SNAS SLOVENSKÁ NÁRODNÁ AKREDITAČNÁ SLUŽBA
Karloveská 63, P. O. Box 74, 840 00 Bratislava 4

Policy

PL –57

SNAS POLICY AND PROCEDURE ON THE ASSESSMENT OF CERTIFICATION BODIES CERTIFYING INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS) ACCORDING TO REQUIREMENTS OF STANDARDS ISO/IEC 27001: 2022 IN ACCORDANCE WITH IAF MD 26: 2023

Approved by: **Ing. Štefan Král, PhD.**
riaditeľ

PURPOSE:
This document determines the SNAS policy and procedure on the assessment of certification bodies certifying Information security management systems according to the requirements of the standards ISO / IEC 27001-1: 2022 in accordance with IAF document MD 26: 2023, issue 2.

Elaborated: **Ing. Alena Trabalková**
Ing. Marcela Kráľová
Date of elaboration: **28.02.2023**

Verified by: **Ing. Gizela Pelechová**

CONTENT

Page

1 POLICY

SNAS assesses the competence of certification bodies certifying the information security management systems (ISMS) according to the requirements of the standards ISO/IEC 17021-1: 2015 and ISO/IEC 27006: 2015 with Appendix 1: 2020.

New version standard ISO/IEC 27001: 2022 was published on October 2022, which replaces the standard ISO/IEC 27001: 2013.

SNAS in accordance with conditions of transition to the new version standard ISO/IEC 27001: 2022 published on 15th February, 2023 in the IAF document MD 26: 2023, issue 2, sets the 36 months transition period for implementation of the ISO/IEC 27001: 2022 **which is ending on 31st October**, **2025**.

To this date, fulfilling the conditions below, all accredited CBs, which meet the requirements of ISO/IEC 17021-1: 2015 and ISO/IEC 27006: 2015 with Apendix 1: 2020 have to demonstrate competence to perform certification ISMS according to new version standard ISO/IEC 27001: 2022, which SNAS verify during planned or extraordinary assessments. In case of their fulfillment, SNAS will decide on to issue or retention of accreditation for the performance of certification ISMS according to standard **ISO 27001: 2022**.

2 ASSESSMENTS PROCEDURE AND TERMS

On the basis of the application for accreditation or reaccreditation, SNAS will assess the compliance with the requirements of ISO/IEC 17021-1: 2015 and ISO/IEC 27006: 2015 with Apendix 1: 2020 for performing of certification according to standard ISO/IEC 27001:2022 **from 30th April, 2023**. CBs accredited for certification of ISMS may request an assessment of compliance with the requirements of ISO/IEC 27001: 2022 **from 1st January, 2023**.

CBs accredited for certification of ISMS according to standards ISO/IEC 27001: 2013, shall notify SNAS in written form **until 31st March, 2023** at the latest, whether they have implemented in their management system the requirements for certification according to ISO/IEC 27001: 2022 or notify the date when they will implement these requirements; however, **no later than on 30th April, 2023**.

During planned or extraordinary assessments or by documentation review, SNAS will verify the fulfilment of requirements for certification according to ISO/IEC 27001: 2022. All assessments for verification of implementation of the requirements for certification according to ISO/IEC 27001: 2022 shall be carried out until **30th June, 2023, at the latest.**

The CBs accredited for certification of ISMS must demonstrate the readiness for the certification according to the standard ISO/IEC 27001: 2022 **within 31st August, 2023** and

SNAS, will decide to issue the accreditation for ISMS certification according to standard ISO/IEC 27001: 2022, **no later than 31st October, 2023**.

The findings from the assessments will be classified in accordance with the system published by SNAS and they must be resolved within a period according to the Act. No. 505/2009 Coll. on the accreditation of the conformity assessment bodies (including amendments to certain acts), as amended, but not later than two months after they were identified and recorded.

Note 1: *Certificates of accreditation issued during the transitional period (3 years) will include two standards, i.e. ISO/IEC 27001: 2013 and ISO/IEC 27001: 2022. Certificates of accreditation issued for ISMS certification according to ISO/IEC 27001: 2013 will be canceled after 31st October, 2025.*

Note 2**:** *Certification Bodies can conduct certification and recertification audits in accordance with standard ISO/IEC 27001: 2013 only till 30nd April, 2023.*

3 SUMMARY OF KEY CHANGES

3.1 KEY CHANGES

Compared with ISO/IEC 27001:2013, the main changes of ISO/IEC 27001: 2022 include, but are not limited to:

1) Annex A references the information security controls in ISO/IEC 27002: 2022, which includes the information of control title and control;
2) The notes of Clause 6.1.3 c) are revised editorially, including deleting the control objectives and using "information security control" to replace "control";
3) The wording of Clause 6.1.3 d) is re-organized to remove potential ambiguity.;
4) Adding a new item 4.2 c) to determine the requirements of the interested parties addressed through an information security management system (ISMS);
5) Adding a new subclause 6.3 - Planning for changes, which defines that the changes to the ISMS shall be carried out by the organization in a planned manner;
6) Keeping the consistency in the verb used in connection with documented information, for example, using "Documented information shall be available as evidence of XXX" in clauses 9.1, 9.2.2, 9.3.3 and 10.2;
7) Using "externally provided process, products or services" to replace "outsourced processes" in Clause 8.1 and deleting the term "outsource";
8) Naming and reordering the subclauses in Clause 9.2 - Internal audit and 9.3 – Management review;
9) Exchanging the order of the two subclauses in Clause 10 – Improvement;
10) Updating the edition of the related documents listed in Bibliography, such as ISO/IEC

27002 and ISO 31000;

11) Some deviations in ISO/IEC 27001: 2013 to the high-level structure, identical core text, common terms and core definitions of MSS are revised for consistency with the harmonized structure for MSS, for example, Clause 6.2 d).

Note 1: The first two items come from ISO/IEC 27001: 2013/DAmd1, the third item is from ISO/IEC 27001: 2013/COR 2: 2015 and the other changes result from the harmonized structure for MSS.

Note 2: Compared with the old edition, the number of information security controls in ISO/IEC 27002: 2022 decreases from 114 controls in 14 clauses to 93 controls in 4 clauses. For the controls in ISO/IEC 27002: 2022, 11 controls are new, 24 controls are merged from the existing controls, and 58 controls are updated. Moreover, the control structure is revised, which introduces "attribute" and "purpose" for each control and no longer uses "objective" for a group of controls.

Note 3: ISO/IEC 27001: 2013/COR 1:2014 is related to Annex A and overlapped by ISO/IEC 27001: 2013/DAMD1.

3.2 THE IMPACT

The impact of the changes in ISO/IEC 27001: 2022 includes, but is not limited to the introduction of a new Annex A and Clause 6.3 - Planning for changes because:

1) ISO/IEC 27001: 2013/COR 2: 2015 has already been published and implemented;
2) Annex A is normative;
3) The harmonized structure for MSS is considered as a minor revision for the high-level structure, identical core text, common terms and core definitions of MSS, in which most of the changes are considered editorial.

The requirements in ISO/IEC 27001 that use the reference control set in Annex A are the comparison process between the information security controls determined by the organization and those in Annex A (6.1.3 c)) and the production of a Statement of Applicability (6.1.3 d)). By comparing the necessary information security controls to those in Annex A, the organization may confirm that any necessary information security control from the reference set in Annex A of ISO/IEC 27001: 2022 is not inadvertently omitted.

Such comparison might not lead to the discovery of any necessary information security control that has been inadvertently omitted. However, if inadvertently omitted necessary information security controls are discovered, the organization shall update its risk treatment plans to accommodate the additional necessary information security controls and implement them.

As implied above, the impact of ISO/IEC 27001: 2022 on the organizations that have implemented ISMS need not be significant.

4 KEY TIMESCALE

Activity	Due Date
AB	
AB to be ready to assess to ISO/IEC 27001: 2022 no later than	**6 months from the last day of publication month of ISO/IEC 27001: 2022 (i.e. 30 April 2023)**
Initial assessment by AB to ISO/IEC 27001: 2022 only, to begin no later than	**6 months from the last day of publication month of ISO/IEC 27001: 2022 (i.e. 30 April 2023)**
AB transitions of CABs completed by	**12 months from the last day of publication month of ISO/IEC 27001: 2022 (i.e. 31 October 2023)**
CAB	
Initial certification and recertification by CAB to ISO/IEC 27001: 2022 only, to begin no later than	**18 months from the last day of publication month of ISO/IEC 27001: 2022 (i.e. 30 April 2024)**
CAB transitions of certified clients completed by	**36 months from the last day of publication month of ISO/IEC 27001: 2022 (i.e. 31 October 2025)**

5 TRANSITION PROCESS ACTIONS

5.1 AB ACTIONS

Activity	YES/NO	Notes:
AB's Arrangements	YES	1) AB shall establish its transition arrangement for ISO/IEC 27001: 2022 considering the requirements of this document. 2) The transition arrangement shall address what the AB shall do and what the CABs shall do. The AB may have several separate documents to address the transition arrangement.

		3)The transition arrangement shall include at least the consideration of the following: • The changes in ISO/IEC 27001 and the gap analysis. • The relevant personnel are competent for ISO/IEC 27001: 2022 and transition process. *Note: The assessment team, as a whole, shall have knowledge of information security technologies and practices (see IAF MD 13: 2020, 4.2). As we all know, ISO/IEC 27002 provides a reference set of generic information security controls including implementation guidance.* • The AB's related processes and documents affected by the change in ISO/IEC 27001 are identified, as well as IT systems for managing accreditation activities, if applicable. • The transition assessment programme. • There is a timely communication to CABs on the transition assessment programme, such as the timeline and transition assessment approach, and the consequences for not completing the transition by the deadline. 4) ABs are encouraged to plan and commence required actions at the earliest opportunity.
CAB Document Review	NO	
CAB Technical Document Review	YES	1) AB shall conduct the technical document review to confirm whether or not CABs are competent for ISO/IEC 27001: 2022. 2) AB shall determine the suitability of the CAB's transition arrangement and, if applicable, the effectiveness of its implementation through reviewing the following information submitted by CABs: • The gap analysis of the changes in ISO/IEC 27001: 2022. • The transition arrangement and its implementation evidence. • The authorization of the related personnel. • The other relevant information deemed necessary by AB.
Technical Assessment at CAB Head Office (on-site or remote) Review)	If applicable	If AB is able to obtain sufficient evidence through the CAB technical document review, then a CAB head office assessment is not required. If AB is not able to verify the effective implementation and conformance with the CAB's transition arrangement, then an office assessment is required.
CAB Witnessed Assessment(s)	NO	-

Is extra time likely to be needed for the transition?	YES	As a minimum, the assessment shall include an additional 0.5 assessment day to confirm transition of the CAB when the transition is done as a separate assessment.
Other	YES	1) AB may define the timeline for submitting the transition application by CABs in the transition assessment programme. 2) AB shall make the transition decision based on the result of transition assessment(s). 3) If applicable, AB shall update the accreditation information of the accredited CABs (e.g. accreditation certificate) if their competence for ISO/IEC 27001: 2022 has been demonstrated. 4) If the accredited CAB does not successfully complete the transition assessment before the related due date listed in Clause 3, the expiry date of their accreditation for ISO/IEC 27001: 2013 shall not be later than the end of the transition period.

5.2 CAB ACTIONS

Activity	YES/NO	Notes
CAB's Arrangements	YES	1) CAB shall establish its transition arrangement for ISO/IEC 27001: 2022 considering the requirements of this document and the transition arrangement of the related AB. 2) The transition arrangement shall address what the CAB shall do and what the client shall do. The CAB may have several separate documents to address the transition arrangement. 3) The transition arrangement shall include at least the consideration of the following: • The changes in ISO/IEC 27001 and the gap analysis. • The need to modify the related certification processes, documents and, if applicable, IT systems for managing certification activities. • The relevant personnel are competent for ISO/IEC 27001: 2022 and transition process. • The audit team, as a whole, shall have knowledge of all information security controls contained in ISO/IEC 27002: 2022 and their implementation (see ISO/IEC 27006: 2015, 7.1.2.1.3 b)). • The transition audit programme. • There is a timely communication to the clients on the transition programme, such as the timeline, transition audit approach, and the consequences if the client

		fails to transition prior to the end of the transition period. 4) CABs are encouraged to plan and commence required actions at the earliest opportunity.
Transition audit	YES	1) CAB may conduct the transition audit in conjunction with the surveillance audit, recertification audit or through a separate audit. 2) The transition audit shall not only rely on the document review, especially for reviewing the technological information security controls. 3) The transition audit shall include, but not be limited to the following: • The gap analysis of ISO/IEC 27001: 2022, as well as the need for changes to the client's ISMS. • The updating of the statement of applicability (SoA). • If applicable, the updating of the risk treatment plan. • The implementation and effectiveness of the new or changed information security controls chosen by the clients. 4) CAB may conduct the transition audit remotely if they ensure the transition audit objectives is met.
Is extra time likely to be needed for the transition?	YES	1) Minimum of 0.5 auditor day for the transition audit when it is carried out in conjunction with a recertification audit. 2) Minimum of 1.0 auditor day for the transition audit when it is carried out in conjunction with a surveillance audit or as a separate audit.
Other		1) CAB may define the timeline for submitting the transition application by the certified clients in the transition audit programme. 2) CAB shall make the transition decision based on the result of transition audit. 3) CAB shall update the certification documents for the certified client if its ISMS meets the requirements of ISO/IEC 27001:2022. *Note: When the certification document is updated because the client successfully completed only the transition audit, the expiration of its current certification cycle will not be changed.* 4) All certifications based on ISO/IEC 27001:2013 shall expire or be withdrawn at the end of the transition period.

5.3 OTHER

5.3.1 The CAB office assessment following the transition decision shall focus on the verification of the implementation of the transition arrangement before the CAB's transition arrangement was totally completed. This office assessment shall include the following, at a minimum:

- The implementation of the CAB's revised processes and procedures.
- The competence of the related personnel is demonstrated before they were involved in the ISO/IEC 27001: 2022 certification activities.
- The progress of the transition for the certified clients to ISO/IEC 27001: 2022.

5.3.2 All witness assessments selected following the transition decision shall be based on ISO/IEC 27001: 2022 and focus on the CAB's competence for conducting an audit based on ISO/IEC 27001: 2022

6 RELATED DOCUMENTS

ISO/IEC 17021-1: 2015	Conformity assessment. Requirements for bodies providing audit and certification of management systems. Part 1: Requirements
ISO/IEC 27001: 2022	Information security, cybersecurity and privacy protection - Information security management systems - Requirements.
ISO/IEC 27002: 2022	Information security, cybersecurity and privacy protection – Information security control
ISO/IEC 27006: 2015	Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
IAF MD 26: 2023	Transition Requirements for ISO/IEC 27001: 2022

Act. No. 505/2009 Coll. on the accreditation of conformity assessment bodies (including amendments to certain acts), as amended

***