

DIN ISO 37301

ICS 03.100.02; 03.100.70

Ersatz für
DIN ISO 19600:2016-12**Compliance-Managementsysteme –
Anforderungen mit Leitlinien zur Anwendung (ISO 37301:2021)**Compliance management systems –
Requirements with guidance for use (ISO 37301:2021)Systèmes de management de la conformité –
Exigences et recommandations pour la mise en œuvre (ISO 37301:2021)

Gesamtumfang 55 Seiten

DIN-Normenausschuss Organisationsprozesse (NAOrg)

Inhalt

	Seite
Nationales Vorwort	4
Nationaler Anhang NA (informativ) Literaturhinweise	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	10
2 Normative Verweisungen	10
3 Begriffe	10
4 Kontext der Organisation	15
4.1 Verstehen der Organisation und ihres Kontextes	15
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	15
4.3 Festlegen des Anwendungsbereichs des Compliance-Managementsystems	15
4.4 Compliance-Managementsystem	16
4.5 Compliance-Verpflichtungen	16
4.6 Compliance-Risikobeurteilung	16
5 Führung	16
5.1 Führung und Verpflichtung	16
5.1.1 Oberstes Organ und oberste Leitung	16
5.1.2 Compliance-Kultur	17
5.1.3 Compliance-Führung	17
5.2 Compliance-Politik	18
5.3 Rollen, Verantwortlichkeiten und Befugnisse	18
5.3.1 Oberstes Organ und oberste Leitung	18
5.3.2 Compliance-Funktion	19
5.3.3 Leitung	20
5.3.4 Personal	20
6 Planung	21
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten	21
6.2 Compliance-Ziele und Planung zu deren Erreichung	21
6.3 Planung von Änderungen	22
7 Unterstützung	22
7.1 Ressourcen	22
7.2 Kompetenz	22
7.2.1 Allgemeines	22
7.2.2 Beschäftigungsprozess	23
7.2.3 Schulung	23
7.3 Bewusstsein	23
7.4 Kommunikation	24
7.5 Dokumentierte Information	25
7.5.1 Allgemeines	25
7.5.2 Erstellung und Aktualisierung dokumentierter Information	25
7.5.3 Lenkung dokumentierter Information	25
8 Betrieb	26
8.1 Betriebliche Planung und Steuerung	26
8.2 Festlegung der Steuerungen und Verfahren	26
8.3 Äußern von Bedenken	26
8.4 Untersuchungsprozesse	27
9 Bewertung der Leistung	27
9.1 Überwachung, Messung, Analyse und Bewertung	27
9.1.1 Allgemeines	27
9.1.2 Feedback-Quellen zur Compliance-Leistung	27
9.1.3 Entwicklung von Indikatoren	28

9.1.4	Compliance-Berichte	28
9.1.5	Aufzeichnungen	28
9.2	Internes Audit	28
9.2.1	Allgemeines	28
9.2.2	Programm des internen Audits	28
9.3	Managementbewertung	29
9.3.1	Allgemeines	29
9.3.2	Eingaben für die Managementbewertung	29
9.3.3	Managementbewertungsergebnisse	30
10	Verbesserung	30
10.1	Fortlaufende Verbesserung	30
10.2	Nichtkonformität und Korrekturmaßnahmen	30
Anhang A (informativ) Anleitung zur Verwendung dieses Dokuments		32
A.1	Hintergrund und Anwendungsbereich	32
A.1.1	Allgemeines	32
A.1.2	Anwendungsbereich	32
A.2	Normative Verweisungen	32
A.3	Begriffe	32
A.4	Kontext der Organisation	33
A.4.1	Verstehen der Organisation und ihres Kontextes	33
A.4.2	Verstehen der Erfordernisse und Erwartungen interessierter Parteien	33
A.4.3	Festlegen des Anwendungsbereichs des Compliance-Managementsystems	34
A.4.4	Compliance-Managementsystem	34
A.4.5	Compliance-Verpflichtungen	35
A.4.6	Compliance-Risikobeurteilung	36
A.5	Führung	37
A.5.1	Führung und Verpflichtung	37
A.5.2	Compliance-Politik	40
A.5.3	Rollen, Verantwortlichkeiten und Befugnisse	41
A.6	Planung	43
A.6.1	Maßnahmen zum Umgang mit Risiken und Möglichkeiten	43
A.6.2	Compliance-Ziele und Planung zu deren Erreichung	43
A.7	Unterstützung	43
A.7.1	Ressourcen	43
A.7.2	Kompetenz	43
A.7.3	Bewusstseinsbildung	45
A.7.4	Kommunikation	45
A.7.5	Dokumentierte Information	45
A.8	Betrieb	46
A.8.1	Betriebliche Planung und Steuerung	46
A.8.2	Festlegung der Steuerungen und Verfahren	47
A.8.3	Äußern von Bedenken	48
A.8.4	Untersuchungsprozesse	48
A.9	Bewertung der Leistung	49
A.9.1	Überwachung, Messung, Analyse und Bewertung	49
A.9.2	Internes Audit	52
A.9.3	Managementbewertung	52
A.10	Verbesserung	53
A.10.1	Fortlaufende Verbesserung	53
A.10.2	Nichtkonformität und Korrekturmaßnahmen	53
Literaturhinweise		55

Bilder

Bild 1 — Elemente eines Compliance-Managementsystems	8
--	---

Nationales Vorwort

Dieses Dokument enthält die deutsche Übersetzung der Internationalen Norm ISO 37301:2021, die vom Technischen Komitee ISO/TC 309 „Governance of organizations“ erarbeitet wurde, dessen Sekretariat von BSI (Verinigtes Königreich) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 175-00-01 AA „Governance und Compliance-Management“ im DIN-Normenausschuss Organisationsprozesse (NAOrg).

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

IEC 31010	siehe	DIN EN 31010
ISO 9000	siehe	DIN EN ISO 9000
ISO 9001	siehe	DIN EN ISO 9001
ISO 14001	siehe	DIN EN ISO 14001
ISO 19011	siehe	DIN EN ISO 19001
ISO 22000	siehe	DIN EN ISO 22000
ISO 26000	siehe	DIN EN ISO 26000
ISO 31000	siehe	DIN ISO 31000
ISO 37001	siehe	DIN ISO 37001
ISO 37002	siehe	DIN ISO 37002
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN ISO 19600:2016-12 wurden folgende Änderungen vorgenommen:

- a) dieses Dokument enthält jetzt Anforderungen mit zusätzlichen Leitlinien zur Nutzung basierend auf diesen Anforderungen;
- b) dieses Dokument folgt den ISO Anforderungen an eine harmonisierte Struktur für Managementsystemnormen.

Frühere Ausgaben

DIN ISO 19600: 2016-12

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN 31010, *Risikomanagement — Verfahren zur Risikobeurteilung*

DIN EN ISO 9000, *Qualitätsmanagementsysteme — Grundlagen und Begriffe*

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO 14001, *Umweltmanagementsysteme — Anforderungen mit Anleitung zur Anwendung*

DIN EN ISO 19001, *In-vitro-Diagnostika — Bereitstellung von Informationen durch den Hersteller von in-vitro-diagnostischen Reagenzien für biologische Färbungen*

DIN EN ISO 22000, *Managementsysteme für die Lebensmittelsicherheit — Anforderungen an Organisationen in der Lebensmittelkette*

DIN EN ISO 26000, *Leitfaden zur gesellschaftlichen Verantwortung*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN ISO 31000, *Risikomanagement — Leitlinien*

DIN ISO 37001, *Managementsysteme zur Korruptionsbekämpfung — Anforderungen mit Leitlinien zur Anwendung*

DIN ISO 37002, *Hinweismanagementsysteme — Leitlinien*

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsinstitute (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees der 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 Normungsthemen 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-Dokumentenarten 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 Patenterklärungen (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, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 309, *Governance of organization* erarbeitet.

Diese erste Ausgabe von ISO 37301 ersetzt ISO 19600:2014, die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zu ISO 19600:2014 sind folgende:

- dieses Dokument enthält jetzt Anforderungen mit zusätzlichen Leitlinien zur Nutzung basierend auf diesen Anforderungen;
- dieses Dokument folgt den ISO-Anforderungen an eine harmonisierte Struktur für Managementsystemnormen.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Einleitung

Organisationen, die langfristig erfolgreich sein wollen, benötigen die Einführung und Pflege einer Kultur der Compliance, die den Bedürfnissen und Erwartungen der unterschiedlichen Anspruchsgruppen Rechnung trägt. Compliance ist daher nicht nur Grundlage, sondern auch Gelegenheit für eine nachhaltig erfolgreiche Organisation.

Compliance ist ein fortlaufender Prozess und das Ergebnis einer Organisation, die ihren Verpflichtungen nachkommt. Die Nachhaltigkeit von Compliance wird erreicht, indem sie in die Kultur der Organisation und das Verhalten sowie die Einstellung ihrer Mitarbeiter eingebettet wird. Das Compliance-Management sollte seine Unabhängigkeit bewahren, gleichzeitig aber in die anderen Managementprozesse und die betrieblichen Anforderungen und Verfahren der Organisation integriert sein.

Ein wirksames, organisationsweites Compliance-Managementsystem versetzt eine Organisation in die Lage, ihr Bekenntnis zur Einhaltung einschlägiger Gesetze, regulatorischer Anforderungen, Industrie- und Organisationsnormen, sowie Good Governance Normen, bewährte Verfahren, ethischer Grundsätze und gesellschaftlicher Erwartungen darzulegen.

Die Auseinandersetzung einer Organisation mit dem Thema Compliance wird durch die Leitung und deren Umgang mit den zentralen Werten und allgemein anerkannten Normen der Good Governance, Ethik und gesellschaftlicher Entwicklung geformt. Die Verankerung von Compliance im Verhalten der Mitarbeiter einer Organisation hängt in erster Linie von der Führung auf allen Ebenen und von eindeutigen Werten einer Organisation sowie der Anerkennung und Umsetzung von Maßnahmen zur Förderung regelkonformer Verhaltensweisen ab. Ist dies nicht auf allen Ebenen der Organisation der Fall, so besteht das Risiko von Non-Compliance.

In verschiedenen Rechtsordnungen haben Gerichte bei der Strafzumessung für Gesetzesverstöße das Bekenntnis einer Organisation zu Compliance durch das Compliance-Managementsystem berücksichtigt. Aus diesem Grund können auch Regulierungsbehörden und Gerichte von diesem Dokument als Bezugspunkt profitieren.

Organisationen sind zunehmend überzeugt, dass sie durch die Anwendung verbindlicher Werte und eines angemessenen Compliance-Managements ihre Integrität wahren und Non-Compliance mit den Compliance-Verpflichtungen der Organisation vermeiden oder minimieren können. Integrität und wirksame Compliance sind daher zentrale Elemente eines guten und sorgfältigen Managements. Compliance trägt darüber hinaus zu einem sozialverantwortlichen Verhalten von Organisationen bei.

Eines der Ziele dieses Dokuments ist es, Organisationen bei der Entwicklung und Verbreitung einer positiven Compliance-Kultur zu unterstützen, unter Berücksichtigung, dass ein wirksames und solides Management von Compliance-Risiken als Chance betrachtet werden sollte, die Organisationen in Anbetracht der verschiedenen Vorteile verfolgt und ergriffen werden sollte, wie beispielsweise:

- Förderung von geschäftlichen Chancen und Nachhaltigkeit;
- Bewahrung und Stärkung des Ansehens und der Glaubwürdigkeit der Organisation;
- Berücksichtigung der Erwartungen der interessierten Parteien;
- Darlegung des Bekenntnisses der Organisation, ihre Compliance-Risiken wirksam und effizient zu bewältigen;
- Stärkung des Vertrauens dritter Parteien in die Fähigkeit der Organisation, nachhaltig erfolgreich zu sein;
- Minimierung des Risikos eines Regelverstößes und der damit verbundenen Kosten und Reputationsschäden.

Dieses Dokument legt Anforderungen fest und bietet Leitlinien für Compliance-Managementsysteme und empfohlene Praktiken. Sowohl die Anforderungen als auch die Leitlinien in diesem Dokument sind als anpassbar

vorgesehen und die Umsetzung kann je nach Größe und Reifegrad des Compliance-Managementsystems einer Organisation und des Kontexts, der Natur und der Komplexität ihrer Aktivitäten und Ziele variieren.

Dieses Dokument ist geeignet, um Compliance-bezogene Anforderungen in anderen Managementsystemen zu verstärken und Organisationen bei der Verbesserung des übergreifenden Managements all ihrer Compliance-Verpflichtungen zu unterstützen.

Bild 1 zeigt eine Übersicht der grundlegenden Elemente eines Compliance-Managementsystems.



Bild 1 — Elemente eines Compliance-Managementsystems

In diesem Dokument werden die folgenden Verbformen verwendet:

- „muss“ bezeichnet eine Anforderung;
- „sollte“ bezeichnet eine Empfehlung;
- „darf“ bezeichnet eine Erlaubnis;
- „kann“ bezeichnet eine Möglichkeit oder Fähigkeit.

Als „ANMERKUNG“ gekennzeichnete Information dient als Leitfaden zum Verständnis oder zur Erläuterung der zugehörigen Anforderung.

Anhang A bietet eine Leitlinie zur Anwendung dieses Dokuments.

1 Anwendungsbereich

Dieses Dokument legt Anforderungen fest und bietet Leitlinien für den Aufbau, die Entwicklung, die Umsetzung, die Bewertung, die Aufrechterhaltung und die Verbesserung eines wirksamen Compliance-Managementsystems innerhalb einer Organisation.

Dieses Dokument ist anzuwenden für alle Arten von Organisationen ungeachtet der Art, der Größe und der Natur der Aktivität und unabhängig davon, ob es sich um eine öffentliche, private oder gemeinnützige Organisation handelt.

Alle Anforderungen in diesem Dokument, die sich auf ein oberstes Organ beziehen, gelten für die oberste Leitung in Fällen, in denen eine Organisation kein oberstes Organ als separate Funktion besitzt.

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: verfügbar unter <https://www.iso.org/obp>

— IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

3.1

Organisation

Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre *Ziele* (3.6) zu erreichen

Anmerkung 1 zum Begriff: Der Begriff Organisation umfasst unter anderem Einzelunternehmer, Gesellschaft, Konzern, Firma, Unternehmen, Behörde, Handelsgesellschaft, Wohltätigkeitsorganisation, Institution, oder Teile oder eine Kombination der genannten, ob eingetragen oder nicht, öffentlich oder privat.

Anmerkung 2 zum Begriff: Wenn die Organisation Teil einer größeren Einheit ist, bezieht sich der Begriff „Organisation“ nur auf den Teil der größeren Einheit, der sich im Anwendungsbereich des Compliance-Managementsystems befindet.

3.2

interessierte Partei (bevorzugter Begriff)

Anspruchsgruppe (zulässiger Begriff)

Person oder *Organisation* (3.1), die eine Entscheidung oder Tätigkeit beeinflussen kann, die davon beeinflusst sein kann, oder die sich davon beeinflusst fühlen kann

3.3

oberste Leitung

Person oder Personengruppe, die eine *Organisation* (3.1) auf der obersten Ebene führt und steuert

Anmerkung 1 zum Begriff: Die oberste Leitung ist innerhalb der Organisation in der Lage, Verantwortung zu delegieren und Ressourcen bereitzustellen.

Anmerkung 2 zum Begriff: Wenn der Anwendungsbereich des *Managementsystems* (3.4) nur einen Teil einer Organisation umfasst, bezieht sich „oberste Leitung“ auf diejenigen, die diesen Teil führen und steuern.

Anmerkung 3 zum Begriff: In diesem Dokument bezieht sich der Begriff „oberste Leitung“ auf die höchste Ebene der Geschäftsleitung.

3.4

Managementsystem

Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer *Organisation* (3.1), um *Politiken* (3.5), *Ziele* (3.6) und *Prozesse* (3.8) zum Erreichen dieser Ziele festzulegen

Anmerkung 1 zum Begriff: Ein Managementsystem kann eine oder mehrere Disziplinen behandeln.

Anmerkung 2 zum Begriff: Die Elemente des Managementsystems beinhalten die Struktur der Organisation, Rollen und Verantwortlichkeiten, Planung sowie Betrieb.

3.5

Politik

Absichten und Ausrichtung einer *Organisation* (3.1), wie von der *obersten Leitung* (3.3) formell ausgedrückt

Anmerkung 1 zum Begriff: Eine Politik kann auch formell durch das *oberste Organ* (3.21) einer Organisation festgelegt werden.

3.6

Ziel

zu erreichendes Ergebnis

Anmerkung 1 zum Begriff: Ein Ziel kann strategisch, taktisch oder betrieblich sein.

Anmerkung 2 zum Begriff: Ziele können sich auf verschiedene Disziplinen (wie beispielsweise Finanzen, Gesundheit und Sicherheit, Umwelt) beziehen. Sie können beispielsweise organisationsweit oder projekt-, produkt-, dienstleistungs- oder prozess- (3.8) spezifisch sein.

Anmerkung 3 zum Begriff: Ein Ziel kann auf andere Weise ausgedrückt werden, z. B. als beabsichtigtes Ergebnis, als Zweck, als betriebstechnisches Kriterium, als *Compliance*- (3.26) Ziel oder durch Verwendung anderer Worte mit ähnlicher Bedeutung (z. B. Zielvorgabe, Zielstellung oder Einzelziel).

Anmerkung 4 zum Begriff: Im Kontext von *Compliance-Managementsystemen* (3.4) werden *Compliance-Ziele* von *Organisationen* (3.1) im Einklang mit ihrer *Compliance-Politik* (3.5) gesetzt, um bestimmte Ergebnisse zu erreichen.

3.7

Risiko

Auswirkung von Ungewissheit auf *Ziele* (3.6)

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 oder seine Wahrscheinlichkeit.

Anmerkung 3 zum Begriff: Risiko wird häufig durch Bezugnahme auf mögliche „Ereignisse“ (definiert in ISO Guide 73) und „Folgen“ (definiert in ISO Guide 73), oder durch 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“ (definiert in ISO Guide 73) seines Eintretens beschrieben.

3.8

Prozess

ein System von in Wechselbeziehung oder Wechselwirkung miteinander stehenden Tätigkeiten, die Eingaben nutzen oder umwandeln, um ein Ergebnis zu liefern

Anmerkung 1 zum Begriff: Ob das Ergebnis eines Prozesses Ergebnis, Produkt oder Dienstleistung genannt wird, ist abhängig vom Kontext der Referenz.

3.9

Kompetenz

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

3.10

dokumentierte Informationen

Information, die von einer *Organisation* (3.1) kontrolliert und aufrechterhalten werden muss, und das Medium, auf dem sie enthalten ist

Anmerkung 1 zum Begriff: Dokumentierte Informationen können in jeglichem Format oder Medium vorliegen, sowie aus jeglicher Quelle stammen.

Anmerkung 2 zum Begriff: Eine dokumentierte Information kann sich beziehen auf:

- das *Managementsystem* (3.4), einschließlich damit verbundener *Prozesse* (3.8);
- Informationen, die für den Betrieb der Organisation geschaffen wurden (Dokumentation);
- Nachweise erreichter Ergebnisse (Aufzeichnungen).

3.11

Leistung

messbares Ergebnis

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

Anmerkung 2 zum Begriff: Leistung kann sich auf das Führen und Steuern von Tätigkeiten, *Prozessen* (3.8), Produkten, Dienstleistungen, Systemen oder *Organisationen* (3.1) beziehen.

3.12

fortlaufende Verbesserung

wiederkehrende Tätigkeit zum Steigern der *Leistung* (3.11)

3.13

Wirksamkeit

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

3.14

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* (3.1) und andere *interessierte Parteien* (3.2) üblich oder allgemeine Praxis ist, dass das entsprechende Erfordernis oder die entsprechende Erwartung vorausgesetzt wird.

Anmerkung 2 zum Begriff: Eine festgelegte Anforderung ist eine, die z. B. in *dokumentierter Information* (3.10) enthalten ist.

3.15**Konformität**

Erfüllung einer *Anforderung* (3.14)

3.16**Nichtkonformität**

Nichterfüllung einer *Anforderung* (3.14)

Anmerkung 1 zum Begriff: Eine Nichtkonformität ist nicht notwendigerweise eine *Non-Compliance* (3.27).

3.17**Korrekturmaßnahme**

Maßnahme zum Beseitigen der Ursache einer *Nichtkonformität* (3.16) und zum Verhindern des erneuten Auftretens

3.18**Audit**

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

Anmerkung 1 zum Begriff: Ein Audit kann ein internes Audit (Erstparteien-Audit) oder externes Audit (Zweit- oder *Drittparteien-* (3.30) Audit) sein und es kann ein kombiniertes Audit (Verbindung zweier oder mehrerer Disziplinen) sein.

Anmerkung 2 zum Begriff: Ein internes Audit wird von der *Organisation* (3.1) selbst durchgeführt, oder von einer externen Seite in ihrem Auftrag.

Anmerkung 3 zum Begriff: „Auditnachweis“ und „Auditkriterium“ sind in ISO 19011 definiert.

Anmerkung 4 zum Begriff: Unabhängigkeit kann dadurch nachgewiesen werden, dass keine Verantwortlichkeit für die zu auditierende Tätigkeit besteht oder keine Vorurteile oder Interessenkonflikte vorliegen.

3.19**Messung**

Prozess (3.8) zum Bestimmen eines Werts

3.20**Überwachung**

Bestimmung des Zustands eines Systems, eines *Prozesses* (3.8) oder einer Tätigkeit

Anmerkung 1 zum Begriff: Zur Bestimmung des Zustands kann es erforderlich sein, zu prüfen, zu beaufsichtigen oder kritisch zu beobachten.

3.21**oberstes Organ**

Person oder Personengruppe mit der höchsten Verantwortung und Befugnis für die Tätigkeiten, Führung und *Politiken* (3.5) einer *Organisation* (3.1) und an welche die *oberste Leitung* (3.3) berichtet und ihr gegenüber rechenschaftspflichtig ist

Anmerkung 1 zum Begriff: Nicht alle Organisationen und insbesondere nicht kleinere Organisationen werden ein oberstes Organ haben, das separat zur obersten Leitung besteht.

Anmerkung 2 zum Begriff: Ein oberstes Organ kann unter anderem einen Aufsichtsrat, Ausschüsse eines Aufsichtsrats, einen Verwaltungsrat oder Treuhänder umfassen.

3.22

Personal

Personen in einer Beziehung, die nach nationalen Gesetzen oder Rechtspraxis als Arbeitsverhältnis anerkannt wird, oder in einer vertraglichen Beziehung steht, die von ihrer Tätigkeit in der *Organisation* (3.1) abhängt

3.23

Compliance-Funktion

Person oder Gruppe von Personen mit der Verantwortlichkeit und Befugnis für den Betrieb des *Compliance-Managementsystems* (3.4)

Anmerkung 1 zum Begriff: Vorzugsweise wird eine Person mit der Beaufsichtigung des Compliance-Managementsystems beauftragt.

3.24

Compliance-Risiko

Wahrscheinlichkeit des Auftretens und die Folgen von *Non-Compliance* (3.27) mit den *Compliance-Verpflichtungen* (3.25) der *Organisation* (3.1)

3.25

Compliance-Verpflichtungen

Anforderungen (3.14), die eine *Organisation* (3.1) zwingend erfüllen muss sowie die Anforderungen, der sie sich freiwillig unterwirft

3.26

Compliance

Erfüllen aller *Compliance-Verpflichtungen* (3.25) einer *Organisation* (3.1)

3.27

Non-Compliance

Nichterfüllung von *Compliance-Verpflichtungen* (3.25)

3.28

Compliance-Kultur

Werte, ethische Grundsätze, Überzeugungen und *Verhalten* (3.29), die in der gesamten *Organisation* (3.1) bestehen und im Zusammenspiel mit den Strukturen und Steuerungssystemen der Organisation einen Verhaltensstandard schaffen, der die *Compliance* (3.26) fördert

3.29

Verhalten

Verhaltensweisen und Praktiken, die Ergebnisse für Kunden, Mitarbeiter, Lieferanten, Märkte und Gemeinschaften beeinflussen

3.30

dritte Partei

Person oder Institution, die von der *Organisation* (3.1) unabhängig ist

Anmerkung 1 zum Begriff: Alle Geschäftspartner sind dritte Parteien, aber nicht alle dritten Parteien sind Geschäftspartner.

3.31

Verfahren

festgelegte Art und Weise, eine Tätigkeit oder einen *Prozess* (3.8) auszuführen

[QUELLE: ISO 9000:2015, 3.4.5]

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes

Die Organisation muss externe und interne Themen bestimmen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Compliance-Managementsystems zu erreichen.

Zu diesem Zweck muss die Organisation eine Vielzahl unterschiedlicher Themen berücksichtigen, unter anderem:

- das Geschäftsmodell einschließlich Strategie, Art, Größe und Umfang, Komplexität und Nachhaltigkeit der Aktivitäten und des Betriebs der Organisation;
- Art und Anwendungsbereich der Geschäftsbeziehungen zu dritten Parteien;
- den rechtlichen und behördlichen Kontext;
- die wirtschaftliche Situation;
- das gesellschaftliche, kulturelle und umweltbezogene Umfeld;
- die internen Strukturen, Politiken, Prozesse, Verfahren und Ressourcen, einschließlich Technologie;
- ihre Compliance-Kultur.

4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Die Organisation muss festlegen:

- die interessierten Parteien, die für ihr Compliance-Managementsystem relevant sind;
- die relevanten Anforderungen dieser interessierten Parteien;
- welche dieser Anforderungen durch das Compliance-Managementsystem behandelt werden.

4.3 Festlegen des Anwendungsbereichs des Compliance-Managementsystems

Die Organisation muss die Grenzen und die Anwendbarkeit des Compliance-Managementsystems bestimmen, um dessen Anwendungsbereich festzulegen.

ANMERKUNG Der Anwendungsbereich des Compliance-Managementsystems soll dazu dienen, die Haupt-Compliance-Risiken der Organisation zu bestimmen und die geografischen oder organisatorischen Grenzen des Anwendungsbereichs des Compliance-Managementsystems oder beides festzulegen, insbesondere, wenn die Organisation Teil einer größeren Einheit ist.

Bei der Festlegung dieses Anwendungsbereichs muss die Organisation Folgendes berücksichtigen:

- die unter 4.1 genannten externen und internen Themen;
- die in 4.2, 4.5 und 4.6 genannten Anforderungen.

Der Anwendungsbereich muss als dokumentierte Information verfügbar sein.

4.4 Compliance-Managementsystem

Die Organisation muss entsprechend den Anforderungen dieses Dokuments ein Compliance-Managementsystem aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern, einschließlich der benötigten Prozesse und ihrer Wechselwirkungen.

Das Compliance-Managementsystem muss die Werte, Ziele, Strategie und Compliance-Risiken der Organisation unter Berücksichtigung des Kontexts der Organisation (siehe 4.1) widerspiegeln.

4.5 Compliance-Verpflichtungen

Die Organisation muss systematisch ihre aus ihren Aktivitäten, Produkten und Dienstleistungen resultierenden Compliance-Verpflichtungen identifizieren und deren Auswirkung auf ihren Betrieb beurteilen.

Die Organisation muss über Prozesse verfügen, um:

- a) neue und veränderte Compliance-Verpflichtungen zu identifizieren, um kontinuierlich Compliance sicherzustellen;
- b) die Auswirkungen der identifizierten Änderungen zu bewerten und alle notwendigen Änderungen des Managements der Compliance-Verpflichtungen einzuführen.

Die Organisation muss dokumentierte Informationen ihrer Compliance-Verpflichtungen aufrechterhalten.

4.6 Compliance-Risikobeurteilung

Die Organisation muss ihre Compliance-Risiken auf der Grundlage einer Compliance-Risikobeurteilung identifizieren, analysieren und bewerten.

Die Organisation muss ihre Compliance-Risiken identifizieren, indem sie ihre Compliance-Verpflichtungen zu ihren Aktivitäten, Produkten, Dienstleistungen und relevanten Aspekten ihrer Geschäftstätigkeit in Beziehung setzt.

Die Organisation muss Compliance-Risiken in Verbindung mit ausgegliederten oder durch dritte Parteien ausgeführten Prozessen beurteilen.

Die Compliance-Risiken müssen regelmäßig und immer dann bewertet werden, wenn wesentliche Veränderungen der Umstände oder des Kontexts der Organisation auftreten.

Die Organisation muss dokumentierte Informationen über die Compliance-Risikobeurteilung und die Maßnahmen zur Behandlung ihrer Compliance-Risiken aufbewahren.

5 Führung

5.1 Führung und Verpflichtung

5.1.1 Oberstes Organ und oberste Leitung

Das oberste Organ und die oberste Leitung müssen in Bezug auf das Compliance-Managementsystem Führung und Verpflichtung zeigen, indem sie:

- sicherstellen, dass die Compliance-Politik und die damit verbundenen Compliance-Ziele festgelegt und mit der strategischen Ausrichtung der Organisation vereinbar sind;
- sicherstellen, dass die Anforderungen des Compliance-Managementsystems in die Geschäftsprozesse der Organisation integriert werden;

- sicherstellen, dass die für das Compliance-Managementsystem erforderlichen Ressourcen zur Verfügung stehen;
- die Bedeutung eines wirksamen Compliance-Managements sowie die Wichtigkeit der Erfüllung der Anforderungen des Compliance-Managementsystems vermitteln;
- sicherstellen, dass das Compliance-Managementsystem seine beabsichtigten Ergebnisse erzielt;
- Personen anleiten und unterstützen, damit diese zur Wirksamkeit des Compliance-Managementsystems beitragen können;
- fortlaufende Verbesserung fördern;
- andere relevante Rollen unterstützen, um deren Führungsrolle in deren jeweiligem Verantwortungsbereich deutlich zu machen.

ANMERKUNG Wenn in diesem Dokument das Wort „Geschäft“ (en: business) verwendet wird, ist dieses im weiteren Sinne zu verstehen und bezieht sich auf Tätigkeiten, die für den Zweck der Organisation bzw. deren Existenz entscheidend sind.

Das oberste Organ und die oberste Leitung müssen:

- die Werte der Organisation festlegen und aufrechterhalten;
- sicherstellen, dass Politiken, Prozesse und Verfahren zur Erreichung der Compliance-Ziele entwickelt und eingeführt werden;
- sicherstellen, dass sie zeitnah über Compliance-Angelegenheiten einschließlich Fällen von Non-Compliance informiert werden und dass geeignete Maßnahmen getroffen werden;
- sicherstellen, dass das Bekenntnis zu Compliance aufrechterhalten wird und Non-Compliance und nicht Compliance gerechtes Verhalten angemessen behandelt werden;
- sicherstellen, dass Verantwortlichkeiten in Bezug auf Compliance angemessen in den Tätigkeitsbeschreibungen enthalten sind;
- eine Compliance-Funktion ernennen oder nominieren (siehe 5.3.2);
- sicherstellen, dass ein System zum Ansprechen und Behandeln von Bedenken in Übereinstimmung mit 8.3. erstellt wird.

5.1.2 Compliance-Kultur

Die Organisation muss eine Compliance-Kultur auf allen Ebenen innerhalb der Organisation entwickeln, aufrechterhalten und fördern.

Das oberste Organ, die oberste Leitung und die Leitung müssen ein aktives, sichtbares, konsistentes und nachhaltiges Bekenntnis zu einem gemeinsamen, organisationweit gültigen Verhaltensstandard zeigen.

Die oberste Leitung muss zu Verhalten ermutigen, das Compliance schafft und unterstützt. Sie muss Verhalten, welches Compliance beeinträchtigt verhindern und darf ein solches nicht tolerieren.

5.1.3 Compliance-Führung

Das oberste Organ und die oberste Leitung müssen sicherstellen, dass die folgenden Grundsätze eingeführt werden:

- direkter Zugang der Compliance-Funktion zu dem obersten Organ;