NATIONAL AUDIT OFFICE OF THE REPUBLIC OF LITHUANIA

PUBLIC AUDIT REPORT

GENERAL AND CREATION CONTROL OF THE INFORMATION SYSTEMS OF THE MINISTRY OF FOREIGN AFFAIRS

31 January 2013, No. VA-P-90-2-2
Vilnius

SUMMARY

Audit started 15 June 2012
Audit completed 31 January 2013

Full audit report in Lithuanian is available on the website of the National Audit Office: www.vkontrole.lt

The Ministry of Foreign Affairs shapes the foreign policy of the state, coordinates activities related to the membership of the European Union, represents the Republic of Lithuania and legitimate interests of its citizens and defends them in international organisations and foreign countries, as well as implements other activity goals specified in of the Regulations of the Ministry[1].

When automating its business functions, since 1999 the Ministry has been using information systems of varying degrees of complexity, which accumulate and process data, including personal

[1] Regulations of the Ministry of the Republic of Lithuania approved by Resolution No. 1155 of the Government of the Republic of Lithuania of 25 September 1998, p. 5.

data and critical personal data. In addition, the Ministry uses networks and systems which automatically process information classified no higher than restricted. In order to ensure confidentiality, accuracy of data processed by the information systems of the Ministry and continuity of the system operation, adequate information systems management control is required.

The objective of the audit was to assess general and creation control of the information systems of the Ministry of Foreign Affairs.

Since the beginning of 2009, the Ministry of Foreign Affairs has achieved considerable progress in the management of the information systems. Development Guidelines have been prepared for targeted development of the information systems. The Ministry has approved a Procedure for Managing Changes in the Functions of the Information Systems, the purpose of which is to manage changes occurring in the information systems of the Ministry, ensuring production and introduction of necessary high quality changes, with minimum disturbance of the functioning of the information systems. Documentation covering security policy has been prepared and incident management measures have been implemented to enhance security of the information systems. However, certain shortcomings in the management and protection of the information system were found during the audit: there is no clear description of the existing electronic data flows (information architecture model); the management of information technologies lacks stronger links between business processes and information technologies; no data supervisors have been appointed; information system risk assessment is not carried out annually, risk reduction measure plans have not been developed, security policy documents have not been updated; the Business Continuity Plan has not been tested; the information systems are upgraded without having updated or drawn up their regulations, specifications; insufficient control of the processing of personal data, critical personal data, and classified information.

The auditors established that the maturity of the internal control of the information systems of the Ministry of Foreign Affairs is defined as the Initial/ad-hoc (1) process[2]. To be able to achieve a higher level of maturity, the links between business processes and information technologies should be enhanced, the Information Systems Development Guidelines of the Ministry should be updated to cover all information systems of the Ministry, and regulations of all information systems of the Ministry should be draw up and approved. The documentation on the management and protection of the information systems of the Ministry should be continuously updated and should reflect the actual situation. It is necessary to carry out regular assessments of risks and information systems security compliance and to ensure process monitoring. The Ministry was recommended to

[2] According to the Capability Maturity Model (CMM).

define information systems architecture, to improve the processes ensuring the security of the information systems, business continuity, data management, and services provided by third persons.

The Minister of Foreign Affairs has already developed a plan for implementing the recommendations provided thereto.

Audit conclusions

1. The Ministry of Foreign Affairs has no single information architecture model covering all information systems. Failure to clearly describe the existing electronic data flows (data structure) may result in additional time and resources required for processing this data and selection of insufficient measures to ensure information safety.

2. The organisational structure of the information technology management should be improved because:

2.1. there is no mechanism in place designed to address, together with the managers of the Ministry, strategic information technologies management issues, so that the needs of the main activity are linked to the possibilities provided by information technologies;

2.2. no data management supervisors have been appointed;

2.3. there is a high information technology staff turnover, however, during the audited period reserve staff for substitution and taking over of duties was not planned.

3. Certain shortcomings in the security management of the information systems of the Ministry have been identified:

3.1. information system risk assessment was not carried out annually, therefore information system risk factors which existed at that time and which could have affected the security of information were not identified and analysed in detail; no plan of measures to reduce (manage) the risk of the information systems has been developed and approved;

3.2. internal documentation does not define the specific components which constitute the information systems of the Ministry, therefore the classification of the information systems by categories is unclear, which may result in inaccurate determination of the need, priorities and level of protection of electronic information processed by the information systems of the Ministry;

3.3. only one assessment of the information technology security compliance has been performed (in 2012) and not all documents on data protection have been updated so the security management measures for the information systems provided for in these documents may be ineffective;

3.4. the management of the automatically processed information classified as restricted is not sufficiently safe because the procedures regulating the management (destruction, transfer, transmission, storage) of such information at the Ministry have not been revised and updated;

3.5. the user account management process has not been sufficiently ensured because access to the ministerial electronic mail may still be allowed for some time after the termination of the employee's employment or service relations with the Ministry of Foreign Affairs. Some discrepancies were also identified between the staff lists provided by the Personnel Department and the lists of information system users in the account management system. User accounts are password protected, but the complexity requirements have not been ensured by technological means (the password length, the number of characters are not checked) in all information systems of the Ministry.

4. The Ministry is insufficiently prepared to ensure continuity of the information systems in contingency situations because:

4.1. priorities of the recovery of the operation of the information systems have not been provided for, therefore less important business processes of the Ministry may be restored in the first place;

4.2. administrators responsible for the maintenance of the information technology equipment have not been indicated, no relevant documentation of the information system setup (lists of information technology equipment, parameters of the equipment, physical and logical interconnection schemes of the computer network, etc.) has been prepared, the list of agreements on data provision and computer, hardware and software maintenance is not being compiled, data exchange agreements have been concluded only with part of data providers and users, which may result in responsibility and service delivery problems;

4.3. tests and efficiency testing of elements of the Information Systems Continuity Management Plan during practical training have not been carried out, therefore in case of an incident the Continuity Management Plan may turn to be ineffective and unfeasible;

4.4. in case of an incident, relevant information system data might not be recovered because no detailed data backup procedures have been established covering data backup facilities, data copy verification, and data recovery from backup.

5. The Ministry does not implement organisational measures of automated personal data processing because:

5.1. not all objectives of the automatically processed personal data at the Ministry have been registered with the State Register of Personal Data Managers, so people have no access to detailed information about the management of their personal data;

5.2. no personal data protection level has been set and no written document describing the application of personal data protection measures as required in the Law on Legal Protection of Personal Data has been drawn up and approved.

6. The information systems were created and upgraded without detailed requirements, the decisions made have not been documented:

6.1. Regulations of the Consular Procedure Management System and the Information System of the Issue of Facilitated Transit Documents have not been approved. The Regulations of the Information Systems of the Ministry of Foreign Affairs have been approved but they have not been coordinated with relevant appropriate authorities;

6.2. no specifications of the Consular Procedure Management System and the Information System of the Issue of Facilitated Transit Documents have been prepared, the specification of the information system of the Ministry of Foreign Affairs has not been updated since 1998. Also, no detailed projects of the upgrading of the Consular Procedure Management System and the Information System of the Issue of Facilitated Transit Documents have been prepared, the detailed plan of the information system of the Ministry of Foreign Affairs has been developed only for the upgrading of one subsystem. The said systems are being upgraded only in accordance with the Terms of Reference of the procurement. Failure to update or prepare the specification and detailed plan of the information system before its upgrading incurs a risk that the functions of the upgraded system will not meet the business needs;

6.3. the information systems are tested in a special environment, however, it is not always that testing plans are developed and end users are involved.

7. The existing Information Systems Development Guidelines of the Ministry of Foreign Affairs are not comprehensive, they have to be updated and specified in more detailed in order to link them with relevant business needs and priorities.

8. Internal auditors do not provide necessary attention to the monitoring and assessment of the management of the information systems, which allows occurrence of potential shortcomings of internal control of the information system management; besides, there are cases of non-compliance to external requirements.

Audit recommendations

To the Minister of Foreign Affairs of the Republic of Lithuania:

1. To establish a business information architecture model recommended in Best Practices, which facilitates optimal creation, use and sharing of business information, while maintaining its integrity.

2. To improve the organisational structure of the management of the information systems of the Ministry:

2.1. to ensure effective implementation of the functions of the information technology strategy and information technology management committees recommended in Best Practices, choosing optimal structural solutions;

2.2. to appoint data management supervisors;

2.3. to plan reserve staff for substitution and taking over of important duties of information technology employees.

3. With a view to ensuring safety of the information managed by the Ministry:

3.1. upon assessment of the risks of the information systems, to develop and approve an Information Systems Risk Reduction (Management) Plan;

3.2. To specify categories of the information systems of the Ministry and components thereof in the Information System Data Safety Regulations;

3.3. to review and update data safety documents (Information System Data Safety Regulations of the Ministry of Foreign Affairs, User Administration Rules, Secure Electronic Information Management Rules, Information Systems Continuity Management Plan, List of Administrators of Information Systems Services;

3.4. to review and update the internal procedures regulating the management of classified information (destruction, transfer, transmission, storage) at the Ministry;

3.5. establish account management procedures and to introduce technological means ensuring complexity requirements for the connection of users in all information systems of the Ministry.

4. With a view to ensuring continuous provision of information system services:

4.1. to establish information systems continuity recovery priorities;

4.2. to test the Information Systems Continuity Management Plan and to organise regular trainings on the Continuity Plan;

4.3. to compile the lists of information technology equipment: to specify the parameters of the equipment and to indicate administrators responsible for its maintenance, to draw up a specification of information technology equipment of minimal functionality, drawings of the premises on all floors of the building and schemes of physical and logical interconnection of the indoor equipment and communication, computer network;

4.4. to set detailed data backup procedures covering data backup facilities, verification of backup data, data recovery from backup;

4.5. to compile a list of agreements on data provision and computer, hardware and software maintenance, to conclude data exchange agreements with all data providers and users;

5. To enhance personal data management and protection;

5.1. to notify the State personal Data Protection Inspectorate of all objectives of personal data automatically processed at the Ministry ;

5.2. to draw up and approve a written document describing the level of protection of personal data processed, specifying organisational and technical measures designed to protect personal data against accidental or unlawful destruction, alteration or disclosure, as well as against any other unlawful management.

6. With a view to ensuring conformity of the development of the information systems to the needs of the activities of the Ministry:

6.1. to review, update, expand and specify the Information Systems Development Guidelines of the Ministry of Foreign Affairs;

6.2. to approve, in the established procedure, the Regulations of the Information Systems of the Ministry of Foreign Affairs, the Consular Procedure Management System and of the Information System of the Issue of Facilitated Transit Documents;

6.3. to draw up specifications of the Consular Procedure Management System and the Information System of the Issue of Facilitated Transit Documents and to update the specification of the information system of the Ministry of Foreign Affairs, to agree and to approve all these specifications following the established procedure. To update or to draw up new regulations, specifications and detailed plans and to agree them following the established procedure prior to the creation of new or upgrading of the existing information systems of the Ministry.

6.4. in the internal procedures, to establish that testing of a newly created or upgraded information system should be carried out after a testing plan has been drawn up and that end users of the information plan are involved in the assessment of the testing results.

7. To carry out regular assessments of the management of control of the information and monitoring of external regulation.