Raad voor Accreditatie (Dutch Accreditation Council RvA)

Specific Accreditation Protocol for Certification in accordance with EN ISO/IEC 27001 and ISO/IEC 27701

Document code:	**RvA-SAP-C010-UK**
	Version 6.0, 08-06-2022

A Specific Accreditation Protocol (SAP) describes the assessment service for a specific accreditation. It should be read in conjunction with the generic RvA regulations and policy documents.
A current version of the SAP is available from the website of the RvA. (www.rva.nl).

Content

Introduction

This SAP should be read in conjunction with SAP-C000, only additional or deviating aspects compared to SAP-C000 are mentioned in this SAP. This means that some paragraph numbers in this SAP may be missing (if all information is already contained in SAP C000). This SAP also contains information about the transition from ISO/IEC 27006:2015 to ISO/IEC 27006:2015/AMD 1:2020. See paragraph 4.

1 Relevant documents

1.2 Additional standards

- ISO/IEC 27006:2015, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems.
- ISO/IEC 27006:2015/AMD 1:2020, Information technology – Security techniques -Requirements for bodies providing audit and certification of information security management systems – Amendment 1
- Additional standard for ISO/IEC 27701: ISO /IEC 27006 supplemented with an own scheme containing requirements for bodies providing audit and certification of privacy information systems.

Note: these requirements shall at least include determination of audit time, competence criteria for auditors and other certification personnel, including criteria for knowledge of ISO 29100, ISO 29151 and ISO 27018.

1.5 Documents related to the conformity assessments to be carried out

Certification bodies certify against:

- EN ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements.
- ISO/IEC 27701: Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines.

Certification bodies may use the following ISO-documents for certification:

- EN ISO/IEC 27000: Information technology - Security techniques - Information security management systems - Overview and vocabulary;
- EN ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls.

2 Scope of accreditation

Accreditation of certification based on EN ISO/IEC 27001 shall be included in the EN ISO/IEC 17021-1 scope of accreditation as follows:

Standard / Normative document	Certification scheme
EN ISO/IEC 27001	Certification of Information Security Management Systems (ISMS) Accreditation provided in accordance with ISO/IEC 27006 *(until March 31, 2022)*

or when the CB has completed the transition during the transition period

Standard / Normative document	Certification scheme
EN ISO/IEC 27001	Certification of Information Security Management Systems (ISMS) Accreditation provided in accordance with ISO/IEC 27006/Amd 1:2020

There are no specific technical areas specified for this scope of accreditation.

ISO 27701

Accreditation of certification based on ISO/IEC 27701 is only possible as an extension to accreditation of certification based on ISO/IEC 27001 and shall be included in the ISO/IEC 17021-1 scope of accreditation as follows:

Standard / Normative document	Certification scheme
ISO/IEC27001 & ISO/IEC 27701 chapter 5 and Annex A and B	Certification of Information Security and Privacy Management Systems (PIMS) Accreditation granted in accordance with ISO/IEC 27006

There are no specific technical areas specified for this scope of accreditation

If the CAB is accredited for ISO/IEC 27001, the extension assessment for ISO/IEC 27701 will consist of a document based assessment and a witness of a ISO/IEC 27701 audit. If the CAB is also accredited for a GDPR scheme (under ISO 17065) the witness of a ISO/IEC 27701 audit will not be necessary.

3 Accreditation assessments

3.1 Documents to be submitted

Additional requirements compared to SAP-C000:

For witnessing:

- the auditee's SoA (Statement of Applicability);
- references to the applicable regulatory and legal requirements related to information security.

3.2 The type and content of assessments

In addition to the generic rules for the type and content of RvA assessments as defined in RvA-BR002, RvA-BR005 and SAP-C000, for this specific accreditation, the requirements from the following table apply. The type, extent and content of the assessment depend on the requested scope of accreditation, existing other accreditations and the functioning of the CB in the past (where relevant).

Assessment method	*Pre-assessment*	*Initial assessment*	*Assessments during the accreditation cycle (surveillance and re-assessment)*	*Scope extension* [3]
Witnessing	-	√ An initial or recertification audit[1][2]	√ Minimum: Per cycle: 1+0,2√c [4]	not applicable

[1] If the CB has not yet applied the stage one / stage two methodology with other accredited schemes , witnessing of a full stage one / stage two audit is required.

[2] If no full stage one / stage two audit is available a re-assessment audit will be witnessed and after accreditation is granted the CB is required to provide RvA with the possibility to witness the first full stage one / stage two audit

[3] Within this accreditation no sub-scopes are defined. Extension for sub-scopes is not applicable.

[4] √c: square root from the total number of certificates. This number may be increased due to factors mentioned in MD17, clause 2.3.3.

The implementation of the EN ISO/IEC 27001 and the ISO/IEC 27701 certification system shall be verified during each surveillance and re-assessment of the RvA.

4 Specific assessment issues

No additional requirements compared to SAP-C000.

Transition to ISO/IEC 27006:2015/AMD 1:2020.

IAF Resolution 2020-18 prescribes the Transitional Arrangement for ISO/IEC 27006:2015 AMD 1:2020 as follows:

- it will be two years from the last day of the month of publication of the amended standard.

Within this transition timeline:

- ABs shall be ready to carry out transition assessments for ISO/IEC 27006:2015 AMD 1:2020, within eight months from the last day of the month of publication of the amended standard.
- CBs shall have completed the transition to ISO/IEC 27006:2015 AMD1:2020, through office assessment, within 24 months from the last day of the month of publication of the amended standard.

This means that:

- the RvA will be able to carry out this transition assessment through an office assessment as per December 1, 2020. This office assessment may be combined with or be part of a regular office assessment. In that case no additional assessment time is needed.
- the CB's shall have completed this transition not later than March 31, 2022.

Points of attention.

Changes concern:

- the experience criteria for selecting an auditor before acting as an ISMS/ISO 27001 auditor (cl 7.2.1.1.)
- the decision making process for proceeding with stage 2 (cl 9.3.1.1.) concerning the audit team members competence (cl 9.3.1.1)
- the definition of the starting point for determination of audit time (B.2.1)
- criteria for inclusion of national and international standards on the certification documents (cl 8.2.1)
- audit time calculation for multi-site (B.6).

B.3.6 has been described more clearly by referring to audit time calculation in accordance with B.3.3 and B.3.4.

Important remark:

Clause 9.1.4 of EN ISO/IEC 17021-1:2015 clearly states that the CB shall have documented procedures for determining audit time taking into account size and number of sites, their geographical locations and multi-site considerations.

With regard to multi-site, this documented procedure shall consider the requirements of both ISO/IEC 27006 and IAF MD1 where the requirements of ISO/IEC 27006 prevail over the requirements of IAF MD1.

5 Changes compared to the previous version of this document

Compared to version 5 of February 2020, the following significant changes have been made:

- 1.2, 2 and 4 the transition from ISO/IEC 27006:2015 to ISO/IEC 27006:2015/AMD 1:2020
- 1.2, 1.5, 2 and 3 including of ISO/IEC 27701.
- Remove Annex 1