility of IS. These documents may include:
   - Agreements of RF BS organisations with its clients and counterparties;
   - Documentation that determines the monitoring and control procedures;
   - Auditing and self-assessment programmes;
   - Audit reports and self-assessment reports.

Key words: Russian banking system, information security, information security self-assessment, information security indicators, current level of information security, information security management system, information security awareness, and information security requirements.

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