



Requirements of ISO/IEC 27006-1: 2024

**National Accreditation Board for
Certification Bodies (NABCB)**



ISO/IEC 27006-1:2024

Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General

ISO/ IEC 27006-1 - Scope

This document specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1.

The requirements contained in this document are demonstrated in terms of competence and reliability by bodies providing ISMS certification. The guidance contained in this document provides additional interpretation of these requirements for bodies providing ISMS certification.

5.2.2 Conflicts of interest

Requirements additional to ISO 17021-1:2015

- CAB may provide OFI based on the audit outcome without recommending solution
- CAB not to provide IS Reviews for the client subject to Certification and remain independent

ISO 27006 -1- 2024 – Key Changes

Requirements additional to ISO 17021-1:2015

IS 7.1.2 Generic competence requirements

IS 7.1.3.1 Competence requirements for ISMS auditing

IS 7.1.3.2 Competence requirements for conducting the application review

IS 7.1.3.3 Competence requirements for reviewing audit reports and making certification decisions

IS 7.2.2 Demonstration of auditor knowledge and experience

ISO 27006 -1- 2024 – Key Changes

7.1.2 Generic competence requirements

Requirements additional to ISO 17021-1:2015

- CAB shall define competence requirements for each certification function relevant for ISMS Technical areas
- Define Knowledge and skills required for certain functions in accordance with Annex A
- Apply additional specific criteria including competence requirement where defined by the standard

ISO 27006:2024 Annexure A (normative)

(Knowledge and skills for ISMS auditing and certification)

Certification functions knowledge and skills	Conducting the application review to determine audit team competence required, to select the audit team members, and to determine the audit time	Reviewing audit reports and making certification decisions	Auditing and Leading the audit teams
Information security management terminology, principles, practices and techniques		X (see 7.1.3.3.2)	X(see 7.1.3.1.2)
Information security management system standards/ normative documents			X (see 7.1.3.1.3)
Business management practices			X (see 7.1.3.1.4)
Knowledge of client business sector	X (see 7.1.3.2.1)	X (see 7.1.3.3.3)	X (see 7.1.3.1.5)
Client products, processes and organization	X (see 7.1.3.2.2)	X (see 7.1.3.3.4)	X (see 7.1.3.1.6)

ISO 27006 -1- 2024 – Key Changes

7.1.3 Competence requirements

Requirements additional to ISO 17021-1:2015

- For ISMS Auditing
 - General requirements

CAB shall have criteria for verifying competence of audit team members such that, their knowledge below can be applied:

 - a) information security; requirements of ISO27001
 - b) the technical aspects of the activity to be audited;
 - c) management systems;
 - d) the principles of auditing;
NOTE Further information on the principles of auditing can be found in ISO 19011.
 - e) ISMS monitoring, measurement, analysis and evaluation.
 - f) Risk assessment and management; business management practices
- Each auditor of team need not have complete range of experience of all areas of IS. However, the audit team as a whole should have collective competence and be able to audit the scope including understanding of tools, methods, techniques, and their application

Can share among the team

For all auditors in the team

ISO 27006 -1- 2024 – Key Changes

7.1.3 Competence requirements

Requirements additional to ISO 17021-1:2015

- For Application review
 - Understanding client business sector
 - Assess audit team competence required, selection, audit time etc.
 - Client products, processes, and organization
 - In addition to above understand the impact of products, processes on the organization from an ISMS perspective
- Reviewing audit reports and making certification decision
 - Understand the scope and its implications while certifying
 - Understand management system in general and auditing processes and procedures
 - Knowledge of ISMS terminology, principles, practices & techniques; legal and regulatory requirements related to IS
 - Understand client business sector and Client products, processes, and organization

ISO 27006 -1- 2024 – Key Changes

7.2 Personnel involved in the certification activities

7.2.2 Demonstration of auditor knowledge and experience

Requirements additional to ISO 17021-1:2015

- General considerations
 - Each auditor to have recognized ISMS specific qualifications; participate in ISMS relevant training; maintain professional development records; ISMS Witness by another ISMS auditor
- Selecting auditors & technical experts (TE)
 - each auditor / TE should have professional education; has practical workplace experience in IT & IS to be an ISMS auditor / act as an expert; trained in ISMS auditing and has skills of auditing; maintains the knowledge



ISO 27006-1: 2024 – Key Changes

Requirements additional to ISO 17021-1:2015

8.2.2 ISMS Certification documents

8.2.3 Reference of other standards in the ISMS certification documents

8.4.2 Access to organizational records



ISO 27006-1: 2024 – Key Changes

8.2.2 & 8.2.3 ISMS Certification documents

Requirements additional to ISO 17021-1:2015

- Certification documents shall be signed by an officer who has been assigned that responsibility. The version of the Statement of Applicability (SoA) shall be included in the certification documents.
- Where no activity of the organization within the scope of the certification is undertaken at a defined physical location at all, the certification document(s) shall state that all activities of the organization are conducted remotely.
- The certification documents may reference national and international standards only if:
 - The organization has compared all its necessary controls with those of the reference control source to ensure none of the controls are omitted
 - A justification for excluded controls is included in the SoA

ISO 27006-1: 2024 – Key Changes

8.4.2 Access to organizational records

Requirements additional to ISO 17021-1:2015

Before the certification audit, the certification body shall ask the client to report if any ISMS related information (such as ISMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information. The certification body shall determine whether the ISMS can be adequately audited in the absence of such information. If the certification body concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, it shall advise the client that the certification audit cannot take place until appropriate access arrangements are granted.

ISO 27006-1: 2024 – Key Changes

Requirements additional to ISO 17021-1:2015

IS 9.1.1.2 Considerations for certification procedures

9.1.3.3 Deployment of remote audit

9.1.3.4 General preparations for the initial audit

9.1.3.5 Review periods

9.1.3.6 Scope of ISMS certification

IS 9.1.3 Audit programme

IS 9.1.4 Audit time

IS 9.1.5 Multiple sites

IS 9.1.6 Multiple management systems

ISO 27006-1: 2024 – Key Changes

9.1.1.2 Considerations for certification procedures

Requirements additional to ISO 17021-1:2015

The certification body's procedures shall not presuppose a particular manner of implementation of an ISMS or a particular format for documentation and records. Certification procedures shall focus on confirming that a client's ISMS meets the requirements specified in ISO/IEC 27001 and the policies and objectives of the client.

NOTE It is possible for an organization to design its own necessary controls or to select them from any source, therefore it is possible that an organization is certified to ISO/IEC 27001 even though none of its necessary controls are those specified in ISO/IEC 27001:2022, Annex A.

ISO 27006-1: 2024 – Key Changes

IS 9.1.3 Audit programme

Requirements additional to ISO 17021-1:2015

9.1.3.4 General preparations for the initial audit

The certification body shall require that a client makes all necessary arrangements for the access to internal audit reports and reports of independent reviews of information security.

9.1.3.5 Review periods

The certification body shall not certify an ISMS unless there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective, and will be maintained covering the scope of certification.

ISO 27006-1: 2024 – Key Changes

9.1.4 Audit time

Requirements additional to ISO 17021-1:2015

The certification body shall use *Annex C* to determine audit time.

NOTE Further guidance and examples on audit time calculation are provided in Annex D.

ISO 27006-1: 2024 – Key Changes

9.1.5.2 Multiple sites

Requirements additional to ISO 17021-1:2015

9.1.5.2.1 Where a client has a number of sites meeting the criteria from a) to c) below, certification bodies may consider using a sample-based approach to multiple-site certification audit:

- a) all sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review;
- b) all sites are included within the client's internal ISMS audit programme;
- c) all sites are included within the client's ISMS management review programme.

9.1.5.2.21 The certification body wishing to use a sample-based approach shall have procedures in place to ensure the following: a to f

ISO 27006-1: 2024 – Key Changes

9.1.6 Multiple management systems

Requirements additional to ISO 17021-1:2015

9.1.6.1 Integration of ISMS documentation with that for other management systems

The certification body may accept documentation that is combined (e.g. for information security, quality, health and safety and environment) as long as the ISMS can be clearly identified together with the appropriate interfaces to the other systems.

9.1.6.2 Combining management system audits

The ISMS audit may be combined with audits of other management systems, provided that it can be demonstrated that the audit satisfies all requirements for certification of the ISMS. All the elements important to an ISMS shall appear clearly and be readily identifiable in the audit reports. The quality of the audit shall not be adversely affected by the combination of the audits.

ISO 27006-1: 2024 – Key Changes

Requirements additional to ISO 17021-1:2015

9.2.1.2 Audit objectives

9.2.3 Audit plan

9.3.2 Initial certification audit

9.4 Conducting audits

9.5.2 Certification decision

9.6.2 Surveillance activities

9.6.3 Re-certification audits

9.8.2 Complaints

ISO 27006-1: 2024 – Key Changes

9.2.1.2 Audit objectives

Requirements additional to ISO 17021-1:2015

The audit objectives shall include:

- a) determining the effectiveness of the management system;
- b) ensuring that the client, based on the risk assessment, has identified the necessary controls; and
- c) determining that the established information security objectives have been achieved.

ISO 27006-1: 2024 – Key Changes

9.2.3 Audit plan

Requirements additional to ISO 17021-1:2015

9.2.3.2 General considerations

The audit plan for ISMS audits shall take the determined information security controls into account.

NOTE It is good practice for a certification body to agree on the timing of the audit with the organization being audited to best demonstrate the full scope of the organization. Considerations can include season, month, day/dates and shifts, as appropriate.

9.2.3.3 Remote audit techniques

The objective of remote auditing techniques should be to enhance audit effectiveness and efficiency, and to support the integrity of the audit process. The audit plan shall reference tools that are used to assist remote auditing.

ISO 27006-1: 2024 – Key Changes

9.3.2 Initial certification audit

Requirements additional to ISO 17021-1:2015

9.3.2.1 Stage 1

In this stage of the audit, the certification body shall obtain documentation on the design of the ISMS covering the documentation required in ISO/IEC 27001.

As a minimum, the following information shall be provided by the client during stage 1 of the certification audit:

- a) general information concerning the ISMS and the activities it covers;
- b) a copy of the required ISMS documentation specified in ISO/IEC 27001 and, where required, other associated documentation.

The certification body shall obtain sufficient understanding of the design of the ISMS in the context of the client's organization, risk assessment and treatment (including the controls determined), information security policy and objectives and, in particular, of the client's preparedness for the audit. This shall be used for planning the stage 2 audit.

ISO 27006-1: 2024 – Key Changes

9.3.2 Initial certification audit

Requirements additional to ISO 17021-1:2015

9.3.2.1 Stage 1 (Cont.)

The results of stage 1 shall be documented in a written report. The certification body shall review the stage 1 audit report before deciding on proceeding with stage 2. The certification body shall confirm the stage 2 audit team members have the necessary competence. This may be done by the auditor leading the team that conducted the stage 1 audit if deemed competent and appropriate.

NOTE Having a person from the certification body who is not involved in the audit reviewing the report, and who decides to proceed and confirms the competence of the audit team members for stage 2, offers a degree of mitigation for the risks involved. However, other risk mitigation measures can already be in place to achieve the same goal.

The certification body shall make the client aware of the further types of information and records that may be required for detailed examination during stage 2.

ISO 27006-1: 2024 – Key Changes

9.3.2 Initial certification audit

Requirements additional to ISO 17021-1:2015

9.3.2.2 Stage 2

Based on the findings documented in the stage 1 audit report, the certification body shall develop an audit plan for the conduct of stage 2. In addition to evaluating the effective implementation of the ISMS, the objective of stage 2 is to confirm that the client adheres to its own policies, objectives and procedures.

Audit shall focus on the client's:

Refer a to g

ISO 27006-1: 2024 – Key Changes

9.4.2 Specific elements of the ISMS audit

Requirements additional to ISO 17021-1:2015

The certification body audit team shall:

- a) require the client to demonstrate that the assessment of information security related risks is relevant and adequate for the ISMS operation within the ISMS scope;
- b) establish whether the client's procedures for the identification, examination and evaluation of information security related risks and the results of their implementation are consistent with the client's policy, objectives and targets.

The certification body shall also establish whether the procedures employed in risk assessment are sound and properly implemented.

9.4.2 Audit report

Requirements additional to ISO 17021-1:2015

9.4.3.1 The audit report shall provide the following information or a reference to it:

- a) an account of the audit of the client's information security risk analysis;
- b) any information security control sets used by the organization for comparison purposes as required by ISO/IEC 27001:2022, 6.1.3 c).

ISO 27006-1: 2024 – Key Changes

9.4.2 Audit report

Requirements additional to ISO 17021-1:2015

9.4.3.1 The audit report shall provide the following information or a reference to it:

- a) an account of the audit of the client's information security risk analysis;
- b) any information security control sets used by the organization for comparison purposes as required by ISO/IEC 27001:2022, 6.1.3 c).

9.4.3.2 The audit report shall be sufficiently detailed to facilitate and support the certification decision. It shall contain:

- a) the significant audit trails followed and audit methodologies utilized (see 9.1.1.2);
- b) a reference to the version of the Statement of Applicability and, where applicable, any useful comparison with the results of previous certification audits of the client

9.4.3.2 Audit report (Cont.)

Requirements additional to ISO 17021-1:2015

Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report. If these methods are used, these documents shall be submitted to the certification body as evidence to support the certification decision. Information about the samples evaluated during the audit shall be included in the audit report, or in other certification documentation.

Where remote audit methods have been used, the report shall indicate the extent to which they have been used in carrying out the audit and their effectiveness in achieving the audit objectives.

Where the activities of the organization are not undertaken at a defined physical location and therefore all activities of the organization are conducted remotely, the audit report shall state that all activities of the organization are conducted remotely.

The report shall consider the adequacy of the internal organization and procedures adopted by the client to give confidence in the ISMS.

The report shall include a summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS requirements and information security controls.

ISO 27006-1: 2024 – Key Changes

9.5 Certification decision

Requirements additional to ISO 17021-1:2015

9.5.2 Certification decision

The certification decision shall be based on the certification recommendation of the audit team as provided in their certification audit report.

Certification shall not be granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective and will be maintained.

ISO 27006-1: 2024 – Key Changes

9.6.2 Surveillance activities

Requirements additional to ISO 17021-1:2015

9.6.2.2 Surveillance audit procedures shall be a subset of those for the certification audit of the client's ISMS as described in this document.

The purpose of surveillance is to verify that the approved ISMS continues to be implemented, to consider the implications of changes to the ISMS initiated as a result of changes in the client's operational practices and to confirm continued compliance with certification requirements.

Surveillance audit programmes shall cover at least:

- a) the ISMS maintenance elements such as information security risk assessment and control maintenance, internal ISMS audit, management review and corrective action;
- b) communications from external parties as required by ISO/IEC 27001 and other documents required for certification

9.6.2 Surveillance activities

Requirements additional to ISO 17021-1:2015

9.6.2.3 As a minimum, every surveillance audit by the certification body shall review the following:

- a) the effectiveness of the ISMS with regard to achieving the objectives of the client's information security policy;
- b) the functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations;
- c) changes to the controls determined, and resulting changes to the SoA;
- d) implementation and effectiveness of controls indicated in the audit programme.

ISO 27006-1: 2024 – Key Changes

9.6.2 Surveillance activities

Requirements additional to ISO 17021-1:2015

9.6.2.4 The certification body shall be able to adapt its programme of surveillance activities to reflect the information security issues related to risks and impacts on the client and justify this programme.

Surveillance audits may be combined with audits of other management systems. Audit reports shall clearly indicate the aspects relevant to each management system.

During surveillance audits, certification bodies shall check the records of appeals and complaints brought before the certification body. Where any nonconformity or failure to meet the requirements of certification is revealed, certification bodies shall check that the client has investigated its own ISMS and procedures, and has taken appropriate corrective action.

A surveillance report shall contain, in particular, information on clearing of nonconformities revealed previously, the version of the SoA and important changes from the previous audit. As a minimum, the reports arising from surveillance shall build up to cover in totality the requirements of 9.6.2.2 and 9.6.2.3.



ISO 27006-1: 2024 – Key Changes

9.6.3.2 Re-certification audits

Requirements additional to ISO 17021-1:2015

Re-certification audit procedures shall be a subset of those for the initial certification audit of the client's ISMS as described in this document.

The time allowed to implement corrective action shall be consistent with the severity of the nonconformity and the associated information security risk





ISO 27006-1: 2024 – Key Changes

9.8.2 Complaints

Requirements additional to ISO 17021-1:2015

Complaints represent a potential incident and an indication of possible nonconformity

ISO 27006-1: 2024 – Key Changes

Requirements additional to ISO 17021-1:2015

10.1.2 ISMS implementation

It is recommended that certification bodies implement an ISMS in accordance with ISO/IEC 27001

Annex C : Audit Time

C 2.1 Number of persons doing work under the organization's control

The total number of persons doing work under the organization's control for all shifts within the scope of the certification is the starting point for determination of audit time.

NOTE The term “persons doing work under the organization's control” is referred to as personnel in ISO/IEC 17021-1.

Reduction for the number of persons, within the scope of certification, performing certain identical activities ?

The square root of the head count of people performing each identical activity may be used to determine the effective number of people, which is used for audit duration calculations, rounded up to the next full number.

Annex C : Audit Time

C 3.7 On-site audit time

It is expected that the time calculated for planning and report writing combined should not typically reduce the total on-site “audit time” to less than 70 % of the time calculated in accordance with C.3.3, C3.4 and C.3.5. Where additional time is required for planning and/or report writing, this shall not be a justification for reducing on-site audit time. Auditor travel time is not included in this calculation and is additional to the audit time referenced in the chart.

(C.3.3 Audit time calculation; C.3.4 Determination of initial number of persons and C.3.5 Factors for adjustment of audit time)

Annex C : Audit Time

C.4 Audit time for surveillance audits

C.5 Audit time for re-certification audit

C.6 Audit time of multi-site

Generally, the total audit time for on-site audit shall be calculated by considering the total number of persons doing work under the organization's control irrespective of their location

The number of total on-site auditor days shall be allocated across the different sites based on the relevance of the site for the management system, the activities conducted at the site and the risks identified. The justification for the allocation shall be recorded by the certification body.

Annex C : Audit Time

C.7 Audit time for scope extensions

For the initial audit of the new scope, the time shall be calculated based on the number of persons and sites being added to the already existing scope

Audit time shall be added to the calculated duration to review the client's ISMS. This additional time shall be at least:

- 1) 0,5 d (auditor days) if the extension to scope audit is conducted in conjunction with a surveillance audit or a recertification audit.
- 2) 1,0 d (auditor days) when the extension to scope audit is conducted as a separate audit

Audit time Calculation Example (Annex D of 27006:2024 – Informative)

Table - Factors related to business and organization (other than IT)		
Category	Grade	
Type(s) of business and regulatory requirements	1	Organization works in non-critical business sectors and non-regulated sectorsa
	2	Organization has customers in critical business sectors a
	3	Organization works in critical business sectors a
Process and tasks	1	Standard processes with standard and repetitive tasks; lots of persons doing work under the organization’s control carrying out the same tasks; few products or services
	2	Standard but non-repetitive processes, with high number of products or services
	3	Complex processes, high number of products and services, many business units included in the scope of certification (ISMS covers highly complex processes or relatively high number or unique activities)
Level of establishment of the MS	1	ISMS is already well established and/or other management systems are in place
	2	Some elements of other management systems are implemented, others not
	3	No other management system implemented at all, the ISMS is new and not established

Critical business sectors are sectors that may affect critical public services that will cause risk to health, security, economy, image and government ability to function that may have a very large negative impact to

Audit time Calculation Example (Annex D of 27006:2024 – Informative)

Table - Factors related to IT Environment		
Category	Grade	
IT infrastructure complexity	1	Few or highly standardized IT platforms, servers, operating systems, databases, networks, etc.
	2	Several different IT platforms, servers, operating systems, databases, networks
	3	Many different IT platforms, servers, operating systems, databases, networks
Dependency on outsourcing and suppliers, including cloud services	1	Little or no dependency on outsourcing or suppliers
	2	Some dependency on outsourcing or suppliers, related to some but not all important business activities
	3	High dependency on outsourcing or suppliers, large impact on important business activities
Information System development	1	None or a very limited in-house system/application development
	2	Some in-house or outsourced system/application development for some important business purposes
	3	Extensive in-house or outsourced system/application development for important business purposes

Audit time Calculation Example (Annex D of 27006:2024 – Informative)

Audit time reduction / Increase matrix		IT Complexity		
		Low 3 to 4	Medium 5 to 6	High 7 to 9
Business Complexity	Low 3 to 4	-10% to -30%	-5% to -10%	5% to 20%
	Medium 5 to 6	-5% to -10%	0%	+10% to 50%
	High 7 to 9	5% to 20%	+10% to 50%	+20% to 100%

Thank You!!

National Accreditation Board for Certification Bodies (NABCB) Quality Council of India

Institution of Engineers Building, 2nd Floor, Bahadur Shah Zafar Marg, New Delhi - 110002, India.

Tel: +91 - 11 - 2337 9921, 2337 8056, 2337 8217, 2337 8057 | Email: nabcb@qcin.org | web.: www.nabcb.qci.org.in

