

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

1. Scope of subject area – Information security: monitoring of parameters of information security, protection of confidential information and evaluation of security of information systems.

1.1. Objectives

- to obtain consulting services and proposals for optimization of the existing system of monitoring of parameters of information security;
- to obtain consulting services and proposals for optimization of the existing system of protection of confidential information from leakage and eavesdropping equipment;
- to obtain consulting services and proposals for optimization of the existing system of evaluation of security of information systems;
- 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. Monitoring of parameters of information security

The above shall be carried out by means of automated facilities (LanDesk, Security Operations Center) manually as well as by way of visual inspections; activities of IT departments shall be also controlled.

The main parameters:

- monitoring and control of printing;
- antivirus protection;
- control of access to peripheral devices;
- control of start of applications;
- monitoring of actions of users and administrators;
- monitoring of parameters of stability of information systems;
- in-presence inspections of the data processing centers, routing centers and telecommunication facilities.

1.1.1.2. Protection of confidential information

The above shall be carried out by way of in-presence inspections of storage of hard copy documents at the work places of users (up to 8 000 employees) as well as inspections of premises and facilities for detecting of possible leakage channels.

1.1.1.3. Evaluation of security of information systems

The above shall be carried out by way of comprehensive inspection of the information system for compliance with the specified requirements to information security. Report shall include detected discrepancies and deviations, analytical conclusions about risks and proposals for further elimination thereof.

1.1.2. Plans

Maximum automation of carried out inspections for compliance with the requirements to information security, increasing of the number of information systems completely complying with the requirements to information security.

2. Automation/ key functions

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

- **Monitoring of parameters of information security**

1. Optimization of operating of the existing facilities of automation of carrying out of inspections;
2. Automation of tools of recording and notification about deviations of parameters of information security;
3. Automation of inspections of infrastructure services and departments;
4. Arrangement of filtration and sorting of acquired information by the specified parameters;
5. Automation of processing of detected discrepancies and taking of measures to eliminate thereof and to notify the responsible services and departments;
6. Automation of reporting on the carried out inspections.

- **Protection of confidential information**

1. Automation of control of storage of hard copy documents by way of implementing of tools of control of printing;
2. Implementation of means for on-line monitoring of possible channels of leakage of information.

- **Evaluation of security of information systems**

3. Automation of tools of evaluation of security of information systems by the specified parameters;
4. Automation of reporting on отчетности по проведенным оценкам защищенности

5. Analysis of application of best practices 5.1. 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.

6. 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.

7. 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-98 On commercial secrets;
- FZ-152 On personal information.

8. 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.

9. 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.

9.1. Issuing of the schedule of submitting of the results of the carried out study with due account for the following requirements: 9.1.1.All the research works may be divided into conceptual blocks; results of each block shall be formalized;

9.1.2.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));

9.1.3.Both independent solutions and integrated solution for automation/ software products may be proposed at each milestone;

9.1.4.Submitting of the results of each block shall be clearly time-bounded, i.e., specific date shall be fixed;

9.1.5.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 within the scope of the subject area;
- To provide activity-specific detailed report on the best practices within the scope of the subject area (shall be made with due account for organizational, technical and legal environment of organizing of information security 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.

10. Requirements to contractor 10.1. Consulting companies which have no less than 10 year experience in the field of information security: monitoring of parameters of information security, protection of confidential information and evaluation of security of information systems 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.