INTERNATIONAL STANDARD

ISO 19011

Third edition
2018-07

Guidelines for auditing management systems

Lignes directrices pour l'audit des systèmes de management

Reference number
ISO 19011:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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 documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Project Committee ISO/PC 302, *Guidelines for auditing management systems*.

This third edition cancels and replaces the second edition (ISO 19011:2011), which has been technically revised.

The main differences compared to the second edition are as follows:

— addition of the risk-based approach to the principles of auditing;

— expansion of the guidance on managing an audit programme, including audit programme risk;

— expansion of the guidance on conducting an audit, particularly the section on audit planning;

— expansion of the generic competence requirements for auditors;

— adjustment of terminology to reflect the process and not the object ("thing");

— removal of the annex containing competence requirements for auditing specific management system disciplines (due to the large number of individual management system standards, it would not be practical to include competence requirements for all disciplines);

— expansion of Annex A to provide guidance on auditing (new) concepts such as organization context, leadership and commitment, virtual audits, compliance and supply chain.

Introduction

Since the second edition of this document was published in 2011, a number of new management system standards have been published, many of which 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 providing guidance that is more generic. Audit results can provide input to the analysis aspect of business planning, and can contribute to the identification of improvement needs and activities.

An audit can be conducted against a range of audit criteria, separately or in combination, including but not limited to:

— requirements defined in one or more management system standards;

— policies and requirements specified by relevant interested parties;

— statutory and regulatory requirements;

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

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

This document provides guidance for all sizes and types of organizations and audits of varying scopes and scales, including 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, complexity and scale 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; this document can provide useful additional guidance (see Table 1).

Table 1 — Different types of audits

1st party audit	2nd party audit	3rd party audit
Internal audit	External provider audit	Certification and/or accreditation audit
	Other external interested party audit	Statutory, regulatory and similar audit

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. Users of this document can, however, apply this guidance 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 auditor training or personnel certification.

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).

This document provides guidance on the management of an audit programme, on the planning and conducting of management system audits, as well as on the competence and evaluation of an auditor and an audit team.

Guidelines for auditing management systems

1 Scope

This document provides 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 activities include the individual(s) managing the audit programme, auditors and audit teams.

It is applicable to all organizations that need to plan and conduct internal or external 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.

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 terminological databases for use in standardization at the following addresses:

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

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

3.1
audit
systematic, independent and documented process for obtaining *objective evidence* (3.8) and evaluating it objectively to determine the extent to which the *audit criteria* (3.7) 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 or governmental agencies.

[SOURCE: ISO 9000:2015, 3.13.1, modified — Notes to entry have been modified]

3.2
combined audit
audit (3.1) carried out together at a single *auditee* (3.13) on two or more *management systems* (3.18)

Note 1 to entry: When two or more discipline-specific management systems are integrated into a single management system this is known as an integrated management system.

[SOURCE: ISO 9000:2015, 3.13.2, modified]

3.3
joint audit
audit (3.1) carried out at a single *auditee* (3.13) by two or more auditing organizations

[SOURCE: ISO 9000:2015, 3.13.3]

3.4
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

[SOURCE: ISO 9000:2015, 3.13.4, modified — wording has been added to the definition]

3.5
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, functions, organizational units, activities and processes, as well as the time period covered.

Note 2 to entry: A virtual location is where an organization performs work or provides a service using an on-line environment allowing individuals irrespective of physical locations to execute processes.

[SOURCE: ISO 9000:2015, 3.13.5, modified — Note 1 to entry has been modified, Note 2 to entry has been added]

3.6
audit plan
description of the activities and arrangements for an *audit* (3.1)

[SOURCE: ISO 9000:2015, 3.13.6]

3.7
audit criteria
set of *requirements* (3.23) used as a reference against which *objective evidence* (3.8) 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* (3.10).

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

[SOURCE: ISO 9000:2015, 3.13.7, modified — the definition has been changed and Notes to entry 1 and 2 have been added]

3.8
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.

Note 2 to entry: Objective evidence for the purpose of the *audit* (3.1) generally consists of records, statements of fact, or other information which are relevant to the *audit criteria* (3.7) and verifiable.

[SOURCE: ISO 9000:2015, 3.8.3]

3.9
audit evidence
records, statements of fact or other information, which are relevant to the *audit criteria* (3.7) and verifiable

[SOURCE: ISO 9000:2015, 3.13.8]

3.10
audit findings
results of the evaluation of the collected *audit evidence* (3.9) against *audit criteria* (3.7)

Note 1 to entry: Audit findings indicate *conformity* (3.20) or *nonconformity* (3.21).

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

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

[SOURCE: ISO 9000:2015, 3.13.9, modified — Notes to entry 2 and 3 have been modified]

3.11
audit conclusion
outcome of an *audit* (3.1), after consideration of the audit objectives and all *audit findings* (3.10)

[SOURCE: ISO 9000:2015, 3.13.10]

3.12
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* (3.13) or the individual(s) managing the audit programme. Requests for external audit can come from sources such as regulators, contracting parties or potential or existing clients.

[SOURCE: ISO 9000:2015, 3.13.11, modified — Note 1 to entry has been added]

3.13
auditee
organization as a whole or parts thereof being audited

[SOURCE: ISO 9000:2015, 3.13.12, modified]

3.14
audit team
one or more persons conducting an *audit* (3.1), supported if needed by *technical experts* (3.16)

Note 1 to entry: One *auditor* (3.15) of the *audit team* (3.14) is appointed as the audit team leader.

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

[SOURCE: ISO 9000:2015, 3.13.14]

3.15
auditor
person who conducts an *audit* (3.1)

[SOURCE: ISO 9000:2015, 3.13.15]

3.16
technical expert
<audit> person who provides specific knowledge or expertise to the *audit team* (3.14)

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

Note 2 to entry: A technical expert to the *audit team* (3.14) does not act as an *auditor* (3.15).

[SOURCE: ISO 9000:2015, 3.13.16, modified — Notes to entry 1 and 2 have been modified]

3.17
observer
individual who accompanies the *audit team* (3.14) but does not act as an *auditor* (3.15)

[SOURCE: ISO 9000:2015, 3.13.17, modified]

3.18
management system
set of interrelated or interacting elements of an organization to establish policies and objectives, and *processes* (3.24) 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 9000:2015, 3.5.3, modified — Note 4 to entry has been deleted]

3.19
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 and likelihood.

Note 3 to entry: Risk is often characterized by reference to potential events (as defined in ISO Guide 73:2009, 3.5.1.3) and consequences (as defined in ISO Guide 73:2009, 3.6.1.3), 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 (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

[SOURCE: ISO 9000:2015, 3.7.9, modified — Notes to entry 5 and 6 have been deleted]

3.20
conformity
fulfilment of a *requirement* (3.23)

[SOURCE: ISO 9000:2015, 3.6.11, modified — Note 1 to entry has been deleted]

3.21
nonconformity
non-fulfilment of a *requirement* (3.23)

[SOURCE: ISO 9000:2015, 3.6.9, modified — Note 1 to entry has been deleted]

3.22
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO 9000:2015, 3.10.4, modified — Notes to entry have been deleted]

3.23
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, for example in documented information.

[SOURCE: ISO 9000:2015, 3.6.4, modified — Notes to entry 3, 4, 5 and 6 have been deleted]

3.24
process
set of interrelated or interacting activities that use inputs to deliver an intended result

[SOURCE: ISO 9000:2015, 3.4.1, modified — Notes to entry have been deleted]

3.25
performance
measurable result

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

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.24), products, services, systems or organizations.

[SOURCE: ISO 9000:2015, 3.7.8, modified — Note 3 to entry has been deleted]

3.26
effectiveness
extent to which planned activities are realized and planned results achieved

[SOURCE: ISO 9000:2015, 3.7.11, modified — Note 1 to entry has been deleted]

4 Principles of auditing

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 a prerequisite for providing 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 below.

a) Integrity: the foundation of professionalism

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

   — perform their work ethically, with honesty and responsibility;

   — only undertake audit activities if competent to do so;

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

   — be sensitive to any influences that may be exerted on their judgement while carrying out an audit.

b) Fair presentation: the obligation to report truthfully and accurately

   Audit findings, audit conclusions and audit reports should reflect truthfully and accurately the audit 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.

c) Due professional care: the application of diligence and judgement in auditing

Auditors should exercise due care in accordance with 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.

d) Confidentiality: security of information

Auditors should exercise discretion in the use and protection of information acquired in the course of their duties. 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 concept includes the proper handling of sensitive or confidential information.

e) Independence: 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. For internal audits, auditors should be independent from the function being audited if practicable. Auditors should maintain objectivity throughout the audit process to ensure that the audit findings and conclusions are based only on the audit evidence.

For small organizations, it may not be possible for internal auditors to be fully independent of the activity being audited, but every effort should be made to remove bias and encourage objectivity.

f) Evidence-based approach: the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process

Audit evidence should be verifiable. It should in general be based on samples of the information available, since an audit is conducted during a finite period of time 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.

g) Risk-based approach: an audit approach that considers risks and opportunities

The risk-based approach should substantively influence 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 which 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 nature, functionality, complexity, the type of risks and opportunities, and the level of maturity of the management system(s) to be audited.

The functionality of the management system can be even more complex when most of the important functions are outsourced and managed under the leadership of other organizations. Particular attention needs to be paid to where the most important decisions are made and what constitutes the top management of the management system.

