



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

Issue Date: 10 July 2026
Implementation Date: 28 August 2026
Version No: 1.0

FURTHER INFORMATION

For further information on this document or other Global Accreditation Cooperation Incorporated (Global ACI) documents, contact the Global ACI Secretariat.

Email: secretariat@global-aci.org

Phone: +1 (571) 569-2614

© Copyright 2026

Global ACI encourages the authorised reproduction of its publications, or parts thereof, by organisations wishing to use such material for areas related to education, standardisation, accreditation, or other purposes relevant to Global ACI's area of expertise or endeavour. The document in which the reproduced material appears must contain a statement acknowledging Global ACI's contribution to the document.

TABLE OF CONTENTS

1. PREAMBLE..... 4

1.1 Purpose 4

1.2 Scope 4

2. NORMATIVE REFERENCES 4

3. TERMS AND DEFINITIONS 4

4. KNOWLEDGE REQUIREMENTS..... 5

5. AMENDMENT TABLE..... 5

ANNEX A - REQUIRED KNOWLEDGE FOR ACCREDITATION BODY PERSONNEL INVOLVED
IN THE ACCREDITATION OF ISMS CERTIFICATION BODIES 6

1. PREAMBLE

1.1 Purpose

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.

1.2 Scope

1.2.1 The objective of this document is to enable Accreditation Bodies (ABs) to harmonise their application of Clause 6.1.2.1 of ISO/IEC 17011:2017 for the accreditation of bodies providing audit and certification to ISO/IEC 27001.

1.2.2 The term “should” is used in this document to indicate recognised means of meeting the requirements of the standard. A Conformity Assessment Body (CAB) can meet these in an equivalent way provided this can be demonstrated to an AB. The term “shall” is used in this document to indicate those provisions which, reflecting the requirements of the relevant standard, are mandatory.

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 17011:2017 Conformity Assessment - General requirements for accreditation bodies accrediting conformity assessment bodies.
- ISO/IEC 17021-1:2015 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements
- ISO/IEC 27006 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 Information technology – Security techniques – Information security management systems – Overview and vocabulary
- ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing
- ISO/IEC TS 27008:2019 Information technology – Security techniques – Guidelines for the assessment of information security controls
- ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management

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 6.1.2.1 requires Accreditation Bodies to describe for each activity involved in the accreditation process the competencies required. Normative Annex A of this document 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.
- 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 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 witnessed audit would be expected to comply with either for the information security field or country/state/province within which they operate.

5. AMENDMENT TABLE

Section	Previous Version	Summary of Changes
All	-	Initial issue of Global ACI document

ANNEX A - REQUIRED KNOWLEDGE FOR ACCREDITATION BODY PERSONNEL INVOLVED IN THE ACCREDITATION OF ISMS CERTIFICATION BODIES

(Normative)

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.

Accreditation Functions Subject	Document Review	Office Assessment	Witness assessment	Reviewing assessment reports and making accreditation decisions	Management of accreditation schemes
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	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, such as ISO/IEC 27005.	X	X	X	X	
A7. CAB's client process and operation associated with ISMS			X		