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 6.1, 25-09-2024

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/ Amd1:2020 to ISO/IEC 27006-1:2024. See paragraph 4.

1 Relevant documents

1.1 Standard used for accreditation

- EN-ISO/IEC 17021-1; Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements

1.2 Additional standards

- ISO/IEC 27006:2015/Amd 1:2020, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27006-1:2024, Information security, cybersecurity and privacy protection – Requirements for bodies providing audit and certification of information security management systems – Part 1: general
- ISO/IEC 27006-2:2021, Requirements for bodies providing audit and certification of information security management systems – Part 2: privacy information management systems (additional standard for ISO/IEC 27701)

1.3 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 27006:2015/Amd-1:2020 *(until March 31, 2026)*

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 27006-1:2024

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/IEC 27001 & 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 27006-2

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/IEC 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) and risks.

Assessment method	*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 27006-1:2024

IAF MD 29 prescribes the Transition Requirements for ISO/IEC 27006-1:2024

The prescribed transition timeline is:

- ABs shall be ready to carry out transition assessments for ISO/IEC 27006-1:2024, within 9 months from the last day of the month of publication of the amended standard.
- CBs shall be completed the transition to ISO/IEC 27006-1:2024 within 24 months from the last day of the month of publication of the amended standard

Accreditation for the ISO/IEC 27001 is granted in accordance with ISO/IEC 27006. The CBs accredited for ISO/IEC 27001 can apply for an extension of accreditation to ISO/IEC 27006-1:2024 from now on. The extension applications that have been sent in and accepted before **October 1, 2024**, will be assessed in a simultaneous procedure. A simultaneous procedure has been decided upon to level the playing field as much as possible for all accredited CBs.

Along with the application for scope extension, apart from the signed application forms F105 and F006-2, the CB must provide:

- the internal audit report about the transition to the new norm;
- a management review about the transition to the new norm;
- a gap analysis of changes in ISO/IEC 27006-1:2024 compared to the last version;
- a plan of action for the transition based on the gap analysis, fulfilling the requirements of MD 29;
- method and content of provision of information by the certification body to its clients about the changes;
- information that proves that auditors and decision makers have been trained for the new standard and how this has been secured in the management system

5 Changes compared to the previous version of this document:

Compared to version 6 of June 2022, the following significant changes have been made:

- 1.2 and 2 ISO 27701: adding ISO/IEC 27006-2
- 1.2, 2 and 4 removing the transition from ISO/IEC 27006:2015 to ISO/IEC 27006:2015/AMD 1:2020 and replace that for the transition from ISO/IEC 27006:2015/AMD 1:2020 to ISO/IEC 27006-1:2024