Raad voor Accreditatie (Dutch Accreditation Council RvA)

Specific Accreditation Protocol for Certification according to ISO/IEC 27001

Document code:	**RvA-SAP-C010-UK**
	Version 3, 20-10-2017

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 through 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 requirements

- EN ISO/IEC 17021-1, Conformity assessment — Requirements for bodies providing audit and certification of management systems;
- ISO/IEC 27006, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems.

1.2 Additional documents

RvA documents applicable for accreditation of ISO/IEC 27001 certification:

- RvA-T045: Implementation of ISO/IEC 27006:2015.

The current version of this document is available on the RvA-website (www.rva.nl).

1.3 Certification documents

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 ISO/IEC 27001 shall be included in the 17021-1 scope of accreditation as follows:

- Standard/normative document: 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 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 or re-assessment*	*Surveillance (see RvA-BR005 for the general policy)*	*Scope extension* [3]
Witnessing	-	√ An initial or recertification audit[1) 2)]	√ Minimum: Per cycle: 0,2√c[4)]	

1) If the CB has not applied the stage one/stage two methodology with other accredited scheme's, witnessing 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.

3.2 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.

3.3 Reassessments and surveillance

No additional requirements compared to SAP C000.

3.4 Scope extension

Not applicable within this scheme.

3.5 Policy concerning witnessing

Previous results of witnessing will be taken into account in the witness strategy.

4 Specific assessment issues

No additional requirements compared to SAP C000.

5 Other information

RvA expertise holder EN ISO/IEC 17021: Corné Cox (corne.cox@rva.nl);

RvA co-ordinator EN ISO/IEC 17021: Carmen Goettsch (carmen.goettsch@rva.nl);

RvA technical expert for the scheme: Jan van den Akker (jan.vanden.akker@rva.nl).

6 Changes to the previous version of this document

Compared to version 2 of March 7, 2014, the following significant changes have been made:

- changes due to the new issue of ISO/IEC 27006:2015;
- update due to new SAP-structure with reference to SAP-C000;
- changes due to the transition to ISO/IEC 17021-1:2015;
- change in the number of witnessed-audits.

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

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