Executive summary of the audit report

MANAGEMENT OF CRITICAL STATE INFORMATION RESOURCES

28 June 2018 No VA-2018-P-900-3-6

The state audit report can be accessed at
the website of the National Audit office at www.vkontrole.lt

SUMMARY

The importance of the audit

State information resources are the totality of information managed by the institutions in the course of performing the functions prescribed by the law and processed by means of information technology, and the information technologies used to process it[1]. Critical state information resources—critical electronic information—are managed in the first category state information systems, registers and cadastres (hereinafter referred to as the IS). These systems provide important public functions, such as public finance management, tax administration, health care. The loss of critical information and the unavailability of IS that processes it can have serious consequences for public security and welfare as well as the economy.

Properly designed and effectively implemented information technology processes enable effective protection of information resources from emerging cyber threats. In recent years, cyber attacks around the world have been increasingly targeting critical information resources used to provide services of public interest and store critical information. The Global Risk Report for 2018 states that in the future, the likelihood of these attacks will increase together with the growing risk of critical information resources being disrupted[2]. According to the data of the National Cyber Security Centre, the number of cyber incidents in Lithuania in 2017 amounted to 54.4 thousand and compared to 2016, the number was one tenth higher[3]. Therefore, as the level of cyber threats grows, it is very important to strengthen the security of critical state information resources. According to the results of the Global Cybersecurity Index[4] for 2017, Lithuania was 57th in the world out of 165 countries, and 23rd out of EU countries. This shows that the effectiveness of security management could be increased.

The assessments of the general control of information technology by the National Audit Office over the period from 2006 to 2016 demonstrated the recurring problems of IT management areas (planning, information architecture definition, organisational structure, changes, security of going concern, data security, IT management monitoring and evaluation). The maturity of IT management of audited public sector entities over the last ten years has, on average, achieved the first level of maturity out of 5[5] and is currently at maturity level of 1.7. The low level of maturity of state information resources is indicative of weaknesses in the formation and implementation of the state information resources policy, which allows for greater vulnerability of these resources.

The National Audit Office has decided to carry out an audit of critical state information resources to assess the state of the management and security of these resources and to provide for measures to improve them.

[1] LAW ON THE MANAGEMENT OF STATE INFORMATION RESOURCES, 15/12/2011 No. XI-1807, Art. 2(17).

[2] Insight Report "The Global Risks Report 2018" by the World Economic Forum. Online access: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

[3] Online access: https://www.nksc.lt/.

[4] Global Cyber Security Index, GCI, online access: https://www.itu.int/pub/D-STR-GCI.01-2017. The index measures cyber resistance capabilities of 195 countries and allows to compare the state of cyber security in them.

[5] According to the COBIT methodology.

Audit goal and scope

The goal is to evaluate the management (general control), maturity of critical state information resources and to identify systemic problems thereof.
The following are subject to audit:

- Ministry of Transport and Communications is developing a policy for the development of state information resources. During the audit, the Government, at its meeting on 20/06/2018, made a decision to approve the amendments to the law, which would reassign the formation and coordination of the state information resources development policy, some of the register policy and information society development policy to the competence of the Ministry of Economy[6];
- The Ministry of the Interior was forming a policy in the field of state information resources until 01/01/2018;
- The Ministry of National Defence is forming a cyber security policy, organises, controls and coordinates its implementation, as of 01/01/2018 is forming a policy in the field of state information resources security;
- The Information Society Development Committee under the Ministry of Transport and Communications is responsible for the interoperability, design, management and development of state information resources.

We assessed the maturity of IT management in 12 public sector organisations[7] that manage 44 first-class IS's, of which 10 assessments were detailed analyses of selected IT management processes. Two organisations were not assessed, because after the initial evaluation, the maturity of one of them was 0, while the other one has undergone no changes since the IT general control audit performed by the National Audit Office.

After performing a preliminary evaluation of all 34 COBIT processes, we have conducted detailed assessments in the following risk areas:

- IT strategic planning;
- Determination of informational architecture;
- IT risk management;
- Change management;
- Assurance of uninterrupted service provision;
- System security;
- Data management;
- Monitoring and evaluation of IT activities;
- IT management assurance.

The process evaluation included both organisational and national IT management, the interaction of these levels of management. We assessed the management and maturity of information

[6] Minutes No. 27 of the meeting of the Government of the Republic of Lithuania on 20/06/2018, class 7, Certificate No. NV-1585 of 20/06/2018 of the Policy Implementation Group of the Government of the Republic of Lithuania.

[7] State Tax Inspectorate, State Enterprise Centre of Registers, Information and Communications Department, State Social Insurance Fund Board, State Enterprise Agricultural Information and Rural Business Centre, Customs Information System Centre, State Food and Veterinary Service, Office of the Seimas of the Republic of Lithuania, Ministry of Finance, Information Society Development Committee, State Patient Fund, State Forest Service.

resources in comparison to the state of 2017. When analysing the coherence and continuity of certain processes, we used the 2014–2017 data.

The audit was performed in accordance with the Public Auditing Requirements and the International Standards of Supreme Audit Institutions. The assessment was carried out in accordance with the COBIT [8] methodology and in compliance with the requirements and recommendations of the legal acts of the Republic of Lithuania on the management of state information resources. The assessment of the management of critical state information resources has been carried out in accordance with the IT Audit Manual[9], the 5300 International Standard of Supreme Audit Institutions, the International Auditing Standards of the Information Systems Audit and Control Association (ISACA), and in accordance with the guidelines and best practices of the ISACA.

The scope and methods of the audit are described in more detail in Annex 2 'Audit Scope and Methods' (p. 38). In carrying out the audit, we assumed that all documents submitted to the auditors were correct, complete and final, and their copies corresponded to the original.

Findings

The trends in the changes of the maturity level of the management of critical state information resources are positive; however, the observed progress, given the growing level of cyber threats, is too slow and the security of these resources needs to be increased. This is due to the following weaknesses:

1. The system for identifying critical state information resources is not sufficiently effective to allow for the implementation of security solutions that meet actual needs:
    1.1. assessments designed to prove the criticality of state information resources lack objectivity, changes are not always evaluated in reassessments, this process is not monitored at the national level, and the guidelines for determining the criticality have not ensured its effective implementation (Section 1.1, p. 12);
    1.2. the system for the identification of critical state information resources and critical information infrastructure is not common; resources and infrastructure are identified in different ways according to the importance of information and services, which complicates the process of identifying these resources (Subsection 1.2, p. 15);
    1.3. no national information architecture has been created that would represent state IS's, their interrelations, show the scale of critical state information resources and allow to make informed decisions regarding the importance of these resources (Subsection 1.2, p. 15).
2. The management of state information resources should be more in line with the best IT management practices and standards in order to achieve integrated improvement of the IT field that would contribute to better progress of the management of critical state information resources:

[8] COBIT (*Control Objectives for Information and Related Technologies*) is a standard of the international ISACA organisation that describes the best IT management practices.

[9] Approved by the State Controller of the Republic of Lithuania by Order No. V-165 of 21/06/2017.

2.1. IT planning is not sustainable: the planned IT tools is presented in different documents, there is a lack of a systematic approach due to the excess of strategic documents, making it difficult to identify the key priorities and channel resources to manage the greatest threats. Under such system, IT development plans are not always prepared, while those that are, are not comprehensive; no detailed plans for implementing measures are prepared (Section 2.1, p. 17);

2.2. IT monitoring does not ensure that organisations measure the efficiency of IT operations and audits carried out by YSVII managers show the actual maturity of IT management. The state of IT management is not observed at the national level, and IT management issues are not systematically analysed. A system for monitoring the compliance of state information resources with the requirements of electronic information security has been created, intended only to facilitate the monitoring of security compliance, but its functionality is not sufficiently utilised (Section 2.2, p. 19).

3. Measures to ensure the resilience of critical information resources to the level of cyber threats are not effective enough; therefore, the risk of vulnerability of these resources remains:

3.1. The effectiveness of the assessment of IT security risks should be increased, as not all relevant risks are identified and their assessment methodology does not comply with the latest IT management practices; timely management of unacceptable risks is not ensured (Section 3.1, p. 23);

3.2. Organisational security measures that can reduce cyber threats are not systematically used: Insufficient testing of security, incomplete training of staff during IS development, upgrading, modification; unmanaged safe software configurations and upgrades; improper management of IT business continuity and backup files threatens the recovery of going concern; security performance measurements are insufficient and do not contribute to security enhancement (Section 3.2, p. 26).

Recommendations

To the Government of the Republic of Lithuania

In order to ensure better quality of the management of state information resources and a higher level of maturity of IT management by YSVII managers, it is necessary to:

1. Create a national information architecture and its management mechanism to allow to objectively determine the criticality of state information resources, and to properly control this process and to harmonise the mechanisms for identification of critical information resources and critical information infrastructure.

2. Develop a management mechanism for state information resources that is consistent with the best IT management practices, ensuring common and top priority-oriented planning, establishing the desired level of maturity of IT management and a mechanism that enables the monitoring of its progress, while effectively utilising the technical tools developed.

To the Ministry of National Defence

To ensure the security of critical state information resources and resistance to growing cyber threats, it is necessary to:

3. Improve cyber security risk management by updating the requirements, methodologies and implementing national IT risk management that allows for effective management of risks of national importance.
4. Enhance the effectiveness of the organisation and implementation of the management of cyber security by creating the necessary control mechanisms that contribute to increasing the security knowledge and skills of human resources, improvement of the state of implementation of security requirements and prevention of IS vulnerabilities.

The measures and time limits for the implementation of the recommendations are presented in the section "Implementation Plan for the Recommendations" (p. 33). Information about the level of IT maturity of the managers of critical state information resources was presented in separate letters.