



DRAFT INTERNATIONAL STANDARD ISO/DIS 19011

ISO/TC 176/SC 3

Secretariat: NEN

Voting begins on:
2010-06-17

Voting terminates on:
2010-11-17

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Guidelines for auditing management systems

Lignes directrices pour l'audit des systèmes de management

[Revision of first edition (ISO 19011:2002)]

ICS 03.120.10; 13.020.10

ISO/CEN PARALLEL PROCESSING

This draft has been developed within the International Organization for Standardization (ISO), and processed under the **ISO-lead** mode of collaboration as defined in the Vienna Agreement.

This draft is hereby submitted to the ISO member bodies and to the CEN member bodies for a parallel five-month enquiry.

Should this draft be accepted, a final draft, established on the basis of comments received, will be submitted to a parallel two-month approval vote in ISO and formal vote in CEN.

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

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.

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

29	Contents	Page
30	Foreword	v
31	Introduction	vi
32	1 Scope	1
33	2 Normative references	1
34	3 Terms and definitions	1
35	4 Principles of auditing	3
36	5 Managing an audit programme	5
37	5.1 General	5
38	5.2 Establishing the audit programme	6
39	5.2.1 Developing the programme objectives	6
40	5.2.2 Role and responsibility of the person(s) managing audit programme(s)	7
41	5.2.3 Competence of the person responsible for managing audit programme(s)	7
42	5.2.4 Determining the extent of an audit programme	8
43	5.2.5 Evaluating audit programme risks	8
44	5.2.6 Establishing audit programme procedures	9
45	5.2.7 Identifying audit programme resources	9
46	5.3 Implementing the audit programme	9
47	5.3.1 General	9
48	5.3.2 Defining individual audit objectives, scope and criteria	10
49	5.3.3 Determining the audit method(s)	10
50	5.3.4 Selecting the audit team	11
51	5.3.5 Assigning responsibility for individual audit(s) to the audit team leader	12
52	5.3.6 Managing and maintaining audit programme records	12
53	5.4 Audit programme monitoring	13
54	5.5 Reviewing and improving audit programmes	14
55	6 Audit activities	14
56	6.1 General	14
57	6.2 Initiating the audit	15
58	6.2.1 General	15
59	6.2.2 Establishing initial contact with the auditee	15
60	6.2.3 Determining the feasibility of the audit	16
61	6.3 Preparing for the audit activities	16
62	6.3.1 Preparing the audit plan	16
63	6.3.2 Assigning work to the audit team	17
64	6.3.3 Preparing work documents	17
65	6.4 Conducting audit activities	18
66	6.4.1 Document review	18
67	6.4.2 Conducting opening meeting	18
68	6.4.3 Communication during the audit	19
69	6.4.4 Roles and responsibilities of guides and observers	19
70	6.4.5 Collection and verification of information	20
71	6.4.6 Audit findings	21
72	6.4.7 Audit conclusions	22
73	6.4.8 Conducting the closing meeting	22
74	6.5 Preparing and distributing the audit report	23
75	6.5.1 Preparing the audit report	23
76	6.5.2 Distributing the audit report	24
77	6.6 Completing the audit	24
78	6.7 Conducting audit follow-up	24

79	7	Competence and evaluation of auditors	25
80	7.1	General.....	25
81	7.2	Determine auditor competence to meet the needs of the audit programme.....	25
82	7.2.1	Personal behaviours	26
83	7.2.2	Knowledge and skills	26
84	7.2.3	Education, work experience, training and audit experience of auditors	29
85	7.3	Establish the evaluation criteria	29
86	7.4	Select the appropriate evaluation method	29
87	7.5	Conduct the evaluation	30
88	7.6	Maintenance and improvement of competence	30
89	Annex A (Informative)	Discipline-specific knowledge and skills of auditors	32
90	A.1	General.....	32
91	A.2	Discipline-specific knowledge and skills of auditors – Quality	32
92	A.3	Discipline-specific knowledge and skills of auditors – Environmental	33
93	A.4	Discipline-specific knowledge and/or skills of auditors – Occupational health and safety	
94		(OH&S)	35
95	A.5	The discipline-specific knowledge and/or skills of auditors – Resilience, security, preparedness	
96		and continuity (RSPC) management	36
97	A.6	The discipline-specific knowledge and/or skills of auditors - Discipline: Transportation safety	
98		management.....	38
99	A.7	Discipline-specific knowledge and skills of auditors – Records.....	39
100	Annex B (Informative)	Examples of discipline specific evaluations of audit team competence	42
101	B.1	General.....	42
102	B.2	Application of the evaluation process for an audit team undertaking an internal audit of an	
103		aviation organization’s quality and environmental management systems	43
104	B.3	Application of the evaluation process for an audit team undertaking an internal audit of an	
105		event management organization’s Quality and OH&S management systems.....	49
106	B.4	Application of the evaluation process for an auditor in a hypothetical resilience, security,	
107		preparedness and/or continuity management internal audit programme.....	52
108	Annex C (Informative)	Additional Guidance for Auditors for Planning and Conducting Audits	61
109	C.1	Applying audit methods.....	61
110	C.2	Sources of information	62
111	C.3	Conducting document review	62
112	C.4	Preparing Work Documents	63
113	C.5	Sampling strategy considerations for audits	63
114	C.6	Guidance for site visits and observations	65
115	C.7	Conducting interviews	66
116	C.8	Audit findings.....	66
117	Bibliography		68
118			

119 Foreword

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

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

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

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

132 ISO 19011 was prepared by Technical Committee ISO/TC 176, *Quality management and quality assurance*,
133 Subcommittee SC 3, *Supporting technologies*.

134 ISO 19011:2011 was prepared under the auspices of the Joint Technical Coordination Group and administered by
135 Technical Committee ISO/TC 176, Quality management and quality assurance, Subcommittee SC 3, Supporting
136 technologies. Members of Working Group 16 under TC 176/SC 3 included representatives of other technical
137 committees (e.g., TC 207, TC 34) and other interested parties for the management systems included within the
138 scope of this standard.

139 This second edition of ISO 19011 cancels and replaces ISO 19011: 2002 which has been technically revised.

140

141 Introduction

142 Since the initial publication of ISO 19011 in 2002, a number of new management system standards have been
143 published. This has resulted in a need to consider a broader scope of management system auditing as well as
144 provide guidance that is more generic.

145 In 2006, ISO CASCO developed a standard with requirements for 3rd party management system certification audit
146 purposes in ISO/IEC 17021.

147 It is in this context that this revision of ISO 19011 provides guidance for all users, including small and medium sized
148 enterprises, specially concentrating on what are commonly termed internal (first party) and second party audit.

149 This International Standard does not state requirements but provides guidance on the management of audit
150 programmes and on the conduct of audits of management systems, as well as on the competence and evaluation of
151 auditors and audit teams. Users of this International Standard may, however, apply this guidance in developing their
152 own audit-related requirements.

153 This guidance is intended to apply to a broad range of potential users, including auditors, organizations
154 implementing management systems, and organizations needing to conduct audits of management systems for
155 contractual or regulatory reasons. It may also be used for the purpose self-declaration. It may also be useful to
156 organizations involved in auditor training or certification

157 The guidance in this International Standard is intended to be flexible. As indicated at various points in the text, the
158 use of this guidance may differ according to the size, level of maturity of an organizations' management system, the
159 nature and complexity of the organization to be audited, as well as the objectives and scope of the audits to be
160 conducted.

161 In this International Standard, Clause 4 describes the principles on which credible auditing is based. These
162 principles help the user to understand the essential nature of auditing and they are important to understanding the
163 guidance set out in Clauses 5 to 7.

164 Clause 5 provides guidance on the establishment and management of audit programmes, including establishing the
165 audit programme objectives, and coordinating auditing activities.

166 Clause 6 provides guidance on conducting audits of management systems.

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

169 Annex A illustrates the application of the guidance in Clause 7 to different disciplines (e.g. quality, environmental,
170 occupational health and safety, resilience, security, preparedness and continuity management and transportation
171 safety management).

172 Annex B provides examples of the evaluation of audit team competencies in various hypothetical organizations in
173 different sectors (e.g. aviation, event management).

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

Guidelines for auditing management systems

1 Scope

This International Standard provides guidance on auditing management systems, including the principles of auditing, managing audit programmes and conducting management system audits, as well as guidance on the evaluation of competence of individuals involved in the audit process including those responsible for audit programme management, auditors and audit teams.

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

The application of this International Standard to other types of audit is possible, provided that special consideration is paid to the specific competences needed.

2 Normative references

Where standards or other documents have been used or referred to (e.g. for some definitions in clause 3) it was decided to include the original text in the present International standard in order to create a stand-alone document.

A bibliography at the end of this present International standard lists these documents as well as other useful source material.

3 Terms and definitions

For the purposes of this document, the following terms and definitions given below apply. All efforts have been taken that these definitions should not conflict with the definitions used in other management system standards.

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 Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself for management review and other internal purposes (e.g. to confirm the intended operation of the management system or to obtain information for improvement of the management system), and may form the basis for an organization's self-declaration of conformity. In many cases, particularly in smaller 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 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 registration or certification.

NOTE 3 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 When two or more auditing organizations cooperate to audit a single **auditee** (3.7), this is termed a joint audit.

- 209 **3.2**
210 **audit criteria**
211 set of policies, procedures or requirements
- 212 NOTE 1 Audit criteria are used as a reference against which **audit evidence** (3.3) is compared.
- 213 NOTE 2 If the audit criteria are selected from legal or other requirements, the audit finding (3.4) is termed compliance or non-
214 compliance.
- 215 NOTE 3 If the audit criteria are selected from standards (internal or external), the audit finding (3.4) is termed a **conformity**
216 (3.16) or **nonconformity** (3.17).
- 217 **3.3**
218 **audit evidence**
219 records, statements of fact or other information, which are relevant to the **audit criteria** (3.2) and verifiable
- 220 NOTE Audit evidence may be qualitative or quantitative.
- 221 **3.4**
222 **audit findings**
223 results of the evaluation of the collected **audit evidence** (3.3) against **audit criteria** (3.2)
- 224 NOTE Audit findings may indicate **conformity** (3.16), **nonconformity** (3.17), and opportunities for improvement or good
225 practices.
- 226 **3.5**
227 **audit conclusion**
228 outcome of an **audit** (3.1), after consideration of the audit objectives and all **audit findings** (3.4)
- 229 **3.6**
230 **audit client**
231 organization or person requesting an **audit** (3.1)
- 232 NOTE The audit client may be the **auditee** (3.7) or any other organization which has the regulatory or contractual right to
233 request an audit.
- 234 **3.7**
235 **auditee**
236 organization being audited
- 237 **3.8**
238 **auditor**
239 person who conducts an **audit** (3.1)
- 240 **3.9**
241 **audit team**
242 one or more **auditors** (3.8) conducting an **audit** (3.1), supported if needed by **technical experts** (3.15)
- 243 NOTE 1 One auditor of the audit team is appointed as the audit team leader.
- 244 NOTE 2 The audit team may include auditors-in-training.
- 245 **3.10**
246 **audit programme**
247 arrangements for a set of one or more **audits** (3.1) planned for a specific time frame and directed towards a
248 specific purpose
- 249 **3.11**
250 **audit plan**
251 description of the activities and arrangements for an **audit** (3.1)

252 **3.12**
 253 **risk**
 254 effect of uncertainty on objectives

255 [ISO 31000:2009, 2.1]

256 **3.13**
 257 **audit scope**
 258 extent and boundaries of an **audit** (3.1)

259 NOTE The audit scope generally includes a description of the physical locations, organizational units, activities and
 260 processes, as well as the time period covered.

261 **3.14**
 262 **competence**
 263 ability to apply knowledge and skills to achieve intended results.

264 NOTE ability implies the appropriate application of personal behaviour during the audit process

265 **3.15**
 266 **technical expert**
 267 person who provides specific knowledge or expertise to the **audit team** (3.9)

268 NOTE 1 Specific knowledge or expertise is that which relates to the organization, the process or activity to be audited, or
 269 language or culture.

270 NOTE 2 A technical expert does not act as an **auditor** (3.8) in the audit team.

271 **3.16**
 272 **conformity**
 273 fulfilment of a requirement

274 [ISO 9000:2005, 3.6.1]

275 **3.17**
 276 **nonconformity**
 277 non-fulfilment of a requirement

278 [ISO 9000:2005 3.6.2]

279 **3.18**
 280 **guide**
 281 person appointed by the auditee to assist the audit team

282 **4 Principles of auditing**

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

288 The following principles relate to auditors and those who manage the audit programme(s).

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

290 Auditors and those who manage the audit programme(s) should:

- 291 — perform their work with honesty, diligence, and responsibility;
- 292 — observe and respect any applicable legal requirements;
- 293 — demonstrate their technical competence while undertaking their work;
- 294 — perform their work in an impartial manner, i.e. remain fair and unbiased in all their dealings;
- 295 — be sensitive to any influences that may be exerted by other interested parties on their judgment while
- 296 carrying out an audit.

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

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

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

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

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

307 Auditors should be prudent in the use and protection of information acquired in the course of their duties. Audit
308 information should not be used inappropriately for the personal gain by the auditor or the audit client or in a
309 manner detrimental to the legitimate interest of the auditee. This concept includes the proper handling of
310 sensitive, confidential or classified information.

311 The following two principles relate to the audit, which is by definition an independent and systematic activity.

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

313 Auditors should be independent of the activity being audited and act in a manner that is free from bias and
314 conflict of interest wherever possible. For internal audits, auditors should be independent from the operating
315 managers of the function(s) being audited. Auditors should maintain an objective state of mind throughout the
316 audit process to ensure that the audit findings and conclusions are based only on the audit evidence.

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

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

321 Audit evidence is verifiable. It is based on samples of the information available, since an audit is conducted
322 during a finite period of time and with finite resources. The appropriate use of sampling is closely related to the
323 confidence that can be placed in the audit conclusions.

324 The guidance given in the remaining clauses of this International Standard is based on the principles set out above.

325 5 Managing an audit programme

326 5.1 General

327 An organization needing to conduct audits should establish an audit programme(s). The audit client should set the
328 objective(s) to be achieved by the audit programme(s). The programme(s) should be able to determine the
329 effectiveness of the auditee's management system in meeting its objectives.

330 The audit client should assign (a) competent person(s) with responsibility for managing the audit programme(s).

331 The programme should be adequately and effectively established and implemented. The audit programme should
332 include planning the types and number of audits needed, as well as providing information and resources necessary
333 to organize and conduct its audits effectively and efficiently within the specified time frames.

334 The extent of an audit programme should be based on the size and nature of the auditee as well as on the nature,
335 functionality, complexity and the level of maturity of the management system to be audited. Priority should be given
336 to allocating the audit programme resources to audit those matters of significance within the management system.
337 These may include the key characteristics of product or service quality, safety and health hazards and risks and
338 significant environmental aspects and their control.

339 NOTE This concept is commonly known as risk-based auditing.

340 The audit programme(s) can include audits of single, multiple or integrated management system(s) conducted
341 either separately or in combination.

342 The results monitored and measured to ensure the objective has been achieved. The audit programme should be
343 reviewed in order to identify the possible improvements.

344 The audit programme should include:

345 — the audit objectives;

346 — extent/number/types/locations/schedule of the audits;

347 — main audit procedure;

348 — audit criteria;

349 — audit methods;

350 — selection of audit team(s);

351 — uncertainty in achieving objectives of the audit programme and preventive measures to be implemented;

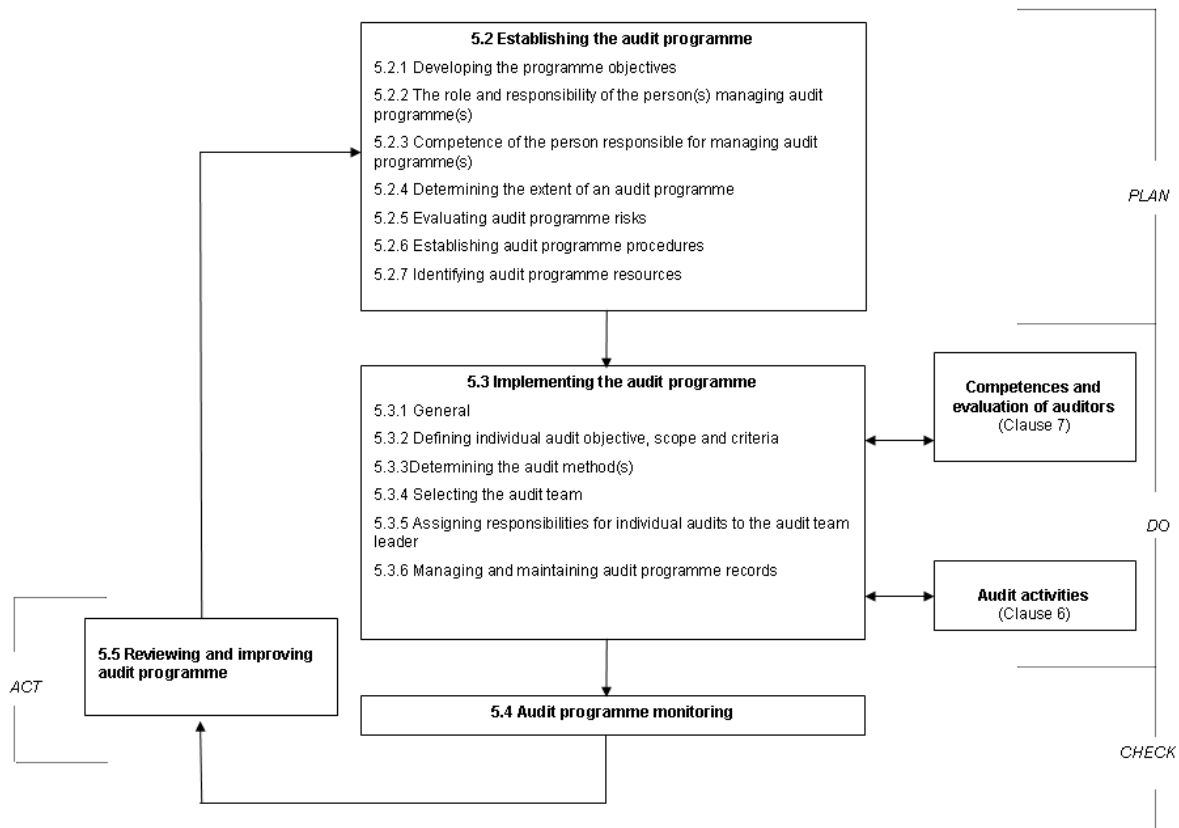
352 — necessary resources, including travel and accommodations;

353 — processes for handling confidentiality, information security and other similar matters;

354

355

356



357
358 **Figure 1 — Illustration of the flow for the management of an audit programme**

359 NOTE 1 Figure 1 also illustrates the application of the Plan-Do-Check-Act methodology in this International Standard.

360 NOTE 2 The numbers in this and all subsequent figures refer to the relevant clauses of this International Standard.

361 **5.2 Establishing the audit programme**

362 **5.2.1 Developing the programme objectives**

363 Objectives for an audit programme(s), to direct the planning and conduct of audits and to ensure the audit
364 programme is implemented effectively.

365 These objectives can vary depending on:

- 366 — management priorities;
- 367 — commercial and/or business intentions;
- 368 — management system(s) requirements;
- 369 — legal and other requirements;
- 370 — need for supplier evaluation;
- 371 — needs and expectations of interested parties (including customers);
- 372 — auditee's level of performance, as reflected in the occurrence of failures or incidents or customer complaints;

373 — risks to the organization being audited;

374 — results of previous audits;

375 — level of maturity of the management system.

376 Examples of audit programme objectives may include the following:

377 — to contribute to the improvement of a management system and its performance;

378 — to meet external requirements, e.g. certification to a management system standard;

379 — to verify conformity with contractual requirements;

380 — to obtain and maintain confidence in the capability of a supplier;

381 — to evaluate compatibility and alignment of the management system objectives with the management system
382 policy and the overall business objectives;

383 **5.2.2 Role and responsibility of the person(s) managing audit programme(s)**

384 The person(s) assigned the responsibility for managing the audit programme(s) should:

385 — establish the extent of the audit programme;

386 — evaluate the risks for the audit programme;

387 — establish audit responsibilities and procedures;

388 — ensure necessary resources are provided, including the evaluation of auditors;

389 — ensure the implementation of the audit programme, such as defining audit objectives, scope and criteria of the
390 individual audits, determining audit methods and selecting the audit team;

391 — ensure that appropriate audit programme records are managed and maintained;

392 — monitor, review and improve the audit programme.

393 The person(s) assigned the responsibility for managing an audit programme(s) should inform the top management
394 on the contents of the audit programme and, where necessary, ask for its approval.

395 **5.2.3 Competence of the person responsible for managing audit programme(s)**

396 The person(s) responsible for managing the audit programme(s) should have competence to manage the audit
397 programme(s) effectively and efficiently as well as competence in the following areas relevant to their organization
398 and the audit programme objectives:

399 — audit principles, procedures, methods and techniques;

400 — management system and reference documents;

401 — applicable legal and other requirements relevant to the activities and/or products of the organization to be
402 audited;

403 — organizational product and processes;

404 — customer(s), supplier(s) and other interested parties of the organization to be audited, where applicable;

405 — risks associated with the audit programme(s).

406 **5.2.4 Determining the extent of an audit programme**

407 The person(s) responsible for managing audit programme(s) should establish the extent of an audit programme
408 which can vary depending on the size and nature of the organization to be audited, as well as on the nature,
409 functionality, complexity and the level of maturity of the management system(s) to be audited. Other factors
410 impacting the extent of an audit programme include:

411 — the scope, objective and duration of each audit to be conducted;

412 — the frequency of the audits to be conducted;

413 — the number, importance, similarity and locations of the activities to be audited;

414 — those matters of significance to the effectiveness of the management system;

415 — legal and other requirements, such as standards, contractual requirements and other audit criteria;

416 — the need to meet external requirements, e.g. for certification;

417 — conclusions of previous internal or external audits or results of a previous audit programme review;

418 — language, cultural and social issues;

419 — the concerns of interested parties, such as customer complaints or regulatory breaches;

420 — significant changes to the organization to be audited or its operations;

421 — the extent and maturity of the information and communications technologies of the auditee, which can impact
422 the use of remote audit methods;

423 — the occurrence of internal and external events such as product failure, contamination, information security leak,
424 health and safety incident, criminal acts or environmental incident.

425 **5.2.5 Evaluating audit programme risks**

426 There are a variety of risks associated with establishing, implementing, monitoring and reviewing an audit
427 programme that may affect the audit programme objectives. The person(s) responsible for managing the audit
428 programme should consider these risks when developing an audit programme. These risks may be associated
429 with:

430 — planning, e.g. failure to set relevant audit objectives and determine the extent of the audit programme;

431 — resources, e.g. allowing insufficient time for the person responsible for managing the audit programme to
432 develop the audit programme;

433 — selection of the audit team, e.g. the team does not have the collective competence to conduct the audit
434 effectively;

435 — implementation, e.g. ineffective communication of the audit programme;

436 — records, e.g. failure to adequately protect audit records to demonstrate audit programme effectiveness;

437 — monitoring, reviewing and improving the audit programme, e.g. ineffective monitoring of audit programme
438 outcomes.

439 5.2.6 Establishing audit programme procedures

440 The person(s) responsible for managing audit programme(s) should establish one or more audit programme
441 procedures, addressing the following:

- 442 — planning and scheduling audits considering audit programme risks;
- 443 — managing information security, confidentiality, risks to the organization from auditing activities and other
444 matters related to the audit programme;
- 445 — assuring the competence of auditors and audit team leaders;
- 446 — selecting appropriate audit teams and assigning their roles and responsibilities;
- 447 — conducting audits, including the use of appropriate sampling methods;
- 448 — conducting audit follow-up, if applicable;
- 449 — reporting to the audit client (e.g. top management) on the overall achievements of the audit programme;
- 450 — maintaining audit programme records;
- 451 — monitoring the performance, risks and effectiveness of the audit programme.

452 5.2.7 Identifying audit programme resources

453 When identifying resources for the audit programme, the person(s) responsible for managing audit program(s)
454 should consider:

- 455 — the financial resources necessary to develop, implement, manage and improve audit activities;
- 456 — audit methods/techniques;
- 457 — the availability of auditors and technical experts having competence appropriate to the particular audit
458 programme objectives ;
- 459 — the extent of the audit programme;
- 460 — travelling time and cost, accommodation and other auditing needs;
- 461 — the extent and maturity of the information and communication systems of the organization to be audited which
462 may impact the use of remote audit methods.

463 5.3 Implementing the audit programme

464 5.3.1 General

465 The person(s) responsible for managing audit programme(s) should implement the audit programme by:

- 466 — communicating the pertinent parts of the audit programme to relevant parties and informing them periodically
467 of its progress;
- 468 — defining objectives, scope and criteria for each individual audit;
- 469 — coordinating and scheduling audits and other activities relevant to the audit programme;
- 470 — ensuring the selection of audit teams with the necessary competence;

- 471 — providing necessary resources to the audit teams;
- 472 — ensuring the conduct of audits in accordance with the audit programme and within the agreed time frame;
- 473 — ensuring that audit activities are recorded and records are properly managed and maintained.

474 **5.3.2 Defining individual audit objectives, scope and criteria**

475 Based on the information contained in the audit programme and in order to develop the audit plan for each
476 individual audit, it is necessary to identify and document the specific audit objectives, scope, methods, criteria and
477 procedures.

478 The audit objectives define what is to be accomplished by the individual audit and should be documented in the
479 audit plan. They may include the following:

- 480 — determination of the extent of conformity of a management system to be audited, or parts of it, with audit
481 criteria;
- 482 — evaluation of the capability of a management system to ensure compliance with legal and other requirements ;
- 483 — evaluation of the effectiveness of a management system in meeting its specified objectives;
- 484 — identification of areas for potential improvement of a management system;
- 485 — treatment of confidential information including the extent of disclosure.

486 The individual audit objectives should be defined by the person responsible for managing the audit programme and
487 be consistent with the overall audit programme objectives.

488 The audit scope should be consistent with the audit programme and audit objectives. It includes such factors as
489 physical locations, organizational units, activities and processes to be audited, as well as the duration of the audit.

490 The audit criteria are used as a reference against which conformity is determined and may include applicable
491 policies, objectives, procedures, standards, legal requirements, management system requirements, contractual
492 requirements or industry/business sector codes of conduct.

493 The audit scope and audit criteria should be defined jointly by the person(s) responsible for managing audit
494 programme and the audit team leader in accordance with audit programme procedures. Any changes to the audit
495 objectives, audit scope or audit criteria should be agreed to by the same parties and the audit programme should
496 be modified accordingly.

497 Where a combined audit is to be conducted, it should be ensured that the:

- 498 — audit objectives arising from different audit programmes are aligned, including those objectives arising from the
499 combination;
- 500 — audit scope is consistent with requirements arising from the specific management system standards;
- 501 — audit criteria are selected so that efficiency can be gained by combining similar requirements/subjects from
502 different references.

503 **5.3.3 Determining the audit method(s)**

504 The person(s) responsible for managing audit programme(s) should select and determine the audit methods for an
505 audit depending on the defined audit objectives, scope and criteria for effectively conducting the audit.

506 NOTE Guidance how to determine audit methods is given in Annex C

507 Where two or more auditing organizations conduct a joint audit in the same auditee, the persons responsible for the
 508 management of the different audit programmes should cooperate and exchange information during the
 509 establishment of the audit programmes. They should pay special attention to the division of responsibilities, the
 510 scheduling of the joint audits, the provision of any additional resources, the competence of the audit team and the
 511 appropriate procedures. Agreement on these matters should be reached before the audit activities start.

512 If an organization to be audited operates two or more management systems of different disciplines, combined
 513 audits may be included in the audit programme. In such a case, special attention should be paid to the competence
 514 of the audit team.

515 **5.3.4 Selecting the audit team**

516 The person(s) responsible for managing audit programme(s) should appoint the members of the audit team,
 517 including the team leader and any technical expert(s) needed for the specific audit.

518 An audit team should be selected, taking into account the competence needed to achieve the objectives of the
 519 individual audit within the defined scope. If there is only one auditor, the auditor should perform all applicable duties
 520 of an audit team leader.

521 NOTE Clause 7 contains guidance on determining the competence required for the audit team members and describes
 522 processes for evaluating auditors.

523 In deciding the size and composition of the audit team for the specific audit, consideration should be given to the
 524 following:

- 525 — the overall competence of the audit team needed to achieve audit objectives, scope and criteria;
- 526 — whether the audit is a combined or joint audit;
- 527 — the kind of audit methods that have been selected;
- 528 — legal and other requirements such as contractual requirements;
- 529 — the need to ensure the independence of the audit team from the activities to be audited and to avoid any
 530 conflict of interest;
- 531 — the ability of the audit team members to interact effectively with the representatives of the auditee and to work
 532 together;
- 533 — the language of the audit, and an understanding of the auditee's particular social and cultural characteristics.
 534 These issues may be addressed either by the auditor's own skills or through the support of a technical expert.

535 To assure the overall competence of the audit team, the following steps should be performed:

- 536 — identification of the knowledge and skills needed to achieve the objectives of the audit;
- 537 — selection of the audit team members so that all of the necessary knowledge and skills are present in the audit
 538 team.

539 If all the necessary competence is not covered by the auditors in the audit team, technical experts with additional
 540 competence may be included in the teams. Technical experts should operate under the direction of an auditor but
 541 should not act as auditors.

542 Auditors-in-training may be included in the audit team, but should participate under the direction and guidance of an
 543 auditor.

544 Both the audit client and the auditee may request the replacement of particular audit team members on reasonable
 545 grounds based on the principles of auditing described in clause 4. Examples of reasonable grounds include conflict
 546 of interest situations (such as in the case of second or third party audits, an audit team member having been a

547 former employee of the auditee or having provided consultancy services to the auditee), lack of competency or
548 previous unethical behaviour. Such grounds should be communicated to the audit team leader and to the person
549 assigned responsibility for managing the audit programme, who should discuss the issue with the audit client and
550 auditee before making any decisions or replacing audit team members.

551 Where a joint audit is conducted, it is important to reach agreement among the organizations conducting the audits
552 before the audit commences, on the specific responsibilities of each party, particularly with regard to the authority
553 of the team leader appointed for the audit.

554 **5.3.5 Assigning responsibility for individual audit(s) to the audit team leader**

555 The person responsible for the management of the audit programme should assign the responsibility for the
556 conduct of the individual audit to an audit team leader. The assignment should be made in sufficient time to ensure
557 the effective planning of the audits.

558 To ensure effective conduct of the individual audit(s), the following information should be provided to the audit team
559 leader:

560 — the audit objectives;

561 — the audit criteria and any reference documents;

562 — the audit methods and procedures;

563 — the audit scope, including identification of the organizational and functional units and processes to be audited;

564 — the composition of the audit team;

565 — the locations (sites), dates, and duration of the audit activities to be conducted;

566 — the allocation of appropriate resources to conduct the audit.

567 The assignment information should also cover the following, as appropriate:

568 — the working and reporting language of the audit where this is different from the language of the auditor and/or
569 the auditee;

570 — audit report contents requested by the audit programme;

571 — matters related to confidentiality and information security, if required by the audit programme;

572 — any follow-up actions, for example, from a previous audit, if applicable;

573 — coordination with other audit activities, in case of a joint audit.

574 The person responsible for the audit programme should ensure that the information provided adequately addresses
575 identified risks to the achievement of audit objectives.

576 **5.3.6 Managing and maintaining audit programme records**

577 The person(s) responsible for managing audit programme(s) should manage and maintain records to demonstrate
578 the implementation of the audit programme. Processes should be established to ensure that any privacy or
579 confidentiality needs associated with the audit records are satisfied.

580 Records should include the following:

581 a) Records related to the audit programme such as;

- 582 — audit programme objectives;
- 583 — those addressing audit programme risks;
- 584 — reviews of the audit programme effectiveness.

585 b) records related to individual audit , such as

- 586 — audit plans and audit reports;
- 587 — nonconformity reports;
- 588 — corrective and preventive action reports;
- 589 — audit follow-up reports, if applicable.

590 c) records related to audit personnel covering subjects such as

- 591 — competence and performance evaluation of the audit team members;
- 592 — audit team selection;
- 593 — maintenance and improvement of competence.

594 The form and level of details of the records should meet the objectives of the audit programme(s).

595 **5.4 Audit programme monitoring**

596 The person(s) responsible for managing audit program(s) should monitor the implementation of the audit
597 programme(s) at periodic intervals considering the need to;

- 598 — review and approve audit reports, and ensure their distribution to the top management and other relevant
599 parties.
- 600 — determine the necessity of any follow-up audit;
- 601 — evaluate the performance of the audit team members;
- 602 — evaluate the ability of the audit teams to implement the audit plan;
- 603 — evaluate conformity with audit programmes, schedules and audit objectives;
- 604 — evaluate feedback from top management, auditees, auditors and other interested parties.

605 Some factors may determine the need to modify the audit programme, before its completion, such as:

- 606 — initial audit findings;
- 607 — demonstrated level of management system effectiveness;
- 608 — changes to the client's or the auditee's management system;
- 609 — change of legal requirements and/or standard;
- 610 — change of supplier.

611 **5.5 Reviewing and improving audit programmes**

612 The person(s) responsible for managing audit programme(s) should review the audit programme to assess whether
613 its objectives have been met. Lessons learned from the audit programme review should be used for the continual
614 improvement process.

615 The audit programme review should consider, for example:

- 616 — results and trends from monitoring;
- 617 — conformity with audit programme procedure(s);
- 618 — evolving needs and expectations of interested parties;
- 619 — audit programme records;
- 620 — alternative or new auditing methods;
- 621 — effectiveness of the measures to address risks associated with audit programme;
- 622 — confidentiality and information security issues relating to the audit programme.

623 The person(s) responsible for managing audit programme(s) should review the overall implementation of audit
624 programme(s), identify the area of improvement and amend the programme if necessary. They should also:

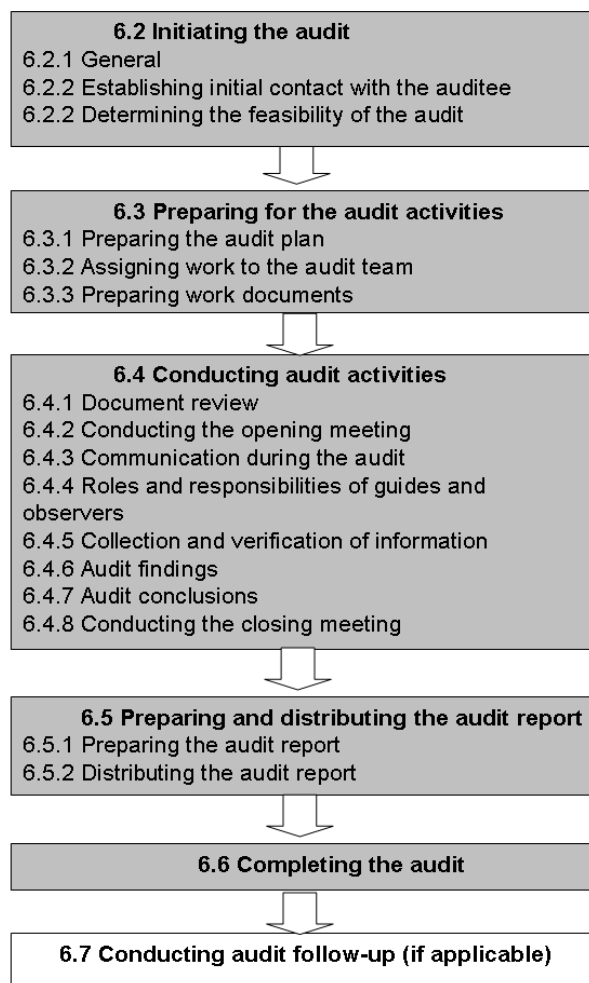
- 625 — review the continual professional development of auditors, in accordance with 7.4, 7.5 and 7.6;
- 626 — report the results of the audit programme review to the top management.

627 **6 Audit activities**

628 **6.1 General**

629 This clause contains guidance on planning and conducting audit activities using different audit methods as part of
630 an audit programme. Figure 2 provides an overview of typical audit activities. The extent to which the provisions of
631 this clause are applicable depends on the scope and complexity of the specific audit and the intended use of the
632 audit conclusions.

633



634
635 **Figure 2 — Overview of typical activities during an audit**

636 **6.2 Initiating the audit**

637 **6.2.1 General**

638 When an audit is initiated, the responsibility for this audit is assigned to the audit team leader, as is defined in the
639 audit programme. This assignment is performed by the person who is responsible for managing of the audit
640 programme by transferring information for the audit (see 5.3.5).

641 The responsibility for conducting the assigned audit remains with the audit team leader until the audit is completed.

642 To initiate an audit, the following steps should be considered, however the sequence can differ depending on the
643 auditee, processes and specific situations.

644 **6.2.2 Establishing initial contact with the auditee**

645 The initial contact for the audit with the auditee can be informal or formal and should be made by the audit team
646 leader. The purposes of the initial contact are:

- 647 — to establish communication channels with the auditee's representative(s);
- 648 — to confirm the authority to conduct the audit;
- 649 — to provide information on the audit scope, audit methods and audit team composition;

- 650 — to request access to relevant documents for planning purposes, including records;
- 651 — to determine applicable legal and other requirements;
- 652 — to confirm the agreement with the auditee regarding the extent of the disclosure and the treatment of the
653 confidential information;
- 654 — to make arrangements for the audit including scheduling the date(s);
- 655 — to agree on the attendance of observers and the need for guides for the audit team;
- 656 — to find out, the expectations and needs the auditee has related to the specific audit.

657 **6.2.3 Determining the feasibility of the audit**

658 The feasibility of an audit determines whether all of the necessary resources, information, arrangements, etc., are
659 in place to provide reasonable confidence that the audit objectives can be achieved.

660 The feasibility of the audit should be determined, taking into consideration such factors as the availability of:

- 661 — sufficient and appropriate information for planning the audit;
- 662 — adequate cooperation from the auditee; and
- 663 — adequate time and resources for performing the audit.

664 Where the audit is not feasible, an alternative should be proposed to the audit client, in agreement with the auditee.

665 **6.3 Preparing for the audit activities**

666 **6.3.1 Preparing the audit plan**

667 The audit team leader should prepare an audit plan based on the information contained in the audit programme
668 and documentation provided by the auditee. The audit plan should consider the effect of the audit on the auditee's
669 processes and provide the basis for the agreement among the audit client, audit team and the auditee regarding
670 the conduct of the audit. The plan should facilitate the efficient scheduling and coordination of the audit activities to
671 achieve an effective outcome.

672 The amount of detail provided in the audit plan should reflect the scope and complexity of the audit as well as risks
673 and the effect of uncertainty on the audit outcome. In preparing the audit plan the audit team leader should be
674 aware of appropriate sampling techniques (see Annex C.5), compatibility of audit team members and risks to the
675 organization created by the audit.

676 NOTE Risks to the organization may include an audit team member who mishandle the auditee's information, creates a
677 safety, health, environmental or a security risk such as a threat to the auditee's products, services, personnel and/or
678 infrastructure.

679 For combined and joint audits, particular attention should be given to the interfaces between processes of the
680 management system(s).

681 The details may differ, for example, between initial and subsequent audits and also between internal and external
682 audits. The audit plan should be sufficiently flexible to permit changes which can become necessary as the audit
683 activities progress.

684 The audit plan should cover or reference the following:

- 685 — the audit objectives;

- 686 — the audit scope, including identification of the organizational and functional units and processes to be audited;
 - 687 — the audit criteria and any reference documents;
 - 688 — the locations, dates, expected times and duration of audit activities to be conducted, including meetings with
689 the auditee's management as well as other meetings;
 - 690 — the audit method to be used including the extent to which audit sampling is needed to obtain sufficient audit
691 evidence and the design of the sampling programme, if applicable;
 - 692 — the roles and responsibilities of the audit team members as well as guides and observers;
 - 693 — the allocation of appropriate resources to critical areas of the audit.
- 694 The audit plan should also cover the following, as appropriate:
- 695 — identification of the auditee's representative for the audit;
 - 696 — the working and reporting language of the audit where this is different from the language of the auditor and/or
697 the auditee;
 - 698 — the audit report topics;
 - 699 — logistics and communications arrangements including specific arrangements for the sites to be audited;
 - 700 — any specific measures taken to address risks and the effect of uncertainty on the audit objectives;
 - 701 — matters related to confidentiality and information security;
 - 702 — any follow-up actions, for example, from a previous audit;
 - 703 — co-ordination with other audit activities, in case of a joint audit.
- 704 The plan should be reviewed and accepted by the audit client, and presented to the auditee, before the audit
705 activities begin.
- 706 Any objections by the auditee should be resolved between the audit team leader, the auditee and/or the person
707 responsible for managing the audit programme. Any revised audit plan should be agreed among the parties
708 concerned before continuing the audit.

709 **6.3.2 Assigning work to the audit team**

710 The audit team leader, in consultation with the audit team, should assign to each team member responsibility for
711 auditing specific processes, functions, sites, areas or activities. Such assignments should respect the
712 independence and competence of auditors and the effective use of resources, as well as different roles and
713 responsibilities of auditors, auditors-in-training and technical experts.

714 Audit team briefings, which should be held on a regular basis by the audit team leader, should allocate work
715 assignments and decide possible changes. Changes to the work assignments can be made as the audit
716 progresses to ensure the achievement of the audit objectives.

717 **6.3.3 Preparing work documents**

718 The audit team members should review the information relevant to their audit assignments and prepare work
719 documents as necessary for reference and for recording audit evidences. Such work documents should include:

- 720 — checklists and audit sampling plans;

721 — forms for recording information, such as supporting evidence, audit findings and records of meetings.

722 The use of checklists and forms should not restrict the extent of audit activities, which can change as a result of
723 information collected during the audit.

724 NOTE Guidance on preparing work documents is given in Annex C.4 of this standard.

725 Work documents, including records resulting from their use, should be retained at least until audit completion.
726 Retention of documents after audit completion is described in 6.7. Those documents involving confidential or
727 proprietary information should be suitably safeguarded at all times by the audit team members.

728 **6.4 Conducting audit activities**

729 **6.4.1 Document review**

730 As a part of the audit activities the relevant auditee management system documentation should be reviewed to:

731 — gather information for the preparation of the audit activities;

732 — get an overview on the extent of the system documentation;

733 — determine the conformity of the system, as far as documented, with audit criteria.

734 NOTE Guidance how to perform a document review is provided in Annex C.3 of this standard.

735 The documentation can include relevant management system documents and records, as well as previous audit
736 reports. The document review should take into account the size, nature and complexity of the auditee's
737 management system and organization, and the objectives and scope of the audit.

738 The review may be combined with the other audit activities and may continue throughout the audit, if this is not
739 detrimental to the effectiveness of the conduct of the audit.

740 If adequate documentation cannot be provided within the time frame given in the audit plan, the audit team leader
741 should inform the person responsible for managing the audit programme, and the auditee. Depending on the audit
742 scope and objectives a decision should be made as to whether the audit should be continued or suspended until
743 documentation concerns are resolved.

744 **6.4.2 Conducting opening meeting**

745 The purpose of the opening meeting is to confirm the audit plan, introduce the audit team and ensure that all
746 planned audit activities are in place.

747 An opening meeting should be held with the auditee management and, where appropriate, those responsible for
748 the functions or processes to be audited.

749 In many instances, for example internal audits in a small organization, the opening meeting may simply consist of
750 communicating that an audit is being conducted and explaining the nature of the audit.

751 For other audit situations, the meeting may be formal and records of the attendance should be kept. The meeting
752 should be chaired by the audit team leader, and the following items should be considered, as appropriate:

753 — introduction of the participants including observers and guides, and an outline of their roles;

754 — confirmation of the audit objectives, scope and criteria;

755 — confirmation of the audit plan and other relevant arrangements with the auditee, such as the date and time for
756 the closing meeting, any interim meetings between the audit team and the auditee's management, and any late
757 changes;

- 758 — presentation of the methods to be used to conduct the audit, including advising the auditee that the audit
759 evidence will be based on a sample of the information available;
- 760 — introduction of methods to manage risks to the organization, products, services, personnel and/or infrastructure
761 associated with the audit;
- 762 — confirmation of formal communication channels between the audit team and the auditee;
- 763 — confirmation of the language(s) to be used during the audit;
- 764 — confirmation that, during the audit, the auditee will be kept informed of audit progress;
- 765 — confirmation that the resources and facilities needed by the audit team are available;
- 766 — confirmation of matters relating to confidentiality and information security;
- 767 — confirmation of relevant health and safety, emergency and security procedures for the audit team;
- 768 — information on method of reporting audit findings including any grading;
- 769 — information about conditions under which the audit may be terminated;
- 770 — information about the closing meeting;
- 771 — information about how to deal with possible findings during the audit;
- 772 — information about any system for feedback from the auditee on the findings or conclusions of the audit,
773 including complaints or appeals.

774 **6.4.3 Communication during the audit**

775 It may be necessary to make formal arrangements for communication within the audit team with the auditee and
776 potentially with external bodies (e.g. regulators) during the audit, especially where legislative requirements require
777 the mandatory reporting of nonconformities.

778 The audit team should confer periodically to exchange information, assess audit progress, and to reassign work
779 between the audit team members as needed.

780 During the audit, the audit team leader should periodically communicate the progress of the audit and any concerns
781 to the auditee and audit client, as appropriate. Evidence collected during the audit that suggests an immediate and
782 significant risk to the auditee should be reported without delay to the auditee and, as appropriate, to the audit client.
783 Any concern about an issue outside the audit scope should be noted and reported to the audit team leader, for
784 possible communication to the audit client and auditee.

785 Where the available audit evidence indicates that the audit objectives are unattainable, the audit team leader
786 should report the reasons to the audit client and the auditee to determine appropriate action. Such action may
787 include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or
788 termination of the audit.

789 Any need for changes to the audit plan which may become apparent as auditing activities progress should be
790 reviewed with and approved by the person responsible for managing the audit programme and, as appropriate, the
791 auditee.

792 **6.4.4 Roles and responsibilities of guides and observers**

793 Guides and observers (e.g. regulator or other interested parties) may accompany the audit team. They should not
794 influence or interfere with the conduct of the audit.

795 Guides, appointed by the auditee, should assist the audit team and act on the request of the audit team leader.
796 Their responsibilities should include the following:

- 797 — establishing contacts and timing for interviews;
- 798 — arranging access to specific parts or sites of the auditee;
- 799 — ensuring that rules concerning site safety and security procedures are known and respected by the audit team
800 members and observers;
- 801 — witnessing the audit on behalf of the auditee;
- 802 — providing clarification or assisting in collecting information.

803 **6.4.5 Collection and verification of information**

804 During the audit, information relevant to the audit objectives, audit scope and audit criteria, including information
805 relating to interfaces between functions, activities and processes, should be collected by means of appropriate
806 sampling and should be verified. Only information that is verifiable should be accepted as audit evidence. Audit
807 evidence relevant to the audit findings should be recorded. If during collection of evidences, the audit team
808 becomes aware of any new or changed risk, they should be addressed accordingly.

809 NOTE Guidance on sampling is given in Annex C.5 of this standard.

810 Figure 3 provides an overview of the process, from collecting information to reaching audit conclusions.

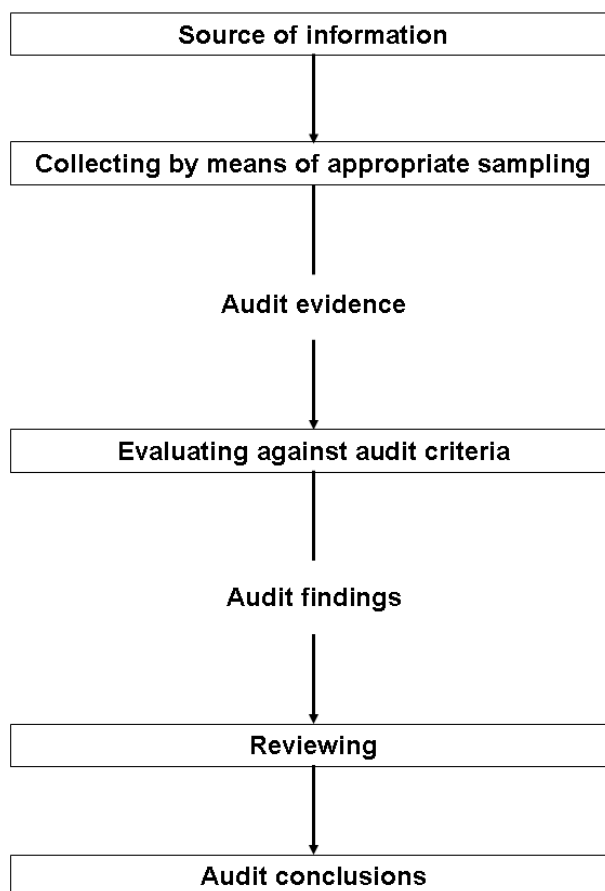
811

812

813

814

815



816

817 **Figure 3 — Overview of the process from collecting information to reaching audit conclusions**

818 Methods of collecting information include:

- 819 — interviews;
- 820 — observations;
- 821 — review of documents.

822 NOTE 1 Guidance on sources of information is given in Annex C.1 of this standard.

823 NOTE 2 Guidance on site-visits is given in Annex C.6 of this standard.

824 NOTE 3 Guidance how to conduct interviews is given in Annex C.7 of this standard.

825 **6.4.6 Audit findings**

826 Audit evidence should be evaluated against the audit criteria to identify the audit findings. Audit findings can
 827 indicate conformity or nonconformity with audit criteria. When specified by the audit objectives, audit findings
 828 should identify opportunities for improvement and provide recommendations for best practice, where this does not
 829 compromise independence.

830 The audit team should meet as needed to review the audit findings at appropriate stages during the audit.

831 Conformity with audit criteria should be summarized to indicate locations, functions or processes that were audited.
832 If included in the audit plan, individual audit findings of conformity and their supporting evidence should also be
833 recorded.

834 Nonconformities and their supporting audit evidence should be recorded. Nonconformities may be graded. They
835 should be reviewed with the auditee to obtain acknowledgement that the audit evidence is accurate, and that the
836 nonconformities are understood. Every attempt should be made to resolve any diverging opinions concerning the
837 audit evidence and/or findings, and unresolved points should be recorded.

838 For combined and joint audits, arrangements on dealing with findings related to criteria coming from the different
839 requirements audited (multiple criteria) should be in place.

840 NOTE Additional guidance on identifying and evaluating of audit findings is given in Annex C.8 of this standard.

841 **6.4.7 Audit conclusions**

842 The audit team should confer prior to the closing meeting to:

- 843 — review the audit findings, and any other appropriate information collected during the audit, against the audit
844 objectives;
- 845 — agree on the audit conclusions, taking into account the uncertainty inherent in the audit process;
- 846 — prepare recommendations, if specified by the audit objectives;
- 847 — discuss audit follow-up, as applicable.

848 Audit conclusions can address issues such as:

- 849 — the extent of conformity of the management system with the audit criteria, including the effectiveness of the
850 management system in meeting the stated objectives;
- 851 — the effective implementation, maintenance and improvement of a management system;
- 852 — the capability of the management review process to ensure the continuing suitability, adequacy, effectiveness
853 and improvement of a management system
- 854 — Attempt to identify root causes of findings, if stated by the audit objectives;
- 855 — Consolidate similar findings made in different areas that were audited for the purpose of identifying trends.

856 If specified by the audit objectives, audit conclusions may lead to recommendations regarding improvements,
857 business relationships, or future auditing activities.

858 **6.4.8 Conducting the closing meeting**

859 A closing meeting, facilitated by the audit team leader, should be held to present the audit findings and conclusions
860 in such a manner that they are understood and acknowledged by the auditee. Participants in the closing meeting
861 should include representatives of the auditee, and may also include the audit client and other parties. If applicable,
862 the audit team leader should advise the auditee of situations encountered during the audit that may decrease the
863 reliance that can be placed on the audit conclusions. If defined in the management system or by agreement with
864 the person responsible for managing the audit programme, the participants should agree, on the time frame for an
865 action plan to address audit findings.

866 For some audit situations, the meeting may be formal and minutes including records of attendance, should be kept.
867 In other instances, for example, internal audits, the closing meeting is less formal and may consist solely of
868 communicating the audit findings and audit conclusions.

869 As appropriate, the following should be explained in the closing meeting:

870 — advising the auditee that the audit evidence collected was based on a sample of the information available;

871 — the method of reporting, including any grading;

872 — the process of handling of audit findings and possible consequences;

873 — presentation of the audit findings in such a manner that they are understood and acknowledged by the auditee;

874 — any related post audit activities.

875 Any diverging opinions regarding the audit findings and/or conclusions between the audit team and the auditee
876 should be discussed and if possible resolved. If not resolved, all opinions should be recorded.

877 If specified by the audit objectives, recommendations for improvements may be presented. It should be
878 emphasized that recommendations are not binding.

879 **6.5 Preparing and distributing the audit report**

880 **6.5.1 Preparing the audit report**

881 The audit team leader should be responsible for the preparation and contents of the audit report.

882 The audit report should provide a complete, accurate, concise and clear record of the audit, and in accordance with
883 the audit procedures should include or refer to the following:

884 — the audit objectives;

885 — the audit scope, particularly identification of the organizational and functional units or processes audited and
886 the period of time covered;

887 — identification of the audit client;

888 — identification of audit team and auditee's participants in the audit;

889 — the dates and locations where the audit activities were conducted;

890 — the audit criteria;

891 — the audit findings;

892 — the audit conclusions;

893 — A statement on the extent of the conformity to the audit criteria.

894 The audit report can also include or refer to the following, as appropriate:

895 — the audit plan;

896 — a summary of the audit process, including the uncertainty and/or any obstacles encountered that may
897 decrease the reliability of the audit conclusions;

898 — confirmation if the audit objectives have been accomplished within the audit scope in accordance with the audit
899 plan;

900 — any areas within the audit scope not covered;

- 901 — a management summary covering the audit conclusions and the main audit findings that support them;
- 902 — any unresolved diverging opinions between the audit team and the auditee;
- 903 — opportunities for improvement, if specified in the audit objectives;
- 904 — strengths and best practices identified;
- 905 — agreed follow-up action plans, if any;
- 906 — a statement of the confidential nature of the contents;
- 907 — the distribution list for the audit report.

908 **6.5.2 Distributing the audit report**

- 909 The audit report should be issued within an agreed period of time. If it is delayed, the reasons should be
910 communicated to the auditee and the person responsible for managing the audit programme.
- 911 The audit report should be dated, reviewed and approved as appropriate in accordance with audit programme
912 procedures.
- 913 The audit report should then be distributed to recipients as defined in the audit procedures.

914 **6.6 Completing the audit**

- 915 The audit is completed when all audit plan activities have been carried out or as otherwise agreed with the person
916 responsible for managing the audit programme.
- 917 Documents pertaining to the audit should be retained or destroyed by agreement between the participating parties
918 and in accordance with audit programme procedures and applicable legal and other requirements.
- 919 Unless required by law, the audit team and the person responsible for managing the audit programme should not
920 disclose the contents of documents, any other information obtained during the audit, or the audit report, to any
921 other party without the explicit approval of the audit client and, where appropriate, the approval of the auditee. If
922 disclosure of the contents of an audit document is required, the audit client and auditee should be informed as soon
923 as possible.
- 924 Lessons learned from the audit should be entered into the continual improvement process of the management
925 system of the organization needing to conduct audits.

926 **6.7 Conducting audit follow-up**

- 927 The conclusions of the audit may, depending on the audit objectives, indicate the need for corrections, corrective,
928 preventive or improvement actions. Such actions are usually decided and undertaken by the auditee within an
929 agreed timeframe. As appropriate, the auditee should keep the person responsible for managing the audit
930 programme and the audit team informed of the status of these actions.
- 931 The completion and effectiveness of the actions should be verified. This verification may be part of a subsequent
932 audit.

933 **7 Competence and evaluation of auditors**

934 **7.1 General**

935 Confidence and reliance in the audit process depends on the competence of those individuals who are involved in
936 planning and conducting the audits, including auditors and audit team leaders. Competence should be evaluated
937 through a process that considers personal behaviours and the ability to apply the knowledge and skills gained
938 through education, work experience, auditor training and audit experience. This process should take into
939 consideration the needs of the audit programme and its objectives. Some of the knowledge and skills described in
940 7.3 are common to auditors of all management system disciplines; others are specific to auditors of specific
941 management system disciplines.

942 The evaluation of auditors should be planned, implemented and documented in accordance with the audit
943 programme to provide an outcome that is objective, consistent, fair and reliable. The evaluation process should
944 include four main steps.

- 945 1) Determine the competence of audit personnel needed for the audit programme;
- 946 2) Establish the evaluation criteria;
- 947 3) Select the appropriate evaluation method;
- 948 4) Conduct the evaluation.

949 The outcome of the evaluation process should provide a basis for:

- 950 — audit team selection as described in 5.3.4;
- 951 — determination of training and other competence enhancement needs; and
- 952 — ongoing performance evaluation of auditors.

953 Auditors should develop, maintain and improve their competence through continual professional development and
954 regular participation in audits (see 7.5 and 7.6).

955 A process for evaluating auditors and audit team leaders is described in 7.5.

956 Audit team leaders should be evaluated against the criteria set out in 7.2.2.2 and 7.2.3.2.

957 **7.2 Determine auditor competence to meet the needs of the audit programme**

958 In deciding the appropriate knowledge and skills, the following should be considered:

- 959 — the size, nature and complexity of the organization(s) to be audited;
- 960 — the management system disciplines to be audited;
- 961 — the objectives and extent of the audit programme;
- 962 — other requirements, such as those imposed by external bodies, where appropriate;
- 963 — the role of the audit process in the management system of the organization(s) to be audited;
- 964 — the complexity of the management system to be audited;
- 965 — the uncertainty in achieving audit objectives.

966 This information should be matched against that listed in 7.3.1, 7.3.2 and 7.3.3.

967 **7.2.1 Personal behaviours**

968 Auditors should possess the necessary qualities to enable them to act in accordance with the principles of auditing
969 as described in clause 4. Auditors should exhibit professional behaviour during the performance of audit activities,
970 including being:

- 971 — ethical, i.e. fair, truthful, sincere, honest and discreet;
- 972 — open minded, i.e. willingness to consider alternative ideas or points of view;
- 973 — diplomatic, i.e. tact in dealing with people;
- 974 — observant, i.e. active observation of physical surroundings and activities;
- 975 — perceptive, i.e. aware of and able to understand situations;
- 976 — adaptable, i.e. adjust readily to different situations;
- 977 — tenacious, i.e. persistence, focus on achieving objectives;
- 978 — decisive, i.e. reaching timely conclusions based on logical reasoning and analysis;
- 979 — self reliant, i.e. acting and functioning independently while interacting effectively with others;
- 980 — acting with fortitude i.e. willing to act responsibly and ethically even though these actions may not always be
981 popular and may sometimes result in disagreement or confrontation;
- 982 — well organized, i.e. exhibiting effective time management, prioritization, planning and efficiency;
- 983 — open to improvement, i.e. learning from situations, striving for better audit results;
- 984 — culturally sensitive, i.e. observe and respect cultural traditions of the auditee;
- 985 — team player i.e. works well with other audit team members.

986 **7.2.2 Knowledge and skills**

987 **7.2.2.1 Generic knowledge and skills of management system auditors**

988 Auditors should have knowledge and skills in the following areas:

- 989 a) Audit principles, procedures and techniques: to enable the auditor to apply those appropriate to different
990 audits and ensure that audits are conducted in a consistent and systematic manner. An auditor should be able:
 - 991 — to apply audit principles, procedures, methods and techniques;
 - 992 — to plan and organize the work effectively;
 - 993 — to conduct the audit within the agreed time schedule;
 - 994 — to prioritize and focus on matters of significance;
 - 995 — to collect information through effective interviewing, listening, observing and reviewing documents, records
996 and data;

- 997 — to understand the appropriateness and consequences of using sampling techniques for auditing;
- 998 — to verify the accuracy of collected information;
- 999 — to confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;
- 1000 — to assess those factors that may affect the reliability of the audit findings and conclusions;
- 1001 — to use work documents to record audit activities;
- 1002 — to prepare audit reports;
- 1003 — to maintain the confidentiality and security of information;
- 1004 — to communicate effectively, orally and in writing (including provisions for use of interpreters and
1005 translators);
- 1006 — to understand the types of risks associated with auditing.
- 1007 b) Management system and reference documents: to enable the auditor to comprehend the scope of the audit
1008 and apply audit criteria. Knowledge and skills in this area should cover:
- 1009 — the application of management systems to different organizations;
- 1010 — interaction between the components of the management system;
- 1011 — specific management system standards, applicable procedures or other management system documents
1012 used as audit criteria;
- 1013 — recognizing the hierarchy of reference documents;
- 1014 — application of the reference documents to different audit situations;
- 1015 — control and protection of information, data, documents and records;
- 1016 — organizational context: to enable the auditor to comprehend the auditee's structure, business and
1017 management practices. Knowledge and skills in this area should cover:
- 1018 — organizational types, governance, size, structure, functions and relationships;
- 1019 — general business and management concepts, processes and related terminology; including planning,
1020 budgeting and management of personnel;
- 1021 — cultural and social aspects of the auditee.
- 1022 c) Applicable legal and other requirements that apply to the auditee to enable the auditor to work within, and be
1023 aware of, the organization's legal and contractual requirements. Knowledge and skills specific to the
1024 jurisdiction and/or auditee's activities and products should cover:
- 1025 — laws and regulations;
- 1026 — basic legal terminology;
- 1027 — contract and liability.

1028 **7.2.2.2 Generic knowledge and skills of audit team leader**

1029 Audit team leaders should have additional knowledge and skills to manage and provide leadership to the audit
1030 team in order to facilitate the efficient and effective conduct of the audit. An audit team leader should have the
1031 knowledge and skills necessary to:

- 1032 — balance the strengths and weaknesses of the individual audit team members;
- 1033 — develop a harmonious working relationship among the team members;
- 1034 — manage the audit process, including:
 - 1035 — planning the audit and making effective use of resources during the audit;
 - 1036 — managing the uncertainty of achieving audit objectives;
 - 1037 — protecting the safety and health of the audit team members during the audit, including ensuring
1038 compliance of the auditors with the relevant health, safety and security requirements;
 - 1039 — organizing and directing the audit team members;
 - 1040 — providing direction and guidance to auditors-in-training;
 - 1041 — preventing and resolving conflicts, as necessary;
- 1042 — represent the audit team in communications with the audit client and auditee;
- 1043 — understand and respect the experts' opinions;
- 1044 — lead the audit team to reach the audit conclusions; and
- 1045 — prepare and complete the audit report;

1046 **7.2.2.3 Discipline and sector specific knowledge and skills of management system auditors**

1047 An auditor who intends to audit a specific type of management system should have the discipline and sector
1048 specific knowledge and skills that are appropriate for auditing the particular type of management system and
1049 industry sector.

1050 Each auditor in the audit team does not need to have the same competence; however, the overall competence of
1051 the audit team needs to be sufficient to meet the audit objectives.

1052 The discipline and sector specific knowledge and/or skills of auditors include the following:

- 1053 — understanding of the discipline and sector specific management system requirements and principles, and their
1054 application;
- 1055 — understanding applicable legal and other requirements relevant to the discipline and sector: to enable the
1056 auditor to work within, and be aware of, the requirements those apply to the organization being audited.
1057 Knowledge and skills specific to the jurisdiction and/or auditee's obligations, activities and products;
- 1058 — understanding of the information (e.g. body of knowledge) that is fundamental to the business and technical
1059 processes, science and technology underlying the discipline sufficient to enable the auditor to evaluate
1060 management system elements associated with the discipline;
- 1061 — understanding of discipline specific knowledge related to the particular sector, nature of operations, or
1062 workplace being audited sufficient for the auditor to evaluate the auditee's activities, services, processes,
1063 products and services;

1064 — understanding risk management principles, methods and techniques relevant to the discipline and sector to
 1065 enable the auditor to examine the auditee's approach to managing risk.

1066 NOTE Detailed guidance of specific knowledge and skills for selected disciplines are provided in Annexes A and B.

1067 **7.2.3 Education, work experience, training and audit experience of auditors**

1068 **7.2.3.1 Auditors**

1069 Auditors should have completed an education sufficient to acquire the knowledge and skills described in 7.3.

1070 They should have work experience that contributes to the development of the knowledge and skills described in
 1071 7.3.3. This work experience should be in a technical, managerial or professional position involving the exercise of
 1072 judgment, decision making, problem solving and communication with managers, professionals, peers, customers
 1073 and/or other interested parties. Part of the work experience should be in a position where the activities undertaken
 1074 contribute to the development of knowledge and skills in a management system for which they intend to audit.

1075 They should have completed training in audit principles, procedures and techniques.

1076 They should acquire audit experience under the supervision of an audit team leader.

1077 **7.2.3.2 Audit team leaders**

1078 An audit team leader should have acquired additional audit experience to develop the knowledge and skills
 1079 described in 7.3.2. This additional experience should have been gained by working under the direction and
 1080 guidance of an audit team leader.

1081 **7.2.3.2.1 Auditors who audit combined or integrated management systems**

1082 Auditors who intend to become an audit team member in the audit of combined or integrated management systems
 1083 should have:

1084 — the competence necessary to audit at least one management system discipline forming part of the combined
 1085 or integrated management systems, as long as the audit team includes auditors with competence for all
 1086 disciplines;

1087 — an understanding of the interaction and synergy between the different management systems;

1088 An audit team leader conducting audits of combined or integrated management systems should meet the above
 1089 recommendations and have discipline specific competence to coordinate the auditing of multiple disciplines.

1090 **7.3 Establish the evaluation criteria**

1091 The criteria may be qualitative (such as having demonstrated personal behaviours, knowledge or the performance
 1092 of the skills, in training or in the workplace) and quantitative (such as the years of work experience and education,
 1093 number of audits conducted, hours of audit training).

1094 **7.4 Select the appropriate evaluation method**

1095 The evaluation should be conducted using two or more of the methods selected from those in Table 1. In using
 1096 Table 1, the following should be noted:

1097 — the methods outlined represent a range of options and may not apply in all situations;

1098 — the various methods outlined may differ in their reliability;

1099 — typically, a combination of methods should be used to ensure an outcome that is objective, consistent, fair and
 1100 reliable.

Evaluation method	Objectives	Examples
Review of records	To verify the background of the auditor	Analysis of records of education, training, employment and audit experience
Feedback	To provide information about how the performance of the auditor is perceived	Surveys, questionnaires, personal references, testimonials, complaints, performance evaluation, peer review
Interview	To evaluate personal behaviours and communication skills, to verify information and test knowledge and to acquire additional information	Personal interviews
Observation	To evaluate personal behaviours and the ability to apply knowledge and skills	Role playing, witnessed audits, on-the-job performance
Testing	To evaluate personal behaviours and knowledge and skills and their application	Oral and written exams, psychometric testing
Post-audit review	To provide information on the auditor performance during the audit activities, identify strengths and weaknesses	Review of the audit report, interviews with the audit team leader, the audit team and, if appropriate, feedback from the auditee.

1101 **Table 1 — Possible Evaluation Methods**

1102 **7.5 Conduct the evaluation**

1103 In this step the information collected about the person is compared against the criteria set in 7.3. Where a person
 1104 expected to participate in the audit programme does not meet the criteria, additional training, work and/or audit
 1105 experience, and a subsequent re-evaluation should be performed.

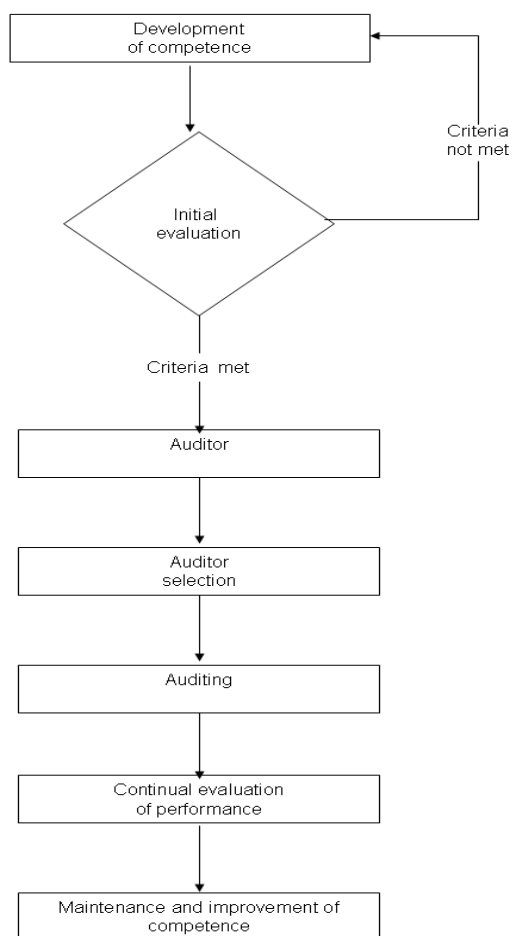
1106 Annex B provides hypothetical examples.

1107 **7.6 Maintenance and improvement of competence**

1108 Auditors should maintain their auditing competence through regular participation in management system audits and
 1109 continual professional development. Continual professional development involves the maintenance and
 1110 improvement of competence. This may be achieved through means such as additional work experience, training,
 1111 private study, coaching, attendance at meetings, seminars and conferences or other relevant activities. Auditors,
 1112 audit team leaders and those responsible for managing the audit programme should continually improve their
 1113 competence.

1114 The organization needing to conduct audits should establish suitable mechanisms for the continual evaluation of
 1115 performance of the auditors, audit team leaders and those responsible for managing the audit programme.

1116 The continual professional development activities should take into account results of post audit reviews, changes in
 1117 the needs of the individual and the organization needing to conduct audits, the practice of auditing, standards and
 1118 other requirements.



1119

1120

Figure 4 — Auditor competence evaluation

1121 **Annex A**
1122 **(Informative)**

1123 **Discipline-specific knowledge and skills of**
1124 **auditors**
1125
1126

1127 **A.1 General**

1128 The following sub-clauses give generic examples of discipline-specific knowledge and skills for auditors of
1129 management systems, intended as guidance to assist those responsible for managing the audit programme(s) to
1130 select or evaluate auditors.

1131 Other examples of discipline-specific knowledge and skills for auditors may be developed for management systems
1132 other than these examples. It is suggested that such examples follow the same general structure where possible in
1133 order to ensure comparability

1134 **A.2 Discipline-specific knowledge and skills of auditors – Quality**

1135 **A.2.1** Understanding of the quality management system requirements – principles and their
1136 applications:

1137 — Quality management system principles and their application.

1138 — Management system requirements for the quality standard being audited against.

1139 **A.2.2** Appreciation of legal and other requirements relevant to quality sufficient to enable the auditor to
1140 evaluate the quality management system:

1141 — Legal and other requirements dealing with quality and conformity assessment.

1142 — Sector-specific Legal and other requirements dealing with quality, if applicable.

1143 — Legal and other requirements dealing with product safety, labelling, prohibited substances, product life cycle,
1144 and acceptable work environment.

1145 — Industry and trade association best practices documents.

1146 — Guidance from regulatory bodies.

1147 — Customer agreements.

1148 **A.2.3** Understanding of the application of quality techniques sufficient to enable the auditor to examine
1149 the management system and generate appropriate audit findings and conclusions.

1150 Examples include:

1151 — Process control (e.g. statistical process control).

1152 — Risk techniques for determining risk (e.g. Failure mode and effect analysis – see ISO/IEC 31010).

1153 — Root cause analysis.

1154 — Process capability.

1155 **A.2.4** Understanding of the information (e.g. body of knowledge) that is fundamental to the processes,
1156 science and technology underlying quality sufficient to enable the auditor to evaluate management
1157 system elements associated with the discipline:

1158 — Quality terminology.

1159 — Measurement science and monitoring techniques.

1160 — Statistics.

1161 — General characteristics of processes and products, including services.

1162 **A.2.5** Understanding of quality knowledge related to the particular resources, assets sector, operation,
1163 or workplace being audited for the auditor to evaluate the auditee's activities, functions, processes,
1164 products and services:

1165 — Sector terminology.

1166 — Fundamental concepts and principals of operations of the sector.

1167 — Sector-specific processes and practices.

1168 — Appreciation of interested parties' expectations (e.g. expectations of the customers of the product/service).

1169 **A.3 Discipline-specific knowledge and skills of auditors – Environmental**

1170 **A.3.1** Understanding of environmental management system requirements and principles, and their
1171 application:

1172 — Environmental management system principles and their application.

1173 — Requirements of the environmental management system standard being audited against.

1174 **A.3.2** Appreciation of legal and other requirements relevant to environment sufficient to enable the
1175 auditor to evaluate the environmental management system:

1176 — Legal and other requirements dealing with the environment.

1177 — Process-specific legal and other requirements dealing with environmental protection, pollution prevention and
1178 resource efficiency.

1179 — Legal and other requirements dealing with labelling, use of hazardous substances, product life cycle, product
1180 stewardship.

1181 — Industry and trade association best practices documents.

1182 — Guidance from regulatory bodies.

1183 — Customer and interested parties agreements (e.g. community, non-governmental organizations, local
1184 authorities).

1185 **A.3.3** Understanding of environmental techniques sufficient to enable the auditor to examine the
1186 management system and generate appropriate audit findings and conclusions.

1187 Examples include:

1188 — Risk techniques for determining risk (e.g. environmental aspects/impact evaluation, including methods for
1189 evaluating significance).

1190 — Life cycle assessment.

1191 — Environmental performance evaluation.

1192 — Pollution control and sustainability practices (e.g. best available technique assessment for pollution control or
1193 energy efficiency).

1194 **A.3.4** Understanding of information (e.g. body of knowledge) that is fundamental to the processes,
1195 science and technology underlying environment sufficient to enable the auditor to evaluate management
1196 system elements associated with the discipline:

1197 — Environmental terminology.

1198 — Source reduction, waste minimization and sustainability (e.g. Carbon footprint and greenhouse gas emissions).

1199 — Measurement science and monitoring techniques.

1200 — Statistics.

1201 — Impact of human activities on the environment, including nuisance, cultural heritage, community impacts.

1202 — Interaction of ecosystems and biodiversity.

1203 — Environmental media (e.g. air, water, land).

1204 — Management of natural resources (e.g. fossil fuels, water, flora and fauna).

1205 — General measures of environmental protection.

1206 **A.3.5** Understanding of environmental knowledge related to the particular resources, sector, operation,
1207 or workplace being audited sufficient for the auditor to evaluate the auditee's activities, functions,
1208 processes, products and services:

1209 — Fundamental concepts and principals of operations of the sector.

1210 — Sector-specific processes and practices.

1211 — Interested parties' expectations (e.g. expectations of the surrounding community).

1212 — Environmental design.

1213 — Key characteristics of processes and products, including services.

- 1214 **A.4 Discipline-specific knowledge and/or skills of auditors – Occupational health and**
 1215 **safety (OH&S)**
- 1216 **A.4.1** Understanding of the OH&S management system requirements and principles, and their
 1217 application:
- 1218 — OH&S terminology.
- 1219 — OH&S management system principles and their application.
- 1220 — The OH&S Management system requirements from the standard (or requirements document) being used for
 1221 audit.
- 1222 **A.4.2** Appreciation of legal and other requirements relevant to OH&S sufficient to enable the auditor to
 1223 evaluate the OH&S management system:
- 1224 — OH&S specific legal and other requirements.
- 1225 — International conventions and treaties on OH&S.
- 1226 — Regulatory frameworks and guidance from regulatory bodies.
- 1227 — Legal and other requirements governing or affecting the organization's (industrial, business or governmental)
 1228 sector.
- 1229 — Industry, trade association and other "best practices" documents.
- 1230 — Employers' association, labour union and customer agreements.
- 1231 **A.4.3** Understanding of the application OH&S techniques sufficient to enable the auditor to examine the
 1232 management system and generate appropriate audit findings and conclusions.
- 1233 Examples include:
- 1234 — Hazard identification, risk assessment, determining controls, and risk communication (the determining of
 1235 controls should be based on the hierarchy of controls and should take account of the key success features of
 1236 the different methods).
- 1237 — The evaluation of health and human factors (including physiological and psychological factors) and the
 1238 principles for assessing them.
- 1239 — The development, use and evaluation of proactive and reactive performance measures and metrics.
- 1240 — The evaluation of the different types and levels of OH&S competence required across an organization and the
 1241 assessment of that competence.
- 1242 — The investigation and evaluation of work-related incidents (including accidents and work-related illnesses).
- 1243 — The encouragement of employee participation and involvement.
- 1244 — The encouragement of employee wellness or well-being and self-responsibility (in relation to smoking, drugs,
 1245 alcohol, weight related issues, exercise, stress, aggressive behaviour etc.), both during working hours and in
 1246 their private lives.

1247 **A.4.4** Understanding of the information that is fundamental to the process, science and technology
1248 underlying the discipline to enable the auditor to evaluate management system elements associated with
1249 the discipline:

- 1250 — The hazards and other factors affecting human performance in the workplace (such as physical, chemical and
1251 biological factors, as well as gender, age, handicap or other physiological, psychological or health factors).
- 1252 — The interaction of humans to machines, processes and the work environment (including workplace, ergonomic
1253 and safe design principles, information and communication technologies (ICT)).
- 1254 — Human behaviour and person to person interactions.
- 1255 — The principles and practices for emergency planning, prevention, response and recovery.
- 1256 — Methodologies for exposure monitoring and assessment.
- 1257 — Methodologies for incident (including accident and work-related illnesses) investigations.
- 1258 — Methodologies for monitoring and reporting on OH&S performance.
- 1259 — Medical information (including medical data).
- 1260 — Health-related information (including work-related exposure and illness monitoring data) – but giving especial
1261 consideration to confidential aspects.
- 1262 — systems of occupational exposure limit values (OEL's).

1263 **A.4.5** Understanding of discipline-specific knowledge related to the particular resources, assets, sector,
1264 operation, or workplace being audited for the auditor to evaluate the auditee's activities, services,
1265 products and processes:

- 1266 — Processes, equipment, raw materials, hazardous substances, process cycles, maintenance, logistics, work
1267 flow organization, working practices, shift-scheduling, organizational culture, leadership, behaviours, and other
1268 issues specific to the operation or sector.
- 1269 — Typical hazards and risks, including health and human factors, for the sector.
- 1270 — Sector-specific legal and other requirements.
- 1271 — Sector-specific OH&S risk assessment, risk control and OH&S management techniques.
- 1272 — Relevant indicators for proactive and reactive performance measures and metrics for the sector.

1273 **A.5 The discipline-specific knowledge and/or skills of auditors – Resilience, security,
1274 preparedness and continuity (RSPC) management**

1275 **A.5.1** Understanding of RSPC management system requirements – principles and applications:

- 1276 — Management system requirements for the RSPC standards being audited against

1277 **A.5.2** Appreciation of applicable legal and other requirements relevant to RSPC sufficient to enable the
1278 auditor to evaluate the RSPC management system:

- 1279 — Discipline specific legal and other requirements.

- 1280 — Statutes, regulations and case law governing or affecting the industry sector and the protection of tangible and
1281 intangible assets (including people, property, the environment, information, intellectual property and reputation)
- 1282 — Industry and trade association best practices.
- 1283 — Guidance from regulatory bodies.
- 1284 — Supply chain obligations and expectations.
- 1285 — Labour union and customer agreements.
- 1286 **A.5.3** Understanding of the application of RSPC techniques that enable the auditor to examine the
1287 management system and generate appropriate audit findings and conclusions.
- 1288 Examples include:
- 1289 — Asset identification and valuation.
- 1290 — Risk assessment (risk identification, analysis, evaluation).
- 1291 — Risk treatment (adaptive, proactive and reactive measures).
- 1292 — Developing performance measures and metrics.
- 1293 — Information integrity and sensitivity.
- 1294 — Exercise and testing methodologies.
- 1295 — Legal and other requirements pertaining to the collection and preservation of evidence.
- 1296 **A.5.4** Understanding of the information (body of knowledge) that is fundamental to the processes,
1297 science and technology underlying RSPC sufficient to enable the auditor to evaluate management
1298 system elements associated with the discipline:
- 1299 — Risk, resilience, security, preparedness, crisis, emergency, continuity and recovery management terminology.
- 1300 — Intelligence.
- 1301 — Principles of risk identification, analysis and evaluation, and risk communication.
- 1302 — Asset protection and physical security.
- 1303 — Prevention, deterrence, and security risk management.
- 1304 — Incident mitigation, response and crisis management.
- 1305 — Business/operational, continuity, emergency, recovery, management.
- 1306 — Emergency communications and services.
- 1307 **A.5.5** Understanding of RSPC knowledge related to the particular resources, assets, sector, operation,
1308 or workplace being audited for the auditor to evaluate the auditee's activities, functions, processes,
1309 products and services:
- 1310 — RSPC related asset, sector and operations terminology.

- 1311 — Asset identification, valuation and criticality analysis.
- 1312 — Asset management.
- 1313 — Information security and management.
- 1314 — Interested parties' needs.
- 1315 — Supply chain roles and interactions.
- 1316 — Sector-specific processes and practices.
- 1317 — Risk treatment and control technologies, techniques and process.

1318 **A.6 The discipline-specific knowledge and/or skills of auditors - Discipline:**
1319 **Transportation safety management**

1320 **A.6.1** Understanding of the transportation safety management system requirements – principles and
1321 applications:

- 1322 — Management system requirements for the safety management standards and/or regulations being audited
1323 against.

1324 **A.6.2** Appreciation of legal and other requirements to which the auditee subscribes relevant to
1325 transportation safety management sufficient to enable the auditor to evaluate the transportation safety
1326 management system:

- 1327 — Legal and other requirements dealing with safety management requirements (aviation, railway, marine, road
1328 traffic).
- 1329 — Statutes, regulations and case law governing or affecting the transportation sector and the protection of
1330 tangible and intangible assets (including people, property, the environment, information, intellectual property
1331 and reputation).
- 1332 — Sector specific industry association best practices.
- 1333 — Sector specific guidance from regulatory bodies.
- 1334 — Sector specific supply chain requirements.
- 1335 — Labour union and customer agreements.

1336 **A.6.3** Understanding of application of transportation safety management techniques that enable the
1337 auditor to examine the management system and generate appropriate audit findings and conclusions

1338 Examples include:

- 1339 — Risk assessment and mitigation.
- 1340 — Human Factor techniques.
- 1341 — Developing proactive and reactive performance measures and metrics.
- 1342 — Understanding safety culture approach.

1343 — Evaluation of operational incidents and accidents.

1344 **A.6.4** Understanding of the information (body of knowledge) that is fundamental to the processes,
 1345 science and technology underlying transportation safety management to enable the auditor to evaluate
 1346 management system elements associated with the discipline:

1347 — Safety management terminology.

1348 — Potential hazards and other workplace factors affecting safety.

1349 — Interaction of humans, machines, processes and the work environment.

1350 — Methodologies for incident investigations.

1351 — Methodologies for monitoring safety performance.

1352 — Human behaviour and interaction.

1353 **A.6.5** Understanding of transportation safety management knowledge related to the particular
 1354 resources, assets, sector, operation or workplace being audited for the auditor to evaluate the auditee's
 1355 activities, functions, processes, products and services:

1356 — Safety management related asset and operations terminology (aviation, railway, marine, road traffic).

1357 — Industry specific technology knowledge (aviation, railway, marine, road traffic).

1358 — Industry specific processes and operating procedures (aviation, railway, marine, road traffic).

1359 — Industry specific global safety network setup.

1360 **A.7 Discipline-specific knowledge and skills of auditors – Records**

1361 **A.7.1** Understanding of management system for records – principles, requirements and their application

1362 — Management system for records principles and their application.

1363 — Requirements of the management system for records standard being audited against.

1364 **A.7.2** Appreciation of business, legal and other requirements relevant to records sufficient to enable the
 1365 auditor to evaluate the management system for records:

1366 — Legal and other requirements dealing with general business requirements with records implications, e.g.
 1367 corporation law, finance and taxation law.

1368 — Legal and other requirements relating specifically to evidence, records and archives; access, privacy, data and
 1369 information protection, electronic commerce and communication.

1370 — Guidance from regulatory bodies.

1371 — Industry sector--specific legal and other requirements dealing with records requirements.

1372 — Industry and trade association best practices documents and international records management standards and
 1373 guidelines.

1374 — Identifiable expectations of the community about what is acceptable behaviour for the specific sector or
1375 organization, including good governance, the proper control of fraudulent or malicious behaviour, and
1376 transparency in decision making.

1377 — Identifiable requirements of business areas interested in evidence-based process and working in a consistent
1378 and recognized manner, e.g. risk management, security management, quality management, business
1379 continuity management, auditing management, environmental management, social responsibility, etc.

1380 **A.7.3** Understanding of techniques applicable to the management system for records sufficient to
1381 enable the auditor to examine the management system and generate appropriate audit findings and
1382 conclusions

1383 Examples include:

1384 — Developing performance measures and metrics.

1385 — The investigation and evaluation of records practices through interviewing, observation and validation.

1386 — Sample analysis of records created in business processes.

1387 — Risk assessment (e.g., assessment of risks through failure to create, maintain and control adequate records of
1388 the organization's business processes).

1389 — The performance and adequacy of records processes to create, capture and control records.

1390 — Assessment of the adequacy and performance of records system/s (including business systems to create and
1391 control records), the suitability of technological tools used, and facilities and equipment established.

1392 — Evaluation of the different levels records competence required across an organization and the assessment of
1393 those competence.

1394 **A.7.4** Understanding of information (e.g. body of knowledge) that is fundamental to the processes,
1395 science and technology underlying records management sufficient to enable the auditor to evaluate
1396 management system elements associated with the discipline:

1397 — Records, records management processes, and management systems for records terminology.

1398 — Significance of the content, context, structure, representation and control information (metadata) required to
1399 define and manage records and records systems.

1400 — Methodologies for developing records-specific instruments.

1401 — Understanding of technologies used for creation, capture, conversion and migration, and long term
1402 preservation of electronic/digital records.

1403 — Key characteristics of records, records systems, records processes and controls.

1404 — Identification and significance of the authorisation documentation for records processes.

1405 **A.7.5** Knowledge and understanding of records requirements and processes related to the particular
1406 resources, assets, sector, operation, or workplace being audited sufficient for the auditor to evaluate the
1407 auditee's activities, functions, processes, products and services in relation to the management system
1408 for records:

1409 — Fundamental concepts and principles of operations of the sector.

- 1410 — Sector-specific processes and practices and their implications for the key characteristics of records, records
- 1411 system, records processes and controls of the sector.
- 1412 — Sector-specific risk assessment and legal and regulatory requirements.
- 1413 — Design of sector processes where records processes have been integrated with sector-specific processes.

1414 **Annex B**
1415 (Informative)

1416 **Examples of discipline specific evaluations of audit team competence**
1417

1418 **B.1 General.**

1419 The following sub-clauses give generic examples of discipline-specific competence for audit teams for management system auditing, intended as guidance to assist those
1420 responsible for managing the audit programme(s) to select or evaluate auditors.

1421 The aim is to illustrate an approach for using the evaluation methodology described in Clause 7 of this International Standard.

1422 The examples below provide discipline-specific competence evaluation criteria for audit teams consistent with existing management systems. Other examples of discipline-
1423 specific competence for audit teams may be developed for management systems other than these examples. It is suggested that such examples comprise the same
1424 general composition where possible in order to ensure comparability.

1425 These examples are guidance for evaluating audit team competence and should not be considered requirements. This guidance provides examples that can be used in a
1426 fit-for-purpose audit team competence evaluation scheme.

1427
1428
1429
1430
1431
1432
1433
1434
1435
1436

1437 **B.2 Application of the evaluation process for an audit team undertaking an internal audit of an aviation organization's quality and**
 1438 **environmental management systems**

1439

Areas of competence	Personal behaviours and skills	Evaluation criteria	Evaluation method
Personnel behaviours	Ethical, open-minded, diplomatic, observant, perceptive, adaptable, tenacious, decisive, self reliant, acting with fortitude, well organized, open to improvement, culturally sensitive, team player.	Satisfactory performance in the workplace	Performance evaluation.
Generic knowledge and skills			
Audit principle, procedures, processes and techniques	Conduct an audit according to in-house procedures, communicating with known workplace colleagues.	Successfully completed an in-house auditor training course. Performed satisfactorily in X audits as a member of an internal audit team.	Review of training record. Observation. Peer review.
Management systems and other reference documents	Apply the relevant parts of the quality and environmental management system manual and related procedures.	Read and understood procedures relevant to the audit objectives, scope and criteria.	Review of training records. Testing. Interview.
Organizational situations	Describe the auditee's local structure and culture and any demarcation issues.	Worked for the auditee for at least five years at supervisor or managerial level.	Review of employment records.
Legal and other requirements	Identify and understand the application of the relevant laws and regulations related to product quality and the environment.	Successfully completed a training course on the laws relevant to the activities, process and/or products and services the subject of this	Review of training records.

		audit. OR Hold recognised certificate, diploma or degree in Country law.	
Risk assessment	Identify and understand the application of the risk assessment process to the auditee's activities.	Completed a training course on risk assessment or conducted risk assessments as part of a work related activity.	Review of training records. Interview. Review of employment records.
Industry (sector) specific skills			
Terminology	Knowledge and understanding of aircraft engineering terminology. Knowledge of Emissions from machining processes, waste oil, plating effluent.	Worked for an aviation company for minimum of five years. Employed as the wastewater treatment supervisor for at least three years.	Review of training record.
Process	Knowledge of engineering processes such as machining, welding, heat treatment. Knowledge of waste water, air emissions from machining.	Worked as an engineer within the aviation sector for not less than five years. Completed an indoor air quality training course.	Verification of professional qualification Supervisor Observation.
Technology	Knowledge of NCM, NDI and X ray. Knowledge of air abatement techniques, heavy metal waste water treatment.	Worked as in a technical capacity as a production supervisor or similar for at least two years. Acted as assistant facilities manager for not less than two years.	Employment record. Observation.

Organization specific skills

Organization specific skills			
Terminology	<p>Knowledge and understanding of landing gear, hydraulic servo's, pumps, cavitations.</p> <p>Understand gaseous emissions from machining processes.</p> <p>Knowledge of miscible oils, surfactants.</p>	<p>Worked for at least five years in supervisory role in the aviation sector.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Undertaken 3 prior audits of a manufacturing facility.</p> <p>Attended a hazardous chemicals training course.</p>	<p>Employment record.</p> <p>Review of training record.</p>
Process	<p>Knowledge of continuous machining, use of CMM, laser alignment techniques.</p> <p>Knowledge and understanding of methods of treatment of effluents and discharges.</p>	<p>Worked for at least five years in supervisory role in the aviation sector.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Acted as assistant facilities manager for not less than two years.</p>	<p>Employment record.</p> <p>Review of training record.</p>
Technology	<p>Knowledge of the application laser technology, CMM.</p> <p>Knowledge and understanding of plating discharges and their impact on local water courses.</p>	<p>Worked for at least five years in supervisory role in the aviation sector.</p> <p>Professional recognition or certification gained through study or registration by an accredited</p>	<p>Employment record.</p> <p>Review of training record.</p>

		<p>body.</p> <p>Acted as assistant facilities manager for not less than two years.</p> <p>Completed waste water discharge training course.</p>	
Statistical techniques	<p>Analytical ability to apply Cp Six Sigma techniques.</p> <p>Knowledge and understanding of statistical techniques applied to waste water treatment, numerical comparison of discharge levels to legal requirements.</p>	<p>Six Sigma black belt</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Completed wastewater discharge training course.</p> <p>Completed a statistical training course.</p>	<p>Employment record.</p> <p>Review of training record.</p>
Products/services	<p>Knowledge of servo's, axles, shock absorbers.</p> <p>Knowledge end of life protocols.</p>	<p>Completed three months working in the Sales and Marketing department.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p>	<p>Employment record.</p>
Risk	<p>Knowledge and understanding of process errors, forging impurities.</p> <p>Knowledge of environmental risks associated</p>	<p>Undertaken a risk management-training course. Assisted in the preparation FMEA studies.</p> <p>Professional recognition or certification gained through study or registration by an accredited</p>	<p>Employment record.</p>

	with discharges and processes.	body. Undertaken aspect/impact training course. Applied training course within the company.	Review of training record.
Interested parties	Aircraft manufacturers. Knowledge of the local regulators re standards and enforcement.	Formerly on staff of the customer complaints department. Previous liaison with regulator.	Employment record. Review of training record.
Management system specific skills (quality & environment)			
Terminology	Quality control, assurance, Cp, concentricity measurement. Aspects and impacts, control methods, resource efficiency.	Six sigma black belt. Completed an ISO 17024 accredited quality or environmental management system auditor training course. Undertaken aspect/impact training course. Applied training course within the company.	Employment record. Review of training record.
Process	Application of auditee's processes applied in different management stages. Knowledge of multiple discharges and their synergy.	Worked for at least five years in supervisory role in the aviation sector. Attended a hazardous chemicals training course. Completed waste water discharge training course. Completed an indoor air quality training course.	Employment record. Review of training record.

<p>Technology</p>	<p>Knowledge of technologies used across the auditee.</p> <p>Knowledge of technologies used across the auditee and its environmental interaction.</p>	<p>Worked for at least five years in supervisory role in the aviation sector.</p> <p>Undertaken 3 prior audits of a manufacturing facility.</p>	<p>Employment record.</p> <p>Review of training record.</p>
<p>Statistical techniques</p>	<p>Analytical ability to interpret statistical results.</p>	<p>Six sigma black belt.</p>	<p>Employment record.</p>
<p>Risk</p>	<p>Understand the auditee's risk assessment processes.</p> <p>Understanding of environmental aspects and impacts and antagonistic discharges.</p>	<p>Undertaken a risk management training course. Assisted in the preparation FMEA studies.</p> <p>Undertaken aspect/impact training course. Applied training course within the company.</p>	<p>Employment record.</p> <p>Review of training record.</p>

1440
1441
1442
1443
1444
1445
1446
1447
1448

1449
1450

B.3 Application of the evaluation process for an audit team undertaking an internal audit of an event management organization's Quality and OH&S management systems

Areas of competence	Personal behaviours and skills	Evaluation criteria	Evaluation method
Personal behaviours	Ethical, open-minded, diplomatic, observant, perceptive, adaptable, tenacious, decisive, self reliant, acting with fortitude, well organized, open to improvement, culturally sensitive, team player.	Satisfactory performance in the workplace.	Performance evaluation.
Generic knowledge and skills			
Audit principles, procedures, processes and techniques	Ability to conduct an audit according to in-house procedures, communicating with known workplace colleagues and subcontractors.	Successfully completed an in-house or external auditor training course. Performed satisfactorily in 3 audits as a member of an internal audit team.	Review of training record. Observation. Peer review.
Management systems and other reference documents	Ability to apply the relevant parts of the Quality and OH&S Management System Manual and related procedures.	Read and understood procedures relevant to the audit objective, scope and criteria.	Review of training records. Testing. Interview.
Organizational situations	Ability to describe the auditee's local structure and culture and any demarcation issues.	Worked for the auditee for at least one year at supervisor or managerial level or a similar organization or been employed by the auditee as a consultant for one year.	Review of employment records.
Legal and other requirements	Identify and understand the application of the relevant laws and regulations related to product quality and OH&S.	Successfully completed a training course on the laws relevant to the activities, process and/or products and services which are the subject of this audit or be registered as an OH&S inspector.	Review of training records.
Risk assessment	Understanding the principles of hazard identification, risk assessment and	Completed a training course on risk assessment or conducted risk	Review of training records.

	determining controls and their application to the auditee's activities.	assessments as part of a work related activity.	Interview. Review of employment records
Industry (sector) specific skills			
Terminology	Knowledge of generic terminology for the sector such as events, banquets, exhibitor, venue, exhibition, main contractor.	Employed in the sector or that similar nature for at least one year as a project/site manager, or designer, or as a subcontractor supervisor.	Review of employment record.
Process	Generic knowledge on the items such as exhibition design, assembly process, non standard and custom design booths.	Employed in the sector or that similar nature for at least one year as a project/site manager, or designer, or as a subcontractor supervisor.	Review of training record. Supervisor Observation.
Technology	Understanding knowledge of computer aided design (CAD) tools, audio visual, electrical and electronic equipment and its compatibility.	Electrical license or certificate in low voltage equipment or equivalent. Completed a training course on CAD or worked as designer for a similar organization for at least one year.	Review of training records. Employment record.
Organization specific skills			
Terminology	Generic knowledge on the items such as banquet, product launch, exhibition, organizer, exhibitor.	Employed in the sector or that similar nature for at least one year as a project/site manager, or designer, or as a subcontractor supervisor.	Employment record.
Process	Spray painting, carpentry, graphic design, interior design and fit out.	Employed as a supervisor or site manager for painting, carpentry, electrical installation or person with 3 years work experience in the relevant discipline or that of similar nature.	Employment record. Observation.
Technology	Hand and power tools. (Electrical or pneumatic), fastener usage, screws nails, nails gun, water based spray painting, and glazing.	Employed as a supervisor or site manager for carpentry, painting, electrical installation or person with 3 years work experience in the relevant discipline or that of similar nature.	Employment record. Observation.
Statistical techniques	Not applicable.		

Products/services	Knowledge of auditee's services such as booth design, interior fit out, event set ups.	Employed in sales department at this or similar organization, worked as a contractor setting up events.	Employment record.
Risk	Understanding OH&S risks associated with the location at which the services are offered.	Conducted or reviewed risk assessments in this sector or a similar sector for not less than one year.	Employment record. Interview.
Interested parties	Exhibitors, venue, organizer, subcontractors, local regulators.	Worked in the sector for not less than 12 months in a managerial or supervisory role. Previous liaison with regulator.	Employment record.
Management system specific skills (quality & occupational health and safety)			
Terminology	Quality control, assurance, customer satisfaction. OH&S hazards and risks, control measures.	Undertaken courses or training in quality control or quality assurance tool, or OH&S hazard identification, and applied training within the organization.	Employment record. Review of training record.
Process	Application of auditee's activities and processes utilized in different stages of the event management.	Worked for at least two years in supervisory role in the sector.	Employment record.
Technology	Generic knowledge such as CAD techniques applied to booth design or of a similar nature.	Worked as designer for at least two years in the sector or of similar nature.	Employment record.
Statistical techniques	Not applicable.		
Risk	Understand the auditee's risk assessment processes. Understanding of physical, chemical, biological and psychological hazards and	Undertaken a risk management-training course. Undertaken courses or training in hazard and risk control and applied training	Employment record. Review of training record.

1451

	risks.	within the organization.	
--	--------	--------------------------	--

1452

1453

B.4 Application of the evaluation process for an auditor in a hypothetical resilience, security, preparedness and/or continuity management internal audit programme

Areas of competence	Personal behaviours, and knowledge and skills	Evaluation criteria	Evaluation methods
Personal behaviours	Ethical, open-minded, diplomatic, observant, perceptive, adaptable, tenacious, decisive, self reliant, acting with fortitude, well organized, open to improvement, culturally sensitive, team player.	Satisfactory performance in the workplace.	Performance evaluation.
Generic knowledge and skills			
Audit principles, procedures and techniques	Ability to conduct an audit according to in-house procedures, communicating with known workplace colleagues.	Completed an ISO 17024 accredited personnel certification training programme. Performed four audits as a member of an internal audit team.	Review of training records. Observation. Peer review.
Management system and reference documents	Ability to apply the relevant parts of the Management System Manual and related procedures.	Read and understood the procedures in the Management System Manual relevant to the audit objectives, scope and criteria. Completed an ISO 17024 accredited resilience, security, preparedness or continuity management system personnel certification training programme.	Review of training records Testing. Interview.

Organizational situations	Ability to operate effectively within the auditee's culture and organizational and reporting structure.	Worked for the auditee (or similar) for at least one year in a supervisory role.	Review of employment records.
Applicable legal and other requirements	<p>Demonstrate knowledge of statutes, regulations and case law governing or affecting the industry sector and the protection of people, property and information including:</p> <ul style="list-style-type: none"> — statutes, regulations and laws pertaining to personnel protection programmes, methods and techniques, — laws pertaining to protection requirements for proprietary information and intellectual property, — laws pertaining to the collection and preservation of evidence, and — laws pertaining to managing the background investigation process. 	<p>Completed training in the legal aspects of resilience, security, crisis, continuity and/or emergency management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Implemented resilience, security, preparedness, response and recovery procedures as part of a work related activity in a decision making capacity for a minimum of 3 years.</p> <p>Security or continuity manager for a minimum of 5 years.</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>
Risk assessment	Identify and understand the application of the risk assessment process to the auditee's activities.	Completed a training course on risk assessment or conducted risk assessments as part of a work related activity for a minimum of 5 years.	<p>Review of training records.</p> <p>Interview.</p> <p>Review of employment records.</p>
Sector specific skills			
Terminology	Knowledge of generic terminology such as security, intelligence, physical protection, surveillance, incidents, emergency response, continuity.	Former member of the defence or police forces. Employment in the security sector as a supervisor or manager for at least 5 years.	Employment record.

Process	Understanding of resilience processes such as protection, vetting/screening, surveillance and monitoring (physical and electronic), warnings, evacuations and continuity planning.	Former member of the defence or police forces. Employment in the security sector as a supervisor or manager for at least 5 years.	Employment record.
Technology	Surveillance technology, electronic identification, vehicle tracking, listening equipment, alarm systems, warning systems, intrusion detection, fire detection and control.	Former member of the defence, emergency services or police forces. Employment in the resilience-related sector as a supervisor or manager for at least 5 years.	Employment record.
Organization specific skills			
Products/services	<p>Ability to identify and value the tangible and intangible assets, the auditee's system (people, property, information, reputation, etc.).</p> <p>Ability to identify and evaluate supply chain role and commitments.</p>	<p>Completed training in the application of risk assessment and management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Conducted risk assessments as part of a work related activity.</p> <p>Demonstrated work place experience.</p> <p>Training in supply chain management.</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p> <p>Observation.</p>
Terminology	<p>Knowledge of terminology related to risk management systems and treatments.</p> <p>Knowledge of terminology related to security management systems and treatments.</p> <p>Knowledge of terminology related to continuity management systems and</p>	<p>Completed training in the application of security risk, crisis, continuity and/or emergency management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Conducted risk assessments as part of</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p> <p>Observation.</p>

	<p>treatments.</p> <p>Knowledge of terminology related to emergency management systems and treatments.</p>	<p>a work related activity.</p> <p>Demonstrated work place experience.</p>	
Processes	<p>Ability to identify the activities, functions, processes and products of an organization and evaluate the consequences of their disruption.</p>	<p>Completed training in the application of risk assessment and management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Conducted risk assessments as part of a work related activity</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p> <p>Observation.</p>
Technology	<p>Ability to comprehend the technological context in which the audit is being conducted including sector-specific terminology, technical characteristics of processes and products, including services, and sector-specific processes and practices.</p> <p>Ability and understand technical risk treatment and control technologies (e.g. perimeter security protection technologies, alarms, access control, emergency management equipment)</p>	<p>Worked for at least five years in supervisory role in the specific industry sector.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Undertaken four prior audits of an appropriate manufacturing, transport, or distribution facility.</p> <p>Attended an industry-training course.</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>
Statistical Techniques	<p>Knowledge of quantitative and qualitative risk assessment methodologies (e.g. ISO 31010).</p>	<p>Completed training in the application of risk assessment and management methods.</p> <p>Professional recognition or certification gained through study or registration by</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>

		<p>an accredited body.</p> <p>Conducted risk assessments as part of a work related activity.</p>	<p>Observation.</p>
Risk	<p>Knowledge of risk assessment and impact analysis to examine efficiency risk management systems and treatments.</p>	<p>Completed training in the application of risk assessment and management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Conducted risk assessments as part of a work related activity.</p> <p>Demonstrated work place experience.</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p> <p>Observation.</p>
Interested parties	<p>Ability to identify appropriate interested parties including: customers, clients, partners, employees, shareholders, owners, vendors, the local community, first responders, government agencies, and regulators.</p>	<p>Completed training in the application of risk assessment and management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Conducted risk assessments as part of a work related activity.</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>
Management system specific skills			
Terminology	<p>Knowledge of terminology of the disciplines of risk, resilience, security, preparedness, crisis, response, emergency, continuity, emergency and disaster management including related technologies.</p>	<p>Completed training in the application of security risk, crisis, continuity and/or emergency management methods.</p> <p>Professional recognition or certification gained through study or registration by</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>

		an accredited body.	
Intelligence	Knowledge of information and intelligence sources, warning systems and their interpretation.	<p>Completed training in the application of risk assessment and management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Experience as security or continuity manager for 5 years.</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>
Management of Risk	<p>Ability to understand:</p> <ul style="list-style-type: none"> — risk, resilience, security, preparedness and continuity management principles and their application; — concepts to develop, manage or conduct risk assessments and impact analyses to determine the probable frequency, severity, and consequences of natural and man-made disasters and criminal activity on the auditee's profitability, resilience and/or ability to deliver products/services; — methodologies to control and manage risk and improve security, preparedness, continuity, recovery and loss prevention systems on a continuous basis through the use of surveys, review and assessment; — development and management of external relations programmes with 	<p>Completed training in the application of risk assessment and management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Conducted risk assessments as part of a work related activity.</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>

	<p>public sector law enforcement or other external organizations to assist in the achievement of loss prevention objectives; and</p> <p>— development and implementation of employee security, preparedness and continuity awareness programmes to achieve organizational goals and objectives.</p>		
Physical Security	<p>Ability to understand the fundamental relationships needed to manage and/or evaluate the current status of the physical security, fire detection and emergency and/or restoration capabilities.</p>	<p>Completed training in the application of physical security management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Implemented physical security analysis and procedures as part of a work related activity in a decision-making capacity for a minimum of 5 years.</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>
Emergency Practices	<p>Ability to understand the mitigation of potential consequences of disruptive incidents and emergency situations by identifying and prioritizing potential hazards and risks and developing plans to manage exposure to loss.</p>	<p>Completed training in the application of security risk, crisis, continuity and/or emergency management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Implemented preparedness, response and recovery procedures as part of a work related activity in a decision-making capacity for a minimum of 5 years.</p> <p>Experience as a member of the</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>

		emergency response team for a minimum of 3 years.	
Personnel Security	Ability to understand the development, implementation, management, and evaluation policies, procedures, programmes and methods for protection of human assets and to provide a secure work environment.	<p>Completed training in the application of security risk, crisis, continuity and/or emergency management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Implemented security, preparedness, response and recovery procedures as part of a work related activity in a decision-making capacity for a minimum of 5 years.</p> <p>Security manager for a minimum of 5 years.</p> <p>Experience as a member of the emergency response team for a minimum of 3 years.</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>
Information Security	Ability to understand the development and implementation of policies, procedures and standards to ensure information is evaluated and protected against all forms of unauthorized/inadvertent access, use, disclosure, modification, destruction or denial.	<p>Completed training in the application of information security management methods.</p> <p>Professional recognition or certification gained through study or registration by an accredited body.</p> <p>Implemented information and recovery procedures as part of a work related activity in a decision-making capacity for a minimum of 3 years.</p> <p>Information security manager for a</p>	<p>Review of training records, course content and results.</p> <p>Review of training and employment records.</p>

		minimum of 5 years.	
--	--	---------------------	--

1454
1455
1456
1457

Annex C (Informative) Additional Guidance for Auditors for Planning and Conducting Audits

1458

C.1 Applying audit methods

1459 An audit can be performed using a range of audit methods. An explanation of common used audit methods can be
1460 found in this Annex. The audit methods chosen for an audit depend on the defined audit objectives, scope and
1461 criteria, as well as duration and location (sites). Available auditor competence and any uncertainty arising from the
1462 application of audit methods should also be considered. Applying a variety and combination of different audit
1463 methods can optimize the efficiency and effectiveness of the audit process and its outcome.

1464 Performance of an audit involves an interaction among individuals with the management system(s) being audited
1465 and the technology used to conduct the audit. Table 1 provides examples of audit methods that can be used,
1466 singly or in combination, in order to achieve the audit objectives. If an audit involves the use of an audit team with
1467 multiple members, both on-site and remote methods may be used simultaneously.

Extent of involvement between the auditor and the auditee	Location of the auditor	
	On-Site	Remote
Human Interaction.	<ul style="list-style-type: none"> — Conducting interviews. — Filling checklists and questionnaires with auditee participation. — Document review with auditee participation. 	<ul style="list-style-type: none"> — Via communication means: <ul style="list-style-type: none"> — Conducting interviews. — Filling checklists and questionnaires. — Document review with auditee participation.
No Human Interaction	<ul style="list-style-type: none"> — Observation of work performed. — Site visit. — Filling checklists. — Sampling (e.g. products). — Document review (e.g. records). 	<ul style="list-style-type: none"> — Document review. — Observation of work performed via surveillance means.

On-site audit activities are performed at the location of the auditee. Remote audit activities are performed at any place other than the location of the auditee, independent of the distance.

Interactive audit activities involve interaction between the auditee's personnel and the audit team. Non-interactive audit activities involve no human interaction with persons being audited but do involve interaction with equipment, facilities and documentation.

1468

Table 1 – Applicable audit methods

- 1469 NOTE Additional information on site visits is given in C.6 of this Annex;
- 1470 The responsibility of the effective application of audit methods for any given audit remains with the person planning
1471 the audit. This will be either the person responsible for managing the audit programme or the audit team leader.
- 1472 The feasibility of remote audits can depend on the level of confidence between auditor and auditee.
- 1473 On the level of the audit programme, it should be ensured that the use of remote and on-site application of audit
1474 methods is balanced, to ensure satisfactory fulfilment of audit programme objectives.

1475 **C.2 Sources of information**

- 1476 The sources of information chosen may vary according to the scope and complexity of the audit and may include
1477 the following:
- 1478 — interviews with employees and other persons;
 - 1479 — observations of activities and the surrounding work environment and conditions;
 - 1480 — documents, such as policies, objectives, plans, procedures, standards, instructions, licences and permits,
1481 specifications, drawings, contracts and orders;
 - 1482 — records, such as inspection records, minutes of meetings, audit reports, records of monitoring programmes and
1483 the results of measurements;
 - 1484 — data summaries, analyses and performance indicators;
 - 1485 — information on the auditee's sampling programmes and on the procedures for the control of sampling and
1486 measurement processes;
 - 1487 — reports from other sources, for example, customer feedback, external surveys and measurements, other
1488 relevant information from external parties and supplier ratings;
 - 1489 — databases and web sites;
 - 1490 — simulations and modelling.

1491 **C.3 Conducting document review**

- 1492 The auditors should consider if:
- 1493 a) the information in the documents provided is :
 - 1494 — complete (all expected content is contained in the document);
 - 1495 — correct (the content is compliant to other reliable sources such as standards and regulations);
 - 1496 — consistent (the document is consistent in itself and to related documents);
 - 1497 — current (the content is up to date).
 - 1498 b) the documents being reviewed cover the audit scope and are capable of providing sufficient information to
1499 support the audit objectives;
 - 1500 c) the use of information and communication technologies, depending on the audit methods should promote
1501 efficient conduct of the audit. Specific care is needed for information security due to applicable regulations on

1502 protection of data (in particular for information, which lies outside the audit scope but is also contained in the
1503 document).

1504 **C.4 Preparing Work Documents**

1505 When preparing work documents, the audit-team should consider the following questions for each document:

1506 — Which audit record will be created by using this work document?

1507 — Which audit activity is affected by this particular work document?

1508 — Who will be the user of this work document?

1509 — What information is needed to prepare this work document?

1510 For combined audits it is essential that thorough preparation of work documents avoids duplication of audit
1511 activities by:

1512 — clustering of similar requirements from different criteria;

1513 — synchronization of related checklists and questionnaires.

1514 The work documents should be adequate to address all those elements of a management system within the scope
1515 of the audit and may be provided in any media.

1516 **C.5 Sampling strategy considerations for audits**

1517 **C.5.1 General**

1518 Audit sampling takes place when it is not practical or cost effective to examine all available information during an
1519 audit, e.g., records are too numerous or too dispersed geographically to justify the examination of every item in the
1520 population. Audit sampling is the process of selecting less than 100% of the items within the total available data set
1521 (population) to obtain and evaluate evidence about some characteristic of that population in order to form a
1522 conclusion concerning the population.

1523 The objective of any audit sampling activity should be to provide a data set in which the auditor(s) can have
1524 sufficient confidence that the data will support the achievement of the audit objectives.

1525 The risk associated with sampling is that the samples are not representative of the population from which they are
1526 drawn and thus the auditor's conclusion may be adversely biased and be different to that which would be reached if
1527 the whole population was examined. There may be other risks depending on the variability within the population to
1528 be sampled and the methodology chosen.

1529 Audit sampling typically involves the following steps:

1530 a) Determine the objectives of the sampling approach.

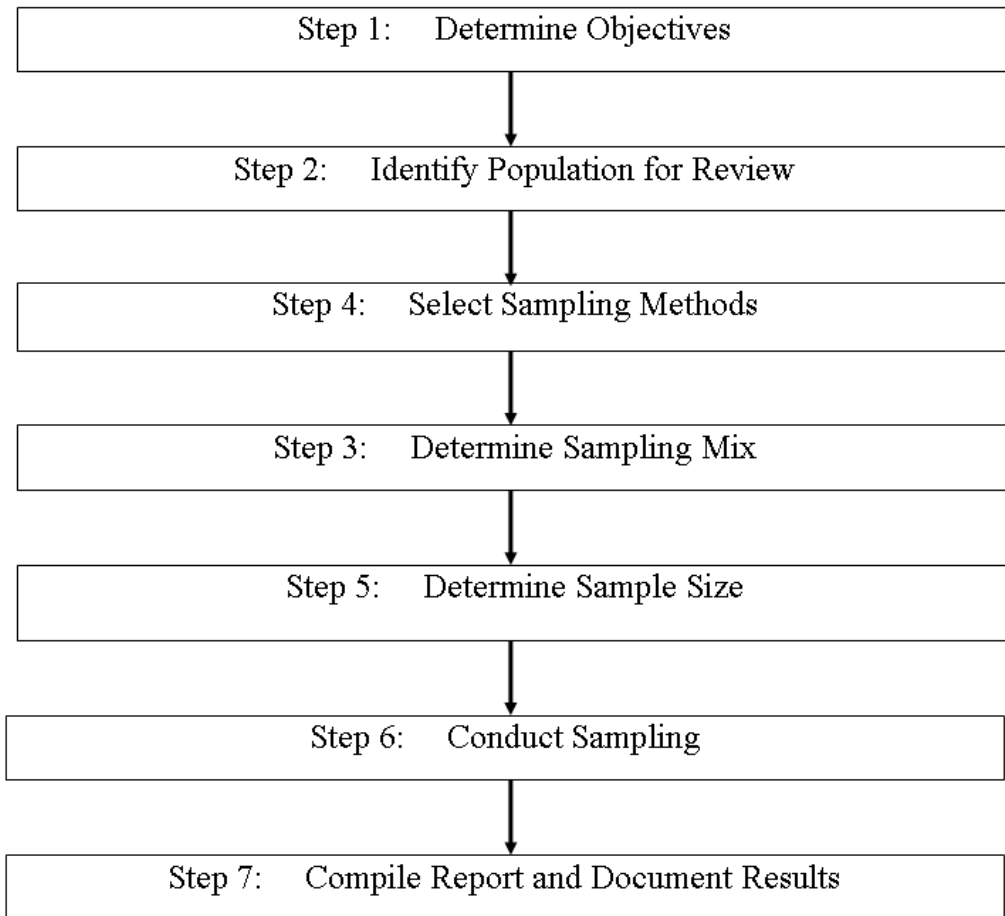
1531 b) Identify the extent and composition of the population to be sampled.

1532 c) Select a sampling method.

1533 d) Determine the sample size to be taken.

1534 e) Conduct the sampling activity.

1535 f) Compile and evaluate the results.



1536

1537

Figure C. 1 — Audit sampling process

1538 In identifying the need for sampling, primary consideration should be given to the quality of the available data, as
 1539 sampling poor data will not provide an accurate or useful result. The selection of an appropriate sample should be
 1540 based on both the type of sample needed and the analysis required, e.g. to infer a particular behaviour pattern or
 1541 draw inferences across a population.

1542 If required, reporting on the sample selected should also take into account the sample size, selection methodology,
 1543 estimates made based on the sample and the confidence level selected.

1544 Sampling in an audit can be based on statistics or judgement.

1545 **C.5.2 Judgemental sampling**

1546 Judgemental sampling relies on the knowledge, skills and experience of the audit team, (see clause 7).

1547 For judgement based sampling the following can be considered:

- 1548 — previous audit experience within the audit scope;
- 1549 — complexity of requirements (including legal requirements) to satisfy the objectives of the audit;
- 1550 — complexity and interaction of the organizations processes and management system elements;

- 1551 — degree of change in technology, human factors and/or system;
- 1552 — previous identified key risk areas and areas of improvement;
- 1553 — output from monitoring of management systems;
- 1554 A potential drawback to judgemental sampling is that there can be no scientific estimate of uncertainty or risk in the
1555 conclusions of the audit.

1556 **C.5.3 Statistical sampling**

1557 If there is a need to use statistical sampling methods the following apply:

- 1558 — statistical sampling designs generally use a sample selection process combined with probability theory. The
1559 result is generally expressed in terms of attributed or variable based outcomes. Attribute sampling is where
1560 there are only two possible outcomes (e.g. correct or incorrect/pass or fail). Variable based is where the
1561 outcome may occur in a continuous range;
- 1562 — sampling plans should be based on whether the auditor is expected to make an attribute based determination
1563 (pass/fail) regarding the proper implementation of the auditee's controls, such as plans, procedures, work
1564 instruction etc., or is examining issues related to product quality and/or a number of food safety, safety and
1565 health or environmental incidents or security breaches where a variable based outcome is likely. All sampling
1566 plans should identify the level of risk (or its inverse - confidence level) that maybe present. For example a
1567 sampling risk of 5% (confidence level of 95%) means that there is a 1:20 chance that the auditor will not detect
1568 something that will materially affect the outcome of the audit.

1569 **C.6 Guidance for site visits and observations**

1570 To minimize interference with the auditee's work processes and to ensure the safety of the audit team during a site
1571 visit or observation, the following should be considered:

1572 **C.6.1 Planning the visit**

- 1573 — ensure permission and access to those parts of the site or the work location, to be visited in accordance with
1574 the audit scope;
- 1575 — provide adequate information (e.g. briefing) to auditors on security, health (e.g. quarantine), occupational
1576 health and safety matters and cultural norms for the site visit including requested and recommended
1577 vaccination and clearances, if applicable;
- 1578 — ensure use of personal protective equipment (PPE) for auditors and arrange with auditee who will provide it, if
1579 applicable;
- 1580 — except for unscheduled ad hoc audits, ensure that personnel being visited will be informed about audit scope
1581 and objectives.

1582 **C.6.2 On-site activities**

- 1583 — avoid any unnecessary disturbance of the operational processes;
- 1584 — ensure that the audit team is using PPE properly;
- 1585 — schedule communication to minimize disruption;
- 1586 — adapt size of the audit team and the number of guides and observers in accordance with the audit scope to
1587 avoid interference of the operational processes as far as practicable;

- 1588 — do not touch or manipulate any equipment, unless explicitly permitted, even when competent and/or licensed;
- 1589 — if an incident occurs during the on-site visit, agree with the auditee on continuation or interruption
1590 (rescheduling) of the audit;
- 1591 — if taking pictures, ask for authorisation from management in advance and consider security and confidentiality
1592 matters and avoid taking photograph of individual persons without their permission;
- 1593 — if taking copies of documents of any kind, ask for permission in advance and consider confidentiality and
1594 security matters;
- 1595 — when taking notes, avoid collecting personal information unless required by the audit objectives and/or audit
1596 criteria.

1597 **C.7 Conducting interviews**

1598 Interviews are one of the important means of collecting information and should be carried out in a manner adapted
1599 to the situation and the person interviewed, either face to face or via communication means. However, the auditor
1600 should consider the following:

- 1601 — interviews should be held with persons from appropriate levels and functions performing activities or tasks
1602 within the scope of the audit;
- 1603 — interviews should be conducted during the normal working hours and, where practical, at the normal workplace
1604 of the person being interviewed;
- 1605 — attempting to put the person interviewed at ease prior to and during the interview;
- 1606 — the reason for the interview and any note taking should be explained;
- 1607 — interviews may be initiated by asking the persons to describe their work;
- 1608 — questions that bias the answers (i.e. leading questions) should be used carefully;
- 1609 — the results from the interview should be summarized and reviewed with the interviewed person;
- 1610 — the interviewed persons should be thanked for their participation and cooperation.

1611 **C.8 Audit findings**

1612 **C.8.1 Recording individual audit findings**

1613 For recording individual audit findings of conformity the following should be considered:

- 1614 — follow-up of previous audit records and conclusions;
- 1615 — requirements of audit clients;
- 1616 — findings exceeding normal practice, to be used as motivator, or opportunity for improvement.

1617 **C.8.2 Recording non conformities**

1618 Records of non conformities should include:

- 1619 — description of audit criteria requirement;

1620 — non conformity declaration;

1621 — audit evidence;

1622 — related audit findings, if applicable.

1623 **C.8.3 Dealing with findings related to multiple criteria**

1624 On an audit, it is possible to identify findings related to multiple criteria. Where an auditor identifies a finding linked
1625 to one criterion on a combined audit, the auditor should consider the possible impact on the corresponding/similar
1626 criteria of the other management systems.

1627 Depending on the arrangements with the audit client, the auditor may raise either:

1628 — separate findings for each criterion; or

1629 — a single finding, combining the references to multiple criteria.

1630 Depending on the arrangements with the person responsible for managing the audit programme, the auditor may
1631 guide the auditee on how to respond to those findings.

1632

Bibliography

1633

1634

1635

1636 [1] ISO9000:2005, Quality management systems -- Fundamentals and vocabulary

1637 [2] ISO 9001:2008, Quality management systems – Requirements

1638 [3] ISO 14001:2004, Environmental management systems -- Requirements with guidance for use

1639 [4] ISO 14050:2009, Environmental management -- Vocabulary

1640 [5] ISO 31000:2009, Risk management -- Principles and guidelines

1641 [6] ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management
1642 systems – Requirements

1643 [7] ISO 22000:2005, Food safety management systems -- Requirements for any organization in the food chain

1644 [8] OHSAS 18001:2007, Occupational Health and Safety Management Systems – Specifications

1645 [9] ISO/IEC 17021:2006, Conformity assessment -- Requirements for bodies providing audit and certification of
1646 management systems

1647 [10] ISO/CD 30301, Information and documentation -- Management system for records -- Requirements¹⁾

1648 [11] ISO 9001 Auditing Practices Group (APG) Papers available at
1649 www.iso.org/tc176/ISO9001AuditingPracticesGroup

1650

1) to be published