VALSTYBĖS KONTROLĖ

Executive summary of the public audit report

MANAGEMENT OF INFORMATION RESOURCES OF THE MINISTRY OF THE INTERIOR

13 October 2016, No. VA-P-90-2-19

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

DEFINITIONS AND ABBREVIATIONS

COBIT – methodology for information technology management and governance developed by ISACA[1]

Information Technology and Communications Department – Information Technology and Communications Department under the Ministry of the Interior of the Republic of Lithuania

IS – information system

IT – information technology

Information resources – state IS and registers

N.SIS – Lithuanian National Schengen Information System

N.VIS – Lithuanian National Visa Information System

PASIS – Information System for Monitoring and Analysis of Public and Administrative Services

CMIS (Lith.: SVIS) – Certificate Management Information System

IAIS (Lith.: VRIS) – Internal Affairs Information System

IAIS CDB (Lith.: VRIS CDB) – IAIS Central Data Bank

Ministry of the Interior – Ministry of the Interior of the Republic of Lithuania

Oter definitions and abbreviations used herein are viewed as defined by the Law on the Management of Public Information Resources of the Republic of Lithuania .

[1] ISACA – Information Systems Audit and Control Association. Accessed via: http://www.isaca.org/about-isaca/Pages/default.aspx [Accessed on 10/06/2015].

SUMMARY

The purpose of the Ministry of the Interior[2] is shaping national policy, organizing, coordinating and controlling its implementation in the fields of public security[3], public administration and public administration of information technology application[4], public information resource security[5], migration, physical education and sports.

Many activities of the Ministry of the Interior require the use of information resources that are of great significance to the entire State, such as the state and departmental registers, and public information systems. Whereas the Ministry has failed to implement some of the public audit recommendations of 2007 and 2010,[6] we analysed, whether there have been any positive changes in the field of IT management. Their impact is important not only because the Ministry manages 16 information resources, which ensure data availability to the population, efficient activity of the services, and operation of the Schengen collaboration tools. The quality of IT management in the Ministry shall also affect the activities of other state institutions: from 05/01/206, the list of public information resources consolidation works is being implemented[7] and the Information Technology and Communications Department under the Ministry of the Interior was appointed one of the four public IT service providers[8].

The purpose of the audit was to assess the management of information resources in the Ministry of the Interior. We assessed how the Ministry ensures planning and organisation, monitoring, assessment and coordination of their management. In addition, we assessed the IT management maturity in the Ministry. We analysed information resources managed by the Ministry (five state registers, eight state IS and three departmental registers), which are used and managed by both the Ministry and institutions and other establishments within the purview of the Ministry.

The audit covered the period from 2013 through to the first quarter of 2016. For data analysis, data from other periods was used. The audit was conducted in the Ministry of the Interior. We also collected information at the Information Technology and Communications Department and State

[2] Resolution No. 291 of 14/03/2001 of the Government of the Republic of Lithuania (new version of 19/10/2010) approving the regulations of the Ministry of the Interior of the Republic of Lithuania, p. 8.

[3] Public order, internal service, fire and civil protection, rescue operations, and State border protection; weapons, ammunition, explosives, and special measures turnover; protection of persons that have been granted the status of a protected person.

[4] E-government, local government, regional development, and civil service.

[5] Insofar as it does not include cyber security.

[6] The public audit report No. IA-9000-2-4 of 10/11/2017 Assessment of Common Control of Information Systems of the Ministry of the Interior and the public audit report No. VA-900-1-27 of 31/12/2010 The Use of Civil Servants in Cyberspace.

[7] Resolution No. 498 of 13/05/2015 of the Government of the Republic of Lithuania on Consolidation of Public Information Resource Infrastructure and Optimization of its Management, p. 11.

[8] The Order No. 1V-4 of 05/01/2016 of the Minister of the Interior of the Republic of Lithuania on the Appointment of the Information Technology and Communications Department under the Ministry of the Interior the Provider of Public Information Technology Services, p. 3.2.3.

Enterprise Regitra which are responsible for administration of the information resources managed by the Ministry as well as data security and development.

During the audit, we discovered that the top management of the Ministry does not pay enough attention to IT management coordination and control; therefore, the maturity of IT management processes in the Ministry of the Interior has not changed for nine years and can currently be defined as the initial (*Ad Hoc*) process. This means that there is evidence suggesting that the management of the Ministry understands that there are problems, which need to be addressed, but the processes remain unstandardised (undefined information architecture model, undetermined levels of IT services provided). In addition, 24 cases of non-compliance with the statutory requirements were found (see Annex 3). A common approach to IT management in the Ministry is non-systematic (a strategic IT plan is not being prepared, the organizational structure of IT management requires improvement, the monitoring and assessment process is inadequate), and *Ad Hoc* methods, which vary with each individual case, are normally used instead of standardized processes.

Taking into consideration the significance of information resources managed by the Ministry of the Interior, and the fact that the Information Technology and Communications Department was appointed one of the four public IT service providers, it is important to eliminate the detected shortcomings of the IT management in time. A higher IT management maturity level can only be achieved through the implementation of the requirements of legal acts of the Republic of Lithuania and our recommendations.

The following public audit conclusions and recommendations were drawn upon the assessment of the audit findings.

CONCLUSIONS

1. The strategic planning of IT field in the Ministry of the Interior is not without shortcomings, which increase the risk of undue distribution of financial, technological and human resources as well as the risk of failure to develop information resources of critical importance in a timely manner, because:
   - the Ministry manages eight public information resources of critical importance, and the Information Technology and Communications Department manages one; however, the Ministry has failed to comply with the Law on the Management of Public Information Resources, i.e. the Ministry has no IT development plans and no one is obliged to draft them (Subsection 1.1, p. 11);
   - the preparatory work for IT development, such as preparation of the investment project, technical and functional requirements as well as their coordination, is not always included into annual action plans (Subsection 1.2, p. 11).
2. The present documentation on information resources managed by the Ministry does not reflect the actual extent of computerized functions and information processed; without establishing the importance and sensitivity of the information managed by the Ministry and

establishments subordinate thereto, the Ministry may fail to ensure the information security requirements when promoting, transferring or disclosing such information:

- not all registers and IS managed by the Ministry have updated provisions (12 of 16 relevant), drawn up and approved technical specifications (4 of 16 absent) (Subsections 2.2 and 2.3, respectively, pp. 14 and 15);
- the Ministry does not have a detailed list of IS, registers and other software used or a general information architecture model. As a result, the interaction between information resources remains unclear (Section 2, p. 12).

3. The organizational structure of IT management used by the Ministry should be improved, because:
   - due to shortcomings of IT organization, the change of employees responsible for management of information resources, and the lack of human resources, performance of the functions of the manager of information resources managed by the Ministry of the Interior cannot be ensured, because their performance does not comply with the statutory requirements (Subsection 3.2, p. 18);
   - there is no mechanism that could be applied to address the IT management issues together with the management in order to link the needs of the primary activities with the opportunities offered by IT (Subsection 3.1, p. 17);
   - the policy shaping and implementation functions were not separated, i.e. one unit of the Ministry both performs the functions of the manager of the Ministry's information resources and shapes e-government and e-security policy (coordinates, plans projects and assesses their compatibility) (Subsection 3.2, p. 18);
   - the Ministry has failed to appoint 13 (of 16) representatives for managing the data of information resources managed by the Ministry, who should monitor how these resources are created and managed, and how investments are used (Subsection 3.3, p. 17).
4. Not all information resources managed by the Ministry have their IT change management procedure defined (three out of 16 – undefined, seven – out of date). When put into practice, the IT change management procedure is often (in 14 out of 16 cases) carried out without compliance with the provisions of the existing procedures, because none of the changes initiated by the activities departments are registered, categorized or prioritized. Therefore, it is not possible to monitor the change status at various stages of change management, and the change impact assessment process has not been defined, which increases the risk of negative impact of changes upon the stability and integrity of IS or the register (Section 4, p. 20).
5. After consolidation of public information resources and making the Information Technology and Communications Department one of the four public IT service providers, the Department will provide these services in accordance with the arrangements for the provision of IT services. High-quality and timely provision of IT services to many public establishments shall only be ensured after approving the catalog of IT services provided by the Department and monitoring of the service provision level (Section 5, p. 22).
6. The supervisory measures applied by the Ministry for ensuring the confidentiality, integrity and accessibility of electronic information (data), as stipulated by the law, were deemed insufficient, because:
   - representatives of the most important areas, i.e. main activities of the Ministry, human resources, IT, security, legal and internal auditing, do not participate when addressing the IS security issues in the Ministry (Subsection 6.1, p. 24);

- two (of 16) information resources managed by the Ministry do not have security representatives appointed; therefore, the risk of these resources and their security compliance with the regulatory requirements remain unassessed (Subsection 6.2, p. 25);
- the implementation of IS risk management measures and elimination of shortcomings detected during the security compliance regulatory assessment remain without control (Subsection 6.2, p. 25).
- three (of 16) legal acts regulating implementation of security policy applied for information resources managed by the Ministry have not been drawn up (Subsection 6.3, p. 26);
- for a year now, the Ministry has been behind schedule with the implementation of e-security requirements: legal acts defining the security policy of 11 (of 16) information resources managed by the Ministry and regulating its implementation were not updated by 01/05/2016 (Subsection 6.3, p. 26).

7. The audit of information resources of critical importance required by the Law on the Management of Public Information Resources[9] was not conducted from 2013 through to the first half of 2016, and the Ministry's Internal Audit Division has not conducted a single audit dealing with information systems and assessment of their security, common control or other IS (IT) aspect. Therefore, the management of the Ministry may be lacking information about the effectiveness of IT processes and their compliance with the performance requirements, unidentified IT control weaknesses and shortcomings, and fails to comply with the statutory requirements (see Annex 3) (Section 7, p. 27).

RECOMMENDATIONS

1. In order to consistently and purposefully develop IS and registers, to develop and validate a strategic IT plan for the purview of the the Ministry of the Interior, taking into consideration operational needs of the entire organization (Conclusion 1).
2. To make and continually update a list of all IS, registers and other software used by the Ministry (Conclusion 2).
3. To make an information architecture model that covers the Ministry-managed information, IS (register) data and technological architecture, specifying all components (applied technology, data, data flows between external and internal IS) (Conclusion 2).
4. To update N.SIS and CMIS provisions to avoid blockage of updating of documents used for implementation of the security policy. To make a decision regarding further existence of IAIS as a public IS and define its structure, which should be simpler and more flexible (Conclusions 2 and 6).

[9] Law on the Management of Public Information Resources of the Republic of Lithuania , 15/12/2011, No. XI-1807, Art. 14. p. 1.

5. In line with the principle of subsidiarity[10], to separate the functions of shaping and implementing e-government and e-security policy (i.e. the IS Manager) (Conclusion 3).
6. When appointing representatives for managing the data of information resources managed by the Ministry, to take into account the areas, where the relevant resources are most commonly used (Conclusion 3).
7. In order to ensure the systematic change management, to revise the current IT change management process and set up (approve) the management procedure for IT changes of all information resources managed by the Ministry. Such management procedure should contain the IT change management provisions that cover planning, categorization, priorities, emergency procedures, and impact assessment processes. In addition, it is necessary to ensure the control of compliance with this procedure (enforcement thereof) (Conclusion 4).
8. To prepare and approve the catalog of IT services provided by the Information Technology and Communications Department and determine the service provision level (Conclusion 5).
9. To develop a structure corresponding to the best practices and addressing IS security issues, which would consist of representatives of the most important areas, i.e. main activities of the Ministry, human resources, IT, security, legal and internal auditing (Conclusion 6).
10. To monitor and assess the condition of internal control of information systems and registers as frequently as legally required (conclusion 7).

Measures and time frames for the implementation of the recommendations are presented in Annex 1, Plan for Implementing Recommendations.

[10] Law on Public Administration No.VIII-1234 of the Republic of Lithuania , 17/06/1999, Art. 4. p. 2.