BANK OF RUSSIA RECOMMENDATIONS ON STANDARDISATION

RS BR IBBS-2.0-2007

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

RECOMMENDED PRACTICES FOR DOCUMENTATION RELATED TO INFORMATION SECURITY MAINTENANCE ACCORDANCE WITH STO BR IBBS-1.0*

Effective date: 2007-05-01

Moscow
2007

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

Foreword

1. ADOPTED AND ENACTED by Bank of Russia Decree No. R-348 of 28 April 2007.

2. ENACTED FOR THE FIRST TIME.

Table of Contents

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

Introduction

Adequate information security (IS) for business needs can only be achieved based on a comprehensive approach involving systematic legal, organisational, software, hardware, and other IS measures on a common conceptual and methodological basis.

To ensure consistency, focus, and conformity of IS activities, these activities must be documented.

IS documents are used to define IS rules and requirements to each employee. These should guide their operational procedures and determine the procedure for controlling their fulfilment.

BANK OF RUSSIA RECOMMENDATIONS ON STANDARDISATION

MAINTENANCE OF INFORMATION SECURITY OF THE RUSSIAN BANKING SYSTEM ORGANISATIONS

RECOMMENDED PRACTICES FOR DOCUMENTATION RELATED TO INFORMATION SECURITY MAINTENANCE IN ACCORDANCE WITH STO BR IBBS-1.0

Effective date: 2007-05-01

1. Scope of Application

This document applies to the Russian Federation (hereafter "RF") Banking System (hereafter "BS") organisations and provides recommendations for the structure, composition, purpose and contents of internal documents regulating information security within RF BS organisations as per the requirements of the Bank of Russia Standard STO BR IBBS-1.0 "Maintenance of Information Security of the Russian Banking System Organisations. General Provisions" (hereafter "STO BR IBBS-1.0").

These recommendations on standardisation should be applied by including references hereto and (or) directly using the provisions contained herein in the internal documents of RF BS organisations.

These recommendations on standardisation are optional, unless certain provisions are bound by the Russian laws, Bank of Russia regulations or the terms of a RF BS organisation's agreements with third parties.

2. Regulatory References

These recommendations include regulatory 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. Structure of Information Security Documents

3.1. RF BS organisations carry out their IS activities based on the following documents:

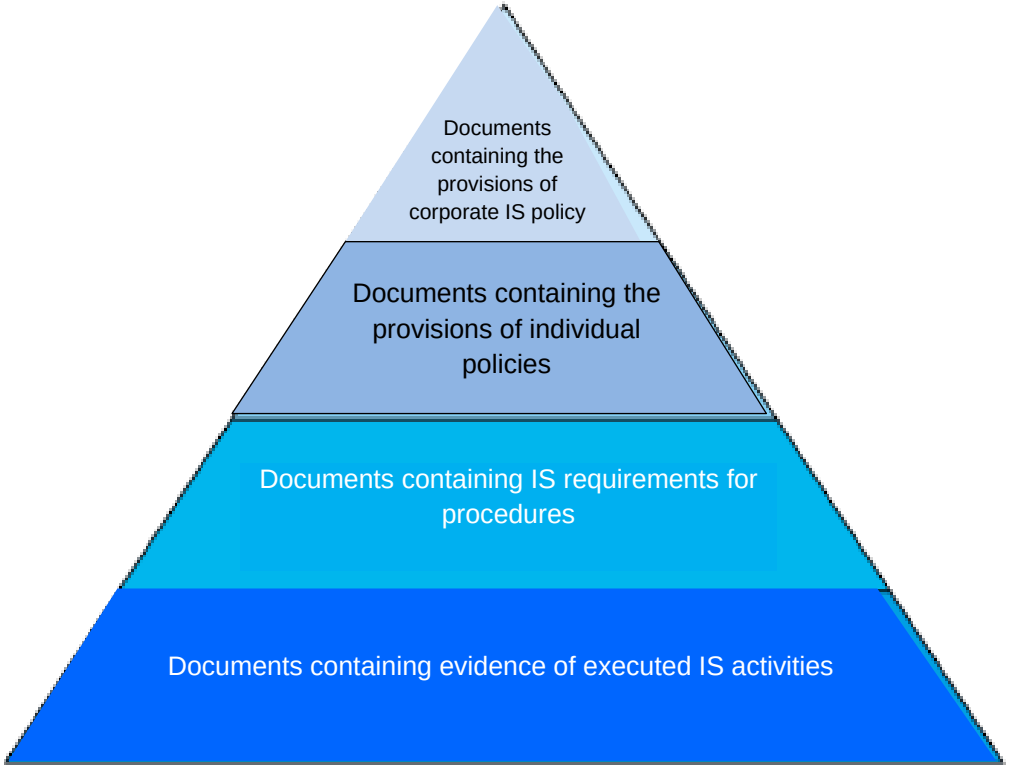
– Applicable laws and regulations of the Russian Federation on information security;
– Bank of Russia regulations;
– RF BS organisations' internal IS documents.

3.2. It is recommended that internal IS documents of RF BS organisations include the following types of documents (documented information) arranged in the hierarchical structure as shown in Figure 1:

– Documents containing provisions of RF BS organisations' corporate policy, define high-level objectives, the content and core areas of its IS activities, and are intended for the organisation as a whole (first-level documents)
– Documents containing provisions of individual policies and specifying the provisions of the corporate IS policy with regard to one or more IS areas, types and technologies of RF BS organisations' activities (second-level documents)
– Documents containing provisions applied to IS procedures (order of actions or operations) and providing rules and parameters for specific IS actions within the scope of operations applied by RF BS organisations, or restrictions on certain actions for implementing protective measures in the applied operations (requirements specifications, rules, procedures, instructions) (third-level documents)
– Documents containing evidence of IS activities and their outcomes (intermediary and final) for RF BS organisations (fourth-level documents).

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

Figure 1. Structure of RF BS Organisations' Internal IS Documents



3.3 It is recommended that the provisions of RF BS organisations' IS documents are:
– Binding, not optional;
– Feasible and controllable. These documents should not include provisions that are difficult or impossible to control or implement;
– Adequate to business requirements and conditions (including IS threats and risks), including in terms of their variability;
– Consistent with each other.

3.4. It is recommended that the documents of RF BS organisations include a document (classifier) containing a list of all their documents which regulate the organisations' IS activities and an explanation of their purpose (for each of the above levels in the hierarchical structure). The said classifier may be used to manage RF BS organisations' documents, raise awareness among its employees, and audit its information security.

3.5. If a RF BS organisation has a branch network (regional institutions), it is recommended that each of its branches (regional institution) have an approved set of uniform IS documents. If it is necessary to consider the specifics of certain branches, they must develop their own documents, taking into account this specificity. The IS documents of a RF BS organisation's branch (regional institution) should be based on the provisions of IS documents adopted by its parent organisation (central head office) and be consistent with them.

3.6. An example of the internal standard [1] requirements for the structure (hierarchy) and contents of an organisation's internal IS documents is provided in Appendix A.

4. Composition of Internal IS Documents

4.1. First-Level Documents

4.1.1. Corporate IS policy defines RF BS organisations' high (general) level IS goals and objectives, including methods of implementing their IS policy. RF BS organisations' corporate IS policy determines the scope, purpose and requirements for their IS activities without indicating any specific details.

4.1.2. The corporate IS policy of RF BS organisations should determine high-level rules and requirements for their risk management activities, including the analysis and development of attitudes towards risk.

4.1.3. The corporate IS policy of RF BS organisations [1] may comprise a set of documents or be a single general document.

[1] The IS policy name must include the name of the organisation that developed said policy.

4.1.4. It is recommended that the corporate IS policy of RF BS organisations include the following provisions:
– A definition of IS in terms of organisations' activities, the scope of policy application, the goals, objectives and principles of IS within the RF BS organisations;
– A statement of intent to ensure IS aims to attain the said IS goals and principles;
– General information about the assets subject to protection and their classification;
– Models of threats and violators (internal and external) per Section 7 of STO BR IBBS-1.0, which are the target of the corporate IS policy;
– High-level IS rules and requirements which hold special importance for the RF BS organisation, for example:
– Regulations of the Russian Federation in the field of information security and Bank of Russia regulations ensuring compliance with legislation;
– IS management requirements;
– Requirements for preventing and detecting computer viruses and other malicious software;
– Requirements for managing business continuity;
– Sanctions and consequences in the event of security policy violations;
– General roles and obligations for ensuring IS, including IS incident notification;
– A list of individual IS policies that develop and specify the provisions of corporate IS policy and a list of the RF BS organisation's subunits responsible for their compliance and/or implementation;
– Provisions for controlling the implementation of corporate information security policy by the RF BS organisation;
– Accountability for executing and maintaining the document;
– Conditions for revising the document (issuing a new version thereof).

4.1.5. It is recommended that RF BS organisations involve representatives of the services below in its information sphere when developing and approving their corporate IS policies:
– RF BS organisation executives;
– Specialized divisions;
– IT service;
– Security (information security) Service.

4.1.6. Corporate IS policy is to be approved by the RF BS organisation's leadership (for example, the chairman, the general director, the president, or the head of a branch).

4.2. Second-Level Documents

4.2.1. Second-level IS documents include documents that set forth the rules, requirements and principles applicable to individual IS areas, types and technologies of RF BS organisations' activities.

Moreover, it is recommended that the documents of this level include the RF BS organisations' IS activity plans and standards.

4.2.2. It is not recommended to repeat the same rules in different individual policies. A rule contained in a different (existing) policy may be included in another policy by making a corresponding reference. For example, to include virus protection requirements into the "Bank Information Operations IS Policy", a reference is to be made to the Virus Protection Policy (if any).

4.2.3. Individual policies are formed based on the principles, requirements and objectives determined in the RF BS organisation's corporate IS policy taking into account detail, specification and additional classification of assets and threats, determination of asset owners, analysis and assessment of risks and possible consequences from threats within the scope of a regulated area or technology.

4.2.4. Individual IS policies developed by RF BS organisations should include provisions determining:
– IS goals and objectives that the individual policy is intended to fulfil;
– The scope of the policy, the objects (assets) subject to protection, the vulnerabilities and threats, and the assessment of risks associated with the objects of protection;
– The types of activities which an individual IS policy is targeted, a complex of bank technologies applied in the course of such activities, and the key operations in which such technologies are implemented, as well as;
– A definition of entities (roles) covered by the document. The subjects (roles) may include both RF BS organisations' structural subunits and individuals;
– The content of the document (requirements and rules);
– IS obligations within the scope of individual IS policies, and a description of functions fulfilled by the subjects (roles) of the objects managed within the scope of regulated operations;
– Composition of reference documents [2];

[2] Reference documents include documents to be reviewed on a mandatory basis for adequate understanding of the IS policy. For example, if a policy describes the requirements for confidential information, the reference documents must include a document listing the confidential information.

– Provisions for control over the implementation of an individual IS policy;
– Accountability for executing and maintaining the document;
– Conditions for revising the document.

4.2.5. It is recommended that RF BS organisations' IS activity plans include, without limitation:
– Plans for the execution and implementation of IS procedures, requirements, and measures;
– Action plans in case of possible IS incidents;
– Action plans for IS management;
– Action plans for IS document management;
– Plans for maintaining the hardware and software used for IS purposes;
– Action plans for training and raising awareness of RF BS organisations' employees.

4.2.6. The IS activity plans should include a list, the procedure, the scope (in any form), and the schedule of IS actions taken by the RF BS organisation, and indicate the supervisors, responsible individuals, and responsibilities for such measures.

4.2.7. At a minimum, IS plans must determine:
– The sequence of events in an effort to ensure information security;
– The start and end dates of the planned activities;
– The subjects (persons or structural subunits) responsible for each action.

4.2.8. IS technologies standards of RF BS organisations establish requirements and characteristics for its general and repeated use. RF BS organisations' IS technology standards may be developed both for specialised IS technologies and technologies implemented by bank information systems.

4.2.9. It is recommended that RF BS organisations develop the structure and contents of their IS technology standards based on GOST R 1.4-2004.

4.2.10. Individual IS policies should be developed and approved in consultation with the representatives of:
– The RF BS organisation's management and specialized subunits;
– IT and security services.

4.2.11. Second-level documents may be approved by RF BS organisations' supervisors (or its specialized subunits), his or her representative for IS matters or other officials competent to address the issues covered by the said documents.

The examples of individual IS policies and IS plans based on STO BR IBBS-1.0 and reconciled with international standards [2] are provided in Appendix B.

4.3. Third-Level Documents

4.3.1. Third-level IS documents include documents that set forth the requirements for IS procedures performed by employees within the scope of operations that implement the technologies targeted by the RF BS organisation's individual IS policies.

4.3.2. It is recommended that the documents with IS requirements for the procedures performed both by the RF BS organisation's structural subunits and employees describe the order of actions and (or) imposed restrictions in detail, which will make it possible to clearly determine the rules for fulfilling IS tasks at each work place and for each IS role, and to establish a specific responsibility for complying with the prescribed requirements.

4.3.3. Documents with IS requirements for procedures include, for example, the following:
– IS instructions, including job descriptions;
– IS manuals, for example, on asset classification;
– Methodological IS recommendations;
– Documents with configuration requirements.

4.3.4. IS instructions, manuals and methodological recommendations contain a set of rules that establish the procedure and method for individual IS operations.

4.3.5. IS instructions, manuals and methodological recommendations are subject to increased requirements for accuracy and clarity of text. The documents at this level, unlike higher level documents, describe specific techniques and the order of actions for employees handling assigned tasks (for example, within the scope of a role) or specific restrictions.

4.3.6. IS instructions, manuals and methodological recommendations should include:
– One or more subjects whose activities are regulated by the instructions and (or) the name of the activities described by the instructions;
– Resources required to perform the activities;
– Detailed description of the operations performed, including the restrictions imposed, and the result of implementing the instructions;
– The subject(s)' obligations within the scope of the regulated activities;
– The rights and responsibilities of the subject(s).

4.3.7. Documents containing configuration requirements determine specific system values and their component parameters, as well as how to configure their parameters, allowing them to provide the required level of information security.

4.3.8. The documents with IS procedure requirements may be approved by the persons responsible for implementing the relevant IS activities.

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

4.4. Fourth-Level Documents

4.4.1. Fourth-level IS documents include documents containing the outcomes of IS activities regulated by documents of the upper hierarchy levels per the document structure provided in Figure 1. Evidence of activities performed in conjunction with documents from the higher levels of the hierarchy may serve as documented proof for meeting IS requirements upon internal control and external audit of IS within an RF BS organisation.

4.4.2. This group includes such documents as:

– Registers and inventories (for example, an inventory of the RF BS organisation's information assets);
– Registration journals, including incident registration journals;
– Protocols (for example, a test protocol);
– Reference lists;
– Obligations (for example, non-disclosure obligations);
– Acts;
– Agreements;
– Reports.

4.4.3. The obligation for RF BS organisations to provide documents with evidence of fulfilled IS activities is determined by the requirements set forth in the internal IS documents of the upper hierarchy levels.

4.4.4. The documents with evidence of fulfilled IS activities may be provided both in an electronic form and in hard-copy.

4.4.5. It is recommended to make a hard copy of documents with containing evidence of fulfilled IS activities that are submitted in an electronic form.

4.4.6. The documents with evidence of IS activities must be archived. The period of storage may be determined by Russian law and Bank of Russia regulations or by the RF BS organisation itself.

5. Management of Information Security Documents

5.1. IS document management is aims to ensure RF BS organisations develop, account, use store, audit and make changes to its IS documents.

5.2. When managing IS documents, the documentation of activities is to be ensured in order to:

– Ensure the validity of documents before they are approved and published;
– Periodically review, update (where necessary) and re-affirm the documents;
– Guarantee the possibility of identifying any changes made to the documents and the possibility of determining the current status of the documents;
– Ensure that the required documents are available and reviewed by the RF BS organisation's employees;
– Ensure that the documents are only accessed by the RF BS organisation's employees who are responsible for such documents;
– Ensure that the documents are protected from unauthorised changes;
– Ensure that documents are legible and identifiable;
– Identify documents created outside the organisation;
– Prevent the use of obsolete documents;
– Use appropriate labelling for outdated documents when storing them for any purpose.

5.3. IS documents must be managed subject to the existing laws and regulatory documents of the Russian Federation, the Bank of Russia regulations, and RF BS organisations' internal documents.

Appendix A
(for reference)

Example of the Requirements Set by International Standard ISO/IEC 13335-1 for the Structure (hierarchy) and Contents of Organisations' Internal IS Documents

This appendix provides an example of ISO/IEC 13335-1 requirements for the composition and contents of an organisation's internal IS documents per subsections 4.2 and 4.3 thereof.

4.2. Hierarchy of Policies

Corporate security policies may consist of security principles and instructions for organisations as a whole. Corporate security policies must reflect wider policies, including those pertaining to personal rights, requirements and standards of law.

Information security policies may contain principles and instructions on protecting information which is sensitive or essential for an organisation. The principles contained in information security policies are derived from the principles set by corporate security policies and, thus, concur with them.

Security policies for corporate information and communication technologies (ICT) should reflect essential ICT security principles and instructions which are applicable to the corporate security policies and the information security policies, as well as general provisions on using ICT systems within an organisation.

ICT systems security policies should reflect the security principles and guidance contained in corporate ICT security policies. It must also contain details of specific security requirements and protective measures to be implemented, as well as the procedures for the correct use of such protective measures in order to ensure adequate security. In all cases, it is essential that the selected approach is effective in terms of the organisation's business needs.

Where appropriate, the corporate ICT security policy may be included in a range of policies, such as technical polices and management policies that altogether constitute the basis for the corporate ICT policy. This policy must include some persuasive words on the importance of security, especially if security is to be reconciled with this policy. Figure 2 gives an example of a possible hierarchical relationship of policies. Regardless of the documentation and the organisational structure, it is crucial that various provisions of the described policies are taken into account and reconciled.

Other more detailed ICT security policies are necessary for special ICT systems and services or for a group of ICT systems and services. They are usually called ICT systems security policies. An important aspect of management is that the scope and limits of such policies are clearly defined and the policies themselves are based on technical and business requirements.

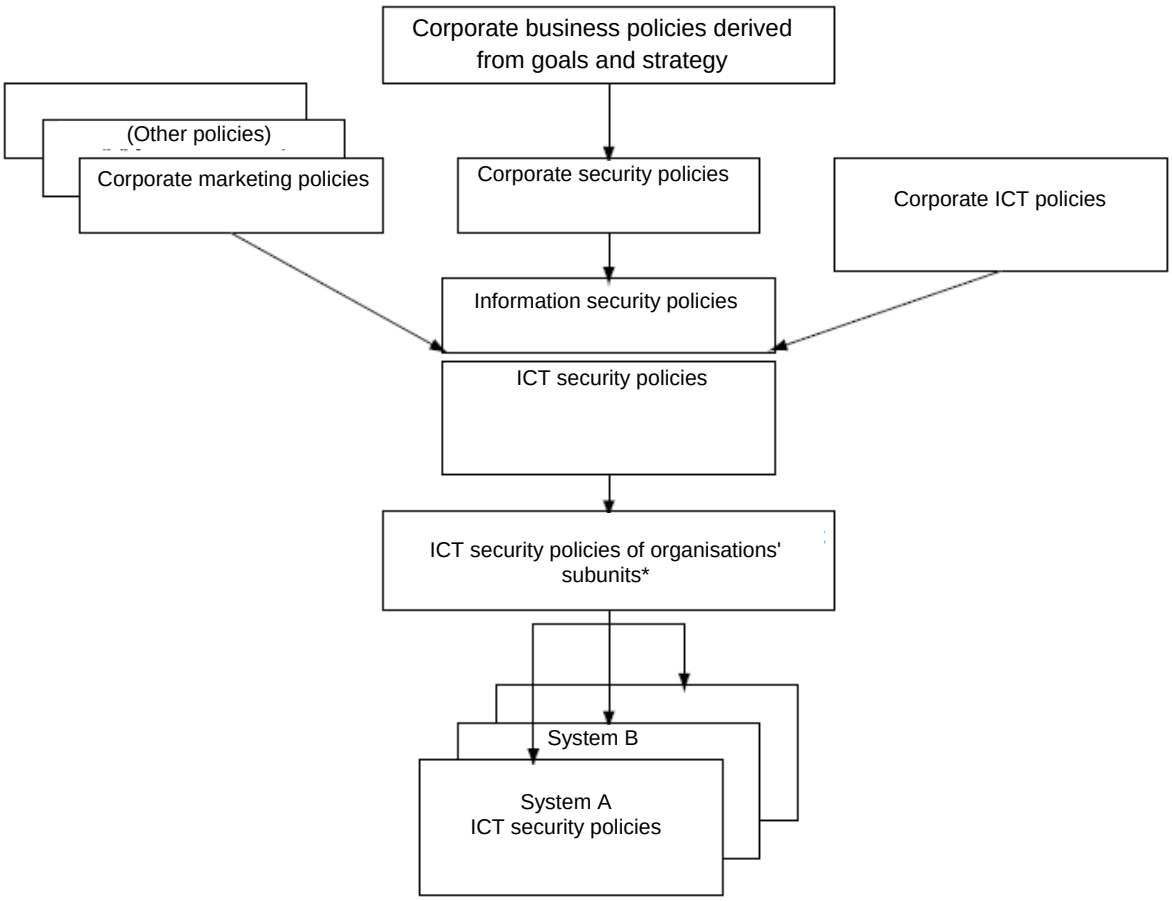
4.3. Elements of Corporate ICT Security Policies

Corporate ICT security policies must be developed based on the adopted corporate ICT goals and strategy. It is essential to establish and maintain corporate ICT security policies that are compatible with other policies such as: legal, regulatory, corporate business, security, information, and communication technologies.

The more an organisation relies on information and communication technologies, the more important it's security becomes, in helping the organisation make sure its business goals will are attained. When an organisation makes its corporate ICT security policy, it must take into account its cultural, environment and structural characteristics as they can affect its approach to security.

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

Figure 2. Hierarchy of Policies



* The depth of the hierarchy (number of levels) depends on a number of factors, for example the size of an organisation.

For example, certain protective measures that can be easily accepted in one environment may become completely unacceptable in another environment. The security activities described in the organisation's corporate ICT security policy may be based on its goals and strategies, the previous assessment of its security risks and management analyses, as well as on the results of actions taken, such as auditing the security of implemented protective measures, audit monitoring, analysing its ICT security in daily use, and reporting on security incidents. Any serious threat or vulnerability detected in the course of such activities must be handled using the corporate ICT security policy that describes the organisation's general approach to dealing with such security problems. Detailed actions are described in various ICT security policies or in other supporting documents, such as operating security procedures.

Development of corporate ICT security policies should involve representatives of organisations' following services:

– Auditing;
– Law;
– Finance;
– Information Systems (technologies and users);
– Utilities/Infrastructure (i.e. persons responsible for the structure of buildings and furniture, electricity supply and air conditioning);
– HR;
– Security;
– Business Management.

Commensurate specifications are determined for corporate ICT security policies in accordance with the organisation's security goals and strategy for attaining its objectives. Corporate ICT security policies must consider the following general areas:

– Scope of its application and purpose;
– Security goals with respect to legal and regulatory obligations, as well as business goals;
– Security requirements for information and communication technologies in terms of confidentiality, integrity, availability, fail-safety, accountability and authenticity of information;
– References to the standards on which the policy is based;

- Administration of information security, including responsibility and powers, both individual and organisational;
- Risk management approach adopted by the organisation;
- Method for determining the priorities in implementing protective measures;
- General level of security and residual risk found by management;
- Any general rules of access management (logical or physical access to buildings, rooms, system and information);
- The organisation's approach to training and skills in security issues;
- General procedures, inspections and support of security;
- General personnel security issues;
- Method for making all relevant persons aware of the policy;
- Circumstances under which the policy is to be revised or audited;
- Method of controlling any changes made to the policy;

Organisations assess their requirements, environment and culture to determine special issues that best meet their circumstances. Such issues may include:

- Security requirements for information and communication technologies, for example in terms of confidentiality, integrity, availability, fail-safety, accountability, authenticity and reliability, especially from the point of view of own assets;
- The organisation's infrastructure and allocation of responsibilities;
- Integration of security in the development and supply systems;
- Definition of methods for classifying information and classes;
- Risk management strategies;
- Business continuity planning;
- HR issues (special attention must be paid to personnel of whom trust is required, for example service staff and system administrators);
- Skills and training;
- Legal and regulatory obligations;
- Management of outsourcing;
- Management of information security incidents.

As discussed earlier in this subsection, the results of previous risk assessment analysis, inspection of security compliance, and information security incidents may affect corporate ICT security policy. This, in turn, may require that the previously determined strategy or policy is revised or clarified. In order to provide adequate support for all security measures, corporate ICT security policies must be approved by the management.

Mandatory instructions for all managers and employees are to be developed, based on corporate ICT security policies. This may require a document to be signed by each employee who recognizes his or her responsibility for the organisation's security. Also, a Skills and Security Training Program must be developed specifying all the said responsibilities.

A person is to be appointed who is responsible for the corporate ICT security policy and for ensuring that the policy includes the organisation's requirements and current status. This position is usually given to a person who is officially responsible for corporate ICT security who, inter alia, is also accountable for other activities that include inspection of security compliance, repeated analyses and audits, handling of security incidents and vulnerabilities and any changes in the corporate ICT security policy which may be required as the result of such actions.

Appendix B
(for reference)

Example of Information Security Documents

B.1. This appendix provides an example of IS documentation support based on the provisions of STO BR IBBS-1.0, and the international standard [2].

B.2. An example of individual IS policies is provided in Table B.1.

Table B.1. Example of individual IS policies

Individual IS policies
E-mail and Internet policy
Antivirus Policy
Policies for monitoring and managing information security incidents
IS policy in access management and registration
IS policy in assigning and distributing roles and ensuring credibility of the personnel
IS policy for bank payment operations
IS policy for IS of bank information operations

B.3. An example of information security plans and justification for such plans is provided in Table B.2.

Table B.2. Example of IS plans

IS plans	Points standards
IS audit plan (external and/or internal)	STO BR IBBS-1.0: 10
Actions plan after IS audit	STO BR IBBS-1.0: 5
IS Training Plan	STO BR IBBS-1.0: 8.2.2
Plan for business continuity and recovery after interruptions	STO BR IBBS-1.0: 9.6

Bibliography

[1] ISO/IEC 13335-1:2004 Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

[2] ISO/IEC 17799:2005 Information Technology — Code of practice for information security management

Key words: Russian banking system, information security, documentation, information security policy, information security regulation, information security instruction, and information security requirements.

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