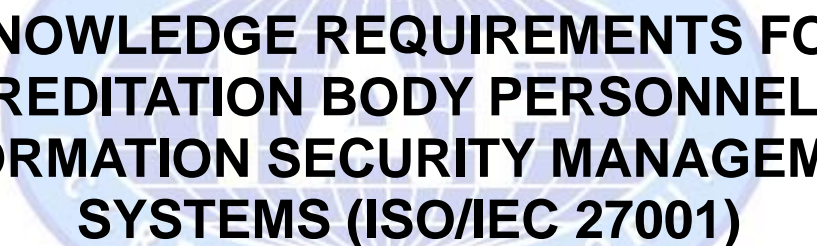




IAF Mandatory Document

A large, light blue watermark of the IAF logo is centered on the page, behind the main title text.

KNOWLEDGE REQUIREMENTS FOR ACCREDITATION BODY PERSONNEL FOR INFORMATION SECURITY MANAGEMENT SYSTEMS (ISO/IEC 27001)

Issue 1, Version 2

(IAF MD 13:2015)

The International Accreditation Forum, Inc. (IAF) facilitates trade and supports regulators by operating a worldwide mutual recognition arrangement among Accreditation Bodies (ABs) in order that the results issued by Conformity Assessment Bodies (CABs) accredited by IAF members are accepted globally.

Accreditation reduces risk for business and its customers by assuring that accredited Conformity Assessment Bodies (CABs) are competent to carry out the work they undertake within their scope of accreditation. Accreditation Bodies (ABs) that are members of IAF and the CABs they accredit are required to comply with appropriate international standards and the applicable IAF application documents for the consistent application of those standards.

ABs that are signatories to the IAF Multilateral Recognition Arrangement (MLA) are evaluated regularly by an appointed team of peers to provide confidence in the operation of their accreditation programs. The structure and scope of the IAF MLA is detailed in IAF PR 4 - Structure of IAF MLA and Endorsed Normative Documents.

The IAF MLA is structured in five levels: Level 1 specifies mandatory criteria that apply to all ABs, ISO/IEC 17011. The combination of a Level 2 activity(ies) and the corresponding Level 3 normative document(s) is called the main scope of the MLA, and the combination of Level 4 (if applicable) and Level 5 relevant normative documents is called a sub-scope of the MLA.

- Main scope of the MLA includes activities e.g. product certification and associated mandatory documents e.g. ISO/IEC Guide 65. The attestations made by CABs at the main scope level are considered to be equally reliable.
- Sub scope of the MLA includes conformity assessment requirements e.g. ISO 9001 and scheme specific requirements, where applicable, e.g. ISO TS 22003. The attestations made by CABs at the sub scope level are considered to be equivalent.

The IAF MLA delivers the confidence needed for market acceptance of conformity assessment outcomes. An attestation issued, within the scope of the IAF MLA, by a body that is accredited by an IAF MLA signatory AB can be recognized worldwide, thereby facilitating international trade.

Issue No 1, Version 2

Prepared by: IAF Technical Committee

Approved by: IAF Members

Issue Date: 19 January 2015

Date: 28 February 2014

Application Date: 26 May 2015

Name for Enquiries:

Elva Nilsen, IAF Corporate Secretary

Contact: Phone: +1 613 454-8159

Email: secretary@iaf.nu

INTRODUCTION TO IAF MANDATORY DOCUMENTS

The term “should” is used in this document to indicate recognised means of meeting the requirements of the standard. An Accreditation Body (AB) can meet these in an equivalent way. The term “shall” is used in this document to indicate those provisions which, reflecting the requirements of the relevant standard, are mandatory.

TABLE OF CONTENTS

1. SCOPE	5
2. NORMATIVE REFERENCES	5
3. TERMS AND DEFINITIONS	5
4. KNOWLEDGE REQUIREMENTS	6
ANNEX A (Normative) Required Knowledge for Accreditation Body Personnel Involved in the Accreditation of ISMS Certification Bodies	7

1. SCOPE

This document defines the specific knowledge requirements for personnel involved in the accreditation of Certification Bodies that provide audit and certification of information security management systems (ISMS) to ISO/IEC 27001.

The objective of this document is to enable Accreditation Bodies to harmonize their application of Clause 6.2.1 of ISO/IEC 17011:2004 for the accreditation of bodies providing audit and certification to ISO/IEC 27001.

2. NORMATIVE REFERENCES

For the purposes of this document, the normative references given in ISO/IEC 17011 and the following apply. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17011:2004 Conformity Assessment - General requirements for accreditation bodies accrediting conformity assessment bodies.

ISO/IEC 17021 – 1:2014 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements

ISO/IEC 27006:2011 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27007:2011 Information technology – Security techniques – Guidelines for information security management systems auditing

ISO/IEC TR 27008:2011 Information technology – Security techniques – Guidelines for auditors on information security controls

3. TERMS AND DEFINITIONS

For the purpose of this document, the terms and definitions given in ISO/IEC 17011 and ISO/IEC 27000 apply.

4. KNOWLEDGE REQUIREMENTS

- 4.1 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.
- 4.2 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 A7 can be held within the team as a whole.
- 4.3 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.
- 4.4 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.
- 4.5 CAB's client process and operation associated with ISMS cover:
- typical business activities related to the technical area (see ISO/IEC 17021:2011, 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.

End of IAF Mandatory Document - Knowledge Requirements for Accreditation Body Personnel for Information Security Management Systems (ISO/IEC 27001).

ANNEX A (Normative)**Required Knowledge for Accreditation Body Personnel Involved in the Accreditation of ISMS Certification Bodies**

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
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		
---	--	--	---	--	--

Further Information

For further Information on this document or other IAF documents, contact any member of IAF or the IAF Secretariat.

For contact details of members of IAF see - IAF Web Site - <<http://www.iaf.nu>>

Secretariat:

IAF Corporate Secretary
Telephone + 1 613 454-8159
Email: secretary@iaf.nu