SLOVENSKI STANDARD
oSIST prEN ISO 19011:2017

01-oktober-2017

Smernice za presojanje sistemov vodenja (ISO/DIS 19011:2017)

Guidelines for auditing management systems (ISO/DIS 19011:2017)

Leitfaden zur Auditierung von Managementsystemen (ISO/DIS 19011:2017)

Lignes directrices pour l'audit des systèmes de management (ISO/DIS 19011:2017)

Ta slovenski standard je istoveten z: prEN ISO 19011

ICS:

03.100.70	Sistemi vodenja	Management systems
03.120.10	Vodenje in zagotavljanje kakovosti	Quality management and quality assurance
13.020.10	Ravnanje z okoljem	Environmental management

oSIST prEN ISO 19011:2017 **en,fr,de**

DRAFT INTERNATIONAL STANDARD
ISO/DIS 19011

ISO/PC **302** Secretariat: **ANSI**

Voting begins on: **2017-08-03** Voting terminates on: **2017-10-25**

Guidelines for auditing management systems

Lignes directrices pour l'audit des systèmes de management

ICS: 03.120.10; 03.100.70; 13.020.10

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 19011:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 19011 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 difference compared with the second edition is as follows:

– updated requirements relating to audit plans; now the output of the audit planning process.

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.

Audits 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 other parties;
- legal 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 users, including small and medium-sized organizations, and concentrates on internal audits (first party), and audits conducted by organizations on their external providers (second party). This document can also be useful for external audits conducted for purposes other than third party management system certification. ISO/IEC 17021-1:2015 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 auditing

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

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

Organizations can operate or use more than one management system.

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 particular situation. This also applies to the use of “person” and “persons”, “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 audits of management systems 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 and on the nature and complexity of the organization to be audited, as well as on the objectives and scope of the audits to be conducted.

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

Clause 3 sets out the key terms and definitions used in this document. All efforts have been taken to ensure that these definitions do not conflict with definitions used in other standards.

In this document the following terms are also used:

-should – indicates a recommendation;

-can – indicates a possibility or a capability;

-may – indicates a permission.

Clause 4 describes the principles on which auditing is based. These principles help the user to understand the essential nature of auditing and are important in understanding the guidance set out in Clauses 5 to 7.

Clause 5 provides guidance on establishing and managing an audit programme, establishing the audit programme objectives, and coordinating auditing activities.

Clause 6 provides guidance on planning and conducting an audit of a management system.

Clause 7 provides guidance relating to the competence and evaluation of management system auditors and audit teams.

Annex A provides additional guidance for auditors on planning and conducting audits.

Guidelines for auditing management systems

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 people may include the person(s) managing the audit programme, auditors and audit teams.

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

The application of this document to other types of audits (including against criteria related to product services, contracts, supply chains) 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.

3.1
audit
systematic, independent and documented process for obtaining **audit evidence** (3.3) and evaluating it objectively to determine the extent to which the **audit criteria** (3.2) are fulfilled

NOTE 1 to entry: Internal audits, sometimes called first party audits, are conducted by the organization itself, or on its behalf, for management review and other internal purposes (e.g. to confirm the effectiveness of the management system or to obtain information for the improvement of the management system). Internal audits can form the basis for an organization’s self-declaration of conformity. In many cases, particularly in small organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited or freedom from bias and conflict of interest.

NOTE 2 to entry: External audits include second and third party audits. Second party audits are conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf. Third party audits are conducted by independent auditing organizations, such as regulators or those providing certification.

NOTE 3 to entry: When two or more management systems of different disciplines (e.g. quality, environmental, occupational health and safety) are audited together, this is termed a combined audit.

NOTE 4 to entry: When two or more auditing organizations cooperate to audit a single **auditee** (3.7), this is termed a joint audit.

[SOURCE: ISO 9000:2015, 3.13.1, modified — Notes 3 and 4 to entry added]

3.2
audit criteria
set of requirements used as a reference against which **audit evidence** (3.3) 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** (3.4).

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

[SOURCE: ISO 9000:2015, 3.13.7, modified, and Notes 1 and 2 to entry added]

3.3
audit evidence
records, statements of fact or other information which are relevant to the **audit criteria** (3.2) and verifiable

NOTE to entry:Audit evidence can be qualitative or quantitative.

[SOURCE: ISO 9000:2015, 3.13.8, modified — Note to entry added]

3.4
audit findings
results of the evaluation of the collected **audit evidence** (3.3) against **audit criteria** (3.2)

NOTE 1 to entry:Audit findings indicate **conformity** (3.18) or **nonconformity** (3.19).

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

NOTE 3 to entry:If the audit criteria are selected from legal or other requirements, the audit finding is termed compliance or non-compliance.

[SOURCE: ISO 9000:2015, 3.13.9]

3.5
audit conclusion
outcome of an **audit** (3.1), after consideration of the audit objectives and all **audit findings** (3.4)

[SOURCE: ISO 9000:2015, 3.13.10]

3.6
audit client
organization or person requesting an **audit** (3.1)

NOTE to entry:In the case of internal audit, the audit client can also be the **auditee** (3.7) or the person(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 to entry added]

3.7
auditee
organization being audited

[SOURCE: ISO 9000:2015, 3.13.12]

3.8

auditor

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

[SOURCE: ISO 9000:2015, 3.13.15]

3.9

audit team

one or more persons conducting an **audit** (3.1), supported if needed by **technical experts** (3.10)

NOTE 1 to entry:One **auditor** (3.8) of the audit team 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, NOTE 2 modified]

3.10

technical expert

person who provides specific knowledge or expertise to the **audit team** (3.9)

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 in the **audit team** (3.9) does not act as an **auditor** (3.8).

[SOURCE: ISO 9000:2015, 3.13.16, Notes 1 and 2 modified]

3.11

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]

3.12

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, 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 persons irrespective of physical locations to execute processes.

[SOURCE: ISO 9000:2015, 3.13.5, modified — Notes to entry added]

3.13

audit plan

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

[SOURCE: ISO 9000:2015, 3.13.6]

3.14

risk

effect of uncertainty

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

3.15
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]

3.16
conformity
fulfilment of a requirement

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

3.17
nonconformity
non-fulfilment of a requirement

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

3.18
management system
set of interrelated or interacting elements of an organization to establish policies and objectives, and processes 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 deleted]

3.19
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.

3.20
process
set of interrelated or interacting activities that use inputs to deliver the intended output

3.21
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** (3.20), products (including services), systems or organizations.

3.22

effectiveness

extent to which planned activities are realized and planned results achieved

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 person(s) managing an audit programme should:

- perform their work with honesty, diligence, and responsibility;
- observe and comply with any applicable legal requirements;
- demonstrate their competence while performing their work;
- 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 reporting output 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 operating managers of the function being audited. Auditors should maintain objectivity throughout the audit process to ensure that the audit findings and conclusions are based only on the audit evidence.