SPECIFIC PROVISIONS FOR THE ACCREDITATION OF CERTIFICATION BODIES IN THE FIELD OF INFORMATION SECURITY MANAGEMENT SYSTEMS (ISO/IEC 27001)

Applicable from : 06.12.2017

DOCUMENT HISTORY

Revision and date of approval	Reason for revision	Impact of revision
0 **20.10.2017**	New document - Formal integration of IAF MD 13:2015 in the management system documentation of BELAC	

SPECIFIC PROVISIONS FOR THE ACCREDITATION OF CERTIFICATION BODIES IN THE FIELD OF INFORMATION SECURITY MANAGEMENT SYSTEMS (ISO/IEC 27001)

1. OBJECTIVES AND REFERENCES TO NORMATIVE DOCUMENTS

This document is intended to document the specific requirements and guidelines that shall apply for the accreditation of certification bodies in the field of information security management systems (ISO/IEC 27001).

It includes in particular :

- The specific requirements and guidelines related to the organization and operation of the certification body;
- The specific requirements and guidelines applicable to BELAC.

The specific requirements and guidelines for the direct performance of the conformity assessment activities are not detailed in the present document but a reference to the relevant documents is included.

The specific requirements and guidelines

- are only endorsed when they comply with the general criteria documented in BELAC document 1-03 ;
- complement the requirements and guidelines that are in force to all BELAC accreditation activities.

2. RECIPIENTS

With follow up of modifications:

- Members of the Coordination Commission
- Members of the Accreditation Board
- Accreditation secretariat
- Assessors and experts
- Accredited bodies

Without follow up of the modifications: Any external request

3. DESCRIPTION OF THE ACTIVITY

3.1 Identification of the activity	**ISMS**
3.2 Type(s) of conformity assessment and accreditation standard	Certification of information security management system according to ISO 27001 • Accreditation according to EN ISO 17021-1
3.3 Classification(s) according to BELAC 6-017	**7.11 and/or 11.5**
3.4 Reference document(s) for the activity ***(hereafter named "the scheme")*** , including the publication date or a version number	• ISO/IEC 27001:2013 • ISO/IEC 27000:2016 • ISO/IEC 27006:2015 • IAF MD 13:2015 (Knowledge of accreditation body personnel for ISMS) www.iaf.nu
3.5 Body responsible for the development and maintenance of the scheme ***(hereafter named « the scheme owner »)***	ISO

4. SPECIFIC REQUIREMENTS APPLICABLE TO THE CONFORMITY ASSESSMENT BODY

During the accreditation assessments according to EN ISO/IEC 17021-1:2015 for certification against ISO 27001 or for conformity assessment activities provided by accredited bodies complying to ISO 27006, a specific evaluation is required to establish the compliance with the specific requirements listed hereafter; the relevant information will be included in the assessment report.

EN ISO/IEC 17021-1:2015	**Specific requirement of ISO/IEC 27006:2015**
Clause 5.2 Management of impartiality	**5.2.1 IS 5.2 Conflicts of interest**
Clause 7.1 Competence of personnel	**7.1.1 IS 7.1.1 Competence of personnel – general considerations** 7.1.1.1 Generic competence requirements 7.1.2.1 Competence requirements for ISMS auditing 7.1.2.1.1 General requirements 7.1.2.1.2 Information security management terminology, principles, practices and techniques 7.1.2.1.3 Information security management system standards and normative documents 7.1.2.1.4 Business management practices 7.1.2.1.5 Client business sector 7.1.2.1.6 Client products, processes and organization 7.1.2.2 Competence requirements for leading the ISMS audit team 7.1.2.3 Competence requirements for conducting the application review 7.1.2.3.1 Information security management system standards and normative documents 7.1.2.3.2 Client business sector 7.1.2.3.3 Client products, processes and organization 7.1.2.4 Competence requirements for reviewing audit reports and making certification decisions 7.1.2.4.1 General 7.1.2.4.2 Information security management terminology, principles, practices and techniques 7.1.2.4.3 Information security management system standards and normative documents 7.1.2.4.4 Client business sector 7.1.2.4.5 Client products, processes and organization
Clause 7.2 Personnel involved in the certification activities	**7.2.1 IS 7.2 Demonstration of auditor knowledge and experience** 7.2.1 Demonstration of auditor knowledge and experience 7.2.1.1 Selecting auditors 7.2.1.2 Selecting auditors for leading the team

Clause 7.3 Use of individual external auditors and external technical experts	**7.3.1 IS 7.3 Using external auditors or external technical experts as part of the audit team**
Clause 8.2 Certification documents	**8.2.1 IS 8.2. ISMS Certification documents**
Clause 8.4 Confidentiality	**8.4.1 IS 8.4 Access to organizational records**
Clause 9.1 Pre-certification activities	**9.1 Pre-certification activities** 9.1.1.1 IS 9.9.1 Application readiness 9.1.3 ISO 9.1.3 Audit Programme 9.1.3.2 Audit methodology 9.1.3.3 General preparations for the initial audit 9.1.3.4 Review periods 9.1.3.5 Scope of certification 9.1.3.6 Certification audit criteria 9.1.4 IS 9.1.4 Determining audit time 9.1.5 IS 9.1.5 Multi site sampling 9.1.6 IS 9.1.6 Multiple management systems 9.1.6.1 Integration of ISMS documentation with that for other management systems 9.1.6.2 Combining management system audits
Clause 9.2 Planning audits	**9.2 Planning audits** **9.2.1 IS 9.2.1 Audit objectives** **9.2.2 IS 9.2.2 Audit team selection and assignments** 9.2.2.1 Audit team 9.2.2.2 Audit team competence **9.2.3 IS 9.2.3 Audit plan** 9.2.3.1 General 9.2.3.2 Network-assisted audit techniques 9.2.3.3 Timing of the audit
Clause 9.3 Initial certification	**9.3 Initial certification** **9.3.1 IS 9.3.1 Initial certification audit** 9.3.1.1 IS 9.3.1.1 Stage1 9.3.1.2 IS 9.3.1.2 Stage 2
Clause 9.4 Conducting audits	**9.4 Conducting audits** **9.4.1 IS 9.4 General** **9.4.2 IS 9.4 Specific elements of an ISMS audit** **9.4.3 IS 9.4 Audit report**
Clause 9.5 Certification decision	**9.5 Certification decision** **9.5.1 IS 9.5 Certification decision**
Clause 9.6 Maintaining certification	**9.6 Maintaining certification** **9.6.2.1 IS 9.6.2 Surveillance activities** 9.6.3 Re-certification **9.6.3.1 IS 9.6.3 Re-certification audits** 9.6.4 Special audits **9.6.4.1 IS 9.6.4 Special cases**
	Annex B (normative) Audit Time

5. KNOWLEDGE REQUIREMENTS APPLICABLE TO THE CONFORMITY ASSESSMENT BODY (IAF MD 13:2015)

5.1 ISO/IEC 17011 Clause 6.2.1 (a) requires Accreditation Bodies to describe for each activity involved in the accreditation process the competencies required. Normative Annex A specifies the areas of knowledge that the Accreditation Body shall define for specific functions for the accreditation of bodies providing auditing and certification of ISMS. The knowledge requirements detailed in this annex are complementary to the basic skills and knowledge required for each function within an Accreditation Body. This document recognizes that the IAF is in the process of defining basic skills and knowledge required for Accreditation Body assessors.

5.2 Generally, each assessor involved in ISMS assessment shall have a level of the knowledge described in A1 to A5 in §6. The knowledge in A6 and A7 can be held within the team as a whole.

5.3 When a group reviews assessment reports and makes accreditation decisions, the knowledge required is to be held within the group as a whole and not by each individual member of the group.

5.4 Personnel involved in scheme management shall have the knowledge of ISO/IEC 17021. If the personnel do not have other knowledge described in Annex A, the Accreditation Body shall ensure the access to necessary knowledge.

5.5 CAB's client process and operation associated with ISMS cover:

- typical business activities related to the technical area (see ISO/IEC 17021-1:2015, clause 7.1.2);
- information and communication technology specific to the technical area;
- information security technologies and practices specific to the technical area, especially identification of information security related threats and vulnerabilities and related mitigations and controls;
- related legal requirements.

Legal requirements identified here are those regulations that the organisation that is the subject of the witness would be expected to comply with either for the information security field or country/state/province within which they operate.

6. REQUIRED KNOWLEDGE FOR ACCREDITATION BODY PERSONNEL INVOLVED IN THE ACCREDITATION OF ISMS CERTIFICATION BODIES (IAF MD 13:2015)

The following table specifies the areas of knowledge that an Accreditation Body shall define for specific accreditation activities in the accreditation of an ISMS Certification Body.
X means the Accreditation Body personnel shall have a general knowledge of the subject.
X+ indicates the Accreditation Body personnel shall have a deeper level of the knowledge of the subject.

Accreditation Functions **Subject**	**Document Review (as part of the assessment)**	**Office Assessment**	**Witness assessment**	**Reviewing assessment reports and making accreditation decisions**	**Scheme management**
Implementation by BELAC	**Assessors**	**Assessors**	**Assessors**	**Technical manager Accreditation Board**	**Technical manager**
A1.ISMS related terminology and principles including ISO/IEC 27000	X	X	X	X	X
A2. ・ Audit techniques included in ISO/IEC 27007 and ISO/IEC TR 27008		X	X		
A3. ISO/IEC 17021 and ISO/IEC 27006	X+	X+	X	X	X
A4. ISO/IEC 27001	X	X+	X+	X	
A5. General legal and regulatory requirements related to ISMSs.	X	X	X+	X	
A6. Generic ISMS related technology including - information security technologies and practices - information and communication technology - risk assessment and risk management	X	X	X	X	
A7. CAB's client process and operation associated with ISMS			X		

7. PRESENTATION OF THE ACCREDITATION SCHEDULE

Accreditation assessments shall be against ISO/IEC 17021-1 including the requirements of ISO/IEC 27006.

The accreditation document scope shall explicitly state that the accreditation is against ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015. EAC or NACE codes are not specified for this schedule

Information Security Management Systems according to ISO/IEC 27001:2013 (ISO 17021-1 in combination with ISO/IEC 27006:2015)

The certification body must be able to demonstrate that it has at least one active application.