

DIN EN ISO 19011

ICS 03.100.70; 03.120.20

Ersatz für
DIN EN ISO 19011:2011-12 und
DIN EN ISO 19011
Berichtigung 1:2013-05

**Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018);
Deutsche und Englische Fassung EN ISO 19011:2018**

Guidelines for auditing management systems (ISO 19011:2018);
German and English version EN ISO 19011:2018

Lignes directrices pour l'audit des systèmes de management (ISO 19011:2018);
Version allemande et anglaise EN ISO 19011:2018

Gesamtumfang 99 Seiten

DIN-Normenausschuss Qualitätsmanagement, Statistik und Zertifizierungsgrundlagen (NQSZ)
DIN-Normenausschuss Grundlagen des Umweltschutzes (NAGUS)
DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)
DIN-Normenausschuss Lebensmittel und landwirtschaftliche Produkte (NAL)

Nationales Vorwort

Dieses Dokument (EN ISO 19011:2018) wurde vom Projektkomitee ISO/PC 302 „Guidelines for auditing management systems“ in Zusammenarbeit mit CCMC erarbeitet.

Das zuständige deutsche Normungsgremium ist der NA 147-00-07 GA „Gemeinschaftsarbeitsausschuss NQSZ/NAGUS/NIA/NAL: Audits“ im DIN-Normenausschuss Qualitätsmanagement, Statistik und Zertifizierungsgrundlagen (NQSZ).

Hinweis zur Übersetzung:

— „nonconformity“ kann im Deutschen auf verschiedene Weise übersetzt werden. Dabei ist „Nichtkonformität“ als die bevorzugte Benennung zu verwenden, „Fehler“ als zulässige Benennung.

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 9000:2015	siehe DIN EN ISO 9000:2015-11
ISO 9001	siehe DIN EN ISO 9001
ISO/IEC 17021-1	siehe DIN EN ISO/IEC 17021-1

Änderungen

Gegenüber DIN EN ISO 19011:2011-12 und DIN EN ISO 19011 Berichtigung 1:2013-05, wurden folgende Änderungen vorgenommen:

- a) Ergänzung der Grundsätze von Audits um den risikobasierten Ansatz;
- b) Erweiterung der Anleitung zur Verwaltung von Auditprogrammen, einschließlich der Risiken durch Auditprogramme;
- c) Erweiterung der Anleitung zur Durchführung eines Audits, insbesondere des Teils zur Auditplanung;
- d) Erweiterung der Anforderungen an allgemeine Kompetenzen von Auditoren;
- e) Anpassung der Terminologie, um den Prozess und nicht den Gegenstand (die „Sache“) wiederzugeben;
- f) Überarbeitung der Anforderungen zu Auditplänen;
- g) Streichung des vormaligen Anhangs A, der Kompetenzanforderungen für Audit-spezifische Managementsystemdisziplinen enthielt, da es aufgrund der Vielzahl der einzelnen Managementsystem-Normen nicht praxisgerecht wäre, Kompetenzanforderungen für alle Disziplinen aufzunehmen;
- h) Erweiterung des vormaligen Anhangs B (neuer Anhang A) um eine Anleitung zum Audit von (neuen) Konzepten, wie Organisationskontext, Führung und Verpflichtung, virtuellen Audits, Compliance und Lieferkette;
- i) Anpassung von Abschnitt 3 „Begriffe“ an DIN EN ISO 9000:2015-11 und Ergänzung von weiteren Begriffen;
- j) Norm redaktionell überarbeitet.

Frühere Ausgaben

DIN ISO 10011-1: 1992-06
DIN ISO 10011-2: 1992-06
DIN ISO 10011-3: 1992-06
DIN EN ISO 14010: 1996-11
DIN EN ISO 14011: 1996-11
DIN EN ISO 14012: 1996-11
DIN EN ISO 19011: 2002-12, 2011-12
DIN EN ISO 19011 Berichtigung 1: 2013-05

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9000:2015-11, *Qualitätsmanagementsysteme — Grundlagen und Begriffe (ISO 9000:2015); Deutsche und Englische Fassung EN ISO 9000:2015*

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 17021-1, *Konformitätsbewertung — Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren — Teil 1: Anforderungen*

Deutsche und Englische Fassung / German and English version

Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018)

Guidelines for auditing management systems
(ISO 19011:2018)

Lignes directrices pour l'audit des systèmes de management
(ISO 19011:2018)

Diese Europäische Norm wurde vom CEN am 18. Juni 2018 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

This European Standard was approved by CEN on 18 June 2018.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel
CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Inhalt

	Seite
Europäisches Vorwort	5
Vorwort	6
Einleitung	8
1 Anwendungsbereich	11
2 Normative Verweisungen	11
3 Begriffe	11
4 Auditprinzipien	18
5 Steuerung eines Auditprogramms	21
5.1 Allgemeines	21
5.2 Festlegen der Auditprogrammziele	25
5.3 Bestimmung und Beurteilung der Auditprogramm-Risiken und - Chancen	26
5.4 Festlegen des Auditprogramms	27
5.4.1 Rollen und Verantwortlichkeiten der Person(en), die das Auditprogramm steuert (steuern)	27
5.4.2 Kompetenz der Person(en), die das Auditprogramm steuert (steuern)	29
5.4.3 Festlegen des Ausmaßes des Auditprogramms	29
5.4.4 Bestimmen von Auditprogrammressourcen	31
5.5 Umsetzen des Auditprogramms	32
5.5.1 Allgemeines	32
5.5.2 Festlegen der Ziele, des Umfangs und der Kriterien für ein einzelnes Audit ...	33
5.5.3 Auswählen und Bestimmen der Auditmethoden	34
5.5.4 Auswählen der Auditteammitglieder ...	35
5.5.5 Zuweisen der Verantwortung für ein einzelnes Audit an den Auditteamleiter	36
5.5.6 Steuerung der Ergebnisse eines Auditprogramms	38
5.5.7 Verwalten und Aufrechterhalten von Aufzeichnungen zu Auditprogrammen	39
5.6 Überwachen des Auditprogramms	40
5.7 Überprüfen und Verbessern des Auditprogramms	41
6 Durchführen eines Audits	42
6.1 Allgemeines	42

Contents

	Page
European foreword	5
Foreword	6
Introduction	8
1 Scope	11
2 Normative references	11
3 Terms and definitions	11
4 Principles of auditing	18
5 Managing an audit programme	21
5.1 General	21
5.2 Establishing audit programme objectives	25
5.3 Determining and evaluating audit programme risks and opportunities ...	26
5.4 Establishing the audit programme	27
5.4.1 Roles and responsibilities of the individual(s) managing the audit programme	27
5.4.2 Competence of individual(s) managing audit programme	29
5.4.3 Establishing extent of audit programme	29
5.4.4 Determining audit programme resources	31
5.5 Implementing audit programme	32
5.5.1 General	32
5.5.2 Defining the objectives, scope and criteria for an individual audit	33
5.5.3 Selecting and determining audit methods	34
5.5.4 Selecting audit team members	35
5.5.5 Assigning responsibility for an individual audit to the audit team leader	36
5.5.6 Managing audit programme results	38
5.5.7 Managing and maintaining audit programme records	39
5.6 Monitoring audit programme	40
5.7 Reviewing and improving audit programme	41
6 Conducting an audit	42
6.1 General	42
6.2 Initiating audit	42
6.2.1 General	42

6.2	Veranlassen des Audits	42	6.2.2	Establishing contact with auditee	42
6.2.1	Allgemeines	42	6.2.3	Determining feasibility of audit.....	43
6.2.2	Herstellen des Kontakts mit der auditierten Organisation	42	6.3	Preparing audit activities.....	44
6.2.3	Bestimmen der Durchführbarkeit des Audits.....	43	6.3.1	Performing review of documented information	44
6.3	Vorbereiten der Audittätigkeiten.....	44	6.3.2	Audit planning.....	44
6.3.1	Durchführen der Überprüfung der dokumentierten Information.....	44	6.3.3	Assigning work to audit team.....	47
6.3.2	Planung des Audits.....	44	6.3.4	Preparing documented information for audit	48
6.3.3	Zuweisen von Arbeit an das Auditteam.....	47	6.4	Conducting audit activities.....	48
6.3.4	Vorbereiten dokumentierter Information für das Audit.....	48	6.4.1	General.....	48
6.4	Durchführen von Audittätigkeiten	48	6.4.2	Assigning roles and responsibilities of guides and observers.....	49
6.4.1	Allgemeines	48	6.4.3	Conducting opening meeting.....	50
6.4.2	Zuweisen von Rollen und Verantwortlichkeiten von Betreuern und Beobachtern	49	6.4.4	Communicating during audit.....	52
6.4.3	Durchführen der Eröffnungsbesprechung.....	50	6.4.5	Audit information availability and access.....	53
6.4.4	Kommunikation während des Audits ..	52	6.4.6	Reviewing documented information while conducting audit.....	53
6.4.5	Verfügbarkeit von und Zugriff auf Auditinformationen.....	53	6.4.7	Collecting and verifying information ..	54
6.4.6	Überprüfen der dokumentierten Information während der Durchführung des Audits	53	6.4.8	Generating audit findings	56
6.4.7	Sammeln und Verifizieren von Informationen.....	54	6.4.9	Determining audit conclusions.....	56
6.4.8	Erarbeiten von Auditfeststellungen	56	6.4.10	Conducting closing meeting	57
6.4.9	Bestimmung der Auditschlussfolgerungen	56	6.5	Preparing and distributing audit report.....	59
6.4.10	Durchführen der Abschlussbesprechung.....	57	6.5.1	Preparing audit report.....	59
6.5	Erstellen und Verteilen des Auditberichts	59	6.5.2	Distributing audit report.....	61
6.5.1	Erstellen des Auditberichts	59	6.6	Completing audit	61
6.5.2	Verteilen des Auditberichts.....	61	6.7	Conducting audit follow-up	62
6.6	Abschließen des Audits.....	61	7	Competence and evaluation of auditors.....	62
6.7	Durchführen von Auditfolgemaßnahmen	62	7.1	General.....	62
7	Kompetenz und Beurteilung von Auditoren	62	7.2	Determining auditor competence.....	64
7.1	Allgemeines	62	7.2.1	General.....	64
7.2	Bestimmen der Kompetenz von Auditoren	64	7.2.2	Personal behaviour	64
7.2.1	Allgemeines	64	7.2.3	Knowledge and skills.....	65
7.2.2	Persönliches Verhalten	64	7.2.4	Achieving auditor competence.....	71
7.2.3	Wissen und Fertigkeiten.....	65	7.2.5	Achieving audit team leader competence	71
7.2.4	Erwerben der Auditor-Kompetenz	71	7.3	Establishing auditor evaluation criteria.....	71
7.2.5	Erwerben der Auditteamleiter- Kompetenz	71	7.4	Selecting appropriate auditor evaluation method.....	72
7.3	Festlegen der Beurteilungskriterien für Auditoren	71	7.5	Conducting auditor evaluation	74
7.4	Auswählen der geeigneten		7.6	Maintaining and improving auditor competence	74
			Annex A (informative)	Additional guidance for auditors planning and conducting audits.....	75
			Bibliography		95

	Beurteilungsmethode für Auditoren....	72
7.5	Durchführen der Auditor- Beurteilung	74
7.6	Aufrechterhalten und Verbessern der Kompetenz des Auditors.....	74
	Anhang A (informativ) Zusätzliche Anleitung für Auditoren zum Planen und Durchführen von Audits.....	75
	Literaturhinweise.....	95

Bilder

Bild 1 — Prozessablauf für die Steuerung eines Auditprogramms	23
Bild 2 — Übersicht eines typischen Prozesses des Sammelns und Überprüfens von Informationen	55

Tabellen

Tabelle 1 —Verschiedene Arten von Audits	9
Tabelle 2 —Methoden zur Beurteilung von Auditoren.....	73
Tabelle A.1 — Auditmethoden.....	76

Figures

Figure 1 — Process flow for the management of an audit programme	24
Figure 2 — Overview of a typical process of collecting and verifying information.....	55

Tables

Table 1 — Different types of audits	9
Table 2 — Auditor evaluation methods	73
Table A.1 — Audit methods	76

Europäisches Vorwort

Dieses Dokument (EN ISO 19011:2018) wurde vom Projektkomitee ISO/PC 302 „Guidelines for auditing management systems“ in Zusammenarbeit mit CCMC erarbeitet.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Januar 2019, und etwaige entgegenstehende nationale Normen müssen bis Januar 2019 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt EN ISO 19011:2011.

Dieses Dokument wurde im Rahmen eines Mandates erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone CEN erteilt haben.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 19011:2018 wurde von CEN als EN ISO 19011:2018 ohne irgendeine Abänderung genehmigt.

European foreword

This document (EN ISO 19011:2018) has been prepared by Technical Committee ISO/PC 302 “Guidelines for auditing management systems” in collaboration with CCMC.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by January 2019, and conflicting national standards shall be withdrawn at the latest by January 2019.

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

This document supersedes EN ISO 19011:2011.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 19011:2018 has been approved by CEN as EN ISO 19011:2018 without any modification.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Themen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumententypen beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patent-erklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO) hinsichtlich technischer Handelshemmnisse (TBT) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Foreword

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

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

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

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

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

Dieses Dokument wurde vom Projektkomitee ISO/PC 302, *Guidelines for auditing management systems* erarbeitet.

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO 19011:2011), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- Ergänzung der Grundsätze von Audits um den risikobasierten Ansatz;
- Erweiterung der Anleitung zur Verwaltung von Auditprogrammen, einschließlich der Risiken durch Auditprogramme;
- Erweiterung der Anleitung zur Durchführung eines Audits, insbesondere des Teils zur Auditplanung;
- Erweiterung der Anforderungen an allgemeine Kompetenzen von Auditoren;
- Anpassung der Terminologie, um den Prozess und nicht den Gegenstand (die „Sache“) wiederzugeben;
- Entfernen des Anhangs, der Kompetenzanforderungen für Audit-spezifische Managementsystemdisziplinen enthielt (da es aufgrund der Vielzahl der einzelnen Managementsystem-Normen nicht praxisgerecht wäre, Kompetenzanforderungen für alle Disziplinen aufzunehmen);
- Erweiterung von Anhang A um eine Anleitung zum Audit von (neuen) Konzepten, wie Organisationskontext, Führung und Verpflichtung, virtuellen Audits, Compliance und Lieferkette.

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

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

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

- addition of the risk-based approach to the principles of auditing;
- expansion of the guidance on managing an audit programme, including audit programme risk;
- expansion of the guidance on conducting an audit, particularly the section on audit planning;
- expansion of the generic competence requirements for auditors;
- adjustment of terminology to reflect the process and not the object (“thing”);
- removal of the annex containing competence requirements for auditing specific management system disciplines (due to the large number of individual management system standards, it would not be practical to include competence requirements for all disciplines);
- expansion of Annex A to provide guidance on auditing (new) concepts such as organization context, leadership and commitment, virtual audits, compliance and supply chain.

Einleitung

Seit der Herausgabe der zweiten Ausgabe dieses Dokuments im Jahre 2011 sind eine Reihe neuer Managementsystem-Normen veröffentlicht worden, von welchen viele eine gemeinsame Struktur, identische Kernanforderungen sowie gemeinsame Begriffe und Kerndefinitionen haben. Daher ist es notwendig, das Auditieren von Managementsystemen in einem breiteren Ansatz zu berücksichtigen, und es müssen Anleitungen bereitgestellt werden, die allgemeinerer Natur sind. Auditergebnisse können Eingaben zu den analytischen Aspekten der Unternehmensplanung liefern und zur Ermittlung von Erfordernissen und Aktivitäten der Verbesserung beitragen.

Ein Audit kann anhand einer Reihe von Auditkriterien, getrennt oder kombiniert, durchgeführt werden, einschließlich, aber nicht beschränkt auf:

- Anforderungen, die in einer oder mehreren Managementsystem-Norm(en) definiert sind;
- Politiken und Anforderungen, die von relevanten interessierten Parteien festgelegt wurden;
- gesetzliche und behördliche Anforderungen;
- einen oder mehrere Managementsystem-Prozess(e), der/die von der Organisation oder anderen Parteien festgelegt wurde(n);
- Managementsystemplan(pläne) in Bezug auf die Bereitstellung spezifischer Leistungen eines Managementsystems (z. B. Qualitätsplan, Projektplan).

Dieses Dokument bietet eine Anleitung für alle Größen und Arten von Organisationen und Audits unterschiedlicher Umfänge und Skalierungen, darunter solche, die von großen Auditteams von in der Regel größeren Organisationen durchgeführt werden und solche, die von einzelnen Auditoren in großen und kleinen Organisationen durchgeführt werden. Diese Anleitung sollte entsprechend des Umfangs, der Komplexität und der Skalierung des Auditprogramms angepasst werden.

Introduction

Since the second edition of this document was published in 2011, a number of new management system standards have been published, many of which have a common structure, identical core requirements and common terms and core definitions. As a result, there is a need to consider a broader approach to management system auditing, as well as providing guidance that is more generic. Audit results can provide input to the analysis aspect of business planning, and can contribute to the identification of improvement needs and activities.

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

- requirements defined in one or more management system standards;
- policies and requirements specified by relevant interested parties;
- statutory and regulatory requirements;
- one or more management system processes defined by the organization or other parties;
- management system plan(s) relating to the provision of specific outputs of a management system (e.g. quality plan, project plan).

This document provides guidance for all sizes and types of organizations and audits of varying scopes and scales, including those conducted by large audit teams, typically of larger organizations, and those by single auditors, whether in large or small organizations. This guidance should be adapted as appropriate to the scope, complexity and scale of the audit programme.

Dieses Dokument konzentriert sich auf interne Audits (Erstparteien-Audit) und Audits, die von Organisationen bezüglich ihrer externen Anbieter und anderer externer interessierter Parteien (Zweitparteien-Audit) durchgeführt werden. Dieses Dokument kann auch für externe Audits nützlich sein, die für andere Zwecke als die Zertifizierung von Managementsystemen von Drittanbietern durchgeführt werden. ISO/IEC 17021-1 beschreibt die Anforderungen zur Auditierung von Managementsystemen für die Drittparteien-Zertifizierung. Dieses Dokument kann nützliche zusätzliche Anleitungen liefern (siehe Tabelle 1).

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

Tabelle 1 — Verschiedene Arten von Audits

Erstparteien-Audit	Zweitparteien-Audit	Drittparteien-Audit
Internes Audit	Audit durch externen Anbieter	Zertifizierungs- und/oder Akkreditierungsaudit
	Audit durch eine andere externe interessierte Partei	gesetzliches, behördliches und vergleichbares Audit

Table 1 — Different types of audits

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

Zur Vereinfachung der Lesbarkeit dieses Dokuments wird bei „Managementsystem“ die Singular-Form bevorzugt. Der Leser kann allerdings die Umsetzung der Anleitungen auf seine Situation anpassen. Dies bezieht sich auch auf die Anwendung der Termini „Person“ und „Personen“, „Auditor“ und „Auditoren“.

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

Dieses Dokument beabsichtigt, einen breiten Nutzerkreis anzusprechen, einschließlich Auditoren, Organisationen, die Managementsysteme verwirklichen, sowie Organisationen, die aus vertraglichen oder behördlichen Gründen Audits von Managementsystemen durchführen müssen. Nutzer dieses Dokuments können diese Anleitung auch bei der Erarbeitung ihrer eigenen, auditbezogenen Anforderungen verwenden.

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

Die Anleitung in diesem Dokument kann auch zum Zwecke der Selbsterklärung verwendet werden, und sie kann ebenfalls für Organisationen nützlich sein, die in die Auditorenschulung oder in die Zertifizierung von Personal einbezogen sind.

Es ist beabsichtigt, die Anleitung in diesem Dokument flexibel zu gestalten. Wie an verschiedenen Stellen im Text angegeben, kann die Nutzung dieser Anleitung entsprechend der Größe und dem Reifegrad des Managementsystems einer Organisation variieren. Die Art und Komplexität der zu auditierenden Organisation sowie die Ziele und der Umfang der durchzuführenden Audits sollten ebenfalls berücksichtigt werden.

Dieses Dokument verfolgt den Ansatz des kombinierten Audits, wenn zwei oder mehrere Managementsysteme verschiedener Disziplinen zusammen auditiert werden. Dort, wo diese Systeme in ein einziges Managementsystem integriert sind, sind die Auditprinzipien und -prozesse dieselben wie bei einem kombinierten Audit (bisweilen als integriertes Audit bekannt).

Dieses Dokument bietet eine Anleitung zur Steuerung eines Auditprogramms, zum Planen und Durchführen von Managementsystem-Audits sowie zur Kompetenz und Beurteilung eines Auditors sowie eines Auditteams.

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

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

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

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

1 Anwendungsbereich

Dieses Dokument bietet eine Anleitung zum Auditieren von Managementsystemen, einschließlich der Auditprinzipien, der Steuerung eines Auditprogramms und der Durchführung von Audits von Managementsystemen, sowie zur Beurteilung der Kompetenz derer, die in den Auditprozess einbezogen sind. Diese Tätigkeiten beziehen die Person(en), die das Auditprogramm steuert (steuern), Auditoren und Auditteams mit ein.

Es ist auf alle Organisationen, die interne oder externe Audits von Managementsystemen planen und durchführen oder ein Auditprogramm steuern müssen, anwendbar.

Die Anwendung dieses Dokuments auf andere Arten von Audits ist möglich, vorausgesetzt, besondere Aufmerksamkeit wird der speziellen Kompetenz, die erforderlich ist, beigemessen.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: unter <https://www.iso.org/obp>
- IEC Electropedia: unter <http://www.electropedia.org/>

3.1 Audit

systematischer, unabhängiger und dokumentierter Prozess zum Erlangen von *objektiven Nachweisen* (3.8) und zu deren objektiver Auswertung, um zu bestimmen, inwieweit *Auditkriterien* (3.7) erfüllt sind

Anmerkung 1 zum Begriff: Interne Audits, manchmal auch „Erstparteien-Audits“ genannt, werden von der Organisation selbst oder in ihrem Auftrag durchgeführt.

1 Scope

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

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

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

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1 audit

systematic, independent and documented process for obtaining *objective evidence* (3.8) and evaluating it objectively to determine the extent to which the *audit criteria* (3.7) are fulfilled

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

Anmerkung 2 zum Begriff: Externe Audits schließen ein, was allgemein „Zweit-“ und „Drittparteien-Audits“ genannt wird. Zweitparteien-Audits werden von Parteien, die ein Interesse an der Organisation haben, z. B. Kunden, oder von anderen Personen in deren Auftrag durchgeführt. Drittparteien-Audits werden von unabhängigen Organisationen durchgeführt, wie zum Beispiel denjenigen, welche eine Registrierung oder Zertifizierung der Konformität bieten, oder durch staatliche Behörden.

[QUELLE: ISO 9000:2015, 3.13.1, modifiziert — Anmerkungen zum Begriff wurden modifiziert]

3.2 kombiniertes Audit

Audit (3.1), das in einer einzelnen *auditierten Organisation* (3.13) an zwei oder mehr *Managementsystemen* (3.18) zusammen durchgeführt wird

Anmerkung 1 zum Begriff: Werden zwei oder mehr disziplinspezifische Managementsysteme in ein einzelnes Managementsystem integriert, wird dieses als ein integriertes Managementsystem bezeichnet.

[QUELLE: ISO 9000:2015, 3.13.2, modifiziert]

3.3 gemeinschaftliches Audit

Audit (3.1) durch zwei oder mehr Auditororganisationen an einer einzelnen *auditierten Organisation* (3.13)

[QUELLE: ISO 9000:2015, 3.13.3]

3.4 Auditprogramm

Festlegungen für einen Satz von einem oder mehreren *Audits* (3.1), die für einen spezifischen Zeitraum geplant werden und auf einen spezifischen Zweck gerichtet sind

[QUELLE: ISO 9000:2015, 3.13.4, modifiziert — Text wurde der Definition hinzugefügt]

3.5 Auditumfang

Ausmaß und Grenzen eines *Audits* (3.1)

Anmerkung 1 zum Begriff: Der Auditumfang schließt üblicherweise eine Beschreibung der physischen und virtuellen Standorte, der Funktionen, der Organisationseinheiten, der Tätigkeiten und Prozesse sowie des betrachteten Zeitraums ein.

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

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

3.2 combined audit

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

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

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

3.3 joint audit

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

[SOURCE: ISO 9000:2015, 3.13.3]

3.4 audit programme

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

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

3.5 audit scope

extent and boundaries of an *audit* (3.1)

Note 1 to entry: The audit scope generally includes a description of the physical and virtual-locations, functions, organizational units, activities and processes, as well as the time period covered.

Anmerkung 2 zum Begriff: Ein virtueller Standort ist ein Standort, an dem eine Organisation Arbeiten durchführt oder einen Dienst mithilfe einer Online-Umgebung leistet, die es Personen ermöglicht, unabhängig von physischen Standorten Prozesse auszuführen.

[QUELLE: ISO 9000:2015, 3.13.5, modifiziert — Anmerkung 1 zum Begriff wurde modifiziert, Anmerkung 2 zum Begriff wurde hinzugefügt]

3.6 Auditplan

Beschreibung der Tätigkeiten und Vorkehrungen für ein *Audit* (3.1)

[QUELLE: ISO 9000:2015, 3.13.6]

3.7 Auditkriterien

Satz von *Anforderungen* (3.23), die als Bezugsgrundlage (Referenz) verwendet werden, anhand derer ein Vergleich mit dem *objektiven Nachweis* (3.8) erfolgt

Anmerkung 1 zum Begriff: Wenn die Auditkriterien rechtliche (einschließlich gesetzliche und behördliche) Anforderungen darstellen, werden in einer *Auditfeststellung* (3.10) oft die Benennungen „compliance“ oder „non-compliance“ verwendet.^{N1)}

Anmerkung 2 zum Begriff: Die Anforderungen können Politiken, Verfahren, Arbeitsanweisungen, rechtliche Anforderungen, vertragliche Verpflichtungen usw. enthalten.

[QUELLE: ISO 9000:2015, 3.13.7, modifiziert — die Definition wurde geändert und die Anmerkungen 1 und 2 zum Begriff wurden hinzugefügt]

3.8 objektiver Nachweis

Daten, welche die Existenz oder Wahrheit von etwas bestätigen

Anmerkung 1 zum Begriff: Objektive Nachweise können durch Beobachtung, Messung, Test oder mit anderen Mitteln erbracht werden.

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

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

3.6 audit plan

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

[SOURCE: ISO 9000:2015, 3.13.6]

3.7 audit criteria

set of *requirements* (3.23) used as a reference against which *objective evidence* (3.8) is compared

Note 1 to entry: If the audit criteria are legal (including statutory or regulatory) requirements, the words “compliance” or “non-compliance” are often used in an *audit finding* (3.10).

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

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

3.8 objective evidence

data supporting the existence or verity of something

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

N1) Nationale Fußnote: Die Anmerkung 1 hat nur für den englischen Text Bedeutung.

Anmerkung 2 zum Begriff: Objektive Nachweise zum Zwecke des *Audits* (3.1) bestehen üblicherweise aus Aufzeichnungen, Tatsachenfeststellungen oder anderen Informationen, die für die *Auditkriterien* (3.7) zutreffen und verifizierbar sind.

[QUELLE: ISO 9000:2015, 3.8.3]

3.9 **Auditnachweis**

Aufzeichnungen, Tatsachenfeststellungen oder andere Informationen, die für die *Auditkriterien* (3.7) zutreffen und verifizierbar sind

[QUELLE: ISO 9000:2015, 3.13.8]

3.10 **Auditfeststellung**

Ergebnisse der Beurteilung der zusammengestellten *Auditnachweise* (3.9) gegen *Auditkriterien* (3.7)

Anmerkung 1 zum Begriff: Auditfeststellungen zeigen *Konformität* (3.20) oder *Nichtkonformität* (3.21) auf.

Anmerkung 2 zum Begriff: Auditfeststellungen können dazu führen, dass Risiken identifiziert, Verbesserungsmöglichkeiten aufgezeigt oder bewährte Praktiken aufgezeichnet werden.

Anmerkung 3 zum Begriff: Wenn die *Auditkriterien* aus gesetzlichen oder behördlichen Anforderungen ausgewählt werden, wird die *Auditfeststellung* im Englischen als „compliance“ oder „non-compliance“ bezeichnet.

[QUELLE: ISO 9000:2015, 3.13.9, modifiziert — Anmerkungen 2 und 3 zum Begriff wurden modifiziert]

3.11 **Auditschlussfolgerungen**

Ergebnis eines *Audits* (3.1) nach Berücksichtigung der *Auditziele* und aller *Auditfeststellungen* (3.10)

[QUELLE: ISO 9000:2015, 3.13.10]

3.12 **Auditauftraggeber**

Organisation oder Person, die ein *Audit* (3.1) anfordert

Anmerkung 1 zum Begriff: Im Falle eines internen *Audits* kann der Auftraggeber auch die *auditierte Organisation* (3.13) oder die Person(en) sein, die das Auditprogramm steuert (steuern). Anfragen nach externen *Audits* können von Quellen wie Behörden, Vertragspartnern oder potentiellen oder bestehenden Auftraggebern kommen.

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

[SOURCE: ISO 9000:2015, 3.8.3]

3.9 **audit evidence**

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

[SOURCE: ISO 9000:2015, 3.13.8]

3.10 **audit findings**

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

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

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

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

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

3.11 **audit conclusion**

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

[SOURCE: ISO 9000:2015, 3.13.10]

3.12 **audit client**

organization or person requesting an *audit* (3.1)

Note 1 to entry: In the case of internal audit, the *audit client* can also be the *auditee* (3.13) or the individual(s) managing the audit programme. Requests for external audit can come from sources such as regulators, contracting parties or potential or existing clients.

[QUELLE: ISO 9000:2015, 3.13.11 modifiziert — Anmerkung 1 zum Begriff wurde hinzugefügt]

3.13

auditierte Organisation

die gesamte Organisation oder Teile davon, die auditiert wird/werden

[QUELLE: ISO 9000:2015, 3.13.12, modifiziert]

3.14

Auditteam

eine oder mehrere Personen, die ein *Audit* (3.1) durchführen, nötigenfalls unterstützt durch *Sachkundige* (3.16)

Anmerkung 1 zum Begriff: Ein *Auditor* (3.15) des *Auditteams* (3.14) wird als Leiter des Auditteams eingesetzt.

Anmerkung 2 zum Begriff: Zum Auditteam können auch in der Ausbildung befindliche Auditoren gehören.

[QUELLE: ISO 9000:2015, 3.13.14]

3.15

Auditor

Person, die ein *Audit* (3.1) durchführt

[QUELLE: ISO 9000:2015, 3.13.15]

3.16

Sachkundiger

<Audit> Person, die spezielles Wissen oder Fachwissen dem *Auditteam* (3.14) zur Verfügung stellt

Anmerkung 1 zum Begriff: Spezielles Wissen oder Fachwissen beziehen sich auf die Organisation, die Tätigkeit, den Prozess, das Produkt, die Dienstleistung oder die Disziplin, die zu auditieren ist, oder die Sprache oder die Kultur.

Anmerkung 2 zum Begriff: Ein Sachkundiger für das *Auditteam* (3.14) handelt nicht als *Auditor* (3.15).

[QUELLE: ISO 9000:2015, 3.13.16, modifiziert — Anmerkungen 1 und 2 zum Begriff wurden modifiziert]

3.17

Beobachter

Person, die das *Auditteam* (3.14) begleitet, aber nicht als ein *Auditor* (3.15) handelt

[QUELLE: ISO 9000:2015, 3.13.17, modifiziert]

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

3.13

auditee

organization as a whole or parts thereof being audited

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

3.14

audit team

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

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

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

[SOURCE: ISO 9000:2015, 3.13.14]

3.15

auditor

person who conducts an *audit* (3.1)

[SOURCE: ISO 9000:2015, 3.13.15]

3.16

technical expert

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

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

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

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

3.17

observer

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

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

3.18

Managementsystem

Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer Organisation, um Politiken, Ziele und *Prozesse* (3.24) zum Erreichen dieser Ziele festzulegen

Anmerkung 1 zum Begriff: Ein Managementsystem kann eine oder mehrere Disziplinen behandeln z. B. Qualitätsmanagement, Finanzmanagement oder Umweltmanagement.

Anmerkung 2 zum Begriff: Die Elemente des Managementsystems beinhalten die Struktur der Organisation, Rollen und Verantwortlichkeiten, Planung sowie Betrieb, Politiken, Praktiken, Regeln, Überzeugungen, Ziele und Prozesse zum Erreichen dieser Ziele.

Anmerkung 3 zum Begriff: Der Anwendungsbereich eines Managementsystems kann die ganze Organisation, bestimmte Funktionen der Organisation, bestimmte Bereiche der Organisation oder eine oder mehrere Funktionsbereiche über eine Gruppe von Organisationen hinweg umfassen.

[QUELLE: ISO 9000:2015, 3.5.3, modifiziert — Anmerkung 4 zum Begriff wurde gelöscht]

3.19

Risiko

Auswirkung von Ungewissheit

Anmerkung 1 zum Begriff: Eine Auswirkung ist eine Abweichung vom Erwarteten — in positiver oder negativer Hinsicht.

Anmerkung 2 zum Begriff: Ungewissheit ist der Zustand des auch teilweisen Fehlens von Informationen im Hinblick auf das Verständnis eines Ereignisses oder Wissen über ein Ereignis, seine Folgen und seine Wahrscheinlichkeit.

Anmerkung 3 zum Begriff: Das Risiko wird häufig durch Bezugnahme auf mögliche Ereignisse (wie nach ISO Guide 73:2009, 3.5.1.3, festgelegt) und Folgen (wie nach ISO Guide 73:2009, 3.6.1.3, festgelegt) oder eine Kombination beider charakterisiert.

Anmerkung 4 zum Begriff: Risiko wird häufig mittels der Folgen eines Ereignisses (einschließlich Veränderungen der Umstände) in Verbindung mit der „Wahrscheinlichkeit“ (wie nach ISO Guide 73:2009, 3.6.1.1, festgelegt) seines Eintretens beschrieben.

[QUELLE: ISO 9000:2015, 3.7.9, modifiziert — Anmerkungen 5 und 6 zum Begriff wurden gelöscht]

3.18

management system

set of interrelated or interacting elements of an organization to establish policies and objectives, and *processes* (3.24) to achieve those objectives

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

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

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

[SOURCE: ISO 9000:2015, 3.5.3, modified — Note 4 to entry has been deleted]

3.19

risk

effect of uncertainty

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

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

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

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

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

3.20

Konformität

Erfüllung einer *Anforderung* (3.23)

[QUELLE: ISO 9000:2015, 3.6.11, modifiziert — Anmerkung 1 zum Begriff wurde gelöscht]

3.21

Nichtkonformität

Fehler

Nichterfüllung einer *Anforderung* (3.23)

[QUELLE: ISO 9000:2015, 3.6.9, modifiziert — Anmerkung 1 zum Begriff wurde gelöscht.]

3.22

Kompetenz

Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen

[QUELLE: ISO 9000:2015, 3.10.4, modifiziert — Anmerkungen zum Begriff gelöscht]

3.23

Anforderung

Erfordernis oder Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist

Anmerkung 1 zum Begriff: „Üblicherweise vorausgesetzt“ bedeutet, dass es für die Organisation und interessierte Parteien üblich oder allgemeine Praxis ist, dass das entsprechende Erfordernis oder die entsprechende Erwartung vorausgesetzt ist.

Anmerkung 2 zum Begriff: Eine festgelegte Anforderung ist eine, die beispielsweise in dokumentierter Information enthalten ist.

[QUELLE: ISO 9000:2015, 3.6.4, modifiziert — Anmerkungen 3, 4, 5 und 6 zum Begriff wurden gelöscht]

3.24

Prozess

Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben zum Erzielen eines vorgesehenen Ergebnisses verwendet

[QUELLE: ISO 9000:2015, 3.4.1, modifiziert — Anmerkungen zum Begriff wurden gelöscht]

3.20

conformity

fulfilment of a *requirement* (3.23)

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

3.21

nonconformity

non-fulfilment of a *requirement* (3.23)

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

3.22

competence

ability to apply knowledge and skills to achieve intended results

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

3.23

requirement

need or expectation that is stated, generally implied or obligatory

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

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

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

3.24

process

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

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

3.25 **Leistung**

messbares Ergebnis

Anmerkung 1 zum Begriff: Leistung kann sich entweder auf quantitative oder qualitative Feststellungen beziehen.

Anmerkung 2 zum Begriff: Leistung kann sich auf das Management von Tätigkeiten, *Prozessen* (3.24), Produkten, Dienstleistungen, Systemen oder Organisationen beziehen.

[QUELLE: ISO 9000:2015, 3.7.8, modifiziert — Anmerkung 3 zum Begriff wurde gelöscht.]

3.26 **Wirksamkeit**

Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden

[QUELLE: ISO 9000:2015, 3.7.11, modifiziert — Anmerkung 1 zum Begriff wurde gelöscht]

4 Auditprinzipien

Das Auditieren stützt sich auf eine Reihe von Prinzipien. Diese Prinzipien sollten dazu dienen, das Audit zu einem wirksamen und zuverlässigen Werkzeug zur Unterstützung von Managementpolitiken und -steuerungen zu machen, indem Informationen bereitgestellt werden, auf deren Grundlage eine Organisation handeln kann, um ihre Leistung zu verbessern. Die Einhaltung dieser Prinzipien ist eine Voraussetzung, um Auditschlussfolgerungen zu liefern, die relevant und ausreichend sind, und um unabhängig voneinander arbeitende Auditoren zu befähigen, zu ähnlichen Schlussfolgerungen unter ähnlichen Umständen zu gelangen.

Die Anleitung in den Abschnitten 5 bis 7 basiert auf den folgenden sieben Prinzipien:

a) Integrität: die Grundlage der Professionalität

Auditoren sowie die Person(en), die ein Auditprogramm steuert (steuern), sollte(n):

- ihre Arbeit moralisch vertretbar, mit Ehrlichkeit und Verantwortung ausführen;
- nur Audittätigkeiten durchführen, bezüglich derer sie Kompetenz besitzen;

3.25 **performance** measurable result

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

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

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

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

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

4 Principles of auditing

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

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

a) Integrity: the foundation of professionalism

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

- perform their work ethically, with honesty and responsibility;
- only undertake audit activities if competent to do so;

- ihre Arbeit unparteiisch ausführen, d. h. sachlich und in ihren Handlungen frei von Voreingenommenheit bleiben;
 - sensibel gegenüber jeglichen Einflüssen auf ihr Urteilsvermögen sein, die während der Durchführung eines Audits ausgeübt werden können.
- b) Sachliche Darstellung: die Pflicht, wahrheitsgemäß und genau zu berichten
- Auditfeststellungen, Auditschlussfolgerungen und Auditberichte sollten die Audittätigkeiten wahrheitsgemäß und genau widerspiegeln. Signifikante, während des Audits festgestellte Hindernisse und ungelöste Meinungsverschiedenheiten zwischen dem Auditteam und der auditierten Organisation sollten berichtet werden. Die Kommunikation sollte wahrheitsgetreu, genau, objektiv, zeitgerecht, klar und vollständig sein.
- c) Angemessene berufliche Sorgfalt: Anwendung von Sorgfalt und Urteilsvermögen beim Auditieren
- Auditoren sollten entsprechend der Bedeutung der Aufgabe, die sie ausführen, und dem Vertrauen, welches der Auditauftraggeber sowie andere interessierte Parteien in sie setzen, Sorgfalt walten lassen. Ein wichtiger Faktor bei der Ausführung ihrer Arbeit mit angemessener beruflicher Sorgfalt ist die Fähigkeit, in allen Auditsituationen begründete Urteile zu fällen.
- d) Vertraulichkeit: Sicherheit von Informationen
- Auditoren sollten bei der Verwendung und dem Schutz von Informationen, die sie im Verlaufe ihrer Aufgaben erworben haben, umsichtig sein. Auditinformationen sollten nicht unangemessen zur persönlichen Bereicherung des Auditors oder des Auditauftraggebers oder in einer Weise verwendet werden, die nachteilig für die berechtigten Interessen der auditierten Organisation ist. Dieses Konzept schließt den ordnungsgemäßen Umgang mit sensiblen oder vertraulichen Informationen ein.
- e) Unabhängigkeit: die Grundlage für die Unparteilichkeit des Audits sowie für die Objektivität der Auditschlussfolgerungen
- perform their work in an impartial manner, i.e. remain fair and unbiased in all their dealings;
 - be sensitive to any influences that may be exerted on their judgement while carrying out an audit.
- b) Fair presentation: the obligation to report truthfully and accurately
- Audit findings, audit conclusions and audit reports should reflect truthfully and accurately the audit activities. Significant obstacles encountered during the audit and unresolved diverging opinions between the audit team and the auditee should be reported. The communication should be truthful, accurate, objective, timely, clear and complete.
- c) Due professional care: the application of diligence and judgement in auditing
- Auditors should exercise due care in accordance with the importance of the task they perform and the confidence placed in them by the audit client and other interested parties. An important factor in carrying out their work with due professional care is having the ability to make reasoned judgements in all audit situations.
- d) Confidentiality: security of information
- Auditors should exercise discretion in the use and protection of information acquired in the course of their duties. Audit information should not be used inappropriately for personal gain by the auditor or the audit client, or in a manner detrimental to the legitimate interests of the auditee. This concept includes the proper handling of sensitive or confidential information.
- e) Independence: the basis for the impartiality of the audit and objectivity of the audit conclusions

Wo immer möglich, sollten Auditoren unabhängig von der Tätigkeit sein, die auditiert wird, und sie sollten in allen Fällen frei von Voreingenommenheit und Interessenkonflikten handeln. Bei internen Audits sollten Auditoren unabhängig von der auditierten Funktion sein, sofern dies in der Praxis umsetzbar ist. Die Auditoren sollten während des gesamten Auditprozesses Objektivität aufrechterhalten, um sicherzustellen, dass sich die Auditfeststellungen und -schlussfolgerungen nur auf die Auditnachweise stützen.

Bei kleineren Organisationen kann es sein, dass die internen Auditoren nicht komplett unabhängig von der Tätigkeit sind, die auditiert wird; es sollten aber alle Anstrengungen unternommen werden, um Voreingenommenheit zu beseitigen und Objektivität zu fördern.

- f) Faktengestützter Ansatz: die rationale Methode, um zu zuverlässigen und nachvollziehbaren Auditschlussfolgerungen in einem systematischen Auditprozess zu gelangen

Auditnachweise sollten verifizierbar sein. Üblicherweise sollten sie auf Stichproben aus den verfügbaren Informationen beruhen, da ein Audit während eines festgelegten Zeitraums und mit begrenzten Ressourcen durchgeführt wird. Die Stichprobenahme sollte angemessen erfolgen, da dies eng mit dem Vertrauen verbunden ist, das in die Auditschlussfolgerungen gesetzt werden kann.

- g) Risikobasierter Ansatz: ein Auditansatz, der Risiken und Chancen berücksichtigt

Der risikobasierte Ansatz sollte die Planung, Durchführung und Berichterstattung von Audits maßgeblich beeinflussen, um sicherzustellen, dass die Audits auf die für den Auditbeauftragten und für die Erreichung der Ziele des Auditprogramms relevanten Themen ausgerichtet sind.

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

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

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

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

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

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

5 Steuerung eines Auditprogramms

5.1 Allgemeines

Es sollte ein Auditprogramm erstellt werden, das Audits einschließen kann, die eine oder mehrere Managementsystem-Normen oder sonstige Anforderungen berücksichtigen und die entweder getrennt oder kombiniert (kombiniertes Audit) durchgeführt werden können.

Das Ausmaß eines Auditprogramms sollte auf der Größe und der Art der auditierten Organisation sowie auf der Art, Funktionalität, Komplexität, Art der Risiken und Chancen und dem Reifegrad des zu auditierenden Managementsystems basieren.

Die Funktionalität des Managementsystems kann noch komplexer sein, wenn der Großteil der wichtigen Funktionen ausgegliedert und unter der Leitung anderer Organisationen gesteuert wird. Dabei muss besonders dort, wo wichtige Entscheidungen getroffen werden und in den Bereichen, die die oberste Leitung des Managementsystems darstellen, Aufmerksamkeit gewidmet werden.

Gibt es mehrere Orte/Standorte (z. B. in unterschiedlichen Ländern) oder werden wichtige Funktionen ausgegliedert und unter der Führung einer anderen Organisation gesteuert, sollte besonders auf die Gestaltung, Planung und Validierung des Auditprogramms geachtet werden.

Bei kleineren oder weniger komplexen Organisationen kann das Auditprogramm entsprechend skaliert werden.

Um den Kontext der auditierten Organisation zu verstehen, sollte das Auditprogramm Folgendes bezüglich der auditierten Organisation berücksichtigen:

- die Ziele der Organisation;
- relevante externe und interne Themen;
- die Erfordernisse und Erwartungen relevanter interessierter Parteien;
- Anforderungen an Informationssicherheit und Vertraulichkeit.

Die Planung interner Auditprogramme und in einigen Fällen von Programmen zum Audit externer Anbieter kann so arrangiert werden, dass sie zu anderen Zielen der Organisation beiträgt.

5 Managing an audit programme

5.1 General

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

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

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

In the case of multiple locations/sites (e.g. different countries), or where important functions are outsourced and managed under the leadership of another organization, particular attention should be paid to the design, planning and validation of the audit programme.

In the case of smaller or less complex organizations the audit programme can be scaled appropriately.

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

- organizational objectives;
- relevant external and internal issues;
- the needs and expectations of relevant interested parties;
- information security and confidentiality requirements.

The planning of internal audit programmes and, in some cases programmes for auditing external providers, can be arranged to contribute to other objectives of the organization.

Die Person(en), die das Auditprogramm steuert (steuern), sollte(n) sicherstellen, dass die Integrität des Audits aufrechterhalten bleibt und kein ungebührlicher Einfluss auf das Audit ausgeübt wird.

Der Zuweisung von Ressourcen und Methoden bezüglich Angelegenheiten in einem Managementsystem mit höherem inhärenten Risiko und niedrigerem Leistungsniveau sollte Auditpriorität gegeben werden.

Die Steuerung des Auditprogramms sollte kompetenten Personen übertragen werden.

Das Auditprogramm sollte Informationen einschließen und Ressourcen identifizieren, sodass die Audits innerhalb des festgelegten Zeitrahmens wirksam und effizient durchgeführt werden können. Die Informationen sollten Folgendes umfassen:

- a) Ziele für das Auditprogramm;
- b) Risiken und Chancen in Verbindung mit dem Auditprogramm (siehe 5.3) und die Maßnahmen zu ihrer Behandlung;
- c) Umfang (Ausmaß, Grenzen, Standorte) jedes Audits innerhalb des Auditprogramms;
- d) Zeitplan (Anzahl/Dauer/Häufigkeit) der Audits;
- e) Auditarten, wie intern oder extern;
- f) Auditkriterien;
- g) anzuwendende Auditmethoden;
- h) Auswahlkriterien für die Auditteammitglieder;
- i) relevante dokumentierte Information.

Einige dieser Informationen sind möglicherweise erst nach Abschluss einer detaillierteren Auditplanung verfügbar.

Die Umsetzung des Auditprogramms sollte fortlaufend überwacht und gemessen werden (siehe 5.6), um sicherzustellen, dass seine Ziele erreicht worden sind. Das Auditprogramm sollte überprüft werden, um eventuell erforderliche Änderungen und mögliche Verbesserungsmöglichkeiten zu ermitteln (siehe 5.7).

Bild 1 veranschaulicht den Prozessablauf für die Steuerung eines Auditprogramms.

The individual(s) managing the audit programme should ensure the integrity of the audit is maintained and that there is not undue influence exerted over the audit.

Audit priority should be given to allocating resources and methods to matters in a management system with higher inherent risk and lower level of performance.

Competent individuals should be assigned to manage the audit programme.

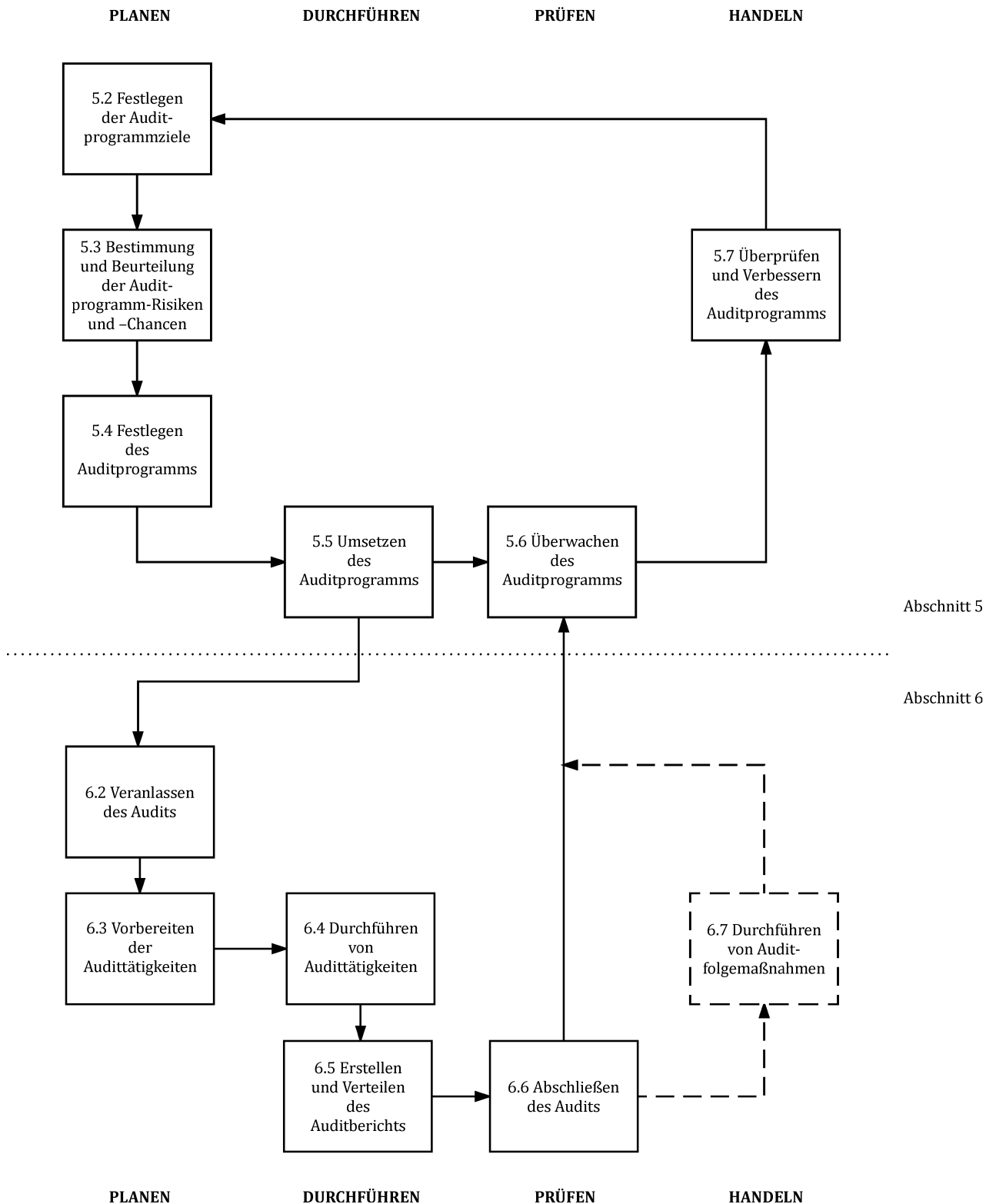
The audit programme should include information and identify resources to enable the audits to be conducted effectively and efficiently within the specified time frames. The information should include:

- a) objectives for the audit programme;
- b) risks and opportunities associated with the audit programme (see 5.3) and the actions to address them;
- c) scope (extent, boundaries, locations) of each audit within the audit programme;
- d) schedule (number/duration/frequency) of the audits;
- e) audit types, such as internal or external;
- f) audit criteria;
- g) audit methods to be employed;
- h) criteria for selecting audit team members;
- i) relevant documented information.

Some of this information may not be available until more detailed audit planning is complete.

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

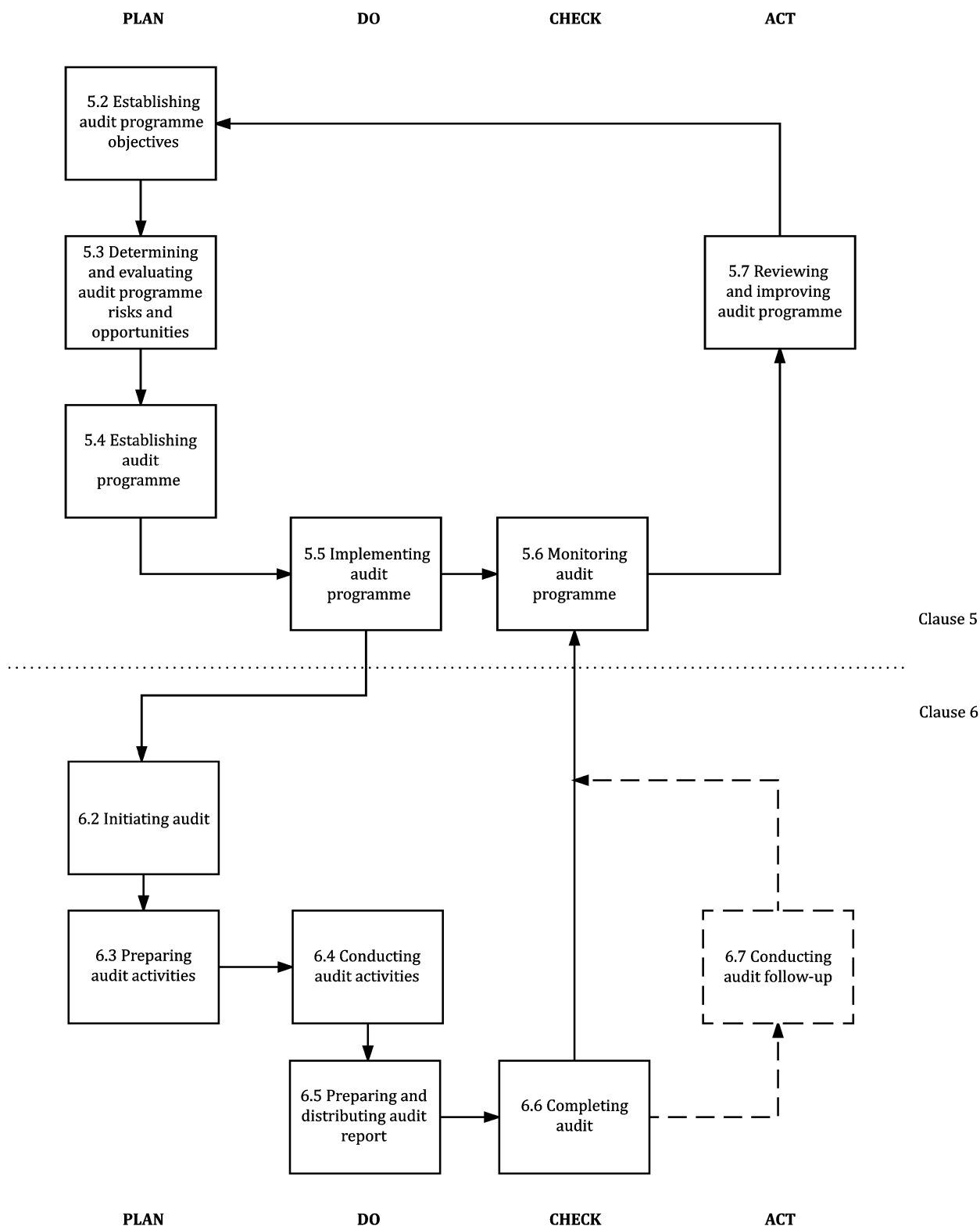
Figure 1 illustrates the process flow for the management of an audit programme.



ANMERKUNG 1 Dieses Bild veranschaulicht den Zyklus Planen-Durchführen-Prüfen-Handeln in diesem Dokument.

ANMERKUNG 2 Die Nummerierung bezieht sich auf die entsprechenden Abschnitte bzw. Unterabschnitte in diesem Dokument.

Bild 1 — Prozessablauf für die Steuerung eines Auditprogramms



NOTE 1 This Figure illustrates the application of the Plan-Do-Check-Act cycle in this document.

NOTE 2 Clause/subclause numbering refers to the relevant clauses/subclauses of this document.

Figure 1 — Process flow for the management of an audit programme

5.2 Festlegen der Auditprogrammziele

Der Auditauftraggeber sollte sicherstellen, dass die Auditprogrammziele erstellt werden, um das Planen und Durchführen der Audits zu lenken, und dass das Auditprogramm wirksam umgesetzt wird. Die Auditprogrammziele sollten im Einklang mit der strategischen Ausrichtung des Auditauftraggebers stehen sowie die Politik und Ziele des Managementsystems unterstützen.

Diese Ziele können auf der Berücksichtigung folgender Aspekte basieren:

- a) Erfordernisse und Erwartungen relevanter interessierter Parteien, sowohl extern als auch intern;
- b) Merkmale von und Anforderungen an Prozesse(n), Produkte(n), Dienstleistungen und Projekte(n) sowie Änderungen an diesen;
- c) Managementsystem-Anforderungen;
- d) Erfordernis der Beurteilung von externen Anbietern;
- e) Leistungsgrad der auditierten Organisation und Reifegrad des/der Managementsystems/Managementsysteme, wie dieser sich durch relevante Leistungsindikatoren (z. B. Schlüsselleistungskennzahlen (KPIs)), das Auftreten von Nichtkonformitäten oder Vorfällen oder Beschwerden interessierter Parteien widerspiegelt;
- f) identifizierte Risiken und Chancen für die auditierte Organisation;
- g) Ergebnisse aus vorangegangenen Audits.

Beispiele von Auditprogrammzielen können Folgendes einschließen:

- Chancen zur Verbesserung eines Managementsystems und dessen Leistungsfähigkeit zu identifizieren;
- die Fähigkeit der auditierten Organisation zu beurteilen, ihren Kontext zu bestimmen;
- die Fähigkeit der auditierten Organisation zu beurteilen, Risiken und Chancen zu bestimmen sowie wirksame Maßnahmen zu identifizieren und durchzuführen, um sie zu behandeln;

5.2 Establishing audit programme objectives

The audit client should ensure that the audit programme objectives are established to direct the planning and conducting of audits and should ensure the audit programme is implemented effectively. Audit programme objectives should be consistent with the audit client's strategic direction and support management system policy and objectives.

These objectives can be based on consideration of the following:

- a) needs and expectations of relevant interested parties, both external and internal;
- b) characteristics of and requirements for processes, products, services and projects, and any changes to them;
- c) management system requirements;
- d) need for evaluation of external providers;
- e) auditee's level of performance and level of maturity of the management system(s), as reflected in relevant performance indicators (e.g. KPIs), the occurrence of nonconformities or incidents or complaints from interested parties;
- f) identified risks and opportunities to the auditee;
- g) results of previous audits.

Examples of audit programme objectives can include the following:

- identify opportunities for the improvement of a management system and its performance;
- evaluate the capability of the auditee to determine its context;
- evaluate the capability of the auditee to determine risks and opportunities and to identify and implement effective actions to address them;

- alle relevanten Anforderungen zu erfüllen, z. B. gesetzliche und behördliche Anforderungen, Compliance-Verpflichtungen, Anforderungen zur Zertifizierung nach einer Managementsystem-Norm;
- Vertrauen in die Fähigkeit eines externen Anbieters zu erlangen und aufrechtzuerhalten;
- Bestimmung der fortdauernden Eignung, Angemessenheit und Wirksamkeit des Managementsystems der auditierten Organisation;
- die Kompatibilität und Abstimmung der Managementsystem-Ziele mit der strategischen Ausrichtung der Organisation zu beurteilen.
- conform to all relevant requirements, e.g. statutory and regulatory requirements, compliance commitments, requirements for certification to a management system standard;
- obtain and maintain confidence in the capability of an external provider;
- determine the continuing suitability, adequacy and effectiveness of the auditee's management system;
- evaluate the compatibility and alignment of the management system objectives with the strategic direction of the organization.

5.3 Bestimmung und Beurteilung der Auditprogramm-Risiken und -Chancen

Mit dem Kontext einer auditierten Organisation sind Risiken und Chancen verbunden, die in Zusammenhang mit einem Auditprogramm stehen und das Erreichen seiner Ziele beeinflussen können. Die Person(en), die das Auditprogramm steuert (steuern), sollte(n) die Risiken und Chancen, die bei der Entwicklung des Auditprogramms und der Ressourcenanforderungen berücksichtigt wurden, ermitteln und dem Auditauftraggeber vorlegen, damit diese angemessen behandelt werden können.

Risiken können mit Folgendem in Verbindung stehen:

- a) der Planung, z. B. das Versäumnis, relevante Auditziele festzulegen und das Ausmaß, die Anzahl, die Dauer, die Standorte und den Zeitplan der Audits zu bestimmen;
- b) den Ressourcen, z. B. nicht genügend Zeit, Ausrüstung und/oder Schulung zur Entwicklung des Auditprogramms bzw. zur Durchführung des Audits einzuräumen;
- c) der Auswahl des Auditteams, z. B. unzureichende Gesamtkompetenz zur wirksamen Durchführung von Audits;
- d) der Kommunikation, z. B. unwirksame externe/interne Kommunikationsprozesse/-kanäle;
- e) der Umsetzung, z. B. unwirksame Koordinierung der Audits im Rahmen des Auditprogramms oder fehlende Berücksichtigung von Informationssicherheit und Vertraulichkeit;

5.3 Determining and evaluating audit programme risks and opportunities

There are risks and opportunities related to the context of the auditee that can be associated with an audit programme and can affect the achievement of its objectives. The individual(s) managing the audit programme should identify and present to the audit client the risks and opportunities considered when developing the audit programme and resource requirements, so that they can be addressed appropriately.

There can be risks associated with the following:

- a) planning, e.g. failure to set relevant audit objectives and determine the extent, number, duration, locations and schedule of the audits;
- b) resources, e.g. allowing insufficient time, equipment and/or training for developing the audit programme or conducting an audit;
- c) selection of the audit team, e.g. insufficient overall competence to conduct audits effectively;
- d) communication, e.g. ineffective external/internal communication processes/channels;
- e) implementation, e.g. ineffective coordination of the audits within the audit programme, or not considering information security and confidentiality;