



**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**

<https://standards.iteh.ai/catalog/standards/sist/ea0a6e90-5b92-4dae-99a1-3af3834c8757/sist-en-iso-19011-2018>

**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

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

[SIST EN ISO 19011:2018](https://standards.iteh.ai/catalog/standards/sist/ea0a6e90-5b92-4dae-99a1-3af3834c8757/sist-en-iso-19011-2018)

<https://standards.iteh.ai/catalog/standards/sist/ea0a6e90-5b92-4dae-99a1-3af3834c8757/sist-en-iso-19011-2018>

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)

# iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO 19011:2018

<https://standards.iteh.ai/catalog/standards/sist/ea0a6e90-5b92-4dae-99a1-3af3834c8757/sist-en-iso-19011-2018>



## **COPYRIGHT PROTECTED DOCUMENT**

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Principles of auditing .....	5
5	Managing an audit programme .....	6
5.1	General .....	6
5.2	Establishing the audit programme objectives.....	9
5.3	Determining and evaluating audit programme risks and opportunities .....	10
5.4	Establishing the audit programme .....	10
5.4.1	Roles and responsibilities of the person(s) managing the audit programme .....	10
5.4.2	Competence of the person(s) managing the audit programme.....	11
5.4.3	Establishing the extent of the audit programme.....	11
5.4.4	Determining audit programme resources.....	12
5.5	Implementing the audit programme .....	13
5.5.1	General .....	13
5.5.2	Defining the objectives, scope and criteria for an individual audit .....	13
5.5.3	Selecting the audit methods.....	14
5.5.4	Selecting the audit team members .....	14
5.5.5	Assigning responsibility for an individual audit to the audit team leader .....	15
5.5.6	Managing the audit programme outcome.....	16
5.5.7	Managing and maintaining audit programme records .....	17
5.6	Monitoring the audit programme .....	17
5.7	Reviewing and improving the audit programme .....	18
6	Conducting an audit.....	19
6.1	General .....	19
6.2	Initiating the audit.....	19
6.2.1	General .....	19
6.2.2	Establishing contact with the auditee .....	19
6.2.3	Determining the feasibility of the audit .....	19
6.3	Preparing audit activities.....	20
6.3.1	Performing review of documented information .....	20
6.3.2	Audit planning .....	20
6.3.3	Assigning work to the audit team.....	22
6.3.4	Preparing documented information for the audit .....	22
6.4	Conducting the audit activities .....	22
6.4.1	General .....	22
6.4.2	Assigning roles and responsibilities of guides and observers.....	22
6.4.3	Conducting the opening meeting .....	23
6.4.4	Communicating during the audit.....	24
6.4.5	Audit information availability and access.....	24
6.4.6	Reviewing documented information while conducting the audit.....	25
6.4.7	Collecting and verifying information.....	25
6.4.8	Generating audit findings .....	26
6.4.9	Determining audit conclusions.....	27
6.4.10	Conducting the closing meeting.....	27
6.5	Preparing and distributing the audit report.....	28
6.5.1	Preparing the audit report .....	28
6.5.2	Distributing the audit report .....	29
6.6	Completing the audit.....	29
6.7	Conducting audit follow-up.....	30
7	Competence and evaluation of auditors .....	30

## ISO/DIS 19011:2017(E)

7.1	General.....	30
7.2	Determining auditor competence.....	31
7.2.1	General.....	31
7.2.2	Personal behaviour.....	31
7.2.3	Knowledge and skills .....	32
7.2.4	Achieving auditor competence .....	34
7.2.5	Audit team leaders.....	35
7.3	Establishing the auditor evaluation criteria .....	35
7.4	Selecting the appropriate auditor evaluation method .....	35
7.5	Conducting auditor evaluation.....	35
7.6	Maintaining and improving auditor competence.....	36
Annex A (informative) Additional guidance for auditors for planning and conducting audits .....		37
A.1	Applying audit methods.....	37
A.2	Methods of auditing.....	38
A.3	Professional judgement .....	38
A.4	Performance outcomes.....	38
A.5	Verifying information.....	39
A.6	Sampling.....	39
A.6.1	General.....	39
A.6.2	Judgement-based sampling .....	40
A.6.3	Statistical sampling .....	40
A.7	Auditing risks and opportunities .....	41
A.8	Life cycle.....	41
A.9	Preparing audit work documents.....	42
A.10	Selecting sources of information.....	42
A.11	Guidance on visiting the auditee's location .....	43
A.12	Conducting interviews .....	44
A.13	Audit findings.....	44
A.13.1	Determining audit findings .....	44
A.13.2	Recording conformities .....	45
A.13.3	Recording nonconformities.....	45
A.13.4	Dealing with findings related to multiple criteria .....	45

## 1 Foreword

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

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

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

12 Attention is drawn to the possibility that some of the elements of this document may be the subject of patent  
13 rights. ISO shall not be held responsible for identifying any or all such patent rights.

14 ISO 19011 was prepared by Project Committee ISO/PC 302, *Guidelines for auditing management systems*.

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

17 The main difference compared with the second edition is as follows:

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

SIST EN ISO 19011:2018

<https://standards.iteh.ai/catalog/standards/sist/ea0a6e90-5b92-4dae-99a1-3af3834c8757/sist-en-iso-19011-2018>

## ISO/DIS 19011:2017(E)

19 **Introduction**

20 Since the second edition of this document was published in 2011, a number of new management system  
21 standards have been published, many of which have a common structure, identical core requirements and  
22 common terms and core definitions. As a result, there is a need to consider a broader approach to  
23 management system auditing, as well as providing guidance that is more generic.

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

- 26 – requirements defined in one or more management system standards;
- 27 – policies and requirements specified by other parties;
- 28 – legal requirements;
- 29 – one or more management system processes defined by the organization or other parties;
- 30 – management system plan(s) relating to the provision of specific outputs of a management system (e.g.  
31 quality plan, project plan).

32 This document provides guidance for all users, including small and medium-sized organizations, and  
33 concentrates on internal audits (first party), and audits conducted by organizations on their external providers  
34 (second party). This document can also be useful for external audits conducted for purposes other than third  
35 party management system certification. ISO/IEC 17021-1:2015 provides requirements for auditing  
36 management systems for third party certification; however, this document can provide useful additional  
37 guidance (see Table 1).

38 .

39 **Table 1 — Different types of auditing**

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

41

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

45 Organizations can operate or use more than one management system.

46 To simplify the readability of this document, the singular form of “management system” is preferred, but the  
47 reader can adapt the implementation of the guidance to their own particular situation. This also applies to the  
48 use of “person” and “persons”, “auditor” and “auditors”.

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



53 The guidance in this document can also be used for the purpose of self-declaration, and can be useful to  
54 organizations involved in auditor training or personnel certification.

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

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

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

64 In this document the following terms are also used:

65 -should – indicates a recommendation;

66 -can – indicates a possibility or a capability;

67 -may – indicates a permission.

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

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

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

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

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



## 76 Guidelines for auditing management systems

## 77 Guidelines for auditing management systems

### 78 1 Scope

79 This document provides guidance on auditing management systems, including the principles of auditing,  
80 managing an audit programme and conducting management system audits, as well as guidance on the  
81 evaluation of competence of individuals involved in the audit process. These people may include the person(s)  
82 managing the audit programme, auditors and audit teams.

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

85 The application of this document to other types of audits (including against criteria related to product services,  
86 contracts, supply chains) is possible, provided that special consideration is given to the specific competence  
87 needed.

### 88 2 Normative references

89 There are no normative references in this document.

### 90 3 Terms and definitions

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

#### 92 3.1

##### 93 audit

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

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

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

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

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

**ISO/DIS 19011:2017(E)**

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

**3.2****audit criteria**

110 set of requirements used as a reference against which **audit evidence** (3.3) is compared

112 NOTE 1 to entry: If the audit criteria are legal (including statutory or regulatory) requirements, the words “compliance” or  
113 “non-compliance” are often used in an **audit finding** (3.4).

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

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

**3.3****audit evidence**

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

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

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

**3.4****audit findings**

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

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

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

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

130 [SOURCE: ISO 9000:2015, 3.13.9]

**3.5****audit conclusion**

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

134 [SOURCE: ISO 9000:2015, 3.13.10]

**3.6****audit client**

136 organization or person requesting an **audit** (3.1)

138 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  
139 audit programme. Requests for external audit can come from sources such as regulators, contracting parties or potential  
140 or existing clients.

141 [SOURCE: ISO 9000:2015, 3.13.11, modified — Note to entry added]

**3.7****auditee**

143 organization being audited

145 [SOURCE: ISO 9000:2015, 3.13.12]

- 146 **3.8**  
147 **auditor**  
148 person who conducts an **audit** (3.1)
- 149 [SOURCE: ISO 9000:2015, 3.13.15]
- 150 **3.9**  
151 **audit team**  
152 one or more persons conducting an **audit** (3.1), supported if needed by **technical experts** (3.10)
- 153 NOTE 1 to entry: One **auditor** (3.8) of the audit team is appointed as the audit team leader.
- 154 NOTE 2 to entry: The audit team can include auditors-in-training.
- 155 [SOURCE: ISO 9000:2015, 3.13.14, NOTE 2 modified]
- 156 **3.10**  
157 **technical expert**  
158 person who provides specific knowledge or expertise to the **audit team** (3.9)
- 159 NOTE 1 to entry: Specific knowledge or expertise relates to the organization, the activity, process, product, service,  
160 discipline to be audited, or language or culture.
- 161 NOTE 2 to entry: A technical expert in the **audit team** (3.9) does not act as an **auditor** (3.8).
- 162 [SOURCE: ISO 9000:2015, 3.13.16, Notes 1 and 2 modified]
- 163 **3.11**  
164 **audit programme**  
165 arrangements for a set of one or more **audits** (3.1) planned for a specific time frame and directed towards a  
166 specific purpose
- 167 [SOURCE: ISO 9000:2015, 3.13.4, modified]
- 168 **3.12**  
169 **audit scope**  
170 extent and boundaries of an **audit** (3.1)
- 171 NOTE 1 to entry: The audit scope generally includes a description of the physical and virtual locations, functions, activities  
172 and processes, as well as the time period covered.
- 173 NOTE 2 to entry: A virtual location is where an organization performs work or provides a service using an on-line  
174 environment allowing persons irrespective of physical locations to execute processes.
- 175 [SOURCE: ISO 9000:2015, 3.13.5, modified — Notes to entry added]
- 176 **3.13**  
177 **audit plan**  
178 description of the activities and arrangements for an **audit** (3.1)
- 179 [SOURCE: ISO 9000:2015, 3.13.6]
- 180 **3.14**  
181 **risk**  
182 effect of uncertainty
- 183 [SOURCE: ISO 9000:2015, 3.7.9, modified — Notes to entry have been deleted]

**ISO/DIS 19011:2017(E)**

- 184 **3.15**  
 185 **competence**  
 186 ability to apply knowledge and skills to achieve intended results
- 187 [SOURCE: ISO 9000:2015, 3.10.4, modified — Notes to entry have been deleted]
- 188 **3.16**  
 189 **conformity**  
 190 fulfilment of a requirement
- 191 [SOURCE: ISO 9000:2015, 3.6.11, modified — Note to entry has been deleted]
- 192 **3.17**  
 193 **nonconformity**  
 194 non-fulfilment of a requirement
- 195 [SOURCE: ISO 9000:2015, 3.6.9, modified – Note to entry has been deleted]
- 196 **3.18**  
 197 **management system**  
 198 set of interrelated or interacting elements of an organization to establish policies and objectives, and  
 199 processes to achieve those objectives
- 200 NOTE 1 to entry: A management system can address a single discipline or several disciplines, e.g. quality management,  
 201 financial management or environmental management.
- 202 NOTE 2 to entry: The management system elements establish the organization's structure, roles and responsibilities,  
 203 planning, operation, policies, practices, rules, beliefs, objectives and processes to achieve those objectives.
- 204 NOTE 3 to entry: The scope of a management system can include the whole of the organization, specific and identified  
 205 functions of the organization, specific and identified sections of the organization, or one or more functions across a group  
 206 of organizations.
- 207 [SOURCE: ISO 9000:2015, 3.5.3, modified, NOTE 4 to entry deleted]
- 208 **3.19**  
 209 **requirement**  
 210 need or expectation that is stated, generally implied or obligatory
- 211 NOTE 1 to entry: "Generally implied" means that it is custom or common practice for the organization and interested  
 212 parties that the need or expectation under consideration is implied.
- 213 NOTE 2 to entry: A specified requirement is one that is stated, for example in documented information.
- 214 **3.20**  
 215 **process**  
 216 set of interrelated or interacting activities that use inputs to deliver the intended output
- 217 **3.21**  
 218 **performance**  
 219 measurable result
- 220 NOTE 1 to entry: Performance can relate either to quantitative or qualitative findings.
- 221 NOTE 2 to entry: Performance can relate to the management of activities, **processes** (3.20), products (including services),  
 222 systems or organizations.
- 223 **3.22**

224 **effectiveness**  
225 extent to which planned activities are realized and planned results achieved  
226

## 227 **4 Principles of auditing**

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

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

234 a) **Integrity:** the foundation of professionalism

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

- 236 – perform their work with honesty, diligence, and responsibility;
- 237 – observe and comply with any applicable legal requirements;
- 238 – demonstrate their competence while performing their work;
- 239 – perform their work in an impartial manner, i.e. remain fair and unbiased in all their dealings;
- 240 – be sensitive to any influences that may be exerted on their judgement while carrying out an audit.

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

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

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

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

251 d) **Confidentiality:** security of information

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

256 e) **Independence:** the basis for the impartiality of the audit and objectivity of the audit conclusions

257 Auditors should be independent of the activity being audited wherever practicable, and should in all cases  
258 act in a manner that is free from bias and conflict of interest. For internal audits, auditors should be  
259 independent from the operating managers of the function being audited. Auditors should maintain  
260 objectivity throughout the audit process to ensure that the audit findings and conclusions are based only  
261 on the audit evidence.