Ensuring Information Security Controls for the Russian Banking Organizations

Andrey Kurilo
The Central Bank of Russia

Natalia Miloslavskaya
The Moscow Engineering Physics Institute (State University)
Kashirskoe highway,31
Moscow, Russia
+7-495-323-90-84
milmur@mephi.edu

Svetlana Tolstaya
The Central Bank of Russia
ait@mephi.edu

ABSTRACT
An approach to develop the controls system (CS) in the field of maintenance of information security (IS) for the Russian banking organizations, based on the well known international and Russian standards, is offered. The CS elements are interconnected with each other by IS control processes (controls or control directions): IS monitoring, IS self-assessment, external IS audit, the analysis of IS maintenance system functioning, IS maintenance system analysis by an organization's management. The general structure of the CS is defined. Relations and connections of processes with each other within the CS are shown. The structured representation (specification) of each of the CS processes is developed, but as two examples only IS monitoring process and IS maintenance analysis by the Organization's management are described in detail.

General Terms
Management, Security

Keywords
Information Security, Security Controls, Banking Organizations, Russia

1. INTRODUCTION
Banking institutions as one of the most sensitive objects could have a wide range of consequences from breaking the security of their banking information (from viewpoint of confidentiality, integrity, availability, accountability, non-repudiation, etc.) ranging from financial loss of an individual to financial crisis of a country.

The banking system of the Russian Federation is formed by the Central Bank of Russia, different credit organizations (for e.g., the Savings Bank, the Vneshtorgbank, the Vnesheconombank, regional banks, etc.), and representative and branch offices of foreign banks. These organizations solve different business problems and have different structures (for e.g., have or have not regional branches).

To increase stable functioning of the Russian banking organizations (further the Organizations), to achieve adequacy of protection measures to real information security (IS) threats and to prevent/reduce damage from IS incidents the Standard of the Central Bank of Russia (STO-1.0) “Ensuring Information Security in Organizations of Banking System of the Russian Federation. Basic principles.” (further the Standard) has been adopted in 2004 [1]. After that the main statements of the Standard have been detailed in its two later editions (2006 and 2008) and in another documents, devoted to various aspects in the field of IS: documentation for IS maintenance system functioning, asset classification, risk analysis, IS audit and self-assessment and so on. But only the basic statements for the named areas, without any detailed description of IS maintenance processes and control actions, allowing to reveal real efficiency of IS maintenance system functioning, are given in these documents.

Thus there is a task of careful developing of the controls system (CS) in the field of IS maintenance for the Organizations.

2. IS MAINTENANCE CONTROL SYSTEM
IS maintenance system of the Organizations is a set of IS system (ISS) and represents IS management system (ISMS) [1], where ISS is a set of the protective measures implementing IS maintenance of the Organization and ISMS is a set of IS management processes, including resource and administrative (organizational) maintenance of these processes.

The control framework is a common one proposed by ISO 27001, CobiT standards and it is used in many markets. But for the first time we use it for the Russian banking system. According to the Standard and ISO 27001 [2] for IS maintenance in the Organization implementation of four groups of the processes (Plan – Do – Check – Act) is necessary. IS maintenance control includes activities within the group of "Check" processes, being carried out by management, departments and employees of the Organization and consisting in checking and assessment of IS maintenance.

IS maintenance control processes (let’s name them controls or control directions), implemented in the Organizations, allow to avoid IS maintenance system degradation due to duly and adequate acceptance of reciprocal measures and to provide required IS level for the Organizations for a long time.

The purpose of IS maintenance control is maintenance of sufficient confidence that IS maintenance system functions effectively, properly (according to IS policies or another accepted by the Organization normative documents), adequately to existing IS threats and also to internal and external conditions of the Organization’s functioning.
According to the best practices the basic requirements to IS maintenance control can be formulated as follows.

1. IS control should be carried out on a regular basis, thus periodicity of IS control depends on speed of decrease in protection mechanisms efficiency (degradation of IS properties of a controllable object).

2. IS control processes (procedures) should be defined in the internal Organization's documents and are regulated (to be carried out according to rules, instructions, manuals, etc.).

3. The principle of division of the rights between persons, whose activity is a subject to control, and the persons, who are carrying out control, should be carried out.

4. IS control results should be objective, authentic, repeated and exact (objectivity is defined as absence of bias and the subjective attitude; reliability is defined as conformity of the validity; accuracy is defined as observance of severity in measurements and the maximal affinity to real data).

5. Results of IS control procedures should be documented, that is prove to be true by the documents containing the certificates and (or) results of their performance.

6. It is necessary to provide trust to IS control results.

Simultaneous performance of these requirements is possible only at realization of a system (so called complex) of control actions, incorporated in the CS in the field of IS maintenance.

3. CS GENERAL STRUCTURE

Thus, the CS (IS control system) is a set of control processes (within the group of ISMS "Check" processes) interconnected with each other and cooperating among themselves for achievement of an overall aim of IS maintenance control of the Organization. This is carried out by implementing the following processes:

- IS monitoring (M);
- IS self-assessment (SA);
- external IS audit (EA);
- IS maintenance system functioning analysis (A);
- IS maintenance analysis by the Organization's management (MA).

Interrelation of the CS processes is shown at Fig.1.

![Figure 1. CS general structure](image)

IS monitoring is carried out continuously. On the basis of IS monitoring results the operative assessment of IS maintenance system state is formed. Reports with IS monitoring results, in particular data on IS events and incidents, are used at carrying out of IS self-assessment, external IS audit, IS maintenance system functioning analysis, including its analysis by the Organization's management.

Periodicity of carrying out of IS self-assessment and external IS audit depends on speed of protective measures and IS maintenance system efficiency decrease. This period is defined in internal documents of the Organization. Results of IS self-assessment and external IS audit are used at IS maintenance system functioning analysis, including its analysis by the Organization's management.

By results of all control actions reports to the Organization's management are formed, which they use at carrying out their own IS maintenance system analysis. Thus the form and the contents of the specified reports depends on a Chief’s level (head of IS department, head supervising IS questions, top management of the Organization). Results of all control actions are analyzed by the Organization's management and are used for preparation of plans on measures for IS maintenance system perfection.

The further description of the Organization’s IS maintenance system should be directed on the detailed specification of each process forming the CS. This specification should contain the following:

- main aim and tasks of activities within each process;
- requirements to activities within each process;
- input data for each process;
- necessary resources;
- requirements on each process management;
- output data for each process.

4. IS MONITORING

Let’s consider the first process – IS monitoring – according to the approach.

The Organization’s IS monitoring can be defined as constant supervision over objects and subjects influencing the Organization’s IS maintenance, and also gathering, analysis and generalization of the specified supervision information [1].

In concept of IS monitoring the continuity of process in time (continuous supervision and registration of the events influencing on IS) is included. These events are exposed to the analysis on the basis of which the conclusion about presence or absence of IS incident is made.

The basic purposes of IS monitoring are the following:

- revealing and analysis of actions and events influencing IS maintenance (revealing supernumerary (including bad-intentioned) actions, revealing of infringements of security requirements (IS incidents) and granting of data both on already come to pass and on potentially possible IS incidents);
• control over observance of IS requirements fixed in IS policies and other internal normative documents on IS maintenance of the Organization;
• operative granting initial data for IS risks assessment and analysis, for formation of the correcting influences minimizing IS risks or reducing them to an acceptable level, and also for prevention of users’ errors or minimization of their consequences, etc.

Performance of activities within the IS monitoring process provides transparency of used technologies (technological processes), and also guarantees their observability during all time of functioning, that as consequence, increases a level of trust of business to the given technologies.

The primary goals of activities, being carried out by the Organization’s personnel, responsible for IS within the IS monitoring process, are the following:
• control and registration of changes in the Organization’s information sphere, analysis of corresponding log files;
• error detection and registration for procedures of generation, storage, processing, transfer and use of the Organization’s information assets, analysis of corresponding log files;
• supervision over the Organization’s information sphere with a view of revealing and registration of IS incidents (successful and unsuccessful infringements of IS requirements (IS policies), analysis of corresponding log files;
• definition of the actions undertaken in reply to arisen IS incident, registration of these actions;
• registration of other actions influencing IS maintenance (for example, actions and events in systems, the most critical from the business point of view and being the subject to a high level of risk, that should be fixed in corresponding documents of the Organization), analysis of corresponding log files;
• supervision over protective measures functioning, registration of corresponding events, analysis of log files, etc.

The Standard defines the following requirements to IS monitoring process implementation [1].

1. Procedures of IS maintenance system monitoring should be documented. The specified procedures should be carried out by the personnel of the Organization, responsible for IS maintenance, and cover all the implemented and maintained protective measures included in the IS maintenance system.

2. Procedures of writing checks documentation, fixing actions of employees of the Organization, events and parameters, concerning functioning of protective measures, should be documentary defined.

3. Procedures of IS maintenance system monitoring should be executed. Results of implementing the specified procedures should be documentary fixed.

4. Information on all incidents, revealed during monitoring, should be stored in a joint database of IS incidents.

5. Procedures of IS maintenance system monitoring should be exposed to the regular and documentary fixed revisions in connection with changes in structure and ways of protective measures usage, revealing of new IS threats and vulnerabilities, and also on the basis of data on IS incidents. The order of revision procedures implementation should be documentary defined.

6. Roles concerning IS maintenance system monitoring procedures implementation and revision of the specified procedures should be documentary defined in the Organization. Persons responsible for performance of the specified roles should be appointed.

7. The process should last in time.

8. Principle of rights division between persons, whose activities is a subject to monitoring, and the persons, who are carrying out monitoring, should be implemented.

9. Types of actions and events subjected to IS monitoring (for example, any changes or attempts of changes of tools and systems configurations) should be defined and fixed.

10. Documentation defined procedures of reaction to the incidents revealed during monitoring IS should be carried out.

11. Documentary defined procedures of storage and usage of the data, gathered during IS monitoring procedures, should be carried out.

12. Integrity, confidentiality and availability of documentary fixed results of IS monitoring procedures, including log files archives, should be provided to the authorized persons during defined time for additional investigations and gathering of IS infringements proofs, etc.

Activities within IS monitoring process is carried out by means of the following methods and mechanisms:
• tools for control over topology, architecture and configuration options of the banking systems and protection tools;
• tools for control over IS policies requirements implementation (for different systems and different technological processes), log files analysis tools, IS events aggregation systems;
• security scanners;
• intrusion detection and prevention systems;
• administrative control over IS requirements implementation fixed in IS policies and other internal normative documents on IS maintenance of the Organization, including administrative control over observance by employees of instructions and rules;
• administrative control over execution of assignments, working plans and other administrative documents;
• documents distribution and usage control;
• control over procedures (carried out actions) documenting.

Operating influences on the given process are the following:
• requirements of the legislation of the Russian Federation, normative legal acts of the Central Bank of Russia, the standards;
• main statements of internal normative and methodical documents containing the requirements to IS monitoring;
• decisions of the Organization’s management, administrative documents of the Organization.

Input data for the process are the following:
• data on the Organization’s assets and infrastructure;
• actions and events occurring in the Organization’s information sphere at realization of technological processes;
• IS maintenance system structure (components and mechanisms of protective measures implementation, processes of protective measures operation, processes of IS management);
• internal documents on IS maintenance containing IS requirements (IS policies, rules, instructions, etc.);
• internal documents on IS maintenance containing evidences of IS requirements implementation (protocols, acts, log files, etc.);
• data on IS threats and possible intruders (models of IS threats and intruders), etc.

Necessary for the process resources are the following:
• financial,
• material (various hardware-software monitoring tools, specialized equipment and software, etc.),
• information,
• time,
• human (IS department).

Output data for the process are the following:
• documentary fixed results of IS monitoring procedures implementation (reports with IS monitoring implementation results);
• registers and log files;
• data on IS threats and possible intruders;
• data on revealed IS threats and vulnerabilities of IS maintenance system.

Thus developed by the paper’s authors IS monitoring process can be illustrated by fig.2.

5. IS MAINTENANCE ANALYSIS BY ORGANIZATION’S MANAGEMENT

Performance of activities within IS maintenance analysis by Organization’s management process allows to make the proved decisions concerning usage of protection measures adequate to ratio of their cost and possibility of IS threats implementation.

The main aims, being carried out within the process, are the following:
• IS maintenance system functioning problems definition and analysis;
• definition of necessity of IS maintenance system strategic improvements.

The primary tasks of activities, being carried out within the process, are the following:
• IS monitoring, IS self-assessment, external IS audit and IS maintenance system functioning results analysis;
• revision (if necessary) of an acceptable risk level;
• analysis of a residual risk level;
• analysis of proposals of the interested parties;
• definition of directions of strategic IS maintenance system improvements.

The Standard defines the following requirements to the process implementation [1].
1. List of the documents (data), given to the Organization’s management for carrying out of analysis, should be approved. In particular, it should include results of IS maintenance system monitoring and control of protective measures, reports with results of its functioning analysis, external IS audits and IS self-assessments; documents, containing information on ways and methods of protection, protective measures or procedures of their usage which could be used for IS maintenance system functioning improvement, on new and just revealed IS vulnerabilities, threats and incidents, on actions carried out by management according to results of previous analyses, on changes, which could affect IS maintenance system (for example, changes in the legislation of the Russian Federation); documents, confirming performance of demanded activities on IS maintenance (for example performance of plans of risk processing) and requirements of a business continuity and its restoration after interruption.

2. Plan of performance of activities under IS maintenance control and analysis should be defined by the Organization’s management. In particular, the specified plan should contain positions on carrying out of meetings at a management level, during which, for example, influencing business IS problems search and analysis is made.

3. Roles concerning preparation of documents, necessary for IS maintenance system analysis by management, should be documentary defined within the Organization. Persons responsible for performance of the specified roles should be appointed.

As IS monitoring, the IS maintenance analysis by Organization’s management process can be illustrated by fig.3.

6. CONCLUSIONS

An approach to develop the CS in the field of maintenance of IS for the banking organizations is offered. The control framework is a common one proposed by ISO 27001, CobiT standards and it is used in many markets, but for the first time it has been used for the Russian banking system. This approach is universal and it can be applied for the other organizations as well. The CS elements are interconnected with each other IS control processes: IS monitoring, IS self-assessment, external IS audit, the analysis of IS maintenance system functioning, IS maintenance system analysis by the Organization’s management. The general structure of the CS is defined within which relations and connections of the processes with each other is shown. The structured representation (specification) of each of the CS processes is developed. As an example only two processes – IS monitoring process and IS maintenance analysis by Organization’s management – are described in detail.

7. REFERENCES
