

# Performing a Cybersecurity Audit of an Electric Power Transmission Systems Operator

日本語版も入手可能  
[www.isaca.org/currentissue](http://www.isaca.org/currentissue)

Electricity is the lifeblood of many modern technologies and one of the often overlooked services that makes life easier. Many people, especially in developed countries, can hardly imagine life without it. Water supplies, heating, cooling, food processing, telecommunications and many other goods and services are fundamentally dependent on electricity. Most countries in the world consider electricity transmission and distribution infrastructure and services fundamental parts of their critical infrastructures. For example, the Republic of Slovenia (Slovenia) declared the electric power transmission organization a crucial element of its infrastructure.

Because power transmission infrastructures are critical, protecting the organizations that run these services from cyberthreats is also crucial, especially because cyberthreats and cyberattacks are increasing.<sup>1</sup> A study from 2021 found that 83 percent of critical infrastructure organizations experienced operational technology breaches in the prior 36 months.<sup>2</sup> One of the first large-scale, well-known cyberattacks on a power grid occurred in Ukraine in December 2015.<sup>3</sup> It set a precedent for the security of power grids around the world.<sup>4</sup> Cybersecurity organizations such

as the European Union Agency for Cybersecurity (ENISA), ISACA®, the International Organization for Standardization (ISO) and the US National Institute of Standards and Technology (NIST) issued guidelines, methods and approaches to address the problem and increase awareness of preparedness against cyberattacks. In the European Union, the ENISA reviewed the status of awareness of cybersecurity among member states.<sup>5</sup> The main purpose of ENISA report is to assist member states in building their cybersecurity capacities by analyzing best practices for raising citizens' awareness of cybersecurity. The report also offers recommendations in four areas:

1. Building capacities for cybersecurity awareness
2. Regularly assessing trends and challenges
3. Measuring cybersecurity behavior
4. Planning cybersecurity awareness campaigns

Nearly every country has a Supreme Audit Institution (SAI), which is an independent national institution that conducts audits of government activities, and nearly every SAI in the world is a member of the International Organization of Supreme Audit Institutions (INTOSAI), which works to establish and disseminate international standards and good practices.

The SAI of Slovenia carried out an audit to assess the cyberthreat preparedness of an organization that operates critical infrastructure for electric power transmission. Understanding how to perform an IT performance audit, report on an organization that is part of a nation's critical infrastructure, and mitigate any possible negative effects of such incidents are critical. Incidents can adversely affect many other services and organizations—and the nation as a whole.

## The Audit Environment

The Court of Audit of Slovenia is the highest audit body for supervising state accounts, the state budget and all public spending in Slovenia.<sup>6</sup> The Court of Audit performs all forms of audits (i.e., compliance, financial, performance) in accordance with domestic legislation and INTOSAI standards. The Court of Audit

### BOSTJAN DELAK | PH.D., CISA

Is an assistant professor at the Faculty of Information Studies (Novo Mesto, Slovenia). Previously he worked as an information system auditor at the Supreme Audit Institution of the Republic of Slovenia. His research interests include information system analysis, due diligence and knowledge management.

### MIROSLAV KRANJC | PH.D.

Is a supreme state auditor and founding leader of the Department for Performance Audit at the Supreme Audit Institution of the Republic of Slovenia. He is passionate about IT and environmental auditing and lectures on various topics related to performance auditing.

of Slovenia audits various types of entities including entities that provide public services or provide goods to the public on a concession basis.<sup>7</sup>

ELES, Ltd., Electricity Transmission System Operator (ELES), a state-owned legal entity, is the operator of the electric power transmission network of Slovenia.<sup>8</sup> ELES has been providing safe, reliable and uninterrupted electric power transmission throughout Slovenia and across its borders for 90 years. ELES endeavors to strategically, responsibly, and sustainably plan, construct, and maintain Slovenia's high-voltage transmission network at three voltage levels: 400 kV, 220 kV and partly in 110 kV.

The electric power transmission network cannot be operated on its own. It must be connected to networks in neighboring countries and integrated into a wider electric power system; therefore, ELES closely cooperates with the neighboring system operators and actively participates in many regional and international associations. ELES, as the only Slovene electric power transmission operator, is actively involved in the design and development of a unified European market through the professional association the European Association for the Cooperation of Transmission System Operators for Electricity (ENSTO-E)<sup>9</sup> and various (inter)regional initiatives and projects.<sup>10</sup> **Figure 1** presents the position of ELES in relation to electricity generation, electricity distribution to end users, supply of electricity to major direct customers and the connection to international transmission networks.

---

**Understanding how to perform an IT performance audit, report on an organization that is part of a nation's critical infrastructure, and mitigate any possible negative effects of such incidents are critical.**

---

## The Audit Motivation and Criteria

The motive of the Court of Audit was to assess the readiness of ELES as a critical infrastructure



manager against cyberthreats and, thus, its potential to reduce the risk of interruptions in the distribution of electricity to consumers.

According to ISSAI 300, auditors should establish suitable criteria that correspond to the audit questions and are related to the principles of economy, efficiency and effectiveness.<sup>11</sup> In the case of auditing readiness of cybersecurity at a critical infrastructure organization, audit criteria were based on provisions of the Critical Infrastructure Act and the NIST Framework for Improving Critical Infrastructure Cybersecurity.

## Legislation

In 2018, Slovenia enacted the Critical Infrastructure Act<sup>12</sup> and the Information Security Act.<sup>13</sup> The Critical Infrastructure Act regulates the identification and determination of the critical infrastructure of Slovenia, the principles and planning of critical infrastructure protection, and the tasks of bodies and organizations in the field of critical infrastructure and information, including reporting, decision support, data protection and control. The act defines critical infrastructure as:

*[T]hose capacities that are of key importance to the state and the cessation of their operation or their destruction would significantly affect and have serious consequences for national security, economy and other key social functions and health, safety, protection and well-being.<sup>14</sup>*

The Information Security Act regulates the field of information security and defines measures to achieve a high level of security of networks and information systems in Slovenia. These measures are essential for the smooth operation of the state in all security conditions and to provide essential services for



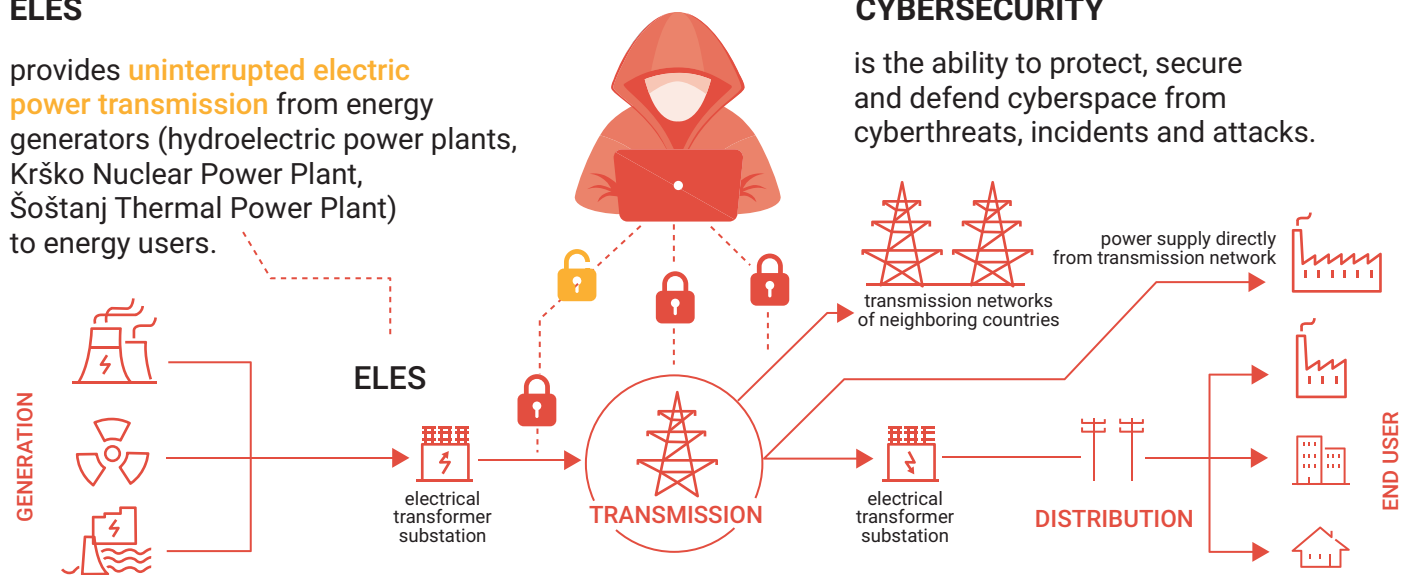
### LOOKING FOR MORE?

- Read *Governance Roundup—What Are You Doing About Environmental, Social and Governance Factors in Your Enterprise?* [www.isaca.org/governance-roundup-esg](http://www.isaca.org/governance-roundup-esg)
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. <https://engage.isaca.org/onlineforums>

**FIGURE 1**  
**Role of ELES**

## ELES

provides **uninterrupted electric power transmission** from energy generators (hydroelectric power plants, Krško Nuclear Power Plant, Šoštanj Thermal Power Plant) to energy users.



## CYBERSECURITY

is the ability to protect, secure and defend cyberspace from cyberthreats, incidents and attacks.

**A cyberattack may paralyze electricity distribution in Slovenia; thus cybersecurity at ELES is of crucial importance.**

Source: Republic of Slovenia Court of Audit, *Audit Report: Efficiency of Managing Cybersecurity Risk of the ELES Company Critical Infrastructure*, 2021, Slovenia, [https://www.rs-rs.si/fileadmin/user\\_upload/Datoteke/Revizije/2021/CS-ELES/ANG/CS\\_ELES\\_infografika-EN.pdf](https://www.rs-rs.si/fileadmin/user_upload/Datoteke/Revizije/2021/CS-ELES/ANG/CS_ELES_infografika-EN.pdf). Reprinted with permission.

maintaining key social and economic activities. With the adoption of this act, Slovenia transposed into Slovenian legislation Directive (EU) 2016/1148 of the European Parliament and of the Council on measures for a high common level of security of networks and information systems in the European Union.<sup>15</sup>

### Critical Infrastructure Act

The Critical Infrastructure Act includes provisions that require critical infrastructure organizations to develop and manage risk assessments and measures to protect critical infrastructure. The risk assessment must abide by the instructions for risk assessment of the operation of critical infrastructure, adopted by the Ministry of Defense of Slovenia. The assessment should also follow expert guidelines prepared for individual critical infrastructure sectors. Ongoing measures are being implemented in all situations, and, in the event of a crisis, emergency or increased threat to critical infrastructure, their implementation may be intensified. Additional measures shall be implemented in the event of an increased threat to critical infrastructure, an emergency or a crisis if ongoing measures, even if their implementation is escalating, are not sufficient.

### NIST Framework for Improving Critical Infrastructure Cybersecurity

For the second set of criteria, the auditors chose the NIST Cybersecurity Framework (CSF) function Detect and Respond, as displayed in the shaded boxes in **figure 2**.<sup>16</sup>

The Identify and Protect functions are covered by the first audit criteria—provisions of the Critical Infrastructure Act. The auditors did not choose the last function, Recover, since ELES had no previous experience with cyberattacks.

### The Audit Process

The audit was a performance audit based on INTOSAI standards and principles.<sup>17</sup> The main audit question was whether ELES had effectively managed cybersecurity in the area of critical infrastructures. The auditing period was from 1 January 2019 to 31 July 2020. The audit started in December 2019 and the final report was published in August 2021. The audit team consisted of one information system auditor and one state auditor with legal knowledge. The audit team prepared the audit plan, requested

the documentation and questionnaires regarding critical infrastructure, completed more than 10 interviews and function tests (one-third live and the rest via videoconferencing systems due to COVID-19 restrictions) and reviewed several on-site locations. For NIST CSF functions testing, auditors used COBIT® 5 and ISO/International Electrotechnical Commission (IEC) standard ISO/IEC 27001:2013 *Information technology—Security techniques—Information security management systems—Requirements controls*.<sup>18</sup> The testing period was from 4 June 2020 to 24 September 2020. During the testing period, all 34 subcategories by informative references/controls were tested. After collecting enough information and evidence to present to the auditee, the team prepared a draft report, which was first coordinated with the Supreme State Auditor and legal service of the Court of Audit and agreed on with the responsible deputy auditor general. The official draft report was sent to ELES, followed by a clearance meeting with the auditee. After accepting comments and amendments from the auditee, the audit report proposal was prepared and issued to the auditee. At that point, there were no other objections, so after additional independent proofreading and review, the final audit report was sent to the auditee and Parliament and was published on the Court of Audit website.

### Audit Findings

The Court of Audit found that ELES introduced risk management in 2009 and set up a comprehensive risk management system in the years that followed. ELES kept a computerized catalog of risk by field of operation and, in 2019, it also introduced records of risk in the field of critical infrastructure. ELES identified sources of risk to critical infrastructure operations, analyzed and evaluated risk to critical infrastructure operations, determined sources of risk, monitored the state of critical infrastructure, duplicated control centers and devised security plans, all in a timely manner. ELES also applied a documented information security management system and is certified in ISO/IEC 27001:2013. The organization was concluding the introduction of a business continuity management system at the time of the audit review. ELES’s business continuity management system was used to carry out risk assessment of critical infrastructure and impose measures to protect critical infrastructure. In addition, ELES responded to the COVID-19 pandemic by adopting various measures, many of which related to the organization of human resources, such as the creation of a sealed control center, in which some employees lived and worked in two-week-long shifts; isolation of power transmission management support teams; and working from home. This ensured continuous operation of the processes related to the transmission of electricity.

**FIGURE 2**  
**NIST CSF Functions and Categories**

Identify	Protect	Detect	Respond	Recover
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security and Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

Source: US National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, USA, 2018, <https://www.nist.gov/cyberframework>. Reprinted with permission.

**Figure 3** presents several of the findings of the audit.

ELES efficiently detected cyberthreats by defining and analyzing security event roles and responsibilities. The organization followed established procedures for submitting information about detected events, continuously improved detection processes and built knowledge bases relating to security events. ELES had a plan for responding to cyberthreats. Its employees were appropriately trained in responding to and reporting on security events to relevant recipients within and outside ELES.

ELES also analyzed notices of security events and took measures to classify security incidents and understand their impact on the organization. It applied processes for monitoring, analyzing and responding to vulnerabilities and for limiting and mitigating security incidents. ELES had no established strategy specifically for the field of cybersecurity; however, it did establish policies pertaining to all segments of the integrated management system through management reviews subject to ongoing inspection and relevant updates.

There are several possibilities for improvements that ELES is aware of and has thus introduced:

- Full implementation of a business continuity management system

- Integration of all detected events to a single dashboard
- Execution of independent penetration tests after current IT projects are finalized
- Implementation of video surveillance of areas in which it does not currently exist

### Opinion of the Court of Audit

According to the opinion of the Court of Audit, ELES was efficient in managing cybersecurity risk relating to critical infrastructure during the period covered by the audit.

The Court of Audit did not demand that ELES submit a response report; however, it proposed several recommendations for further improvements:<sup>19</sup>

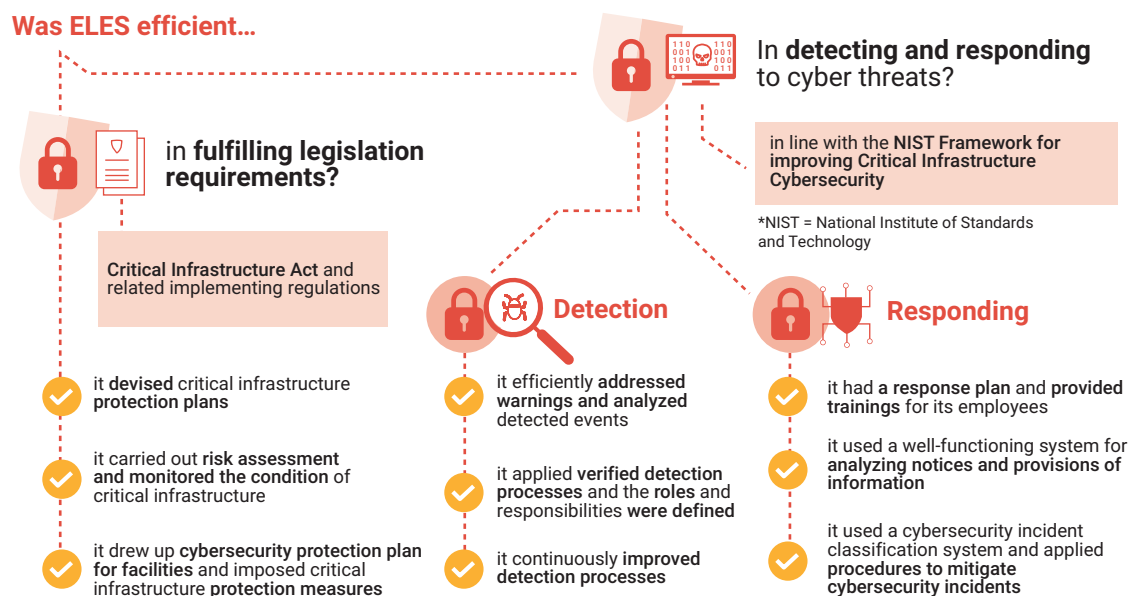
- Periodically manage the transmission of electricity from the reserve control center
- Regularly (e.g., annually) plan and conduct penetration testing
- Periodically test the process of reporting security events to external stakeholders
- Examine the possibility of establishing a common knowledge base on detected events and their resolutions

**Figure 4** presents the opinion of the Court of Audit.

**FIGURE 3**

## Audit Findings

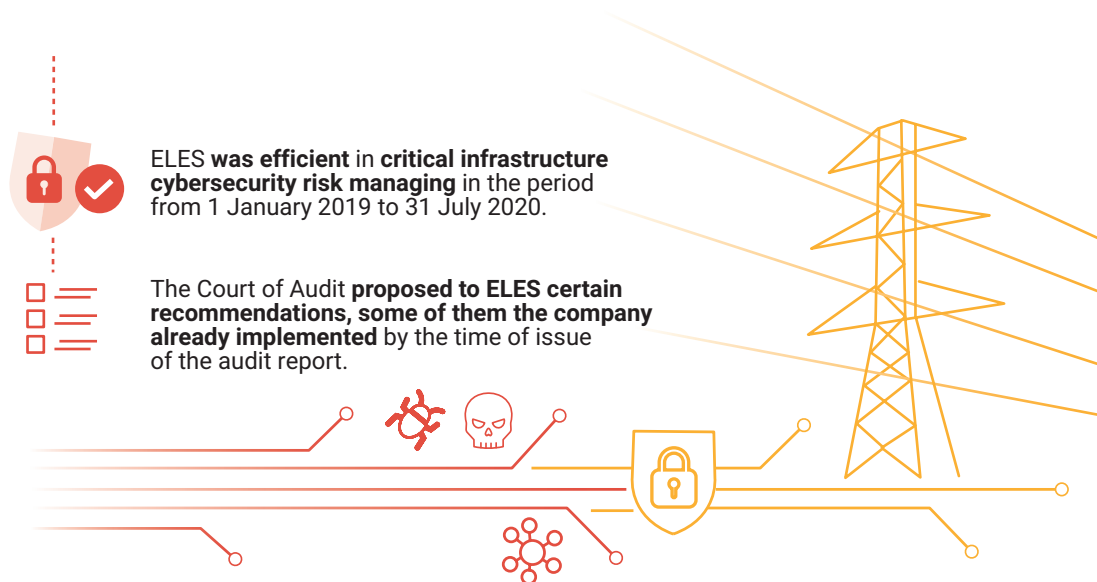
### Was ELES efficient...



Source: Republic of Slovenia Court of Audit, *Audit Report: Efficiency of Managing Cybersecurity Risk of the ELES Company Critical Infrastructure*, 2021, Slovenia, [https://www.rs-rs.si/fileadmin/user\\_upload/Datoteke/Revizije/2021/CS-ELES/ANG/CS\\_ELES\\_infografika-EN.pdf](https://www.rs-rs.si/fileadmin/user_upload/Datoteke/Revizije/2021/CS-ELES/ANG/CS_ELES_infografika-EN.pdf). Reprinted with permission.

FIGURE 4

## Opinion of the Court of Audit



Source: Republic of Slovenia Court of Audit, *Audit Report: Efficiency of Managing Cybersecurity Risk of the ELES Company Critical Infrastructure*, [https://www.rs-rs.si/fileadmin/user\\_upload/Datoteke/Revizije/2021/CS-ELES/ANG/CS-ELES\\_infografika-EN.pdf](https://www.rs-rs.si/fileadmin/user_upload/Datoteke/Revizije/2021/CS-ELES/ANG/CS-ELES_infografika-EN.pdf). Reprinted with permission.

## Audit Limitations

Though it ultimately proved effective, the audit had several limitations of note. The audit did not include an assessment of the auditee's business continuity management system or the continuous operation of the auditee's information system. It also did not account for penetration tests.

## Conclusion

The Court of Audit chose ELES as the subject of its first performance audit on cybersecurity of critical infrastructure because the organization operates the transmission of electricity from a source to larger customers. The audit showed that ensuring that the audit team included an expert in IT systems and information security and a legal expert was helpful. The selection of audit criteria was also beneficial for reviewing in detail the readiness of ELES for potential cyberattacks. This case study also shows that additional experts in the field of hacking and penetration testing should be included in the audit team to perform a more detailed cybersecurity audit. The Court of Audit will invest effort to continue to plan and perform cybersecurity performance audits of organizations that manage critical infrastructure to assess their cybersecurity risk management and confirm their decisions on spending public money to mitigate cyberthreats.

## Endnotes

- 1 Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents Since 2006*, USA, 2021, [https://csis-website-prod.s3.amazonaws.com/s3fs-public/220104\\_Significant\\_Cyber\\_Events.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/220104_Significant_Cyber_Events.pdf)
- 2 Dark Reading, "Eighty-Three Percent of Critical Infrastructure Organizations Suffered Breaches, 2021 Cybersecurity Research Reveals," 9 November 2021, <https://www.darkreading.com/vulnerabilities-threats/83-of-critical-infrastructure-organizations-suffered-breaches-2021-cybersecurity-research-reveals>
- 3 International Cyber Law: Interactive Tool Kit, "Power Grid Cyberattack in Ukraine (2015)," 4 June 2021, [https://cyberlaw.ccdcoe.org/wiki/Power\\_grid\\_cyberattack\\_in\\_Ukraine](https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine)
- 4 Zetter, K., "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 3 March 2016, <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>
- 5 European Union Agency for Cybersecurity (ENISA), *Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies*, Greece, 29 November 2021, <https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity>

- 6 Republic of Slovenia Court of Audit, <https://www.rs-rs.si/en/>
- 7 Republic of Slovenia Court of Audit, Court of Audit Act, Article 20, <https://www.rs-rs.si/en/about-the-court-of-audit/legal-basis/court-of-audit-act/>
- 8 ELES Company, <https://www.eles.si/en>
- 9 The European Association for the Cooperation of Transmission System Operators for Electricity (ENTSOE), <https://www.entsoe.eu/>
- 10 ELES Company, "About the Company," <https://www.eles.si/en/about-the-company>
- 11 International Organisation of Supreme Audit Institutions (INTOSAI), ISSAI 300: Performance Audit Principles, Austria, 2019, [https://www.intosai.org/fileadmin/downloads/documents/open\\_access/ISSAI\\_100\\_to\\_400/issai\\_300/ISSAI\\_300\\_en\\_2019.pdf](https://www.intosai.org/fileadmin/downloads/documents/open_access/ISSAI_100_to_400/issai_300/ISSAI_300_en_2019.pdf)
- 12 National Assembly of the Republic of Slovenia, Critical Infrastructure Act, <http://www.pisrs.si/Pis.web/npbDocPdf?idPredpisa=ZAK08464&idPredpisaChng=ZAK07106&type=pdf>
- 13 National Assembly of the Republic of Slovenia, Information Security Act, <http://www.pisrs.si/Pis.web/npbDocPdf?idPredpisa=ZAK08380&idPredpisaChng=ZAK07707&type=pdf>
- 14 *Op cit* Critical Infrastructure Act
- 15 Directive (EU) 2016/1148 of the European Parliament and of the Council, *Official Journal of the European Union*, Belgium, 6 July 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN>
- 16 National Institute of Standards and Technology (NIST), NIST Cybersecurity Framework, USA, <https://www.nist.gov/cyberframework>
- 17 *Op cit* INTOSAI
- 18 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2013 *Information technology—Security techniques—Information security management systems—Requirements*, Switzerland, 2013, <https://www.iso.org/standard/54534.html>
- 19 Republic of Slovenia Court of Audit, *Audit Report 2021: Effectiveness of Cyber Security Management for the Field of Critical Infrastructure in ELES*, Slovenia, 2021, [https://www.rs-rs.si/fileadmin/user\\_upload/Datoteke/Revizije/2021/CS-ELES/CS\\_ELES\\_RSP\\_RevizijskoP.pdf](https://www.rs-rs.si/fileadmin/user_upload/Datoteke/Revizije/2021/CS-ELES/CS_ELES_RSP_RevizijskoP.pdf)

## Convenient, Personal and Informative Training

Our Virtual Instructor-Led Training (VILT) sessions connect you with highly-qualified and experienced instructors in an online classroom setting. Sessions include interactive lectures and demonstrations all focused on helping you develop your expertise and get ready for exam day.

[www.isaca.org/VILT-jv1](http://www.isaca.org/VILT-jv1)

