International Standard

ISO 19011

Guidelines for auditing management systems

Lignes directrices pour l'audit des systèmes de management

Fourth edition
2026-05

Reference number
ISO 19011:2026(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Project Committee ISO/PC 302, *Guidelines for auditing management systems*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 1, *Criteria for conformity assessment bodies*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This fourth edition cancels and replaces the third edition (ISO 19011:2018), which has been technically revised.

The main changes are as follows:

— expansion of guidance on remote auditing methods through the introduction of guidance contained in ISO/IEC TS 17012;

— expansion of Annex A to provide guidance on remote auditing methods and virtual locations.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Since the third edition of this document was published in 2018, several management system standards have been published in new fields. Most of them have a common structure, identical core requirements, and common terms and core definitions. As a result, there is a need to consider a broader approach to management system auditing, as well as to provide guidance that is more generic.

This document provides guidance which can be applied to audit against a range of audit criteria (separately or in combination) including, but not limited to:

— requirements specified in one or more management system standards;

— policies, processes and requirements specified by the organization or other relevant interested parties;

— statutory and regulatory requirements;

— one or more management system processes defined by the organization and/or other parties;

— management system plan(s) relating to the provision of specific results of a management system (e.g. quality plan, project plan).

This document provides guidance for all organizations regardless of their size and type, and audits of varying scopes. This includes those conducted by large audit teams, typically of larger organizations, and those by single auditors, whether in large or small organizations. This guidance should be adapted as appropriate to the scope and complexity of the audit programme.

This document concentrates on internal audits (first party) and audits conducted by organizations on their external providers and other external interested parties (second party). This document can also be useful for external audits conducted for purposes other than third-party management system certification. ISO/IEC 17021-1 provides requirements for auditing management systems for third-party certification; however, this document can provide useful additional guidance (see Table 1).

Table 1 — Different types of audits

First party	Second party	Third party
Internal audit	External provider audit	Certification audit or accreditation assessment
	Audit by the external interested party of an organization	Statutory, regulatory and similar audit

ISO/IEC TS 17012 addresses the growing need for remote auditing methods. Its aim is to provide guidance on implementing remote auditing methods effectively while supporting the general principles of auditing as outlined in this document.

To simplify the readability of this document, the singular form of "management system" is preferred, but the reader can adapt the implementation of the guidance to their own situation. This also applies to the use of "individual" and "individuals", "auditor" and "auditors".

This document is intended to apply to a broad range of potential users, including auditors, organizations implementing management systems and organizations needing to conduct management system audits for contractual or regulatory reasons. The guidance in this document can be applied to users in developing their own audit-related requirements.

The guidance in this document can also be used for the purpose of self-declaration and can be useful to organizations involved in the training, qualification and certification of persons participating in the audit programme.

The guidance in this document is intended to be flexible. As indicated at various points in the text, the use of this guidance can differ depending on the size and level of maturity of an organization's management system. The nature and complexity of the organization to be audited, as well as the objectives and scope of the audits to be conducted, should also be considered.

This document adopts the combined audit approach when two or more management systems of different disciplines are audited together. Where these systems are integrated into a single management system, the principles and processes of auditing are the same as for a combined audit (sometimes known as an "integrated audit").

Guidelines for auditing management systems

1 Scope

This document gives guidance on auditing management systems, including the principles of auditing, managing an audit programme and conducting management system audits, as well as guidance on the evaluation of competence of individuals involved in the audit process. These individuals include those managing the audit programme, auditors and audit teams.

It is applicable to all organizations that need to plan and conduct audits of management systems or manage an audit programme.

The application of this document to other types of audits is possible, provided that special consideration is given to the specific competence needed and the objectives to be achieved.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
audit
systematic, independent and documented *process* (3.25) for obtaining *objective evidence* (3.9) and evaluating it objectively to determine the extent to which the *audit criteria* (3.8) are fulfilled

Note 1 to entry: Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the organization itself.

Note 2 to entry: External audits include those generally called second and third-party audits. Second-party audits are conducted by parties having an interest in the organization, such as customers, or by other individuals on their behalf. Third-party audits are conducted by independent auditing organizations, such as those providing certification/registration of *conformity* (3.21) or governmental agencies and regulatory authorities.

[SOURCE: ISO 9000:2026, 3.12.1, modified — "documented and "objective" added to the definition. Notes to entry replaced.]

3.2
combined audit
audit (3.1) carried out together at a single *auditee* (3.14) on two or more *management systems* (3.19)

[SOURCE: ISO 9000:2026, 3.12.2, modified — Note 1 to entry deleted.]

3.3
joint audit
audit (3.1) carried out at a single *auditee* (3.14) by two or more auditing organizations

[SOURCE: ISO 9000:2026, 3.12.3]

3.4
remote auditing method
method used for conducting audit activities from any place other than the location of the *auditee* (3.14)

Note 1 to entry: Remote auditing methods can be used in combination with on-site methods to achieve a full and effective *audit* (3.1).

Note 2 to entry: Remote auditing methods can be used for virtual locations, i.e. where an organization performs work or provides a service using an online environment, enabling individuals to execute *processes* (3.25) irrespective of physical locations.

Note 3 to entry: Remote auditing methods can be used by the *auditor* (3.16) at one site of the auditee to audit another site.

[SOURCE: ISO/IEC TS 17012:2024, 3.1]

3.5
audit programme
arrangements for a set of one or more *audits* (3.1) planned for a specific time frame and directed towards a specific purpose

3.6
audit scope
extent and boundaries of an *audit* (3.1)

Note 1 to entry: The audit scope generally includes a description of the physical and virtual locations (see 3.4, Note 2 to entry), functions, organizational units, activities and *processes* (3.25), as well as the time period covered.

3.7
audit plan
description of the activities and arrangements for an *audit* (3.1)

3.8
audit criteria
set of *requirements* (3.24) used as a reference against which *objective evidence* (3.9) is compared

Note 1 to entry: If the audit criteria are legal (including statutory or regulatory) requirements, the words “compliance” or “non-compliance” are often used in an *audit finding* (3.11).

Note 2 to entry: Requirements may include policies, procedures, work instructions, legal requirements, contractual obligations, industry standards, etc.

3.9
objective evidence
data supporting the existence or verity of something

Note 1 to entry: Objective evidence can be obtained through observation, measurement, test or by other means.

[SOURCE: ISO 9000:2026, 3.8.6, modified — Note 2 to entry deleted.]

3.10
audit evidence
records, statements of fact or other information, which are relevant to the *audit criteria* (3.8) and verifiable

3.11
audit finding
results of the evaluation of the collected *audit evidence* (3.10) against *audit criteria* (3.8)

Note 1 to entry: Audit findings indicate *conformity* (3.21) or *nonconformity* (3.22).

Note 2 to entry: Audit findings can lead to the identification of *risks* (3.20), opportunities for improvement or recording good practices.

Note 3 to entry: If the audit criteria are selected from statutory requirements or regulatory requirements, the audit finding is termed "compliance" or "non-compliance".

3.12
audit conclusion
result of an *audit* (3.1), after consideration of the audit objectives and all *audit findings* (3.11)

3.13
audit client
organization or person requesting an *audit* (3.1)

Note 1 to entry: In the case of internal audit, the audit client can also be the *auditee* (3.14) or the individual(s) managing the *audit programme* (3.5). Requests for external audit can come from sources such as regulatory authorities, contracting parties, or potential or existing customers.

[SOURCE: ISO 9000:2026, 3.12.4, modified — Note 1 to entry added.]

3.14
auditee
organization as a whole or parts thereof being audited

3.15
audit team
one or more persons conducting an *audit* (3.1), supported if needed by *technical experts* (3.17)

Note 1 to entry: One *auditor* (3.16) of the audit team is appointed as the audit team leader.

Note 2 to entry: The audit team can include auditors-in-training.

3.16
auditor
person who conducts an *audit* (3.1)

3.17
technical expert
<audit> person who provides specific knowledge or expertise to the *audit team* (3.15)

Note 1 to entry: Specific knowledge or expertise relates to the organization, the activity, *process* (3.25), product, service, discipline to be audited, language or culture.

Note 2 to entry: A technical expert to the audit team does not act as an *auditor* (3.16).

3.18
observer
individual who accompanies the *audit team* (3.15) but does not act as an *auditor* (3.16) nor a *technical expert* (3.17)

3.19
management system
set of interrelated or interacting elements of an organization to establish policies and objectives, as well as *processes* (3.25) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines, e.g. quality management, financial management or environmental management.

Note 2 to entry: The management system elements establish the organization's structure, roles and responsibilities, planning, operation, policies, practices, rules, beliefs, objectives and processes to achieve those objectives.

Note 3 to entry: The scope of a management system can include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

[SOURCE: ISO 9000:2026, 3.4.2, modified — Examples added to Note 1 to entry. Note 2 to entry expanded. Notes 3 and 4 to entry deleted.]

3.20
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential events and consequences, or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

[SOURCE: ISO 9000:2026, 3.7.2, modified — Note 5 to entry deleted.]

3.21
conformity
fulfilment of a *requirement* (3.24)

[SOURCE: ISO 9000:2026, 3.5.9, modified — Note 1 to entry deleted.]

3.22
nonconformity
non-fulfilment of a *requirement* (3.24)

[SOURCE: ISO 9000:2026, 3.5.13]

3.23
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO 9000:2026, 3.10.6]

3.24
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in documented information.

[SOURCE: ISO 9000:2026, 3.5.1, modified — Notes 3, 4 and 5 to entry deleted.]

3.25
process
set of interrelated or interacting activities that use inputs to deliver an intended result

[SOURCE: ISO 9000:2026, 3.3.1, modified — "or transforms" deleted and "intended" added in the definition. Notes to entry deleted.]

3.26
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to managing activities, *processes* (3.25), products, services, systems or organizations.

[SOURCE: ISO 9000:2026, 3.7.3]

3.27
effectiveness
extent to which planned activities are realized and planned results are achieved

[SOURCE: ISO 9000:2026, 3.7.17]

4 Principles of auditing

4.1 General

Auditing is characterized by reliance on a number of principles. These principles should help to make the audit an effective and reliable tool in support of management policies and controls, by providing information on which an organization can act in order to improve its performance. Adherence to these principles is fundamental to provide audit conclusions that are relevant and sufficient, and for enabling auditors, working independently from one another, to reach similar conclusions in similar circumstances.

The guidance given in Clauses 5 to 7 is based on the seven principles outlined in 4.2 to 4.8.

4.2 Integrity

Integrity is the foundation of professionalism.

Auditors and the individual(s) managing an audit programme should:

a) perform their work ethically, with honesty and responsibility;

b) only undertake auditing activities if they are competent to do so;

c) perform their work in an impartial manner, i.e. remain fair and unbiased in all their dealings;

d) be sensitive to any influences that can be exerted on their judgement while carrying out an audit.

4.3 Fair presentation

Fair presentation is the obligation to report truthfully and accurately.

Audit findings, audit conclusions and audit reports should reflect truthfully and accurately the auditing activities. Significant obstacles encountered during the audit and unresolved diverging opinions between the audit team and the auditee should be reported. The communication should be truthful, accurate, objective, timely, clear and complete.

4.4 Due professional care

Due professional care is the application of diligence and judgement in auditing.

Auditors should exercise due care irrespective of the importance of the task they perform, and the confidence placed in them by the audit client and other interested parties. An important factor in carrying out their work with due professional care is having the ability to make reasoned judgements in all audit situations.

4.5 Confidentiality

Confidentiality is security and privacy of information.

Auditors should exercise discretion in the use and protection of information acquired in the course of their auditing activities. Audit information should not be used inappropriately for personal gain by the auditor or the audit client, or in a manner detrimental to the legitimate interests of the auditee. This principle includes the proper handling of sensitive or confidential information.

4.6 Independence

Independence is the basis for the impartiality of the audit and objectivity of the audit conclusions.

Auditors should be independent of the activity being audited wherever practicable and should in all cases act in a manner that is free from bias and conflict of interest. Auditors should maintain objectivity throughout the audit process to ensure that the audit findings and conclusions are based only on the audit evidence.

When it is not possible for internal auditors to be independent of the activity being audited, every effort should be made to remove bias and encourage objectivity.

4.7 Evidence-based approach

Evidence-based approach is the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process.

Audit evidence should be verifiable. It should be based on samples of the information available, since an audit is conducted during a specified duration and with finite resources. An appropriate use of sampling should be applied, since this is closely related to the confidence that can be placed in the audit conclusions.

4.8 Risk-based approach

Risk-based approach is an audit approach that considers risks and opportunities.

The risk-based approach should substantively influence the planning and implementation of the audit programme, and the planning, conducting and reporting of audits in order to ensure that audits are focused on matters that are significant for the audit client, and for achieving the audit programme objectives.

5 Managing an audit programme

5.1 General

An audit programme should be established. It can include audits addressing one or more management system standards or other requirements, conducted either separately or in combination (combined audit).

The extent of an audit programme should be based on the size and nature of the auditee, as well as on the functionality, complexity, the type of risks and opportunities, the scope, and the level of maturity of the management system(s) to be audited.

The functionality of the management system can be even more complex in the case of multiple locations or when important functions are sourced externally.

Particular attention should be paid to where important decisions are made and to the design, planning and review of the audit programme.

The audit programme should be scaled in accordance with the size and complexity of the organization.

In order to understand the context of the auditee, the audit programme should take into account the organization's:

— organizational objectives;

— relevant external and internal issues;

— needs and expectations of relevant interested parties;

— application of technology such as digital tools;

— information security and confidentiality requirements.

When allocating resources and methods to the audit programme, priority should be given to matters in the management system with higher inherent risk and lower levels of performance.

Competent individuals should be assigned to manage the audit programme (see 5.4.2).

The audit programme should include information and identify resources to enable the audits to be conducted effectively within the specified time frames. The information should include:

a) objectives for the audit programme (see 5.2);

b) risks and opportunities associated with the audit programme (see 5.3) and the actions to address them;

c) scope (extent, boundaries, locations) of each audit within the audit programme;

d) schedule (number/duration/frequency) of the audits;

e) audit types, such as internal or external;

f) audit criteria;

g) auditing methods to be employed, including remote auditing methods (see Clause A.16);

h) criteria for selecting the audit team (audit team leader, auditors and, if needed, technical experts);

i) criteria for participation of observers, where relevant;

j) the organization's context based on external and internal issues;

k) relevant documented information.

Some of this information is not always available until more detailed audit planning is completed.

The implementation of the audit programme should be monitored and assessed on an ongoing basis (see 5.6) to ensure its audit programme objectives have been achieved. The audit programme should be reviewed in order to determine the need for changes and possible opportunities for improvements (see 5.7).

Figure 1 illustrates the process flow for the management of an audit programme.