Declared: 19 December 2019 Time version of the regulation effective as of: 1 January 2020
The content of this document is legally binding.

(Effective as: 31 March 2020)

COLLECTIONS OF LAWS

OF THE SLOVAK REPUBLIC

2019

436

DECREE

of the National Security Authority

of 11 December 2019

on Cybersecurity Audit and Auditor's Knowledge Standard

The National Security Authority pursuant to Article 32 (1) letters d) and f) of the Act No. 69/2018 Coll. on Cybersecurity and on Amendment and Supplementing of certain Acts (hereinafter referred to as "the Act") lays down:

Article 1

(1) A cybersecurity audit (hereinafter referred to as "audit") shall verify the fulfilment of obligations pursuant to the Act and assess the conformity of adopted security measures with the requirements of the Act and related specific legal regulations connected with the security of networks and information systems[11]) of the operator of essential services for respective networks and information systems of the essential service and for those that support essential services to ensure the required level of cybersecurity and to prevent cybersecurity incidents. The audit shall identify deficiencies in ensuring cybersecurity by the operator of essential services in order to adopt measures to correct and remedy them and to prevent cybersecurity incidents.

(2) The audit shall be performed by the conformity assessment body pursuant to Article 29 (3) of the Act, which is the cybersecurity auditor (hereinafter referred to as "auditor").

(3) In order to conduct audit the auditor shall meet the conditions of the knowledge standard according to Annex 1, verified by an exam documented according to the recommendations of

[1]) For example Article 2 of Act of the National Council of the Slovak Republic No. 566/1992 Coll. on the National Bank of Slovakia, as amended, Article 14 of Act No. 429/2002 Coll. on Stock Exchanges, as amended, Act No. 541/2004 Coll. on the Peaceful Use of Nuclear Energy (Atomic Act) and on Amendment and Supplementing of certain Acts as amended, Article 2 (9) of the Act No. 747/2004 Coll. on Supervision of the Financial Market and on Amendment and Supplementing of certain Acts, as amended by the Act No. 132/2013 Coll., Act No. 492/2009 Coll. on Payment Services and on Amendment and Supplementing of certain Acts, Act No. 95/2019 Coll. On Information Technologies in Public Administration and on Amendment and Supplementing of certain Acts.

internationally recognized technical standards[2]) or other similar and generally accepted procedures.

(4) The auditor shall be responsible for accuracy, scope and expertise in conducting the audit and preparing the final report on audit outcomes.

(5) The auditor shall conduct the audit professionally, objectively, impartially, on the basis of evidence in accordance with the recommendations of technical standards[2]) or other similar and generally accepted procedures.

(6) The duration of the audit shall be determined by the auditor to be sufficient to assess compliance with the obligations pursuant to the Act and the effectiveness of the security measures adopted, and their status shall be assessed by sampling, where the extent of samples shall be determined with regard to performed information classification and categorization of networks and information systems, performed cybersecurity risk analysis and the audit-ability pursuant to paragraph 1.

(7) The auditor in conducing the audit shall in particular

a) accept the audit request to the extent of the minimum requirements stipulated in Annex 2 and assess the completeness of the information in the application; the auditor may ask additional information required for audit preparation and conduct thereof,

b) prepare an audit conducting schedule, including especially

1. identification of organizational units, processes, audited networks and information systems and physical sites of the operator of essential services, indicating the time, and

2. name, surname and contact details of the responsible employee of the operator of essential services who shall provide the auditor with the necessary cooperation during the audit,

c) determine the scope of the audit according to Annex 3,

d) determine the audit methods according to Annex 4,

e) prepare background materials and working documents necessary for conducting the audit,

f) examine the security documentation, evaluate security measures and prepare an audit trail of security measures audited (hereinafter referred to as the "audit trail") according to Annex 4,

g) collect, gather and evaluate the evidence on audit findings,

h) inform in writing the responsible employee of the operator of essential services of the identified deficiencies and prepare a set of recommended corrective actions,

i) draw up a final report on audit outcomes.

Article 2

(1) The final report on audit outcomes shall evaluate the results of the audit and introduce the evidence on which the assessment was based.

(2) The final report on audit outcomes shall contain in particular:

a) name, surname, auditor's valid certificate number, date of issue and signature,

---

[2]) For example STN EN ISO/IEC 17024 Conformity assessment — General requirements for bodies operating certification of persons (ISO/IEC 17024:2012).

b) definition of the scope of audit conducted,

c) audit objectives,

d) methods of audit conducted,

e) summary of audit findings and declaration of compliance or non-compliance with the requirements for the security of networks and information systems,

f) the auditor's recommended corrective actions after identification of deficiencies,

g) documents, especially

1. copy of the auditor's certificate,

2. copy of the audit request,

3. calculation of the audit duration and justification for its shortening or prolonging,

4. audit trail with the statement of the operator of essential services regarding the audit findings,

5. the audit schedule,

6. list of assessed documentation,

7. specification and justification for changes and differences in the audit compared to the planned schedule,

8. assessment of the fulfilment of obligations pursuant to the Act and the overall state of security measures adopted for each information system related to the essential service, declaration of compliance or non-compliance with the requirements for the security of networks and information systems and a specification of deficiencies,

h) information on the status of corrective actions adopted if those corrective actions had to be adopted by the operator of essential services as a consequence of a previous audit.

(3) The final report on audit outcomes shall include a report on identified deficiencies in case of non-compliance with the requirements for the security of networks and information systems where the operator of essential services shall indicate the deadline for corrective actions to be adopted in order to ensure the required compliance with the requirements for the security of networks and information systems. Corrective actions shall be adopted so that they can be included in the final report on audit outcomes.

(4) If all identified deficiencies are removed at the agreed time before the final report on audit outcomes is drawn up, it shall be possible to declare the compliance with the requirements for the security of networks and information systems in the final report on audit outcomes.

Article 3

This Decree enters into force on 1 January 2020.

Roman Konečný

Annex 1 to Decree No. 436/2019 Coll.

AUDITOR'S KNOWLEDGE STANDARD

1. General requirements

Minimum requirements for auditor's qualification and experience:

Qualification and required certificates or diplomas	Professional experience and method of demonstrating it (alternatives to submitted documents)
Full secondary general education and full secondary trade education (evidence of obtained level of education and qualification)	- experience in the field of information technology, cybersecurity - at least ten years of professional experience (CV including the details of a referee contact for further verification, a list of conducted audits with the details of a referee contact for further verification), - experience in the field of information systems audit - at least seven years of professional experience (an international certificate from the field of information systems audit, a list of audits conducted with the details of a referee contact for further verification)
Higher education – Bachelor's Degree (diploma)	- experience in the field of information technology, cybersecurity - at least seven years of professional experience (CV including the details of a referee contact for further verification, a list of audits conducted), - experience in the field of information systems audit - at least five years of professional experience (an international certificate from the field of information systems audit, a list of audits conducted with the details of a referee contact for further verification)
Higher education – Master's Degree (diploma)	- experience in the field of information technology, cybersecurity - at least five years of professional experience (CV including the details of a referee contact for further verification, a list of audits conducted), - experience in the field of information systems audit - at least three years of professional experience (an international certificate from the field of information systems audit, a list of audits conducted with the details of a referee contact for further verification)

Knowledge:

- Knowledge of cybersecurity audit or information security audit or information systems audit shall be demonstrated by a certificate of the certification auditor pursuant to a technical standard[3]) or by an equivalent certificate of competence to conduct information audit or cybersecurity audit documented by an internationally valid auditor's certificate.

Prerequisites:

- independence (the auditor shall be independent in assessment of security measures if they have not participated in managing or operating the audited information systems during the last three years prior to the audit; it shall be documented by a declaration for each audit),
- objectivity (absence of granted complaints about objectivity during the professional experience),
- integrity.

[3]) For example STN EN ISO/IEC 27001, STN ISO/IEC 20000-1.

2. Special requirements

Minimum requirements for the auditor's professional competence:

Role name	Field / process	Knowledge, skills and requirements
Auditor	Cybersecurity audit	Knowledge of information and cybersecurity management system and processes.
		Knowledge of principles of information and cybersecurity organization.
		Knowledge of principles of personnel security.
		Knowledge of principles of access and identity control.
		Knowledge of methods of use of cryptographic security mechanisms.
		Knowledge of principles of cybersecurity testing. Knowledge of principles of cybersecurity audit. Knowledge of legal regulation, policies, compliance requirements and standards related to cybersecurity.
		Knowledge of legal regulation, policies, compliance requirements and standards related to personal data protection.
		Knowledge of policies and standards related to information security and cybersecurity.
		Knowledge of policies and standards related to personal data protection.
		Knowledge of principles of personal data protection.
		Ability to design and implement security strategies and policies.
		Knowledge of risk management processes and methodologies.
		Knowledge of risk analysis procedures.
		Knowledge of typical threats and procedures for identification of threats and vulnerabilities.
		Knowledge of security mechanisms.
		Knowledge of business architecture methodologies. Knowledge of cybersecurity incident handling processes.
		Knowledge of principles of operation recovery plans in case of disaster.
		Knowledge of business continuity management processes and principles of disaster recovery plans.
		Knowledge of principles of logging and security monitoring.
		Knowledge of principles of physical and building security management.
		Knowledge of security mechanisms in physical and building security.
		Knowledge of principles of service management in the field of information technologies.
		Knowledge of principles of cost management and budget rules.
		Ability to prioritize tasks and allocate resources efficiently.
		Knowledge of principles of human resource management.
		Knowledge of computer network concepts.
		Knowledge of principles of project management. Knowledge of principles of supply service management.
		Knowledge of principles of design and development of applications and information systems.
		Knowledge of principles of information systems procurement.
		Knowledge of principles of application security. Knowledge of principles and processes for auditing.
		Technical knowledge of audited systems.
		Knowledge of risk assessment methods sufficient to evaluate audit risks and risk assessment, and categorization of information systems of operators.
		Knowledge of the requirements of the Act and respective decrees.
		Ability to assess the evidence.
		Ability to analyse risks.
		Ability to prepare a complete and transparent final report on cybersecurity audit outcomes.
		Ability to analyse and evaluate security mechanisms and solutions.

Annex 2 to Decree No. 436/2019 Coll.

MINIMUM REQUIREMENTS FOR THE REQUEST FOR CONDUCTING A CYBERSECURITY AUDIT

1. Identification of the operator of essential service.

2. Identification of essential services supported by audited networks and information systems.

3. Number of employees of the operator of essential service.

4. List of information systems and their classification linked to the essential service and for each of them at least information on the information system and

a) identification of organizational units of the operator of essential service and a number of employees operating networks and information systems; for outsourced activities of information system management, the extent of used services provided in man-days; external staff not counted when providing audit outcomes for outsourced activities,

b) connection of network and information systems to the essential service provided; which essential service is dependent on the information system, what is the impact of the information system failure on the essential service,

c) number of users of the essential service, territorial distribution and consequences of a breakdown of the essential service to its users,

d) management system; internal and external resources, identification of key suppliers and contracts and agreements on the level of provided services,

e) network architecture diagram showing the nodes of interconnection of networks and connections to external networks,

f) list of assets and used technologies with reliance on other information systems and services of suppliers, providing the owners of these assets and identification of sensitivity according to a specific legal regulation,[4])

g) organizational units and numbers of staff operating the networks and information systems, including the number of suppliers; in the presence of the supplier's employees at the operator's workplace during the audit, the supplier's sites shall not be counted,

h) report from the last penetration testing of the information system, used methodology and scope of testing, and evidence of qualification of the staff conducting penetration tests, if penetration tests have been conducted.

5. Name, surname and contact details of the responsible employee of the operator of essential service who shall give the required assistance to the auditor during the audit and shall accompany the auditor.

6. Records of cybersecurity incidents affecting the provision of essential services since the last audit or the last two years of the first audit.

7. Decision to impose a fine in the field of cybersecurity, if any, and other cases of breach of obligations pursuant to the Act, if occurred.

8. Security documentation pursuant to Article 20 (5) of the Act or a specific legal regulation.[5])

9. Valid industrial security clearance certificate number, if issued.

---

[4]) Decree of the National Security Authority No. 362/2018 Coll. laying down the Content of Security Measures, the Content and Structure of Security Documentation and the Scope of General Security Measures.

[5]) For example Act No. 95/2019 Coll., Decree of the Office for Personal Data Protection of the Slovak Republic No. 158/2018 Coll. on Procedure for Data Protection Impact Assessment.

Annex 3 to Decree No. 436/2019 Coll.

DURATION AND TIME PERIOD OF THE CYBERSECURITY AUDIT
A: DETERMINATION OF THE AUDIT DURATION

An auditor shall be responsible for determining the duration of the audit to assess the subject of the audit adequately. When calculating the audit duration, the auditor shall take into account information from the request for a cybersecurity audit and from information requested additionally, in particular from

a) number of users of networks and information systems,

b) number of employees participating in the operation of networks and information systems,

c) categorization of networks and information systems,

d) the extent of third party's participation in the operation of the information system and in ensuring the security measures,

e) the quantity, scope and complexity of the documentation related to the operation of the information system and ensuring the security measures, including the results of previous audits and conducted risk analyses.

Calculation of days of the audit duration for each information system and operator's site individually.

Number of employees participating in the system operation and ensuring the security measures	Audit in man-days
1~10	5
11~20	6
21~30	7
31~50	8
51~70	9
71~90	10
>90	+ 1 day for every additional 20 employees

Any other information system shall be a set of related and interdependent assets (hardware, software, supplier services) that support another essential service, or the operation of networks and information systems is carried out by other employees or an organizational unit, or is located at a different site. In the presence or participation of employees from other sites (a supplier in outsourced activities) involved in the operation of the same information system through remote connection, it is not required to increase the number of audit days.

If the same persons are responsible for several information systems and for ensuring the security measures, the number of audit days shall not be increased provided that several information systems are audited simultaneously.

Factors reducing the scope of the audit (to a maximum of 1/3 with the factor combinations).

The audit duration from the calculation of days according to the table above shall be reduced

a) to 1/3, if the auditor has available the final report on audit outcomes from the previous cybersecurity audit conducted in accordance with this Decree and there have been no changes in the number of employees operating the systems, in assets, used technologies and essential services supported by information systems in the final report on audit outcomes. The auditor shall primarily verify if any changes have occurred, as well as pay attention to areas identified in the audit trail that are mandatory for each audit,

b) to ½, if all information systems are classified in sensitivity category I,

c) to ½, if the operator of essential services is the holder of the certificate according to a technical standard[6]) and the certified area includes audited information systems,

d) to ½, if the audited information system is certified in accordance with the requirements for information technology cybersecurity certification,[7])

e) to a different extent upon decision of the auditor; the auditor shall duly justify this decision.

Factors increasing the scope of the audit

The audit duration from the calculation of days according to the table above shall be

a) doubled if information systems are classified in sensitivity category III,

b) doubled if a serious cybersecurity incident has occurred since the time of the last audit or a fine has been imposed for the breach of obligations pursuant to the Act,

c) increased to a different extent upon decision of the auditor following an arrangement with the operator of essential service; the auditor shall duly justify this decision.

The audit duration shall include the auditor's time for assessing the request for a cybersecurity audit, delivering the required additional documentation, preliminary analysis of performing the duties, assessing the mandatory documentation and processing the final report on audit outcomes, together, up to a maximum of 1/3 of the total audit time required.

B: DETERMINATION OF THE AUDIT TIME PERIOD

The audit shall be conducted

a) every two years, and

b) due to any significant change, no later than two months after the change has had a significant impact on the implemented security measures.

A significant impact shall mean in particular

a) an impact on accepted information classification and categorization of networks and information systems,

b) a change of impact criteria of the essential service,

c) a change or exchange of the information system and operating parameters of the essential service,

d) establishing a new network or a new information system on which the essential service depends, or

e) introducing a new technology on which the essential service depends.

---

6) For example, STN ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013 including Cor. 1:2014 and Cor. 2:2015).

7) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (Text with EEA relevance).

Annex 4 to Decree No. 436/2018 Coll.

AUDIT TRAIL OF AUDITED SECURITY MEASURES

An audit trail shall contain a set of requirements for the security of networks and information systems pursuant to the Act and its implementing regulations and specific legal regulations. In the case of common requirements for the operator of essential service, a common audit trail shall be completed for all audit-relevant information systems. Security measures that are different for each audited information system shall be completed separately for each information system or network.

The auditor shall specify in the audit trail the following:

a) compliance or non-compliance with the requirements for the security of network and information systems for security measures adopted,

b) audit findings for respective requirements for the security of networks and information systems,

c) obtained evidence supporting the audit findings, and

d) a reference to used audit method, for example

- observation of activities and state of security measures,

- analysis of submitted records,

- analysis of submitted procedures, regulations and documents,

- interviews and questionnaires.

The audit trail shall also include verification of completeness of required security documentation and verification of information classification and categorization of networks and information systems.

If the audited information systems are subject to additional requirements beyond the security measures specified in the Act or in a specific legal regulation,[5]) the auditor shall indicate in the audit trail the manner of compliance in accordance with the valid requirements applicable to the operator of essential service.

The auditor shall inform a responsible person of the operator of essential service of any deficiencies found through the audit and shall document the recommended corrective actions.

The auditor shall maintain the audit trail with a professional care and with respect to the sensitivity of the information within for two years after the completion of the audit.

The published of the Collection of Laws of the Slovak Republic, content administrator and operator of the Slov-Lex legal and information portal accessible at www.slov-lex.sk is the Ministry of Justice of the Slovak Republic, Župné námestie 13, 813 11 Bratislava, tel.: 02 888 91 137, fax: 02/52442853, e-mail: helpdesk@slov-lex.sk