

Structure of the report on investigation of the Best practices in the domain of the information security management system (Sustainability of IS*)
Information Security.

1. Frames of the subject domain-scope of the research must lie in the following frames:

- as far as it relates to business risks analysis;
- as far as it relates to the regulation as an element of ISO 27001;
- as far as it relates to information protection (disaster recovery, fail safety, arrangement of the archival storage and other generally accepted requirements in IS which are focused on integrity maintenance, confidentiality, information accessibility)
- as far as it relates to problem settlement of information security;
- as far as it relates to IT-solutions implementation control and ITIL as a part.

1.1. Objects are as follows:

- to get advice as far as it relates to the assessment correctness of the identified risks of IS with the optimization suggestions
- to get a conformance evaluation of the current situation with the ISO 27001 standard and optimization suggestions;
- to get advice on the best methodology as far as it relates to information protection in the complex systems;
- to get advice on the applied elements of ITIL as far as it relates to implementation control of the IT-solutions and problem management of the information security with the optimization suggestions including related processes in the IT domain.

1.1.1.Decomposition of the subject domain.

Risks assessment

In the framework of the internal processes definition and maintenance of the current state of the main principals of the information security provision, information security risks, models of would-be intruders and as a result risk assessment of information security with the definition of risk severity and probability of incurrence of a certain risk category are held.

The indicated activities to maintain the current state of the regulatory structure form the current policy of the information security arrangement.

Information security management system.

The formal information security management system regulated by the standard ISO 27001 is not available.

However its actual existence is detected by expertise which accounts for the availability and interconnection of activities by risk management, creation, implementation, monitoring, support and improvement of the parameters of information security of different elements (first of all- IT) of such system as an organization.

Such activities are considered to be normal and are held in the frame of the internal rules.

Information protection.

Information protection is realized by specifying and controlling requirements' fulfillment of information security, different requirements applied in each certain requirements' system, be it an information system or some premises/a building a construction.

The following main requirements are controlled: maintenance of the information integrity, of confidential information, of information accessibility, prevention of the illegal use of the resources of the applied system/ of a system's element.

The process of information security problem management is realized fully and includes IS problem identification, assessment of risks of the unsolved problem of IS and also an action plan focused on elimination of IS problems and further control of the repeated incidents followed by IS problem identification.

Information security in ITIL.

As a minimum the requirements traceability in respect to IS is needed in 2 suggested ITIL processes (due to ITSM).

Control procedure of the IT-solution implementation is realized when configuration and

modifications management is carried out.

At each stage either of a life-cycle of the IT-system or of an object which is regarded to be of interest in relation with the IS some measurement of the parameters of IS, their accounting and action plan of them are held which are focused on the elimination of noncompliances with the compliances for this or that object of the IS requirements.

1.1.2. Action plans:

Availability of a distinct policy of the information security stipulates information classification which is generated in the organization in due confidentiality categories, in the plans of the task realization on automation of a list of confidential information which can be applied as an expert reference- book in the organization.

2. Automation/ main functions are as follows:

to provide consulting services on automation of the main functions of the below indicated processes focused on the sustainability increase of IS:

• Observation of the corporate regulations in the information security.

1. Development and issuing standard acts regulating the non-disclosure regime at the Company.
2. Monitoring of the parameters of the information security.
3. Arrangement of the agent examinations to maintain IS parameters.
4. Fixation of violations.
5. Issuing of reports on the fixed results, the analysis.

• Provision of sustainability of information storage.

1. Definition of the necessity of the centralized data back-up, issuing and maintenance of the relevant list of information resources.
2. Paperwork and accountancy of the procedure of the backup.
3. Archival storage of the sets of the backup, archive restoration due to requests and accountancy.
4. Optimization of movement of the sets of back-up in archives, of storage terms for the systems and data of various importance.
5. Cost optimization and adaptability of storage back-up with due regard to modern tendencies on the storage market.

• Implementation control of objects of the information security.

1. Control on the stage of the project development preparation for the project creation/ modification of the IT-solution.
2. Control on the stage of the project realization of the creation/ modification of the ITsolution.
3. Control of the input of the key configuration item of the IT-solution into operation.
4. Maintenance in the actual state of the compliance Register of the IT-systems with the sustainability parameters.
5. Control on the stage of the project initiation for the creation/ building modification/ premises/ offices where processing of confidential information will be performed.
6. Inspection checks arrangement of the indicated objects and compliance Register keeping for buildings/premises/ offices where processing of confidential information is performed with the information security requirements.

• Maintenance of the secure communication links.

1. Joint efforts with the bank to develop the project of the technical solution to create/to modify the secure communication link. Arrangement of the confidence technology, issuing credentials for the staff in charge.
2. Construction and putting into operation of the on-line banking type system and similar secure communication links.
3. Maintenance of the secure communication links, shut down. Maintenance of the certificate stores.

• security problem management

1. Events analysis of the information security, problem identification of the information security.
2. Search for the problem solution of the information security, making administrative

arrangements.

3. Assessment of the problem solution completeness in the information security, keeping analytics, problems' register of the information security.

3. Application analysis of the Best practices.

3.1. **Report requirements:** All suggestions and recommendations shall be recorded, issued in the Russian

language and submitted as a hard copy and in a digital form as a PDF/DOC format.

Each report shall contain the following structure:

3.1.1. A front page;

3.1.2. A table of contents;

3.1.3. Regulatory references, definitions, designations and abbreviations (if there are such);

3.1.4. Introduction;

3.1.5. The main part;

3.1.5.1. Suggestions to construct/ optimize a business-process

- To submit the Best practice how to construct a business process. To give not less than 3 examples of suggestion application at the company with the headcount of more than 2500 people.

3.1.5.2. Suggestions to arrange / optimize the organizational structure

- Structure arrangement when IS implementation /optimization. Suggestions to optimize the interaction between the functional departments.

3.1.5.3. Requirements to the knowledge and skills of the staff

- Merit rating of the process participants, submitting requirements to the staff which are necessary to perform functions after implementation/ optimization of IS.

- To suggest a list of recommended training courses for the further staff training applied in the Best practices.

3.1.5.4. Suggestions to construct/ optimize KPI, SPI indicators, accountancy

- Detection and analysis of the applied KPI, PPI indicators/ indicators of the executor's motivation applied in the Best practices fostering achievements of high results in the activity of the subject domain.

3.1.5.5. Suggestions to motivate the business-process participants

- Motivation of the participants of business-processes/ KPI, SPI indexes applied for the wages payment of the executors and incentive and motivation methods of the business process participants fostering achievements of high results in the activity in the frame of the subject domain.

3.1.5.6. Suggestions for the documentation

- Assessment of the valid forms and document conformance rules necessary for the control and analysis of indexes applied in the Best practices. Creation of new forms and rules when IS implementation/optimization.

3.1.5.7. A possibility of submitting activities to the outsourcing.

- Not to consider!

3.1.5.8. Contract forms

- Current contract template assessment as it relates to risks, completeness of the description of demands applied in the Best practices.

3.1.5.9. Automation means

- A consultant will have to propose as minimum 3 different types of automation means for the processes indicated in section 2. Means must be selected among the best ones, preferably some positive experience of application in Russia and full localization are desired.

- For each automation means a feasibility study must be developed and an assessment of technical and organizational risks is held when implementation and also its advantages and disadvantages must be given.

3.1.6. a conclusion;

3.1.7. a list of resources applied;

3.1.8. appendixes.

New forms of documents suggested for the application at the Moscow Domodedovo Airport must be issued as templates in separate appendixes to the main documents.

4. Standards for the production means/ Forms of the documents

- No special requirements to the production means are required.
- In the frame of consulting a list of the main forms / form of documents necessary in the frame of the subject domain applied for the fulfillment of the Best practices must be submitted. A list of documents shall contain requirements to the contents and documentation forms.

5. Standards (obligatory/ optional)

In his/her activities the following practices and standards must be applied by a consultant:

- ISO/IEC 27000;
- ISO/IEC 17799:2005;
- 27001;
- BS 7799-1:2005.

6. The best courses and companies

To suggest a list of the best training programs/ courses and counterparts for the employees involved in the design and business-process automation for the purpose of the further training.

7. Activities' distribution into blocks/ stepwise acceptance

1.1.), An advisory support must take not more than 6 months. It may be divided into the following stages (1 stage is equal to one point from the section 1.1), it is recommended to organize activities parallel to each stage.

7.1. Issuing a plan-schedule of the representation of results of the carried out research with due regard to the following requirements:

7.1.1. All research activities can be divided into conceptual blocks, the result of each block must be formalized.

7.1.2. The represented results on each block can be sequential (i.e. each next block must be either based on the previous block/(-s), or parallel (if blocks are not dependent from the previous and/or the following ones);

7.1.3. At each stage both independent solutions on the automation/ software products and a single solution can be suggested;

7.1.4. Submission of the results for each block can be distinctly limited in time, i.e. a certain date can be indicated;

7.1.5. In the course of the works at each block/ stage intermediate meetings are held every 10 operating days and in a mandatory manner before the final delivery of the investigation findings of each conceptual block/ stage;

- To organize the awareness procedure with the operational practice at the Moscow airport "Domodedovo";
- To hold an assessment of the best world practices in the domain of the low current system maintenance;

- To provide a subject itemized statement on the best practices in the domain of the low current system maintenance (recommendations must take into account organizational, technical and legal features of the activities of IT at the Moscow Airport "Domodedovo").

Acceptance is made on a stage basis. The fact of a stage acceptance is confirmed by the Customer's agreement with the completeness and explicitness of the provided results in accordance with the represented plan-schedule.

8. Requirements to the counterpart

8.1. Consulting companies with the experience in the "information security management system" for more than 10 years having successfully realized consulting projects in the domain "information security management system" for the last 3 years, written testimonials of not fewer than 2 major customers- companies with the headcount of more than 2500 people.

PricewaterhouseCoopers (PricewaterhouseCoopers), Deloitte (Deloitte), Ernst & Young (Ernst&Young), KPMG (KPMG)./This being so the consulting companies must not belong to either of the "Big Four": PricewaterhouseCoopers (PricewaterhouseCoopers), Deloitte (Deloitte), Ernst & Young (Ernst&Young), KPMG (KPMG)

8.2. Requirements to the staff of a consulting company/ a consulting subdivision conducting a survey:

8.2.1. Each employee of a research group must be experienced:

- in the advisory field for not less than 5 years,
- Participation in not less than 2 successful projects of the “information security management system”,

8.2.2. A head of the research group should:

- be experienced in the field of consulting and practical activities in the “information security management system” for more than 10 years,
- be a head of a group/ a division who successfully hold not less than 2 projects on the “information security management system”.

8.2.3. A consultant must involve into the project the Russian-speaking staff, or attract to the project professional interpreters and translators specializing in the indicated domain.