VALSTYBĖS KONTROLĖ
PUBLIC AUDIT

ENSURING CYBERSECURITY

27 October 2022

No VAE-10

SUMMARY

Relevance of the Audit

Critical information infrastructure, related electronic information systems and services are vital for the Republic of Lithuania. The increasing digitalisation of services and processes, the COVID-19 pandemic, geopolitical challenges and tensions increase the threats of cyber and hybrid attacks and their social and economic impact. According to the National Cybersecurity Centre[1], 11,659 cyber incidents have been reported in the last 3 years: 3,241 in 2019, 4,330 in 2020 and 4,088 in 2021. Due to the high number of cyber incidents, their modernisation and the potential risk of critical consequences of cyber-attacks and incidents, it is increasingly important to ensure cyber security at the national level.

Ensuring cybersecurity is based on risk assessment of threats and vulnerabilities that may affect the security of critical information infrastructure, information and communication systems. Management of risk is essential for the development, implementation, support and improvement of an effective security requirements management system. The security requirements management system includes the identification and enforcement of requirements (measures, rules, and procedures) for the security of information systems of institutions and organisations networks, monitoring and review (compliance assessment), prevention, detection, response, recovery, assessment of cyber incidents, also response and preventive measures, security technology management, staff training, and awareness programmes.

Aware that cybersecurity risk management, cyber incident management, and preventive activities, including cybersecurity exercises and training, are important elements (factors) of an effective security management system that determine the ensuring of cybersecurity, we have decided to conduct a public audit.

[1] Internet access: https://www.nksc.lt/aktualu.html (National cybersecurity status reports, accessed on 8 July 2022).

Objective and Scope of the Audit

The objective of the audit is to assess whether cybersecurity is ensured.

Key audit questions:

- whether the cybersecurity risk management is ensured at the national level;
- whether the legal regulation of cybersecurity and the system for assessing compliance with requirements established by legal acts is effective;
- whether the management of cyber incidents is ensured;
- whether the consistent implementation of cybersecurity planning is ensured.

Audited entities:

- Ministry of National Defence, as it develops cybersecurity policy, organises, controls, and coordinates its implementation[2];
- The National Cybersecurity Centre, as it implements cybersecurity policy and is responsible for monitoring cyber incidents and analysis of risks in cyberspace at the national level, monitoring the implementation of cybersecurity requirements, and assessment of the security status of cybersecurity entities[3].

During the audit, we collected information from the Ministry of National Defence and the National Cybersecurity Centre and surveyed 212 cybersecurity entities[4]. We communicated with the representatives of the State Data Protection Inspectorate, Communications Regulatory Authority, Informatics and Communications Department, Lithuanian Criminal Police Bureau, and Kaunas University of Technology.

The audited period is 2019–2021. In some cases, we used the data of the previous years (2015–2018) and 2022 to assess trends and developments.

The audit was carried out in accordance with 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” (p. 43).

Key Results of the Audit

The cybersecurity assurance framework needs to be improved as adequate management of cybersecurity risks and incidents is not ensured at the national level, adequate conditions for monitoring compliance with security requirements are not provided, legal regulation on cybersecurity and electronic information safety is still unconsolidated, and consistent implementation of cybersecurity planning is not ensured. An effective cybersecurity assurance framework would increase resilience against cyber threats,

[2] Law on Cyber Security, Article 4(2)

[3] Ibid., Art. 4(3), Art. 8(2)

[4] Managers and processors of state information resources listed on the http://www.registrai.lt/ website and critical information infrastructure managers (accessed on 18 August 2022).

effectively protect critical information infrastructure and information resources, and strengthen the response to cyber threats.

1. The security management system is not effective enough

- Information on cybersecurity risks identified by cybersecurity entities is not being collected and managed at the national level. More than a third (38 %, 81 out of 212) of cyber security entities surveyed do not carry out a cybersecurity risk assessment, which may lead to new or recurrent threats affecting their safety status and activities. The cybersecurity risk assessment process requires specific knowledge in this area and institutions' risk assessment experts are not able to assess cybersecurity risks qualitatively, therefore it is appropriate to have guidelines for risk assessment. More than half (56 %, 74 out of 131) of cybersecurity entities carrying out assessments do not provide information on identified cybersecurity risks to the National Cybersecurity Centre. The legislation does not impose an obligation for cybersecurity entities managing and/or processing State information resources to periodically submit risk assessment reports on communications and information systems to the National Cybersecurity Centre. Since the national cybersecurity risks are not identified, the national cybersecurity risk management plan is not prepared and the acceptable national cybersecurity risk and its tolerance limits are not established, therefore risk management process is not coordinated at the national level to ensure the use of the necessary protection, prevention and response measures and capabilities (Section 1.1, p. 13).
- In the period 2019–2021, almost half (45 %, 80 out of 176) of State information resource managers/administrators never carried out compliance assessment of information technology security, thereby not being aware of the status of their information security management system in order to take timely action to improve it if necessary. The number of information technology security compliance assessments is increasing every year, but in 2021, 81 % of the State's IT security compliance assessment reports were not submitted. A significant proportion (41 %, 39 out of 96) of the State information resource managers/administrators who carried out IT security compliance assessments did not provide data to the System for Monitoring Compliance of Public Information Resources with Information Security Requirements. This reduces the capacity of centrally managing information on cases of IT security non-compliance and ensuring monitoring of compliance with requirements at the national level. In 2018, the National Audit Office of Lithuania identified weaknesses[5] and the recommendation measure had to be implemented by 1 June 2019. However, the problems have not been resolved to this day, as the existing software code does not allow for a functional extension of the System for Monitoring Compliance of Public Information Resources with Information Security Requirements, therefore, the problems that have not been resolved for years negatively affect this sustainability, create the conditions for the emergence of vulnerabilities (Section 1.2, p. 15).
- In 2015, when the Ministry of National Defence took over the functions of cyber security and in 2018 - the policy-making of the State information resources

[5] The system for monitoring the compliance of State information resources with information safety requirements has been established to facilitate the monitoring of compliance of State information resources with electronic information safety requirements, however, its functionality is used not sufficiently.

(electronic information security), the legal framework for these areas was not consolidated. In 2015, the National Audit Office made a recommendation[6] to review and harmonise (consolidate) cybersecurity and electronic information security requirements. The Ministry of National Defence and the Ministry of the Interior have committed to implementing it by the fourth quarter of 2016, however, the draft of the unified framework of security requirements has not been developed so far. Certain requirements for cybersecurity and electronic information security set out in different legal acts are identical, which complicates the implementation of security requirements for cybersecurity entities managing and/or processing State information resources (Section 1.3, p. 17).

2. Management of cyber incidents should be improved

- The institutions managing and/or investigating cyber incidents (National Cybersecurity Centre, State Data Protection Inspectorate, Police Department) do not in all cases exchange information on cyber incidents that are relevant to them according to the nature of their activity, therefore, these institutions do not create preconditions for the rapid identification of different types of cyber incidents and the submission of information to competent institutions to enable the latter to prevent criminal offences or infringements, which could harm cybersecurity entities and the society, in a timely manner. Cybersecurity entities and institutions managing and/or investigating cyber incidents are required to transmit information on cyber incidents through the Cybersecurity Information Network or, where this is not possible, by other secure means of transmission of information, however, the National Cybersecurity Centre only accept information on cyber incidents from entities and institutions through other secure means of transmission of information, but not via the network. We found that cybersecurity entities passively use the network (in the last 3 months, 59 %, or 125 out of 212 entities did not use the network), and in the opinion of stakeholders (Department of Informatics and Communications, Communications Regulatory Authority, State Data Protection Inspectorate, Ministry of National Defence), the network is currently working inefficiently and could be adapted for wider use (Section 2.1, page 21).
- Cybersecurity exercises, training and consultations on cybersecurity are carried out but are not sufficiently successful to strengthen the capacity of cybersecurity entities to effectively counter and prevent cyber-attacks. National cybersecurity exercises, cybersecurity training, consultations, and methodological recommendations are organised annually; the majority of cybersecurity entities, i.e. 73 %, 101 out of 138 and 72 %, or 73 out of 102 participants, evaluate them positively, however, the involvement of cybersecurity entities in the exercise and training is insufficient: in the last three years (2019–2021), as many as 35 % (74 out of 212) entities never participated in the exercises, 52 % (110 out of 212) in the training. Every fourth of cyber security entities (26 %, 55 out of 212) does not have a cyber incident management plan/procedure, and there is no approved typical cyber incident management plan, which would serve as a model for cybersecurity entities. If these entities were obliged to participate regularly in cybersecurity exercises or training, and a typical cyber incident management plan was adopted, the strengthening of their cybersecurity competencies and skills would be ensured and they would be aware of the actions

[6] Internet access: https://www.valstybeskontrole.lt/LT/Product/23587/kibernetinio-saugumo-aplinka-lietuvoje (accessed on 18 August 2022).

to be taken in the event of a cyber incident, to effectively manage it and prevent potential threats (Section 2.2, p. 23).

3. Consistent implementation of cybersecurity planning is not ensured

- The monitoring and control of the implementation of the National Cybersecurity Strategy focus on continuous reporting on the progress made, but the results of the implementation of the 2019–2021 Strategy have not been reviewed annually: since the entry into force of the Law on Strategic Management since 2021, the Ministry of National Defence did not collect and systematise information on the results of the implementation of the National Cybersecurity Strategy, and the managers of the Strategy did not monitor all measures and assessment criteria. Of the 28 measures foreseen in the Interinstitutional Operational Plan for the implementation of the National Cybersecurity Strategy, only 17 have been implemented fully, 4 have not been implemented, and the implementation of 7 has been started. However, due to the COVID-19 pandemic and pending public procurement procedures, they have been implemented not fully or the status of their implementation is unknown due to the completion of the monitoring of the measures. For the same reasons, 11 (out of 38) strategic indicators are not reached and the status of 5 out of 38 is unknown. A draft amendment to the Interinstitutional Operational Plan was under preparation in 2020 but was suspended due to non-compliance with the provisions of the Law on Strategic Management. The inconsistent implementation and insufficient monitoring of planned cybersecurity strengthening measures led to the fact that the objectives and targets set by the national cybersecurity planning documents for strengthening State cybersecurity and the development of cyber defence capabilities, fostering cybersecurity culture and innovation development, have not been fully achieved when assessing the results of the implementation of the 2021 National Cybersecurity Strategy against the foreseen assessment criteria. It should be noted that the changes are foreseen in the strategic planning - by Q4 2022 the Ministry of National Defence must prepare a National Cyber Security Development Programme to define new measures for progress (cybersecurity strengthening) (Section 3, p. 28).

Recommendations

To the Ministry of National Defence

1. In order to ensure the use of cyber-protection, prevention and countermeasures, a process for managing information technology security risks (including cyber) needs to be implemented and coordinated at the national level, allowing the information obtained on the state of cybersecurity risk to be used for strategic decisions to strengthen cybersecurity (Key audit result 1).

2. In order to implement the security requirements laid down in legal acts more effectively for cybersecurity entities, to develop a common methodology for the compliance assessment of cybersecurity and information technology security of State information resources, enabling a comprehensive assessment of compliance with legal requirements, which will allow the supervisory and monitoring institution to provide more effective data-based analysis, insights and summary of the actual state at the national level (Key audit result 1).

3. In order to enable all cybersecurity entities to be aware of the actions to be taken in the event of a cyber incident or in order to prevent potential threats, the Ministry should:

   - adopt measures to facilitate the cyber incidents communication through the cybersecurity information network;
   - oblige cybersecurity entities (State information resource managers and administrators, critical information infrastructure managers) to participate in national cybersecurity exercises and to provide indicators for the assessment of the educational activities carried out by the National Cybersecurity Centre and to monitor them periodically;
   - develop and approve a detailed, typical cyber incident management plan and oblige cybersecurity entities to prepare or update their internal cyber incident management plans/procedures in accordance with the model of this typical plan (Key audit result 2).

   Measures and deadlines for the implementation of the recommendations, the expected impact of the audit and indicators for measuring change are set out in the "Recommendations Implementation Plan" section of the Report (p. 34). Relevant information on the status of implementation of the recommendations, results and developments is published as open data on the National Audit Office of Lithuania website https://www.valstybeskontrole.lt/LT/AtviriDuomenys.