

Structure of the Report on Studies of Best Practices within the scope of the subject area of access control

- 1. Scope of subject area** – Information security: technologies of control of information access, Access Monitoring and Control System (hereinafter AMCS), control of accounts and cryptographic protection of information

1.1. Objectives

- to obtain consulting services and proposals for optimization of the existing system of control of access to information resources;
- to obtain consulting services and proposals for optimization of the existing AMCS (a set of security software and hardware designed for restriction and recording of entry/ exit of objects (personnel, transportation vehicles) in the specified territory through passage points (doors, gates, checkpoints));
- to obtain consulting services and proposals for optimization of the existing system of creation and management of accounts;
- to obtain consulting services and proposals for optimization of the existing system of encryption of documents when making electronic payments, message exchange and accessing to data;
- to obtain assessment of the current situation within the scope of the subject area, based on ISO/ IEC 27000 and CobiT international standards together with recommendations for achieving of compliance with these standards;
- to obtain detailed report on possibilities to apply the best practices and methodologies of the best world-wide practices within the scope of the subject area;
- to obtain recommendations for acquiring of new technologies, optimization of costs and technical policy within the scope of the subject area.

1.1.1. Decomposition of subject area

1.1.1.1. Recording and control of information access

The above shall be carried out in special-purpose information system on the IBM Lotus Notes platform. A set of access rights of the end system shall be recorded in the record card of automated work station (hereinafter AWS). Change of access parameters shall be implemented on requests approved by the responsible persons. Pool of requests shall determine job competency profile. When an employee is appointed to a post, the respective job competency profile shall be available automatically. Requests for changes of access parameters shall be processed automatically or sent to access administrators. List of access rights required for performing of functions shall be determined by the internal regulations and procedures.

The main parameters of the system:

- more than 5 500 record cards of AWS;
- automated processing without involvement of the access administrator by way of including of user accounts in the Active Directory (AD) is implemented for 55 % of AWS or for the end system;
- up to 40 000 requests for changing of access parameters shall be processed on a monthly basis;
- there shall be more than 7 000 active system users;

- accesses for more than 300 information systems on the IBM Lotus Notes platform, 200 information systems on other platforms, more than 200 file resources and 100 technical resources for different privileges in the corporate network shall be recorded.

1.1.1.2. AMCS

Recording of passage points in the Access Control System and approval of access to the objects shall be carried out similar to recording and access to information resources (as described in p. 1.1.1.1). Changing of access parameters for third party users shall be carried out when giving of ID cards or via the Service Desk. Apacs 2.x and Apacs 3000 shall be used as the run-time system. Changing of access parameters on requests shall be carried out by the access administrator manually.

The main parameters of the system:

- more than 1 500 passage points equipped with the Access Control System (hereinafter ACS);
- up to 5 000 requests for changing of parameters of access to the objects shall be processed on a monthly basis;
- 20 000 identifiers (ID cards) shall be available in the system.

1.1.1.3. User accounts

Acquisition of information required for registration shall be carried out in presence when providing employment or when approving access to any new information system using its own accounts.

The main parameters of the system:

- up to 20 000 employees using two and more accounts.

1.1.1.4. Cryptographic protection of information

- Using of cryptographic algorithms when encrypting documents on the IBM Lotus Notes platform and dedicated systems for storage of documents in electronic format;
- Using of encryption operations and digital signature when exchanging messages and making of electronic payments by means of PGP, CryptoPro and LanCrypto (up to 300 users) software products.

1.1.2. Plans

Steady operating of the Access Control System and of the AMCS, automation of the processes of access life cycles (full automation of access to the AMCS, maximum automation of access to information resources) and automation of the processes of account life cycles.

2. Automation/ key functions

To render consulting services with respect to automation of the key functions of the following production processes:

• Control of access to information resources

1. Automation of changing of access parameters on request in the end systems on different platforms; exclusion of the access administrator from the process of request processing and minimization of the impact of the human factor and of risks when granting access;

2. Automation of generation of requests for changing of access parameters on the basis of automated forms of the internal regulations and procedures; minimization of manual execution of requests for changing of access parameters;
3. Automation of the process of generation of record cards of AWS on the basis of automated templates when putting the information system into operation;
4. Reducing of the average time required for granting of access;
5. Audit of the granted access, automated inspection of the authorized and actual accesses, automated correcting and updating of access parameters if discrepancies are detected.

- **AMCS**

1. Automation of changing of access parameters on request; exclusion of the access administrator from the process of request processing and minimization of the impact of the human factor and of risks when granting access;
2. Automation of generation of requests for changing of access parameters on the basis of automated forms of the internal regulations and procedures; minimization of manual execution of requests for changing of access parameters;
3. Automation of the process of generation of record cards of access objects on the basis of information about new hardware received from the run-time system;
4. Audit of the granted access, automated inspection of the authorized and actual accesses, automated correcting and updating of access parameters if discrepancies are detected;
5. Automation of request and granting of access to external counterparts via profiles available in the web-interface;
6. Implementation of the function of control of reentry in the entire territory of the airport facilities;
7. Integration with BMS.

- **Management and control of user accounts**

1. Automation of generation, changing, blocking and deleting of accounts;
2. Implementation of IAM technologies;
3. Implementation of Single Sign-On technologies.

- **Cryptographic protection of information**

1. Automation of key life cycles (generation, support and response);
2. Automation of checking of cryptographic keys for compliance with the requirements of information security.

Other innovation solutions aimed at reduction of staff, mitigation of risks of information security within the scope of the subject area and reduction of time required for carrying out of operations.

3. Analysis of application of best practices

3.1. Requirements to reports:

All the proposals and recommendations shall be documented in Russian and submitted in hard copy and in electronic format (PDF/ DOC).

Every report shall have the following structure:

3.1.1. Title page;

- 3.1.2. Table of contents;
 - 3.1.3. References, definitions, notations and abbreviations (if any), based on standards and regulations;
 - 3.1.4. Introduction;
 - 3.1.5. Body of report:
 - 3.1.5.1. Proposals for establishing/ optimization of business process:
 - To describe the best practice in establishing of business process; to give no less than 3 examples of using of proposals in companies with headcount of more than 2 500;
 - 3.1.5.2. Proposals for establishing/ optimization of organizational structure:
 - Establishing of structure when implementing/ optimizing of business processes; proposals with respect to methods of optimization of interaction between functional departments;
 - 3.1.5.3. Requirements to knowledge and skills of employees:
 - Appraisal of the required qualification of the process participants; submitting of the requirements to employees to ensure performing of functions after implementing/ optimizing of business processes;
 - To propose a list of recommended training courses used in the best practices for improving of skills and qualification of employees;
 - 3.1.5.4. Proposals for establishing/ optimization of metrics of KPI, SPI and reports:
 - Finding and analysis of KPI/ PPI / measures of employee motivation used in the best practices which contribute to achieving of significant performances within the scope of the subject area;
 - 3.1.5.5. Proposals for motivation of participants of business process:
 - Motivation of participants of business processes/ KPI and SPI indicators used for remuneration of labor of employees and methods of stimulation and motivation of participants of business processes which contribute to achieving of significant performances within the scope of the subject area;
 - 3.1.5.6. Proposals with respect to documentation:
 - Assessment of the existing forms and rules of approval of documents required for control and analysis of the indicators used in the best practices; establishing of new forms and rules when implementing/ optimizing of business processes;
 - 3.1.5.7. Possibility to outsource activities:
 - Not to be considered;
 - 3.1.5.8. Forms of agreements:
 - Assessment of the existing templates of agreements used in the best practices with respect to risks and completeness of description of needs and requirements; proposals of changes;
 - 3.1.5.9. Automation facilities:
 - Consultant shall propose at least 3 different facilities for automation of the processes specified in paragraph 2. The best facilities shall be selected; positive experience in application thereof in Russia is advisable and desirable; such facilities shall be completely localized;
 - Feasibility study shall be issued, technical and organizational risks of implementation shall be assessed as well as advantages and disadvantages shall be described for each automation facilities;
 - 3.1.6. Conclusion;
 - 3.1.7. List of used references;
 - 3.1.8. Annexes (if required).
- New types of documents proposed for use in DME shall be executed as templates in the form of separate annexes to the baseline documents.

4. Standards on production facilities/ document forms

- There are no special requirements to production facilities.
- List of the main types/ forms of documents required with respect to the subject area and for application of the best practices shall be submitted within the scope of consulting. The list of documents shall include requirements to the contents and the rules of drawing up thereof.

5. Standards (mandatory/ guidance)

Consultant shall use the following practices, standards and Federal Laws:

- ISO/ IEC 27000;
- GOST R ISO/ IEC 27001;
- ITIL / ITSM
- CobiT;
- FZ-63 On electronic signature;
- FZ-98 On commercial secrets;
- FZ-152 On personal information;
- FZ-161 On the national payment system.

6. Best training courses and companies

To propose a list of the best training programs/ courses and counterparts for the employees involved in designing and automation of business processes for the purpose of improving in qualification.

7. Milestones/ step-by-step acceptance

Consulting shall be rendered during a period of time not exceeding 6 months. Consulting may be rendered in accordance with the following milestones (1 milestone equals one point of paragraph 1.1); it is recommended to carry out works under several milestones in parallel.

7.1. Issuing of the schedule of submitting of the results of the carried out study with due account for the following requirements:

- 7.1.1. All the research works may be divided into conceptual blocks; results of each block shall be formalized;
- 7.1.2. Results of each block may be submitted consistently (i.e., each subsequent block shall be based on the previous block(s) or in parallel (if blocks are independent on the previous and/ or subsequent blocks));
- 7.1.3. Both independent solutions and integrated solution for automation/ software products may be proposed at each milestone;
- 7.1.4. Submitting of the results of each block shall be clearly time-bounded, i.e., specific date shall be fixed;
- 7.1.5. In the course of works under each block/ milestone, interim meetings shall be held every 10 working days and mandatory prior to submitting of the final results of studies under each conceptual block/ milestone;
 - To learn about the practices applied in DME;
 - To provide assessment of the best world-wide practices in the field of maintenance and support of weak current systems;
 - To provide activity-specific detailed report on the best practices with respect to maintenance and support of weak current systems (recommendations shall be made with due account for organizational, technical and legal environment of organizing of IT activities in DME);

Acceptance shall be carried out in a step-by-step manner. Consent of the Customer with completeness and clearness of the results submitted in accordance with the proposed schedule shall be deemed to be the fact of acceptance of any milestone.

8. Requirements to contractor

8.1. Consulting companies which have no less than 10 year experience in the field of information security: technologies of control of information access, AMCS, control of accounts and cryptographic protection of information and consulting projects for the said line of activity successfully implemented over the last 3 years and confirmed by letters of recommendation from at least 2 large customers (companies with headcount of more than 2 500);

8.2. Requirements to employees of the consulting company/ consulting department involved in carrying out of research:

8.2.1. Every employee of the research team shall:

- have no less than 5 year experience in the field of consulting;
- have participated in at least 2 successful projects within the scope of the subject area;

8.2.2. The leader of research team shall:

- have no less than 10 year experience in the field of consulting and no less than 10 year hands-on experience within the scope of the subject area;
- have been the leader of team/ department involved in at least 2 successful projects within the scope of the subject area;

8.2.3. To implement the project, consultant shall involve Russian speaking experts/ personnel or professional interpreters/ translators having knowledge in this area.