



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

The versions of documents from the BELAC management system, available on the BELAC website ([www.belac.be](http://www.belac.be)) are considered as the only valid versions.

Applicable from: 24.10.2023

## HISTORY OF THE DOCUMENT

Revision and date of approval	Reason for revision	Type of revision
0 20.10.2017	New document - Formal integration of IAF MD 13:2015 in the management system documentation of BELAC	
1 CC 04.03.2021	<ul style="list-style-type: none"> <li>- Integration of IAF MD 13:2020: Minor changes on formulation of competence requirements. (not significant)</li> <li>- Update of references</li> <li>- Lay-out optimisation Full document</li> </ul>	\$6  Full document
2 CC 29.09.2023	<ul style="list-style-type: none"> <li>- Integration of IAF MD 13:2023</li> <li>- Integration of ISO/IEC 27001:2022</li> <li>- Update of references</li> </ul>	Full document

## TABLE OF CONTENTS

1	OBJECTIVES AND NORMATIVE REFERENCES .....	4
2	RECIPIENTS OF THIS DOCUMENT .....	4
3	DESCRIPTION OF THE ACTIVITY .....	5
4	SPECIFIC REQUIREMENTS APPLICABLE TO THE CONFORMITY ASSESSMENT BODY .....	6
5	KNOWLEDGE REQUIREMENTS APPLICABLE TO THE ACCREDITATION BODY (IAF MD 13:2023) .....	9
6	REQUIRED KNOWLEDGE FOR ACCREDITATION BODY PERSONNEL INVOLVED IN THE ACCREDITATION OF ISMS CERTIFICATION BODIES (IAF MD 13:2020).....	9
7	PRESENTATION OF THE ACCREDITATION SCHEDULE .....	11

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

## **1 OBJECTIVES AND NORMATIVE REFERENCES**

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 OF THIS DOCUMENT**

- The members of the Coordination Committees
- The members of the Accreditation Board
- The accreditation secretariat
- The assessors and experts
- The accredited bodies

### 3 DESCRIPTION OF THE ACTIVITY

<b>3.1</b> Identification of the activity	<b>ISMS</b>
<b>3.2</b> Type(s) of conformity assessment and accreditation standard	<p>Certification of information security management system according to ISO/IEC 27001:2022</p> <ul style="list-style-type: none"> <li>- Accreditation according to EN ISO/IEC 17021-1:2015 in combination with ISO/IEC 27006:2015/AMD 1:2020</li> </ul>
<b>3.3</b> Classification(s) according to BELAC 6-017	<b>7.5</b>
<b>3.4</b> Reference document(s) for the activity ( <i>hereafter named "the scheme"</i> ) , including the publication date or a version number	<ul style="list-style-type: none"> <li>- ISO/IEC 27001:2022</li> <li>- ISO/IEC 27000:2018</li> <li>- ISO/IEC 27006:2015/AMD 1:2020</li> <li>- IAF MD 13:2023 (Knowledge requirements for accreditation body personnel for Information Security Management Systems (ISO/IEC 27001))</li> </ul>
<b>3.5</b> Body responsible for the development and maintenance of the scheme ( <i>hereafter named « the scheme owner »</i> )	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/IEC 27001 or for conformity assessment activities provided by accredited bodies complying to ISO/IEC 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/AMD 1:2020
<b>Clause 5.2</b> <b>Management of impartiality</b>	<b>5.2.1 IS 5.2 Conflicts of interest</b>
<b>Clause 7.1</b> <b>Competence of personnel</b>	<b>7.1.1 IS 7.1.1 Competence of personnel – general considerations</b> <ul style="list-style-type: none"> <li>- 7.1.1.1 Generic competence requirements</li> </ul> <b>7.1.2 IS 7.1.2 Determination of Competence Criteria</b> <ul style="list-style-type: none"> <li>- 7.1.2.1 Competence requirements for ISMS auditing <ul style="list-style-type: none"> <li>o 7.1.2.1.1 General requirements</li> <li>o 7.1.2.1.2 Information security management terminology, principles, practices and techniques</li> <li>o 7.1.2.1.3 Information security management system standards and normative documents</li> <li>o 7.1.2.1.4 Business management practices</li> <li>o 7.1.2.1.5 Client business sector</li> <li>o 7.1.2.1.6 Client products, processes and organization</li> </ul> </li> <li>- 7.1.2.2 Competence requirements for leading the ISMS audit team</li> <li>- 7.1.2.3 Competence requirements for conducting the application review <ul style="list-style-type: none"> <li>o 7.1.2.3.1 Information security management system standards and normative documents</li> <li>o 7.1.2.3.2 Client business sector</li> <li>o 7.1.2.3.3 Client products, processes and organization</li> </ul> </li> <li>- 7.1.2.4 Competence requirements for reviewing audit reports and making certification decisions <ul style="list-style-type: none"> <li>o 7.1.2.4.1 General</li> <li>o 7.1.2.4.2 Information security management terminology, principles, practices and techniques</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ 7.1.2.4.3 Information security management system standards and normative documents</li> <li>○ 7.1.2.4.4 Client business sector</li> <li>○ 7.1.2.4.5 Client products, processes and organization</li> </ul>
<b>Clause 7.2 Personnel involved in the certification activities</b>	<b>7.2.1 IS 7.2 Demonstration of auditor knowledge and experience</b> <ul style="list-style-type: none"> <li>- 7.2.1.1 Selecting auditors</li> <li>- 7.2.1.2 Selecting auditors for leading the team</li> </ul>
<b>Clause 7.3 Use of individual external auditors and external technical experts</b>	<b>7.3.1 IS 7.3 Using external auditors or external technical experts as part of the audit team</b>
<b>Clause 8.2 Certification documents</b>	<b>8.2.1 IS 8.2. ISMS Certification documents</b>
<b>Clause 8.4 Confidentiality</b>	<b>8.4.1 IS 8.4 Access to organizational records</b>
<b>Clause 9.1 Pre-certification activities</b>	<b>9.1.1 Application</b> <ul style="list-style-type: none"> <li>- 9.1.1.1 IS 9.9.1 Application readiness</li> </ul> <b>9.1.3 Audit programme</b> <ul style="list-style-type: none"> <li>- 9.1.3.1 IS 9.1.3 Audit Programme</li> <li>- 9.1.3.2 IS 9.1.3 Audit methodology</li> <li>- 9.1.3.3 IS 9.1.3 General preparations for the initial audit</li> <li>- 9.1.3.4 IS 9.1.3 Review periods</li> <li>- 9.1.3.5 IS 9.1.3 Scope of certification</li> <li>- 9.1.3.6 IS 9.1.3 Certification audit criteria</li> </ul> <b>9.1.4 Determining audit time</b> <ul style="list-style-type: none"> <li>- 9.1.4.1 IS 9.1.4 Determining audit time</li> </ul> <b>9.1.5 Multi-site sampling</b> <ul style="list-style-type: none"> <li>- 9.1.5.1 IS 9.1.5 Multi site sampling</li> </ul> <b>9.1.6 Multiple management systems</b> <ul style="list-style-type: none"> <li>- 9.1.6.1 IS 9.1.6 Integration of ISMS documentation with that for other management systems</li> <li>- 9.1.6.2 IS 9.1.6 Combining management system audits</li> </ul>
<b>Clause 9.2 Planning audits</b>	<b>9.2.1 Determining audit objectives, scope and criteria</b> <ul style="list-style-type: none"> <li>- 9.2.1.1 IS 9.2.1 Audit objectives</li> </ul> <b>9.2.2 Audit team selection and assignments</b>

	<ul style="list-style-type: none"> <li>- 9.2.2.1 IS 9.2.2 Audit team</li> <li>- 9.2.2.2 IS 9.2.2 Audit team competence</li> </ul> <b>9.2.3 Audit plan</b> <ul style="list-style-type: none"> <li>- 9.2.3.1 IS 9.2.3 General</li> <li>- 9.2.3.2 IS 9.2.3 Network-assisted audit techniques</li> <li>- 9.2.3.3 IS 9.2.3 Timing of the audit</li> </ul>
<b>Clause 9.3 Initial certification</b>	<b>9.3.1 IS 9.3.1 Initial certification audit</b> <ul style="list-style-type: none"> <li>- 9.3.1.1 IS 9.3.1.1 Stage 1</li> <li>- 9.3.1.2 IS 9.3.1.2 Stage 2</li> </ul>
<b>Clause 9.4 Conducting audits</b>	<b>9.4.1 IS 9.4 General</b> <b>9.4.2 IS 9.4 Specific elements of an ISMS audit</b> <b>9.4.3 IS 9.4 Audit report</b>
<b>Clause 9.5 Certification decision</b>	<b>9.5.1 IS 9.5 Certification decision</b>
<b>Clause 9.6 Maintaining certification</b>	<b>9.6.2 Surveillance activities</b> <ul style="list-style-type: none"> <li>- 9.6.2.1 IS 9.6.2 Surveillance activities</li> </ul> <b>9.6.3 Re-certification</b> <ul style="list-style-type: none"> <li>- 9.6.3.1 IS 9.6.3 Re-certification audits</li> </ul> <b>9.6.4 Special audits</b> <ul style="list-style-type: none"> <li>- 9.6.4.1 IS 9.6.4 Special cases</li> </ul>
<b>Clause 9.8 Complaints</b>	<b>9.8.1 IS 9.8 Complaints</b>
<b>Clause 10.1 Options</b>	<b>10.1.1 IS 10.1 ISMS implementation</b>
	<b>Annex B (normative) Audit Time</b>



## **5 KNOWLEDGE REQUIREMENTS APPLICABLE TO THE ACCREDITATION BODY (IAF MD 13:2023)**

5.1 ISO/IEC 17011 Clause 6. 1. 2.1 requires Accreditation Bodies to describe for each activity involved in the accreditation process the competencies required. Normative Annex A of IAF MD 13:2023 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 general competency required for each function within an Accreditation Body , which are defined in ISO/IEC 17011:2017.

5.2 Generally, each assessor involved in ISMS assessment shall have a level of the knowledge described in A1 to A5 in Annex A. The knowledge in A6 and A 7 can be held within the team as a whole.

5.3 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 organization that is the subject of the witnessed audit 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 13:2020)**

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.

<div>Accreditation Functions</div> <div>Subject</div>	Document Review (as part of the assessment)	Office Assessment	Witness assessment	Reviewing assessment reports and making accreditation decisions	Scheme management
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 TS 27008		X	X		
A3. ISO/IEC 17021-1 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 <ul style="list-style-type: none"> <li>- information security technologies and practices</li> <li>- information and communication technology</li> <li>- risk assessment and risk management such as ISO/IEC 27005.</li> </ul>	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/AMD 1:2020. EAC or NACE codes are not specified for this schedule

Information Security Management Systems according to ISO/IEC 27001:2022 (ISO/IEC 17021-1:2015 in combination with ISO/IEC 27006:2015/AMD1:2020)
--

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

---