NATIONAL AUDIT OFFICE OF LITHUANIA

STATE INFORMATION RESOURCES MANAGED BY THE CENTRE OF REGISTERS

6 December 2021

No. VAE-7

SUMMARY

Relevance of the audit

State information resources is the totality of information managed by the institutions in performing their functions provided for in the laws and information technology measures for processing this information.[1]. The Centre of Registers manages critical state information resources: Real Estate Register, Register of Legal Entities, Electronic Health Services and Cooperation Infrastructure Information System, etc. Data of information resources managed by the Centre of Registers are used for the implementation of state functions: protection of state finance and asset management, health care, etc. Protection of the critical state information from loss and availability of state information resources is important for ensuring public security, well-being and economic development.

The entity provides 300 types of administrative and public services. Between 2018 and 2020, the number of services provided increased by 2.4. In 2020, 293 million items of services were provided to public authorities, other legal and natural persons. EUR 130.7 million revenue was received for the services provided in 2018-2020.

The National Audit Office decided to audit the state information resources managed by the Centre of Registers, because reliable, coherent and confidential data, their continuous provision from registers and information systems become even more relevant in the event of the state-level emergency when reliable data are needed to make rapid decisions.

Objective and scope of the audit

The objective of the audit is to assess whether the proper management of the information resources of the Centre of Registers is ensured.

[1] Law on the Management of State Information Resources, Art. 2(17)

The main audit questions are:

- Whether conditions are in place for the development of state information resources;
- Whether the proper management of business processes related to the supervision, service and maintenance of state information resources is ensured.

In order to answer the audit questions, we analysed whether the management of state information resources processes managed by the Centre of Registers complies with the provisions of good practice of COBIT5 — a generally recognised internal control instrument for the management of information technology processes and with the requirements of legislation.

"Audited entity" means the State Enterprise Centre of Registers, which performs state functions assigned by the Government of the Republic of Lithuania.

We also collected information from the Ministries of Economics and Innovation, Justice, Health Care, Communications, Interior, Agriculture, and Culture, National Centre of General Functions, National Court Administration, State Consumer Rights Protection Authority, Information Society Development Committee.

The audit period is 2018-2020. In some cases, data for 2017 and 2021 were used to assess developments and compare data: 2017 data were used to assess the safety management process, 2021 data - to assess strategic management, budget management and project management processes and changes in other processes.

The audit was carried out in accordance with the Public Auditing Requirements and the International Standards of Supreme Audit Institutions. The scope of the audit and the methods used are described in more detail in Annex 2 "Scope and methods of audit" (page 49).

Main results of the audit

The Centre of Registers must ensure that state information resources are managed in such a way that the data contained therein are reliable, secure, quickly and conveniently accessible to state and municipal institutions and bodies, businesses and the public. It was found that improving the processes of management of state information resources managed by the Centre of Registers would provide for better conditions ensuring high availability of critical sate information resources, sufficient speed and data security.

1. Insufficient conditions for the development of state information resources

- It is not ensured that the managers of all state information resources managed by the Centre of Registers are involved in the adoption of strategic decisions which may have an impact on the development of state information resources. The IT strategic management process has been integrated into the overall strategic management of the Centre's activities, but 7 out of 9 managers were not involved. Only the Ministry of Economy and Innovation, as the body implementing the rights and obligations of the owner, which approves the centre's operational strategy, and the Centre of Registers participated. Therefore, it was not possible to reconcile the needs of all other state

information resource managers (Section 1.1, p. 14) during the strategy development phase.

- We did not identify cases of non-compliance with legal requirements in providing data free of charge and reimbursing the costs incurred by the Centre of Registers, but the possibilities of reducing the need for public budget funds to compensate for services provided free of charge are underestimated at national level. The Centre of Registers may provide 17.2 %. (45 out of 262) in the "system-system" of data provision services, which is the cheapest in comparison with other means (paper and electronic). Even a small part of the services provided outside the "system-system" significantly increases the public budget's expenditure to compensate for the cost of services provided free of charge. It is estimated that in 2020, only 1 % of the extended historical extracts of the Register of Legal Entities were provided in electronic form, not by the system-system means. For this service EUR 270.3 thousand state budget compensation was calculated, which could be 94 times lower (EUR 2.9 thousand) if the service were provided by means of a "system-system". The Ministry of Economy and Innovation, as the body implementing the rights and obligations of the owner of a business, does not analyse why recipients of data which are not free of charge, who have access to the data in this way, do not always use it and choose a more expensive method. The state incurs costs by compensating for more expensive services that could be used to create additional integrative interfaces so that as many data users as possible can access services through a system-system (section 1.3, page 18).
- There is insufficient monitoring and control over the implementation of information technology projects in the company. A draft Project Management Methodology and some of its provisions were developed in February 2020, but this did not ensure the timely implementation of all measures foreseen to manage the risks of IT projects. Out of the four analysed, two projects were not implemented at the planned time (19 months late), and the implementation of the activities of the two parts of the projects was delayed. Indicators for assessing the expected benefits of projects have not been established. Projects not implemented on time also lead to delays in the implementation of the restructurings planned by the public institutions, and in the absence of indicators to assess the benefits, it is not possible to assess objectively whether the project has achieved the intended benefits (Section 1.4, page 21).
- The Architecture Committee is set up together and operates in the Centre of Registers whose purpose is to ensure the integrity of the information technology solutions of the information resources managed by the Centre by implementing the organisation's operational strategy, but it has not been approved. The Centre does not have a common information technology architecture, there is no common information technology architecture document describing the existing IT architecture and targeted (planned) architecture, architecture strategy, policy, so there are not enough possibilities for informed decisions on the development of the information resources managed by the Centre (Section 1.5, page 23).
- Lack of efficiency in the human resource management process. The Centre of Registers does not sufficiently justify the need for the necessary competences when planning the human resources of the Information Technology Centre. The number of employees actually employed in 2020 did not correspond to the planned needs: an increase of 24 employees was planned, but the actual increase was only 8 (33.3 %). In 2021, external information technology specialist services were purchased for risk management. The information technology centre has identified critical posts and a plan for monitoring

their succession planning, but the plan does not contain detailed information on 27 % of the critical employees identified. The effectiveness of this plan, or sufficient skills for the critical staff succession planning, is not verified, leading to insufficient management of the risks to the company's information technology activities due to the potential loss of skills and skills of the employees performing critical functions (Section 1.6, page 25).

2. Failure to properly manage maintenance, service and support processes of state information resources managed by the Centre of Registers

- Insufficient monitoring and analysis of the safety status of the information technology infrastructure and its elements. The security agents of the Centre of Registers did not ensure that the safety assessments of the State information resources managed were carried out at the intervals specified in the legislation[2]: half of the public information resources (11[3] out of 21) for which safety compliance assessments were to be carried out were not carried out in 2018-2020, others were less frequent than those identified, thus not allowing timely detection of non-compliances with safety requirements, assessment of new or changed safety risks, and measures to address them. The implementation and maintenance of the safety policy is hampered by the fact that during the audited period the safety of state information resources managed by the Centre of Registers was regulated by 9 safety policies approved by different managers (data protection regulations) and 45 documents implementing them (section 2.1, page 27).
- Sufficient measures are not taken to ensure the high availability of public information resources managed by the Centre of Registers. The planning of the Centre's information infrastructure capacity needs is not in line with good practice: there are no plans for the development of state information resources capacity that quantify and predict future performance, processor load, disk and memory utilisation, network and electronic communications bandwidth, high-speed needs, and the use of new technologies. In some months in 2020, 6 (out of 8) inactivity time of the first category information systems exceeded the time limit established in legal acts[4], thus not ensuring that vital state information resources were made available to the maximum for users (Section 2.2, page 28).
- The existing conditions do not allow to react rapidly to user queries and to deal with all types of incidents. The incident management procedures[5] of the Centre of Registers

[2] Description of the General Electronic Information Safety Requirements approved by Government Resolution No 716 of 24 July 2013, Technical Requirements for the Safety of Electronic Information of State Registers (cadastres), Service Registers, State Information Systems and other Information Systems approved by Order No 1V-832 of the Minister of the Interior of 4 October 2013, Description of Technical Requirements for the Safety of Electronic Information of State Registers (cadastres), Service Registers, State Information Systems and other Information Systems approved by Order No V-941 of the Minister of National Defence of 4 December 2020.

[3] Real estate cadastre, Real estate, Legal persons, Addresses, Population, Mortgage, Property freezing orders registers, Legal persons participants, E-delivery, E-invoice information systems.

[4] Order No 1V-832 of the Minister of the Interior of 4 October 2013 approved the Technical Requirements for the Safety of Electronic Information of State Registers (cadastres), Service Registers, State Information Systems and other Information Systems. Order No V-941 of the Minister of National Defence of 4 December 2020 approved the Description of Technical Requirements for the Safety of Electronic Information of State Registers (cadastres), Service Registers, State Information Systems and other Information Systems.

[5] Incident management procedure of the State Enterprise Centre of Registers approved by Order No v-162 of 4 July 2013 of the Director of the State Enterprise Centre of Registers, the Rules for the Management of Information

do not define the classification schemes for incidents of state information resources, and the management of queries is not regulated. The IT Helpdesk system does not record all information needed to describe a query or incident, and does not properly assess the quality of the process. 54 % in 2018-2020 (18 613 out of 34 699) queries and 43 % (5 556 out of 12 853) incidents were pending and not resolved in time (section 2.3, page 31).

- The implementation of the IT problem management process launched in 2019 is insufficiently effective. The recurrence of incidents, their dynamics, trends are not analysed, the problem management process is not defined: no criteria for recording problems, classification schemes, lack of description of procedures, no responsibility, no information on known errors. In the second half of 2019[6] - 2020 70% (37 out of 53) problems were resolved, but the number of incidents is increasing: in 2018, 1209 incidents were recorded, in 2019 - 3664, in 2020 - 8 143 incidents (22 per day on average) and 44 problems were recorded (section 2.4, page 34).
- No adequate management of change is ensured. This process has been defined in a fragmented manner. Its performance indicators have been defined, but are not measured and monitored. In 2018-2020, no deadline for implementation was set for 83 % (17 581 out of 21 267) of change requests, and 81 % (2 982 out of 3 686) of change requests for which a deadline was set were completed with a delay. 3 % (94 out of 3 686) were still not implemented in the course of the audit[7] (Chapter 2.5, page 36).
- The effectiveness of the measures put in place to ensure the continuity of the activities of the State information resources managed by the Centre of Registers is not always verified. Continuity management plans and back-up data are tested less frequently than prescribed, and not all responsible staff identified in the safety documentation are involved in the tests, thus underestimating their readiness to address the consequences of significant incidents and to restore the operation and data of the systems (Chapter 2.6, page 38).

Changes at the time of the audit

During the audit, changes were made to the budget management process of the Centre of Registers[8]: the criteria for prioritising planned investments and costs were established on 23 July 2021, and the procedure for adjusting the budget was detailed. Therefore, we do not recommend the improvement of this process. Other changes and assessments made during the audit are presented in the “Audit results” section of the report.

Recommendations

For the Ministry of the Economy and Innovations as the body implementing the rights and obligations of the owner of the State Enterprise Centre of Registers

Technology Incidents of the State Enterprise Centre of Registers approved by Order No VE-727 (1.3E) of 27 October 2021 of the Director General of the State Enterprise Centre of Registers.

[6] The first problem was registered on 15 June 2019.

[7] JIRA system indicates the status of changes as of 8 March 2021.

[8] Procedure for the preparation and monitoring of the budget approved by Order No VE-432 (1.3 E) of 23 July 2021 of the Director-General of the State Enterprise Centre of Registers, pp. 35-36.

1. In order to reduce the need for public budget resources to compensate for the cost of services provided free of charge, provide for measures to ensure that state and municipal institutions and bodies use the most cost-effective way of obtaining data (key audit result 1).

2. In order to optimise the safety management of state information resources managed by the Centre of Registers, by reducing the administrative burden for all entities involved in the preparation, harmonisation and approval of safety documents, to assess the expediency of legitimization of provision for legal preconditions for state information resource managers to jointly approve common safety documents when the data of the state information resources they manage are processed by the same data manager (key audit result 2).

For the State Enterprise Centre of Registers

3. In order to improve the conditions for the development of state information resources managed by the Centre of Registers and to ensure the continuity of good practice in information technology management (key audit result 1):

    3.1. provide for measures to ensure the succession planning of all staff performing important information technology functions and the planning of the IT Centre's competence needs in accordance with generally accepted good practices;

    3.2. involve all managers of state information resources managed by the Centre of Registers in the process of strategic decision-making related to the development of state information resources;

    3.3. provide for measures to strengthen the control of the implementation and monitoring of projects, to ensure the timely implementation of projects, and assessment of the benefits of the completed projects;

    3.4. institutionalise the Architecture Committee and approve a common architecture consisting of business processes, information, data, applications and technology architecture layers.

4. In order to ensure high availability, sufficient speed and continuity of the state information resources managed by the Centre of Registers (key audit result 2):

    4.1. provide for measures to ensure that safety assessments of all state information resources managed by the Centre of Registers are carried out at specified intervals;

    4.2. establish measures to ensure periodic analysis of the state of play of state information systems resources managed by the Centre of Registers and planning of future capacity needs based on operational requirements, impact analysis and risk assessment;

    4.3. specify the incident classification schemes, establish the request management procedures, service levels applied by the Information Technology Helpdesk, roles and responsibilities of participants in the process;

    4.4. establish criteria for recording problems, process procedures, roles and responsibilities of participants, monitoring and control of the process;

4.5. provide for the monitoring and control of the change management process to ensure that all changes are implemented within a set timeframe;

4.6. establish controls to ensure adequate compliance with the requirements set out in business continuity management plans.

The measures and deadlines for the implementation of the recommendations are set out in the “Recommendations Implementation Plan” section of the report (page 41).