

DIN ISO 37301



ICS 03.100.01; 03.100.02; 03.100.70

Einsprüche bis 2020-05-13
Vorgesehen als Ersatz für
DIN ISO 19600:2016-12

Entwurf

**Compliance-Managementsysteme –
Anforderungen mit Anleitung zur Anwendung (ISO/DIS 37301:2020);
Text Deutsch und Englisch**

Compliance management systems –
Requirements with guidance for use (ISO/DIS 37301:2020);
Text in German and English

Systèmes de management de la compliance –
Exigences et lignes directrices pour son utilisation (ISO/DIS 37301:2020);
Texte en allemand et anglais

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-03-13 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an info@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Organisationsprozesse (NAOrg), 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 100 Seiten

DIN-Normenausschuss Organisationsprozesse (NAOrg)

Inhalt

	Seite
Nationales Vorwort	4
Nationaler Anhang NA (informativ) Literaturhinweise	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Kontext der Organisation	13
4.1 Verstehen der Organisation und ihres Kontextes	13
4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien	14
4.3 Festlegen des Anwendungsbereichs des Compliance-Managementsystems	14
4.4 Compliance-Managementsystem	14
5 Führung	14
5.1 Führung und Verpflichtung	14
5.1.1 Oberstes Organ und oberste Leitung	14
5.1.2 Compliance-Kultur	15
5.1.3 Compliance-Führung	15
5.2 Politik	16
5.3 Rollen, Verantwortlichkeiten und Befugnisse	16
5.3.1 Oberstes Organ und oberste Leitung	16
5.3.2 Compliance-Funktion	17
5.3.3 Leitung	18
5.3.4 Personal	19
6 Planung	19
6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten	19
6.2 Compliance-Ziele und Planung zu deren Erreichung	19
6.3 Compliance-Verpflichtungen	20
6.4 Compliance-Risikobeurteilung	20
7 Unterstützung	21
7.1 Ressourcen	21
7.2 Kompetenz	21
7.2.1 Allgemeines	21
7.2.2 Beschäftigungsprozess	21
7.2.3 Schulung	21
7.3 Bewusstseinsbildung	22
7.4 Kommunikation	22
7.5 Dokumentierte Informationen	23
7.5.1 Allgemeines	23
7.5.2 Erstellen und Aktualisieren	23
7.5.3 Lenkung dokumentierter Informationen	23
8 Betrieb	24
8.1 Betriebliche Planung und Steuerung	24
8.2 Entwicklung der Kontrollen und Verfahren	24
8.3 Äußern von Bedenken	25
8.4 Untersuchungsprozess	25
9 Bewertung der Leistung	25
9.1 Überwachung, Messung, Analyse und Bewertung	25
9.1.1 Allgemeines	25
9.1.2 Feedback-Quellen zur Compliance-Leistung	26
9.1.3 Entwicklung von Indikatoren	26
9.1.4 Compliance-Berichte	26

9.1.5	Aufzeichnungen	26
9.2	Internes Audit	26
9.3	Managementprüfung	27
10	Verbesserung	28
10.1	Nichtkonformität, Non-Compliance und Korrekturmaßnahmen	28
10.2	Ständige Verbesserung	28
Anhang A (informativ) Anleitung zur Verwendung dieses Dokuments		30
A.1	Anwendungsbereich	30
A.2	Normative Verweisungen	30
A.3	Begriffe	30
A.4	Kontext der Organisation	31
A.4.1	Verstehen der Organisation und ihres Kontextes	31
A.4.2	Verstehen der Erfordernisse und Erwartungen der interessierten Parteien	31
A.4.3	Festlegen des Anwendungsbereichs des Compliance-Managementsystems	32
A.4.4	Compliance-Managementsystem	32
A.5	Führung	33
A.5.1	Führung und Verpflichtung	33
A.5.2	Compliance-Politik	35
A.5.3	Rollen, Verantwortlichkeiten und Befugnisse	36
A.6	Planung	38
A.6.1	Maßnahmen zum Umgang mit Risiken und Möglichkeiten	38
A.6.2	Compliance-Ziele und Planung zu deren Erreichung	38
A.6.3	Compliance-Risikobeurteilung	39
A.7	Unterstützung	42
A.7.1	Ressourcen	42
A.7.2	Kompetenz	42
A.7.3	Bewusstseinsbildung	43
A.7.4	Kommunikation	43
A.7.5	Dokumentierte Informationen	44
A.8	Betrieb	44
A.8.1	Betriebliche Planung und Steuerung	44
A.8.2	Entwicklung der Kontrollen und Verfahren	45
A.8.3	Äußern von Bedenken	46
A.8.4	Untersuchungsprozess	46
A.9	Bewertung der Leistung	47
A.9.1	Überwachung, Messung, Analyse und Bewertung	47
A.9.2	Internes Audit	50
A.9.3	Managementprüfung	50
A.10	Verbesserung	51
A.10.1	Nichtkonformität und Korrekturmaßnahmen	51
A.10.2	Ständige Verbesserung	51
Literaturhinweise		53

Bilder

Bild 1	8
------------------	---

Nationales Vorwort

Dieses Dokument enthält die deutsche Übersetzung der Internationalen Norm ISO 37301:2020, die vom Technischen Komitee ISO/TC 309 „Governance of organizations“ erarbeitet wurde, dessen Sekretariat von BSI (Vereinigtes Königreich) gehalten wird.

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

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

ISO 9001	siehe	DIN EN ISO 9001
ISO 10002	siehe	DIN ISO 10002
ISO 14001	siehe	DIN EN ISO 14001
ISO 19011	siehe	DIN EN ISO 19011
ISO 22000	siehe	DIN EN ISO 22000
ISO 26000	siehe	DIN ISO 26000
ISO 31000	siehe	DIN ISO 31000
ISO 37001	siehe	DIN ISO 37001

Änderungen

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

- a) das Dokument wurde von einer Typ-B-Managementsystemnorm, die ausschließlich Empfehlungen enthält, in eine Anforderungsnorm vom Typ A überführt und überarbeitet;
- b) redaktionelle Überarbeitung der Norm.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

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

DIN EN ISO 19011, *Leitfaden zur Auditierung von Managementsystemen*

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

DIN ISO 10002, *Qualitätsmanagement — Kundenzufriedenheit — Leitfaden für die Reklamationsbearbeitung in Organisationen*

DIN ISO 26000, *Leitfaden zur gesellschaftlichen Verantwortung*

DIN ISO 31000, *Risikomanagement — Leitlinien*

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

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-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 organizations* erarbeitet.

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.

Dieses Dokument ersetzt ISO 19600:2014-10.

In dieser Internationalen Norm werden die folgenden Modalverben 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.

Einleitung

Organisationen, die langfristig erfolgreich sein möchten, müssen eine Kultur der Integrität und Compliance in Anbetracht der Bedürfnisse und Erwartungen interessierter Parteien einführen und aufrechterhalten. Integrität und Compliance sind daher nicht nur die Grundlage, sondern auch eine Möglichkeit für eine erfolgreiche und nachhaltige Organisation.

Compliance ist ein anhaltender Prozess und das Ergebnis einer Organisation, die ihre Verpflichtungen erfüllt. Die Dauerhaftigkeit von Compliance wird durch ihre Einbettung in die Kultur der Organisation und das Verhalten und die Einstellung ihrer Mitarbeiter erreicht. Compliance-Management sollte seine Unabhängigkeit bewahren, aber gleichzeitig in die anderen Managementprozesse und betrieblichen Anforderungen und Verfahren der Organisation integriert werden.

Ein effektives organisationsweites Compliance-Managementsystem ermöglicht es einer Organisation, ihre Verpflichtung zur Einhaltung relevanter Gesetze einschließlich legislativer Anforderungen, Industrievorschriften und Organisationennormen sowie der Normen der guten Unternehmensführung, besten Praktiken, ethischen Grundsätze und Erwartungen der Gesellschaft zu beweisen.

Der Compliance-Ansatz einer Organisation wird durch die Art und Weise bestimmt, in der die Leitung Kernwerte und allgemein anerkannte Normen der Unternehmensführung, Ethik und Gesellschaft anwendet. Die Einbindung von Compliance in das Verhalten der Mitarbeiter einer Organisation hängt vor allem von der Leitung auf allen Ebenen und klaren Werten einer Organisation sowie der Anerkennung und Implementierung von Maßnahmen zur Förderung konformer Verhaltensweisen ab. Ist dies nicht auf allen Ebenen des Unternehmens der Fall, besteht das Risiko von Compliance-Mängeln.

Gerichte in verschiedenen Ländern haben die Verpflichtung einer Organisation zur Compliance durch ihr Compliance-Managementsystem im Rahmen der Festlegung angemessener Strafen für Verstöße gegen anzuwendende Gesetze betrachtet. Aus diesem Grund können auch regulatorische und Gerichtsbehörden von diesem Dokument als Referenz profitieren.

Organisationen sind zunehmend überzeugt, dass sie durch die Anwendung verbindlicher Werte und eines geeigneten Compliance-Managements ihre Integrität wahren und Verstöße gegen die Compliance-Verpflichtungen der Organisation vermeiden oder minimieren können. Integrität und effektive Compliance sind daher wesentliche Elemente eines guten und sorgfältigen Managements. Compliance trägt darüber hinaus zu einem sozialverantwortlichen Verhalten von Organisationen bei.

Eines der Ziele dieses Dokuments besteht darin, Organisationen bei der Entwicklung und Verbreitung einer positiven Compliance-Kultur zu unterstützen. Hierbei wird berücksichtigt, dass ein effektives und fundiertes Management compliance-bezogener Risiken als zu verfolgende und nutzende Gelegenheit in Anbetracht der Vorteile für die Organisation betrachtet werden sollte.

Dieses Dokument legt Anforderungen fest und bietet Leitlinien für Compliance-Managementsysteme und empfohlene Praktiken. Die Anforderungen und Leitlinien in diesem Dokument sind als anpassbar vorgesehen und ihre Implementierung 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 erhöhen und eine Organisation bei der Verbesserung des allgemeinen Managements ihrer Compliance-Verpflichtungen zu unterstützen.

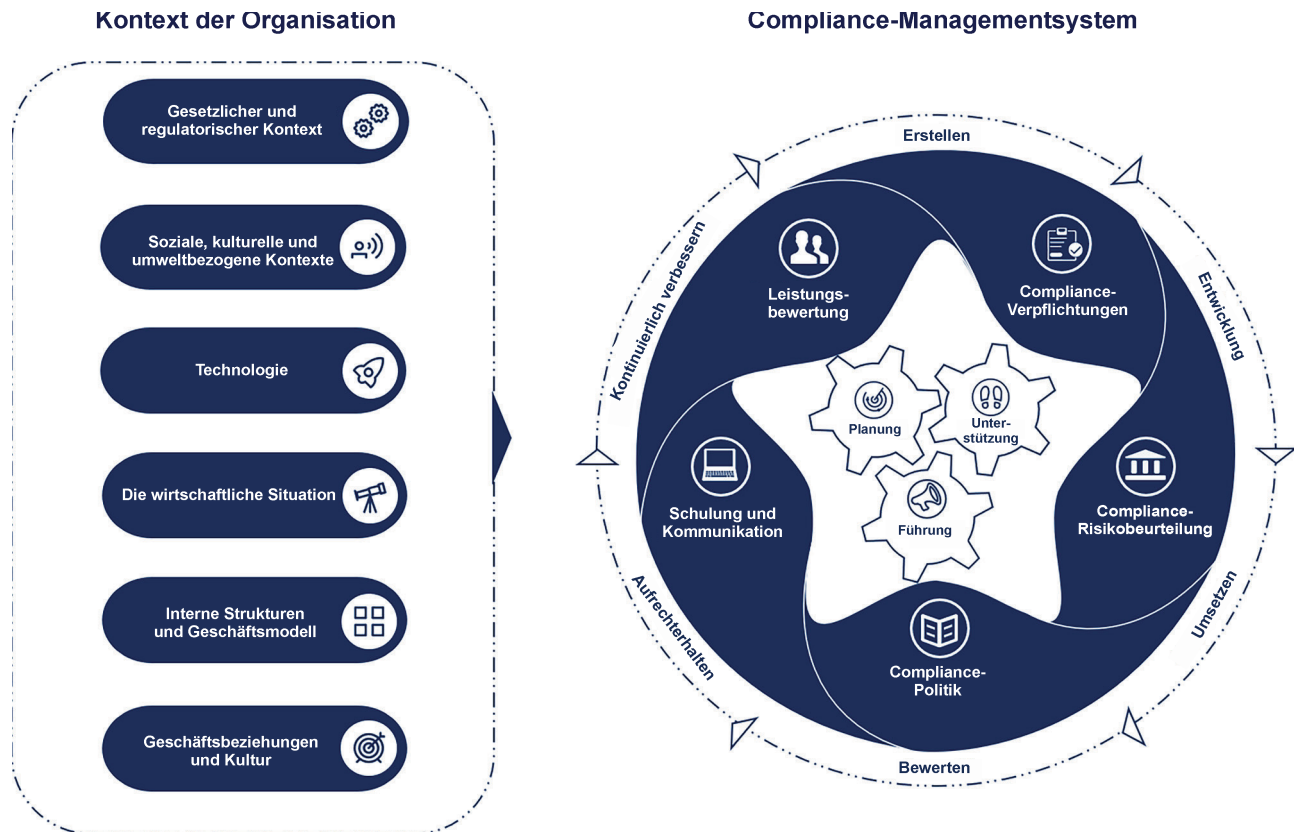


Bild 1

1 Anwendungsbereich

Dieses Dokument legt Anforderungen fest und bietet Anleitung für den Aufbau, die Entwicklung, die Implementierung, die Bewertung, die Instandhaltung und die Verbesserung eines effektiven Compliance-Managementsystems innerhalb einer Organisation.

Dieses Dokument gilt 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 führen die terminologischen Datenbanken zur Verwendung in der Normung unter folgenden Internet-Adressen:

— ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

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

3.1

Organisation

Einzelperson oder Gruppe von Menschen mit eigenen Aufgabenbereichen, die mit Verantwortlichkeiten, Befugnissen und Beziehungen verbunden sind, um eigene *Zielsetzungen* (3.8) zu erreichen

Anmerkung 1 zum Begriff: Das Konzept einer Organisation umfasst, ist jedoch nicht begrenzt auf Ein-Mann-Unternehmen, Unternehmen, Kapitalgesellschaften, Firmen, Wirtschaftsunternehmen, Behörden, Partnerschaften, Wohlfahrtseinrichtungen oder Anstalten oder Teile bzw. Kombinationen davon, eingetragen oder nicht, öffentlich oder privat.

3.2

interessierte Partei (bevorzugter Begriff)

Anspruchsgruppe (zulässiger Begriff)

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

3.3

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 andere interessierte Parteien übliche 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 enthalten ist.

3.4

Managementsystem

Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer *Organisation* (3.1), um *Politiken* (3.7), *Ziele* (3.8) und *Prozesse* (3.12) zum Erreichen dieser Ziele festzulegen

Anmerkung 1 zum Begriff: Ein Managementsystem kann auf einen einzelnen Bereich oder auf verschiedene Bereiche ausgerichtet sein.

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

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

3.5

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.

3.6

Effektivität

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

3.7

Politik

Absichten und Ausrichtung einer *Organisation* (3.1), wie von der *obersten Leitung* (3.5) und/oder dem *Leistungsorgan* (3.22) formell ausgedrückt

3.8

Zielsetzung

zu erreichendes Ergebnis

Anmerkung 1 zum Begriff: Eine Zielsetzung kann strategisch, taktisch oder betrieblich sein.

Anmerkung 2 zum Begriff: Zielsetzungen können sich auf verschiedene Bereiche beziehen (z.B. finanzielle, gesundheits-, sicherheits- und umweltbezogene Zielsetzungen) und können auf verschiedenen Ebenen auftreten (z.B. strategisch, organisationsweit, Projekt, Produkt und *Prozess* (3.12)).

Anmerkung 3 zum Begriff: Eine Zielsetzung kann anderweitig ausgedrückt werden, z. B. als beabsichtigtes Ergebnis, Zweck, betriebstechnisches Kriterium, als Compliance-Zielsetzung oder durch Verwendung anderer Worte mit ähnlicher Bedeutung (z. B. Zielvorgabe, Zielstellung oder Einzelziel).

Anmerkung 4 zum Begriff: Im Zusammenhang mit Compliance-Managementsystemen werden zum Erreichen bestimmter Ergebnisse Compliance-Zielsetzungen durch die Organisation in Übereinstimmung mit deren Compliance-Politik festgelegt.

3.9

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 oder seine Wahrscheinlichkeit.

Anmerkung 3 zum Begriff: Risiken werden 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.

3.10

Kompetenz

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

3.11

dokumentierte Information

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 Information kann in jeglichem Format oder Medium vorliegen, sowie aus jeglicher Quelle stammen.

Anmerkung 2 zum Begriff: Eine dokumentierte Information kann Bezug nehmen auf:

- das *Managementsystem* (3.4), einschließlich damit verbundener *Prozesse* (3.12);
- zusammengestellte Informationen, die die Organisation in die Lage versetzen, arbeiten zu können (Dokumentation);
- Nachweise erreichter Ergebnisse (Aufzeichnungen).

3.12

Prozess

mehrere zusammenhängende oder sich gegenseitig beeinflussende Tätigkeiten, die Eingaben in Ergebnisse umwandeln

3.13

Leistung

messbares Ergebnis

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

Anmerkung 2 zum Begriff: Leistung kann sich auf das Führen und Steuern von Tätigkeiten, *Prozessen* (3.12), Produkten (einschließlich Dienstleistungen), Systemen oder *Organisationen* (3.1) beziehen.

3.14

ausgliedern

eine Vereinbarung treffen, bei der eine externe *Organisation* (3.1) einen Teil einer Funktion oder eines *Prozesses* (3.11) einer Organisation wahrnimmt bzw. durchführt

Anmerkung 1 zum Begriff: Eine externe Organisation befindet sich außerhalb des Anwendungsbereichs des *Managementsystems* (3.4), obwohl die ausgegliederte Funktion oder der ausgegliederte Prozess im Rahmen des Anwendungsbereichs liegen.

3.15

Überwachung

Bestimmung des Zustands eines Systems, eines *Prozesses* (3.12) oder einer Tätigkeit

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

3.16

Messung

Prozess (3.12) zum Bestimmen eines Werts

3.17

Audit

systematischer, unabhängiger und dokumentierter *Prozess* (3.12) 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-Audit) sein und es kann ein kombiniertes Audit (Kombination zweier oder mehrerer Wissensgebiete) sein.

Anmerkung 2 zum Begriff: Ein internes Audit wird von der Organisation selbst durchgeführt, oder von einer externen Stelle 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.

3.18

Konformität

Erfüllung einer *Anforderung* (3.3)

3.19

Nichtkonformität

Nichterfüllung einer *Anforderung* (3.3)

Anmerkung 1 zum Begriff: Eine Nichtkonformität ist nicht notwendigerweise eine *Non-Compliance* (3.28).

3.20

Korrekturmaßnahme

Maßnahme zum Beseitigen der Ursache(n) einer *Nichtkonformität* (3.19) oder einer *Non-Compliance* (3.28) und zum Verhindern des erneuten Auftretens

3.21

ständige Verbesserung

wiederkehrende Tätigkeit zum Steigern der *Leistung* (3.13)

3.22

oberstes Organ

Person oder Gruppe von Personen mit der endgültigen Verantwortlichkeit und Befugnis für die Tätigkeiten, Führung und Politiken einer *Organisation* (3.1), und der die *oberste Leitung* (3.5) berichtet und durch die die oberste Leitung Rechenschaft ablegt

Anmerkung 1 zum Begriff: Nicht alle Organisationen und insbesondere kleine Organisationen werden ein oberstes Organ separat zur obersten Leitung haben.

Anmerkung 2 zum Begriff: Ein oberstes Organ kann unter anderem einen Vorstand, Ausschüsse des Vorstands, einen Aufsichtsrat oder Treuhänder umfassen.

3.23

Personal

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

3.24

Compliance-Funktion

Person oder Gruppe von Personen mit der Verantwortlichkeit oder Befugnis für den Betrieb des *Compliance-*(3.27) *Managementsystems* (3.4)

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

3.25

Compliance-Risiko

Wahrscheinlichkeit des Auftretens und der Folgen von *Non-Compliance* (3.17) mit den *Compliance-Verpflichtungen* (3.26) der Organisation

3.26

Compliance-Verpflichtung

Anforderungen (3.3), die eine *Organisation* (3.1) zwingend erfüllen muss sowie zu deren Erfüllung sich eine *Organisation* (3.1) freiwillig entschließt

3.27

Compliance

das Ergebnis der Erfüllung aller *Compliance-Verpflichtungen* (3.26) der Organisation

3.28

Non-Compliance

Nichterfüllung einer *Compliance-Verpflichtung* (3.26)

3.29

Compliance-Kultur

Werte, ethische Grundsätze und Überzeugungen, die in der gesamten *Organisation* (3.1) bestehen und mit den Strukturen und Steuerungssystemen der Organisation interagieren, um Verhaltensnormen zu erzeugen, die die *Compliance* (3.27) unterstützen

3.30

Verhalten

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

3.32

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.

3.33

Verfahren

festgelegte Art und Weise, eine Tätigkeit oder einen *Prozess* (3.12) 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, einschließlich:

- gesetzlicher und regulatorischer Kontext;
- gesellschaftliche, kulturelle und umweltbezogene Kontexte;
- Technologie;

- die wirtschaftliche Situation;
- interne Strukturen, Politiken, Verfahren, Prozesse und Ressourcen;
- Geschäftsmodell einschließlich Strategie, Natur, Größe und Umfang, Komplexität und Nachhaltigkeit der Aktivitäten und des Betriebs einer Organisation;
- Art und Anwendungsbereich der Geschäftsbeziehungen zu dritten Parteien;
- die aktuelle Compliance-Kultur.

4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien

Die Organisation muss festlegen:

- die interessierten Parteien, die für ihr Compliance-Managementsystem relevant sind;
- die relevanten Anforderungen dieser interessierten Parteien.

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 dient dazu, die Haupt-Compliance-Risiken der Organisation und die geografischen und/oder organisatorischen Grenzen des Anwendungsbereichs des Compliance-Managementsystems zu klären, insbesondere, wenn die Organisation Teil einer größeren Organisation ist.

Bei der Festlegung dieses Anwendungsbereichs muss die Organisation Folgendes berücksichtigen:

- die unter 4.1 genannten externen und internen Themen;
- die in 4.2 und 6.3 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, bewerten, implementieren, 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.

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;
- ständige Verbesserung fördern;
- andere relevante Führungskräfte 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, Verfahren und Prozesse zur Erreichung der Compliance-Ziele entwickelt und implementiert werden;
- sicherstellen, dass sie zeitnah über Compliance-Angelegenheiten einschließlich Fällen von Non-Compliance informiert werden und dass geeignete Maßnahmen getroffen werden;
- sicherstellen, dass die Compliance-Verpflichtung aufrechterhalten wird und Non-Compliance und nicht-konformes Verhalten angemessen behandelt werden;
- sicherstellen, dass Compliance-Verantwortlichkeiten gegebenenfalls in der Tätigkeitsbeschreibung enthalten sind;
- eine Compliance-Funktion ernennen oder nominieren (siehe 5.3.2).

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 eine aktive, sichtbare, konsistente und dauerhafte Verpflichtung zu einer gemeinsamen Verhaltensnorm und einem Verhalten beweisen, das in der gesamten Organisation gefordert wird.

Die oberste Leitung muss ein Verhalten fördern, das Compliance schafft und unterstützt, und muss Verhalten, das Compliance beeinträchtigt, verhindern und nicht tolerieren.

5.1.3 Compliance-Führung

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

- direkter Zugang der Compliance-Funktion zu dem obersten Organ;
- Unabhängigkeit der Compliance-Funktion;
- entsprechende Befugnis und Kompetenz der Compliance-Funktion.

ANMERKUNG 1 Der direkte Zugang könnte umfassen: direkte Berichtslinien zu dem obersten Organ, die Vorlage regelmäßiger Berichte an das oberste Organ und Teilnahme an seinen Besprechungen.

ANMERKUNG 2 Unabhängigkeit bedeutet die Abwesenheit unnötiger Störungen und/oder von Druck in Bezug auf den Betrieb der Compliance-Funktion.

5.2 Politik

Das oberste Organ und die oberste Leitung müssen eine Compliance-Politik erstellen, die:

- a) dem Zweck der Organisation entspricht;
- b) einen Rahmen zum Festlegen von Compliance-Zielen bietet;
- c) eine Verpflichtung zur Erfüllung der anzuwendenden Anforderungen beinhaltet;
- d) eine Verpflichtung zur ständigen Verbesserung des Compliance-Managementsystems enthält.

Die Compliance-Politik muss:

- a) mit den Werten, den Zielen und der Strategie der Organisation abgestimmt sein;
- b) die Konformität mit den Compliance-Verpflichtungen der Organisation fordern;
- c) die Grundsätze der Compliance-Führung nach Abschnitt 5.1.3 unterstützen;
- d) die Folgen der Nichtbeachtung der Compliance-Verpflichtungen, Politiken, Verfahren und Prozesse der Organisation beschreiben;
- e) das Melden von Bedenken fördern und jede Form von Vergeltung verbieten;
- f) in einfacher Sprache formuliert sein, damit alle Mitarbeiter die Grundsätze und die Absicht leicht verstehen können;
- g) angemessen implementiert und durchgesetzt werden.

Die Compliance-Politik muss:

- a) als dokumentierte Information verfügbar sein;
- b) innerhalb der Organisation kommuniziert werden;
- c) gegebenenfalls für interessierte Parteien verfügbar sein.

5.3 Rollen, Verantwortlichkeiten und Befugnisse

5.3.1 Oberstes Organ und oberste Leitung

Das oberste Organ und die oberste Leitung müssen sicherstellen, dass innerhalb der Organisation Verantwortlichkeiten und Befugnisse für relevante Rollen zugewiesen und kommuniziert werden.

Das oberste Organ und die oberste Leitung müssen Verantwortlichkeit und Befugnis erteilen für:

- a) das Sicherstellen, dass das Compliance-Managementsystem die Anforderungen dieses Dokuments erfüllt;
- b) das Berichten an das oberste Organ und die oberste Leitung über die Leistung des Compliance-Managementsystems.

Das oberste Organ muss:

- a) sicherstellen, dass die oberste Leitung an der Erreichung der Compliance-Ziele gemessen wird;
- b) die oberste Leitung hinsichtlich der Anwendung des Compliance-Managementsystems beaufsichtigen.

Die oberste Leitung muss:

- a) ausreichende und angemessene Ressourcen für die Erstellung, Entwicklung, Implementierung, Bewertung, Aufrechterhaltung und Verbesserung des Compliance-Managementsystems zuweisen;
- b) sicherstellen, dass wirksame Systeme für eine zeitnahe Berichterstattung über die Compliance-Leistung vorhanden sind;
- c) die Verantwortung für die Berichterstattung (siehe 9.1.4) über das Compliance-Managementsystem an das oberste Organ und die oberste Leitung zuweisen;
- d) die Abstimmung zwischen den strategischen und betrieblichen Zielen und den Compliance-Verpflichtungen sicherstellen;
- e) Verantwortungsmechanismen einschließlich Disziplinarmaßnahmen und Konsequenzen erstellen und aufrechterhalten;
- f) die Integration der Compliance-Leistung in Leistungsbewertungen des Personals sicherstellen.

5.3.2 Compliance-Funktion

Die Compliance-Funktion muss für den Betrieb des Compliance-Managementsystems einschließlich des Folgenden verantwortlich sein:

Die Compliance-Funktion muss verantwortlich sein für:

- die Erleichterung der Identifizierung von Compliance-Verpflichtungen;
- die Beurteilung des Compliance-Risikos (siehe Abschnitt 6.4);
- das Sicherstellen, dass Compliance-Verpflichtungen in Politiken integriert werden;
- die Erstellung eines Berichts- und Dokumentationssystems für Compliance;
- die Erstellung von Compliance-Leistungsindikatoren;
- die Erstellung eines Systems zur Meldung von Bedenken, und Sicherstellen, dass Bedenken behandelt werden.

Die Compliance-Funktion muss überwachen:

- dass die Verantwortlichkeiten für die Erreichung identifizierter Compliance-Verpflichtungen in der gesamten Organisation angemessen zugewiesen sind;

- dass Compliance-Verpflichtungen in die Verfahren und Prozesse integriert werden;
- dass das gesamte Personal nach Bedarf geschult wird.

Die Compliance-Funktion muss verantwortlich sein für:

- die Überwachung und Messung der Compliance-Leistung;
- die Analyse und Bewertung der Leistung des Compliance-Managementsystems, um zu erkennen, ob Korrekturmaßnahmen erforderlich sind;
- das Sicherstellen, dass das Compliance-Managementsystem in geplanten Intervallen geprüft wird (siehe 9.2 und 9.3).

Die Compliance-Funktion muss:

- dem Personal Zugang zu Ressourcen für Compliance-Politiken, -Prozesse und -Verfahren zur Verfügung stellen;
- die Organisation in Compliance-Fragen beraten.

ANMERKUNG Die spezifischen Pflichten der Compliance-Funktion befreien das andere Personal nicht von seiner Verpflichtung für die Compliance.

Die Organisation muss sicherstellen, dass die Compliance-Funktion Zugang erhält zu:

- führenden Entscheidungsträgern und der Möglichkeit, sich frühzeitig an dem Entscheidungsfindungsprozess zu beteiligen;
- allen Ebenen der Organisation;
- dem gesamten Personal sowie erforderlichen dokumentierten Informationen und Daten;
- fachlicher Beratung zu relevanten Gesetzen, Verordnungen, Kodizes und Organisationsnormen.

5.3.3 Leitung

Die Leitung muss Verantwortung für die Compliance in ihrem Verantwortungsbereich übernehmen durch:

- die Zusammenarbeit mit und Unterstützung der Compliance-Funktion und die Anregung des Personals, dies ebenfalls zu tun;
- Sicherstellen, dass ihr Personal die Compliance-Verpflichtungen, -Politiken, -Verfahren und -Prozesse der Organisation erfüllt;
- Identifizieren und Kommunizieren von Compliance-Risiken in ihren betrieblichen Aktivitäten;
- Einbinden von Compliance-Verpflichtungen in bestehende Geschäftspraktiken und Verfahren in ihren Verantwortungsbereichen;
- Teilnahme an und Unterstützung von Compliance-Schulungsaktivitäten;
- Förderung des Bewusstseins des Personals für Compliance-Verpflichtungen und Anweisung desselben zur Erfüllung der Schulungs- und Kompetenzerfordernisse;
- Ermutigen des Personals, Compliance-Bedenken zu melden, und Unterstützung des Personals und Ausschluss jeder Form von Vergeltung;

- aktive Beteiligung an der Handhabung und Auflösung von Compliance-Zwischenfällen und -Problemen im Bedarfsfall;
- Sicherstellen, dass im Anschluss an die Identifizierung des Erfordernisses von Korrekturmaßnahmen geeignete Korrekturmaßnahmen empfohlen und implementiert werden.

5.3.4 Personal

Das gesamte Personal muss:

- die Compliance-Verpflichtungen, -Politiken, -Verfahren und -Prozesse der Organisation beachten;
- Compliance-Bedenken, -Probleme und -Fehler melden;
- bei Bedarf an Schulungen teilnehmen.

6 Planung

6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten

Bei Planungen für das Compliance-Managementsystem muss die Organisation die in 4.1 genannten Themen und die in 4.2 genannten Anforderungen berücksichtigen sowie die Risiken und Chancen bestimmen, die behandelt werden müssen, um:

- sicherzustellen, dass das Compliance-Managementsystem seine angestrebten Ergebnisse erzielen kann;
- unerwünschte Auswirkungen zu verhindern oder zu verringern;
- eine ständige Verbesserung zu erreichen.

Bei Planungen für das Compliance-Managementsystem muss die Organisation Folgendes berücksichtigen

- ihre Compliance-Ziele (siehe 6.2);
- die identifizierten Compliance-Verpflichtungen (siehe 6.3) und
- die Ergebnisse der Compliance-Risikobeurteilung (siehe 6.4).

Die Organisation muss:

- a) Maßnahmen zum Umgang mit diesen Risiken und Möglichkeiten planen;
- b) wie:
 - die Maßnahmen in die eigenen Prozesse des -Compliance-Managementsystems integriert und implementiert werden;
 - die Wirksamkeit dieser Maßnahmen bewertet wird.

6.2 Compliance-Ziele und Planung zu deren Erreichung

Die Organisation muss die Compliance-Ziele für relevante Funktionen und auf relevanten Ebenen festlegen.

Die Compliance-Ziele müssen:

- a) im Einklang mit der Compliance-Politik stehen;

- b) messbar sein (sofern machbar);
- c) zu erfüllende Anforderungen berücksichtigen;
- d) überwacht werden;
- e) vermittelt werden;
- f) soweit erforderlich, aktualisiert werden.

Die Organisation muss dokumentierte Informationen zu den Compliance-Zielen aufbewahren.

Bei der Planung zum Erreichen ihrer Compliance-Ziele muss die Organisation bestimmen:

- was getan wird;
- welche Ressourcen erforderlich sind;
- wer verantwortlich sein wird;
- wann die Ziele erreicht sein werden;
- wie die Ergebnisse bewertet werden.

6.3 Compliance-Verpflichtungen

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

Die Organisation muss über Prozesse verfügen, um:

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

Die Organisation muss dokumentierte Information ihrer bindenden Verpflichtungen aufrechterhalten.

6.4 Compliance-Risikobeurteilung

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

Die Organisation muss Compliance-Risiken durch die Relation ihrer Compliance-Verpflichtungen mit ihren Aktivitäten, Produkten, Dienstleistungen und relevanten Aspekten ihres Betriebs identifizieren.

Die Compliance-Risiken müssen regelmäßig beurteilt werden und 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.

7 Unterstützung

7.1 Ressourcen

Die Organisation muss die erforderlichen Ressourcen für den Aufbau, die Verwirklichung, die Aufrechterhaltung und die ständige Verbesserung des Compliance-Managementsystems bestimmen und bereitstellen.

7.2 Kompetenz

7.2.1 Allgemeines

Die Organisation muss:

- die erforderliche Kompetenz der Person(en) festlegen, die unter ihrer Aufsicht Arbeit verrichtet (verrichten), die ihre Compliance-Leistung beeinflusst;
- sicherstellen, dass diese Personen auf Grundlage angemessener Ausbildung, Schulung oder Erfahrung kompetent sind;
- wo zutreffend, Maßnahmen einleiten, um die benötigte Kompetenz zu erwerben, und die Wirksamkeit der getroffenen Maßnahmen bewerten;
- angemessene dokumentierte Informationen als Nachweis der Kompetenz aufbewahren.

ANMERKUNG Geeignete Maßnahmen können zum Beispiel Schulung, Mentoring oder Versetzung von gegenwärtig angestellten Personen oder Anstellung oder Beauftragung kompetenter Personen sein.

7.2.2 Beschäftigungsprozess

Die Organisation muss in Bezug auf ihr gesamtes Personal Prozesse so entwickeln, erstellen, implementieren und aufrechterhalten, dass:

- a) die Beschäftigungsbedingungen von dem Personal die Einhaltung der Compliance-Verpflichtungen, -Politiken, -Verfahren und -Prozesse der Organisation fordern;
- b) das Personal innerhalb eines angemessenen Zeitraums vom Beginn seiner Beschäftigung eine Kopie von der oder den Zugang zur Compliance-Politik und Schulung in Bezug zu dieser Politik erhält;
- c) entsprechende Disziplinarmaßnahmen gegen Personal getroffen werden, das gegen die Compliance-Verpflichtungen, -Politiken, -Verfahren und -Prozesse verstößt.

Die Organisation muss als Teil des Beschäftigungsprozesses die mit dem Personal verbundenen Compliance-Risiken berücksichtigen und vor jeder Einstellung und Beförderung gegebenenfalls Prüfungsverfahren anwenden.

Die Organisation muss einen Prozess für eine regelmäßige Prüfung der Leistungsziele, der Leistungsprämien und andere Anreize implementieren, um zu überprüfen, ob geeignete Maßnahmen vorhanden sind, um die Förderung von Non-Compliance zu verhindern.

7.2.3 Schulung

Die Organisation muss dem relevanten Personal regelmäßige Schulungen ab dem Beginn des Arbeitsverhältnisses und in geplanten Intervallen nach Maßgabe der Organisation zur Verfügung stellen.

Die Schulung muss:

- a) für die Rollen des Personals und die Compliance-Risiken, denen es ausgesetzt ist, geeignet sein;

- b) hinsichtlich ihrer Wirksamkeit beurteilt werden;
- c) regelmäßig geprüft werden.

Die Organisation muss unter Berücksichtigung der identifizierten Compliance-Risiken sicherstellen, dass Verfahren, die das Compliance-Bewusstsein und die Schulung für dritte Parteien, die in ihrem Auftrag handeln und ein Compliance-Risiko für die Organisation darstellen könnten, behandeln, implementiert werden.

Die Schulungsprotokolle müssen als dokumentierte Informationen aufbewahrt werden.

7.3 Bewusstseinsbildung

Personen, die unter der Aufsicht durch die Organisation tätig sind, müssen sich folgender Dinge bewusst sein:

- Compliance-Politik;
- ihres Beitrags zur Wirksamkeit des Compliance-Managementsystems, einschließlich der Vorteile einer verbesserten Compliance-Leistung;
- der Folgen einer Nichterfüllung der Anforderungen des Compliance-Managementsystems.

Personen, die unter der Aufsicht durch die Organisation tätig sind, müssen sich folgender Dinge bewusst sein:

- der Mittel und Verfahren zur Meldung von Compliance-Bedenken (siehe 8.3);
- der Unterstützung der Compliance-Kultur.

7.4 Kommunikation

Die Organisation muss die für das Compliance-Managementsystem relevante interne und externe Kommunikation bestimmen, einschließlich:

- a) zu welchen Themen sie kommunizieren wird;
- b) wann zu kommunizieren ist;
- c) mit wem zu kommunizieren ist;
- d) wie etwas mitgeteilt wird.

Die Organisation muss die Aspekte der Diversität und potenzieller Barrieren bei der Betrachtung ihrer Kommunikationsbedürfnisse berücksichtigen.

Die Organisation muss sicherstellen, dass den Ansichten interessierter Parteien bei der Aufstellung ihres(ihrer) Kommunikationsprozesses(-prozesse) Rechnung getragen wird.

Wenn die Organisation ihre Kommunikationsprozesse aufbaut, muss sie:

- die Kommunikation in ihre Compliance-Kultur, Compliance-Ziele und Compliance-Verpflichtungen einbinden;
- sicherstellen, dass die zu kommunizierenden Compliance-Informationen mit den Informationen übereinstimmen, die innerhalb des Compliance-Managementsystems erzeugt werden, und dass diese verlässlich sind.

Die Organisation muss auf relevante Äußerungen bezogen auf ihr Compliance-Managementsystem reagieren.

Die Organisation muss, soweit angemessen, dokumentierte Information als Nachweis für ihre Kommunikation aufbewahren.

Die Organisation muss:

- für das Compliance-Managementsystem relevante Informationen zwischen den verschiedenen Ebenen und Funktionsbereichen der Organisation intern kommunizieren, einschließlich Änderungen des Compliance-Managementsystems, soweit angemessen;
- sicherstellen, dass ihr(e) Kommunikationsprozess(e) es dem Personal ermöglicht/ermöglichen, zu der ständigen Verbesserung des Compliance-Managementsystems beizutragen.

Die Organisation muss Informationen, die nach dem/den Kommunikationsprozess(en) der Organisation relevant sind, extern kommunizieren und die Kommunikation zu ihrer Compliance-Kultur, den Compliance-Zielen und den Compliance-Verpflichtungen einbinden.

7.5 Dokumentierte Informationen

7.5.1 Allgemeines

Das Compliance-Managementsystem der Organisation muss Folgendes beinhalten:

- a) die durch dieses Dokument geforderten dokumentierten Informationen;
- b) dokumentierte Informationen, welche die Organisation als notwendig für die Wirksamkeit des Compliance-Managementsystems bestimmt hat.

ANMERKUNG Der Umfang dokumentierter Informationen für ein Compliance-Managementsystem kann sich von Organisation zu Organisation unterscheiden, und zwar aufgrund:

- der Größe der Organisation und der Art ihrer Tätigkeiten, Prozesse, Produkte und Dienstleistungen;
- der Komplexität ihrer Prozesse und deren Wechselwirkungen;
- Der Kompetenz der Personen.

7.5.2 Erstellen und Aktualisieren

Beim Erstellen und Aktualisieren dokumentierter Informationen muss die Organisation:

- die angemessene Kennzeichnung und Beschreibung (z. B. Titel, Datum, Autor oder Referenznummer);
- das angemessene Format (z. B. Sprache, Softwareversion, Bilder) und Medium (z. B. Papier, elektronisch);
- eine angemessene Überprüfung und Genehmigung im Hinblick auf Eignung und Angemessenheit sicherstellen.

7.5.3 Lenkung dokumentierter Informationen

Die für das Compliance-Managementsystem erforderlichen und von diesem Dokument geforderten dokumentierten Informationen müssen gelenkt werden, um sicherzustellen, dass sie:

- a) für eine Nutzung geeignet und jederzeit und an jedem Ort verfügbar sind, an dem sie benötigt werden;
- b) ausreichend geschützt sind (z. B. vor dem Verlust der Vertraulichkeit, einem unsachgemäßen Gebrauch oder dem Verlust der Unversehrtheit).

Zur Lenkung der dokumentierten Informationen muss die Organisation sich im notwendigen Umfang mit folgenden Punkten befassen:

- Verteilung, Zugang, Abfrage und Verwendung;
- Lagerung und Erhaltung, einschließlich dem Erhalt der Lesbarkeit;
- Änderungskontrolle (z. B. Versionskontrolle);
- Laufzeit und Anordnung.

Dokumentierte Informationen externer Herkunft, die von der Organisation als notwendig für Planung und Betrieb des Compliance-Managementsystems bestimmt wurden, müssen angemessen gekennzeichnet und gelenkt werden.

ANMERKUNG Zugriff kann eine Entscheidung voraussetzen, mit der die Erlaubnis erteilt wird, dokumentierte Information lediglich zu lesen, oder die Erlaubnis und Befugnis zum Lesen und Ändern dokumentierter Information.

8 Betrieb

8.1 Betriebliche Planung und Steuerung

Die Organisation muss die Prozesse, die zum Erfüllen der Anforderungen und zum Umsetzen der unter 6.1 festgelegten Tätigkeiten benötigt werden, durch Folgendes planen, einführen und kontrollieren:

- Festlegung von Prozesskriterien;
- Umsetzung von Prozesskontrollen in Übereinstimmung mit den Kriterien;
- Aufbewahrung der dokumentierten Information in dem Umfang, der notwendig ist, um das Vertrauen zu haben, dass die Prozesse wie geplant ausgeführt wurden.

Die Organisation muss geplante Änderungen steuern, die Auswirkungen unabsichtlicher Änderungen überprüfen und, falls notwendig, Maßnahmen zur Eindämmung nachteiliger Auswirkungen ergreifen.

Die Organisation muss sicherstellen, dass ausgegliederte Prozesse gesteuert und überwacht werden.

ANMERKUNG Die Ausgliederung des Betriebs einer Organisation befreit diese nicht von ihrer gesetzlichen Verantwortung oder ihren Compliance-Verpflichtungen.

Die Organisation muss sicherstellen, dass durch dritte Parteien ausgeführte Prozesse gesteuert und überwacht werden.

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

8.2 Entwicklung der Kontrollen und Verfahren

Die Organisation muss Kontrollen für das Management ihrer Compliance-Verpflichtungen und der damit verbundenen Compliance-Risiken implementieren. Diese Kontrollen müssen aufrechterhalten, regelmäßig überprüft und geprüft werden, um ihre dauerhafte Wirksamkeit sicherzustellen.

ANMERKUNG Die Prüfung von Kontrollen beinhaltet eine geplante Übung, um festzustellen, ob die Kontrolle ihren vorgesehenen Zweck erfüllt oder nicht, umgangen werden kann oder tatsächlich wirksam die Auswirkung oder Wahrscheinlichkeit des Risikos reduziert.

8.3 Äußern von Bedenken

Die Organisation muss einen Prozess zur Förderung und Ermöglichung — wenn Grund zu der Annahme besteht, dass die Informationen wahr sind — der Meldung versuchter, vermuteter oder tatsächlicher Verstöße gegen die Compliance-Politik oder Compliance-Verpflichtungen festlegen, implementieren und aufrechterhalten.

Dieser Prozess muss:

- in der gesamten Organisation sichtbar und zugänglich sein;
- Berichte vertraulich behandeln;
- anonyme Berichte annehmen;
- meldende Personen vor Vergeltung schützen;
- es Personen ermöglichen, Ratschläge zu erhalten.

Die Organisation muss sicherstellen, dass das gesamte Personal die Berichtsverfahren, seine Rechte und seinen Schutz kennt und diese nutzen kann.

8.4 Untersuchungsprozess

Die Organisation muss Prozesse entwickeln, erstellen, implementieren und aufrechterhalten, um Berichte über vermutete oder tatsächliche Non-Compliance-Fälle zu beurteilen, bewerten, untersuchen und abzuschließen. Diese Prozesse müssen den Grundsätzen der Sorgfalt, dem Recht auf Anhörung und dem Recht auf einen fairen und objektiven Entscheidungsfindungsprozess unterliegen.

Die Untersuchungsprozesse müssen unabhängig und ohne Interessenkonflikt von kompetentem Personal ausgeführt werden.

Die Organisation muss das Ergebnis der Untersuchungen zur Verbesserung (siehe Abschnitt 10) des Compliance-Managementsystems verwenden, sofern zutreffend.

Die Organisation muss regelmäßig Bericht über die Anzahl und die Ergebnisse der Untersuchungen des obersten Organs oder der obersten Leitung erstatten.

Die Organisation muss dokumentierte Informationen zu der Untersuchung aufbewahren.

9 Bewertung der Leistung

9.1 Überwachung, Messung, Analyse und Bewertung

9.1.1 Allgemeines

Die Organisation muss das Compliance-Managementsystem überwachen, um sicherzustellen, dass die Compliance-Ziele erreicht werden.

Die Organisation muss festlegen:

- a) was überwacht und gemessen werden muss;
- b) die Verfahren für Überwachung, Messung, Analyse und Bewertung, soweit zutreffend, um gültige Ergebnisse zu erhalten;
- c) wann die Überwachung und Messung durchgeführt werden müssen;

d) wann die Ergebnisse der Überwachung und Messung analysiert, beurteilt und gemeldet werden müssen.

Die Organisation muss die entsprechenden dokumentierten Informationen als Nachweis für die Ergebnisse aufbewahren.

Die Organisation muss die Compliance-Leistung und die Wirksamkeit des Compliance-Managementsystems bewerten.

9.1.2 Feedback-Quellen zur Compliance-Leistung

Die Organisation muss Prozesse erstellen, implementieren, bewerten und aufrechterhalten, um Feedback zu ihrer Compliance-Leistung aus verschiedenen Quellen zu suchen und zu erhalten. Die Informationen müssen analysiert und kritisch beurteilt werden, um die Grundursachen der Non-Compliance zu ermitteln, sicherzustellen, dass geeignete Maßnahmen getroffen werden, und diese Informationen in der nach 6.4 geforderten regelmäßigen Risikobeurteilung wiederzugeben.

9.1.3 Entwicklung von Indikatoren

Die Organisation muss eine Reihe geeigneter Indikatoren entwickeln, die sie bei der Bewertung der Erreichung ihrer Ziele und der Beurteilung der Compliance-Leistung unterstützen.

9.1.4 Compliance-Berichte

Die Organisation muss Prozesse für die Compliance-Berichterstattung erstellen, implementieren und aufrechterhalten, um sicherzustellen, dass:

- a) geeignete Kriterien für die Berichterstattung definiert werden;
- b) Zeitrahmen für die regelmäßige Berichterstattung festgelegt werden;
- c) ein Ausnahme-Berichterstattungssystem implementiert wird, das Ad-hoc-Berichterstattung ermöglicht;
- d) Systeme und Prozesse implementiert werden, um die Genauigkeit und Vollständigkeit der Informationen sicherzustellen;
- e) korrekte und vollständige Informationen den korrekten Funktionen oder Bereichen der Organisation zur Verfügung gestellt werden, um die zeitnahe Einleitung von Korrektur- und Nachbesserungsmaßnahmen zu ermöglichen.

Alle von der Compliance-Funktion an das oberste Organ oder die oberste Leitung übermittelten Berichte müssen ausreichend gegen Manipulation geschützt sein.

9.1.5 Aufzeichnungen

Korrekte und aktuelle Aufzeichnungen der Compliance-Aktivitäten der Organisation sind aufzubewahren, um den Überwachungs- und Überprüfungsprozess zu unterstützen und die Konformität mit dem Compliance-Managementsystem nachzuweisen.

9.2 Internes Audit

9.2.1 Die Organisation muss in geplanten Abständen interne Audits durchführen, um Informationen darüber zu erhalten, ob das Compliance-Managementsystem:

- a) Folgendem entspricht:
 - 1) den eigenen Anforderungen der Organisation an ihr Qualitätsmanagementsystem;
 - 2) den Anforderungen dieses Dokuments;

b) wirksam verwirklicht und aufrechterhalten wird.

9.2.2 Die Organisation muss:

- a) (ein) Auditprogramm(e) einschließlich der Anwendungshäufigkeit, Verfahren, Verantwortlichkeiten, Planungsanforderungen und Berichterstattung planen, einführen, umsetzen und aufrechterhalten. Das (die) Auditprogramm(e) muss (müssen) die Bedeutung der betreffenden Prozesse und die Ergebnisse zuvor durchgeführter Audits berücksichtigen;
- b) die Auditkriterien und den Anwendungsbereich für jedes Audit festlegen;
- c) Auditoren auswählen und Audits durchführen, um die Objektivität und die Unparteilichkeit des Auditprozesses sicherzustellen;
- d) sicherstellen, dass die Auditergebnisse der relevanten Leitung berichtet werden;

ANMERKUNG 1 Die relevante Leitung könnte die Compliance-Funktion, die oberste Leitung und das oberste Organ umfassen.

- e) dokumentierte Informationen als Nachweis für die Umsetzung des/der Auditprogramms/Auditprogramme und der Auditergebnisse aufbewahren.

ANMERKUNG 2 Weitere Informationen zu Auditmanagementsystemen sind in ISO 19011:2018 enthalten.

9.3 Managementprüfung

Das oberste Organ und die oberste Leitung müssen das Compliance-Managementsystem der Organisation in geplanten Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.

Die Managementüberprüfung muss Folgendes berücksichtigen:

- a) den Status von Maßnahmen als Ergebnis früherer Managementüberprüfungen;
- b) Veränderungen bei externen und internen Themen, die das Compliance-Managementsystem betreffen;
- c) Informationen über die Compliance-Leistung, einschließlich Entwicklungen bei:
 - Nichtkonformität, Non-Compliance und Korrekturmaßnahmen;
 - Ergebnissen von Überwachungen und Messungen;
 - Auditergebnissen;
- d) Möglichkeiten einer ständigen Verbesserung.

Die Managementprüfung muss Folgendes berücksichtigen:

- die Eignung der Compliance-Politik;
- den Umfang, in dem die Compliance-Ziele erfüllt wurden;
- Eignung von Ressourcen;
- die Wirksamkeit der bestehenden Kontrollen und Leistungsindikatoren;

- Kommunikation von Personen, die Bedenken melden, interessierten Parteien, einschließlich Feedback (siehe 9.1.2) und Beschwerden;
- Untersuchungen (siehe 8.4);
- die Wirksamkeit des Berichtssystems.

Die Ergebnisse der Managementprüfung müssen Entscheidungen zu Möglichkeiten für die ständige Verbesserung sowie eventuell erforderliche Änderungen am Compliance-Managementsystem beinhalten.

Die Organisation muss dokumentierte Informationen als Nachweis der Ergebnisse der Managementüberprüfungen aufbewahren.

10 Verbesserung

10.1 Nichtkonformität, Non-Compliance und Korrekturmaßnahmen

Wenn eine Nichtkonformität oder Non-Compliance auftritt, muss die Organisation:

- a) auf die Nichtkonformität oder Non-Compliance reagieren und, falls zutreffend:
 - Maßnahmen zur Überwachung und zur Korrektur ergreifen;
 - mit den Folgen umgehen;
- b) die Notwendigkeit von Maßnahmen zur Beseitigung der Ursachen von Nichtkonformitäten und/oder Non-Compliance bewerten, damit diese nicht erneut oder an anderer Stelle auftreten, und zwar durch:
 - Prüfung der Nichtkonformität und/oder Non-Compliance;
 - Ermittlung der Ursache der Nichtkonformität und/oder Non-Compliance;
 - Bestimmen, ob vergleichbare Nichtkonformitäten und/oder Non-Compliance-Fälle bestehen oder möglicherweise auftreten können;
- c) jegliche erforderliche Maßnahme einleiten;
- d) die Wirksamkeit jeglicher ergriffener Korrekturmaßnahme überprüfen;
- e) falls erforderlich, das Compliance-Managementsystem ändern.

Die Korrekturmaßnahmen müssen den Auswirkungen der vorgefundenen Nichtkonformitäten und/oder Non-Compliance angemessen sein.

Die Organisation muss dokumentierte Informationen aufbewahren, die als Nachweis dienen für:

- der Art der Nichtkonformität und/oder Non-Compliance sowie jeder daraufhin getroffenen Maßnahme;
- der Ergebnisse jeder Korrekturmaßnahme.

10.2 Ständige Verbesserung

Die Organisation muss die Eignung, Angemessenheit und die Wirksamkeit des Compliance-Managementsystems kontinuierlich verbessern.

Wenn die Organisation feststellt, dass Änderungen des Compliance-Managementsystems erforderlich sind, müssen diese Änderungen geplant durchgeführt werden.

Die Organisation muss Folgendes berücksichtigen:

- den Zweck der Änderungen und ihre potenziellen Folgen;
- die Gestaltung und betriebliche Wirksamkeit des Compliance-Managementsystems;
- die Verfügbarkeit angemessener Ressourcen;
- die Zuweisung oder Neuzuweisung von Verantwortlichkeiten und Befugnissen.

Anhang A **(informativ)**

Anleitung zur Verwendung dieses Dokuments

Die Anleitung in diesem Anhang dient dazu, Ansätze und Arten von Maßnahmen anzuzeigen, die eine Organisation bei der Implementierung ihres Compliance-Managementsystems (CMS) anwenden kann. Sie ist nicht dafür vorgesehen, umfassend oder bindend zu sein. Auch ist keine Organisation verpflichtet, alle Vorschläge in dieser Anleitung zu verwirklichen, um über ein Compliance-Managementsystem zu verfügen, welches mit den Anforderungen dieses Dokuments übereinstimmt. Die von einer Organisation unternommenen Schritte sollten hinsichtlich der Art und des Ausmaßes von Konformitätsrisiken, denen die Organisation gegenübersteht, angemessen sein, um ihre Compliance-Verpflichtungen zu erfüllen.

Die Organisation kann sich entscheiden, dieses Compliance-Managementsystem als separates System zu implementieren. Es sollte jedoch idealerweise in Verbindung mit den anderen Managementsystemen der Organisation wie etwa für Risiko, Qualität, Umwelt, Informationssicherheit, Lebensmittelsicherheit und zur Bekämpfung von Korruption, um nur einige Beispiele zu nennen, implementiert werden. In diesen Fällen kann die Organisation auf ISO 9001, ISO 14001, ISO/IEC 27001, ISO 22000, ISO 37001 sowie ISO 26000 und ISO 31000 verweisen.

A.1 Anwendungsbereich

Organisationen jeder Größe, Komplexität oder Industrie können diese Norm anwenden, um ein Compliance-Managementsystem durch Beachtung der Anforderungen der Norm zu erstellen. Dies wird ihnen ein Verständnis für ihren Kontext, den Geschäftsbetrieb sowie die daraus resultierenden Verpflichtungen und Compliance-Risiken vermitteln und sie bei der Implementierung angemessener Schritte für diesen Kontext zur Erfüllung ihrer Verpflichtungen unterstützen. Es sollte jedoch jede der Anforderungen in dem Dokument erfüllt werden. Die Anleitung in diesem Anhang ist informativ.

In der Praxis ist es oftmals leichter, ein Compliance-Managementsystem entsprechend dieser Norm in kleinen Organisationen zu implementieren, da sie weniger komplex sind. Kleine und mittelständische Organisationen werden ihre Organisationspraktiken durch die Anwendung der Grundsätze der Anforderung dieser Norm verbessern.

Dieses Dokument bezieht sich auf das oberste Organ und die oberste Leitung und legt fest, was diese Begriffe in unterschiedlichen Kontexten und an unterschiedlichen Orten bedeuten können. Genauso wie die Norm von allen Organisationen verwendet werden kann, gilt: Wenn Ihre jeweilige Organisation diese Begriffe nicht nutzt, beachten Sie den Zweck ihrer Anwendung; die Anforderungen oder Anweisungen sollten für die Person oder Gruppe von Personen gelten, die zur Leitung der Organisation befugt und hierfür verantwortlich sind.

A.2 Normative Verweisungen

Dieses Dokument enthält keine normativen Verweisungen. Anwender können die Literaturhinweise für weitere Informationen und gegebenenfalls für die Compliance relevante ISO-Normen nutzen.

A.3 Begriffe

Für die verbesserte Angleichung der Internationalen Normen für Managementsysteme hat dieses Dokument die von der ISO entwickelte allgemeine Struktur (en: high-level structure, HLS) angewendet. Die HLS-Struktur beschreibt die Abfolge der Abschnitte, die allgemeinen Begriffe und die identischen Haupttexte, die den Kern der ISO-Managementsystem-Normen bilden. Dies bedeutet, dass einige Begriffe möglicherweise nicht in der Art und Weise genutzt werden, mit der Sie vertraut sind. Beachten Sie die angegebenen Begriffe, wenn Sie dieses Dokument verwenden, zur Klärung.