Summary of the audit report
Efficiency of managing cybersecurity riskof the ELES company critical infrastructure

The Court of Audit implemented the audit of the efficiency of the company **ELES, Ltd., Electricity Transmission System Operator** (hereinafter referred to as: ELES) in critical infrastructure cybersecurity risk managing in the period from 1 January 2019 to 31 July 2020. According to the opinion of the Court of Audit, ELES was efficient in managing cybersecurity risk relating to critical infrastructure in the period covered by the audit.

ELES imposed risk management already in 2009 and set up a comprehensive risk management system over the following years, representing a crucial part of the company’s integrated management system together with the internal control system. Risk management of ELES followed
a process-based model, namely risks in individual processes. ELES kept a computerised record of risks by fields of operations, and in 2019 also established a record of risks in the field of critical infrastructure and in the field of providers of essential services. On the basis of Critical Infrastructure Act, guidelines of the Ministry of Defence, professional guides of critical infrastructure sector operators and own risk assessment methodology, ELES timely identified sources of risks to critical infrastructure operations, analysed and evaluated risks to critical structure operations, determined sources of risks, monitored the state of critical infrastructure, it had duplicated management centres and it devised security plans. ELES also applied a documented information security management system, and was just concluding with the introduction of a business continuity management system at the time of the audit review, as stipulated by Critical Infrastructure Act. In accordance with demands of critical infrastructure sector operators, ELES carried out risk assessment of critical infrastructure and imposed measures for protection of critical infrastructure. Additionally, ELES responded to COVID-19 epidemic caused by the SARS-CoV-2 virus by adopting various measures and thus ensured continuous operation of processes.

ELES efficiently detected cyber threats, namely by various documented activities, there were roles and responsibilities for detecting security events defined, and it performed various detection activities. ELES followed established procedures for submitting information on detected events, it also continuously improved detection processes and built knowledge bases relating to security events. ELES had a repose plan for managing response to cyber threats. Its employees were appropriately trained for responding and reported and submitted information on the events to the relevant recipients within and outside ELES. Furthermore, it cooperated with certain organisations in voluntary exchange of information on incidents. ELES managed responding also by analysing notices and understanding of the impact of incidents on the organisation, as well as by classifying security incidents. ELES applied processes for monitoring, analysing and responding to vulnerabilities, and for limiting and mitigating security incidents. ELES had no special strategy for the field of cybersecurity, however, it did establish policies pertaining to all segments of the integrated management system that were through management reviews subject to ongoing inspection and relevant updating. There exist possibilities for improvements that ELES is aware of and has thus introduced them.

The Court of Audit did not demand from ELES to submit a response report but it proposed several recommendations to further improve the existing situation.

Ljubljana, 23 August 2021