Raad voor Accreditatie (Dutch Accreditation Council RvA)

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

Document code:	**RvA-SAP-C010-UK**
	Version 4, 19-3-2019

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).

1 Relevant documents

1.1 Accreditation standard

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

1.2 Additional standards

- ISO/IEC 27006, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems.

1.5 Documents related to the conformity assessments to be carried out

Certification bodies certify against:

- EN ISO/IEC 27001:2017, Information technology – Security techniques – Information security management systems – Requirements.

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 17021-1 scope of accreditation as follows:

- Standard/normative document: EN ISO/IEC 27001;
- Certification scheme: Certification of Information Security Management Systems (ISMS), Accreditation provided in accordance with ISO/IEC 27006.

See Annex 1 for an example of the scope.

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

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: $1+0,2\sqrt{c}$[4)]	not applicable

1) If the CB has not yet applied the stage one / stage two methodology with other accredited scheme's, 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 the CB is required to report the first full stage one / stage two audit as a witness candidate.
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.

4 Specific assessment issues

No additional requirements compared to SAP C000.

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 3 of October 2017, the following significant changes have been made:

- reference to RvA-T045 has been removed;
- remarks have been added to chapter 4 concerning audit time in case of multi-site certification.

Annex 1: Example of a scope for EN ISO/IEC 27001

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