

DIN ISO 19600

ICS 03.100.02; 03.100.70

**Compliance-Managementsysteme –
Leitlinien (ISO 19600:2014)**Compliance management systems –
Guidelines (ISO 19600:2014)Systèmes de management de la compliance –
Lignes directrices (ISO 19600:2014)

Gesamtumfang 39 Seiten

DIN-Normenausschuss Organisationsprozesse (NAOrg)

Inhalt

	Seite
Nationales Vorwort.....	3
Einleitung	4
1 Anwendungsbereich.....	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Kontext der Organisation	12
4.1 Verstehen der Organisation und ihres Kontextes.....	12
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	12
4.3 Festlegen des Anwendungsbereichs des Compliance-Managementsystems	12
4.4 Compliance-Managementsystem und Grundsätze der Good Governance.....	12
4.5 Bindende Verpflichtungen	13
4.6 Identifikation, Analyse und Bewerten von Compliance-Risiken	14
5 Führung.....	15
5.1 Führung und Verpflichtung.....	15
5.2 Compliance-Politik.....	16
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	17
6 Planung.....	21
6.1 Maßnahmen zum Umgang mit Compliance-Risiken.....	21
6.2 Compliance-Ziele und Planung zu deren Erreichung	22
7 Unterstützung	22
7.1 Ressourcen.....	22
7.2 Kompetenz und Schulung	23
7.3 Bewusstsein.....	24
7.4 Kommunikation	26
7.5 Dokumentierte Information	27
8 Betrieb	28
8.1 Betriebliche Planung und Steuerung	28
8.2 Einrichten von Steuerungen und Prozessen.....	29
8.3 Ausgegliederte Prozesse	30
9 Bewertung der Leistung	30
9.1 Überwachung, Messung, Analyse und Bewertung.....	30
9.2 Audit	35
9.3 Managementbewertung	36
10 Verbesserung	37
10.1 Nichtkonformität, Non-Compliance und Korrekturmaßnahmen.....	37
10.2 Fortlaufende Verbesserung.....	38
Literaturhinweise.....	39

Nationales Vorwort

Diese Deutsche Norm ist die Übersetzung der Internationalen Norm ISO 19600:2014, die im Technischen Komitee ISO/TMBG „Technical Management Board – groups“ erarbeitet wurde.

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

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. Das DIN [und/oder die DKE] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Compliance-Managementsysteme — Leitlinien

Einleitung

Organisationen, die langfristig erfolgreich sein wollen, müssen eine Kultur der Integrität und Regelkonformität (Compliance) pflegen und die diesbezüglichen Bedürfnisse und Erwartungen von interessierten Parteien berücksichtigen. Daher sind Integrität und Regelkonformität nicht nur Grundlage, sondern auch Gelegenheit für eine nachhaltig erfolgreiche Organisation.

Compliance ist ein Ergebnis einer Organisation, die ihren Verpflichtungen nachkommt und wird nachhaltig, indem sie in der Kultur der Organisation, wie auch im Verhalten und der Einstellung der Personen, die für die Organisation arbeiten, verankert wird. Vorzugsweise ist das Compliance-Management, unter Aufrechterhaltung der Unabhängigkeit, in das Finanz-, Risiko-, Qualitäts-, Umwelt- und Gesundheitsmanagement der Organisation und die betrieblichen Gegebenheiten und Prozesse integriert.

Ein wirksames, organisationsweites Compliance-Managementsystem erlaubt es einer Organisation, ihre Bekenntnis zur Regelkonformität, also der Einhaltung der geltenden Gesetze, Branchenkodizes und Organisationsstandards, sowie der Berücksichtigung von Grundsätzen der Corporate Governance, von Best Practice, der Ethik und gesellschaftlicher Erwartungen zum Ausdruck zu bringen.

Die Auseinandersetzung einer Organisation mit dem Thema Compliance ist idealerweise geprägt durch die Leitung, welche zentrale Werte und allgemein anerkannte Grundsätze der Corporate Governance sowie ethische und gesellschaftliche Anforderungen anwendet. Die Verankerung von Compliance im Verhalten der Personen, die für eine Organisation arbeiten, hängt in erster Linie von der Führung auf allen Ebenen und von klar definierten Werten einer Organisation sowie von der Anerkennung und der Verwirklichung von Maßnahmen zur Förderung regelkonformen Verhaltens ab. Sind diese Voraussetzungen nicht auf allen Ebenen der Organisation erfüllt, besteht das Risiko von Regelverstößen.

Die Gerichte verschiedener Staaten haben bei der Beurteilung von Regelverstößen und der Zumessung von Strafen das Bekenntnis einer Organisation zu Compliance und einem Compliance-Managementsystem berücksichtigt. Vor diesem Hintergrund können auch Regulierungs- und Gerichtsbehörden von dieser Internationalen Norm als Maßstab Nutzen ziehen.

Organisationen sind zunehmend davon überzeugt, dass sie durch die Vorgabe verbindlicher Werte und das Betreiben eines adäquaten Compliance-Managements ihre Integrität schützen und die Regelverstöße verhindern oder minimieren können. Integrität und wirksame Compliance sind deshalb zentrale Elemente guten, sorgfältigen Managements. Compliance fördert zudem sozialverantwortliches Verhalten von Organisationen.

Diese Internationale Norm legt keine Anforderungen fest, sondern enthält Empfehlungen zu Compliance-Managementsystemen und bewährten Praktiken. Die Empfehlungen dieser Internationalen Norm sollen flexibel umgesetzt werden können und die Anwendung der Empfehlungen kann je nach Größe und Reifegrad des Compliance-Managementsystems einer Organisation und je nach Kontext, Art und Komplexität der Tätigkeiten der Organisation, einschließlich der Compliance-Grundsätze und -Ziele variieren.

Das Ablaufdiagramm in Bild 1 stimmt konzeptionell mit dem anderer Managementsysteme überein und basiert auf dem Grundsatz der fortlaufenden Verbesserung („Planen-Durchführen-Prüfen-Handeln“ / „Plan-Do-Check-Act“).

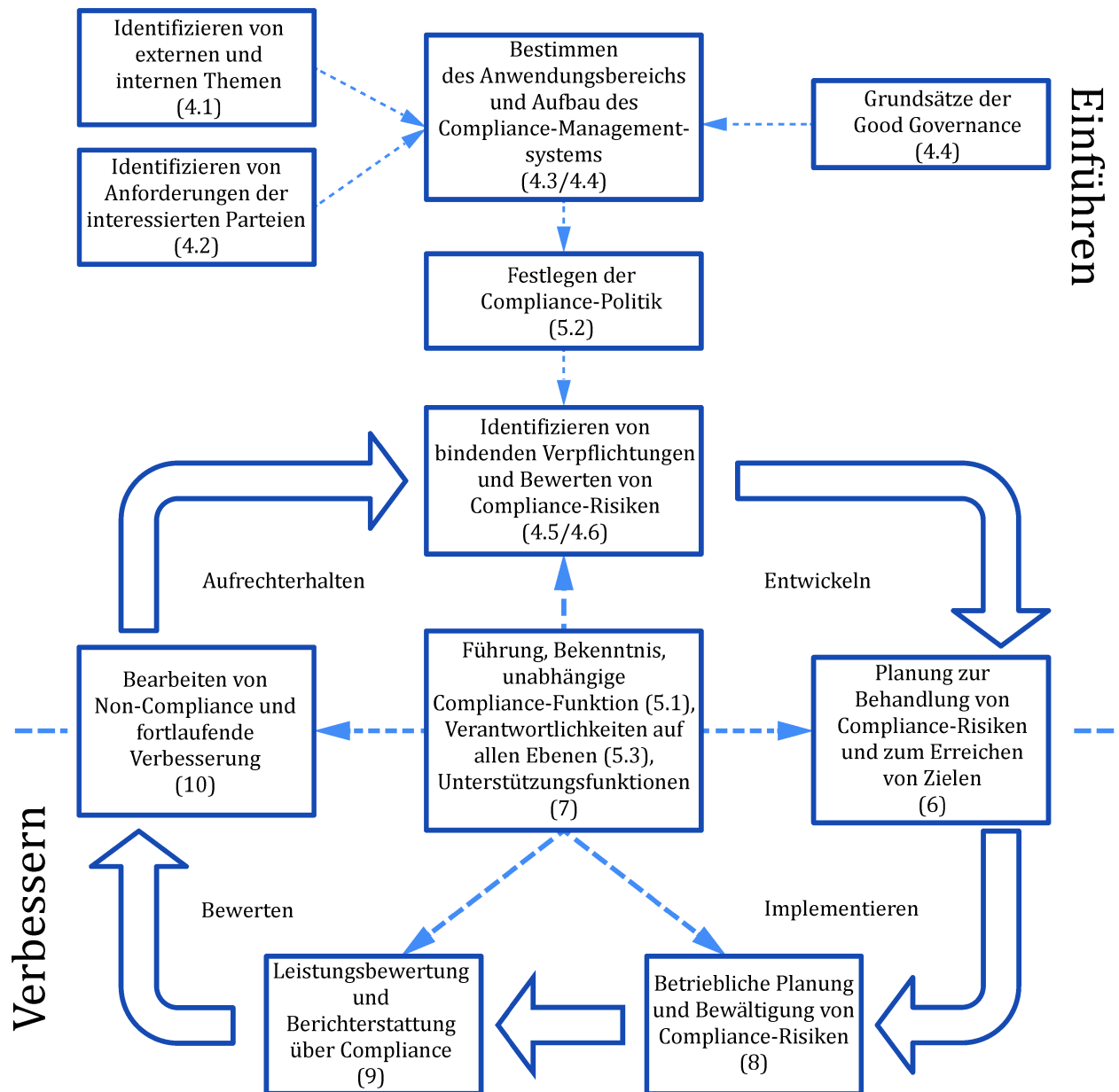


Bild 1 — Ablaufdiagramm eines Compliance-Managementsystems

Diese Internationale Norm wendet die „High-Level-Structure“ an (d.h. feste Abschnittsreihenfolge, einheitlicher Text und einheitliche Terminologie), die von der ISO erarbeitet wurde, um die Internationalen Normen für Managementsysteme anzugleichen. Zusätzlich zu ihren allgemeinen Leitlinien für ein Compliance-Managementsystem bietet diese Norm auch einen Rahmen für die Umsetzung von spezifischen Compliance-bezogenen Anforderungen in einem Managementsystem.

Organisationen, die keinen Managementsystem-Standard oder kein Compliance-Management-Rahmenwerk anwenden, können diese Internationale Norm mit geringem Aufwand als eigenständige Leitlinie auf ihre Organisation anwenden.

Diese Internationale Norm ist geeignet, die Compliance-bezogenen Anforderungen in anderen Managementsystemen besser zu erreichen und eine Organisation dabei zu unterstützen, das Gesamtmanagement ihrer Compliance-Pflichten zu verbessern.

Diese Internationale Norm kann mit bestehenden Managementsystem-Normen (z. B. ISO 9001, ISO 14001, ISO 22000) und allgemeinen Leitlinien (z. B. ISO 31000, ISO 26000) kombiniert werden.

1 Anwendungsbereich

Diese Internationale Norm gibt Empfehlungen für den Aufbau, die Entwicklung, die Umsetzung, die Bewertung, die Aufrechterhaltung und die Verbesserung eines adäquaten und wirksamen Compliance-Managementsystems innerhalb einer Organisation.

Diese Leitlinien für Compliance-Managementsysteme gelten für alle Formen von Organisationen. Der Umfang der Anwendung dieser Leitlinien hängt von der Größe, Struktur, Art und Komplexität der Organisation ab. Diese Internationale Norm basiert auf den Grundsätzen der Good Governance, der Verhältnismäßigkeit, der Transparenz und der Nachhaltigkeit.

2 Normative Verweisungen

Diese Norm enthält keine normativen Verweisungen.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

Organisation

Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre *Ziele* (3.9) 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.

3.2

interessierte Partei

Anspruchsgruppe

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* (3.7) nur einen Teil einer Organisation umfasst, bezieht sich „oberste Leitung“ auf diejenigen, die diesen Teil führen und steuern.

3.4

oberstes Organ

Person oder Personengruppe, die eine *Organisation* (3.1) überwacht, die Ausrichtung festlegt und der gegenüber die *oberste Leitung* (3.3) rechenschaftspflichtig ist

3.5

Beschäftigter

natürliche Person in einem Vertragsverhältnis, das nach dem anwendbaren Recht und der Rechtspraxis als Arbeitsvertrag gilt

3.6

Compliance-Funktion

Person(en) mit der Verantwortung für das *Compliance*-Management (3.17)

Anmerkung 1 zum Begriff: Vorzugsweise wird die Gesamtverantwortung für das *Compliance*-Management (3.17) einer bestimmten Einzelperson übertragen.

3.7

Managementsystem

Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer *Organisation* (3.1), um *Politiken* (3.8), *Ziele* (3.9) und *Prozesse* (3.10) zum Erreichen dieser Ziele festzulegen

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

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

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

3.8

Politik

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

3.9

Ziel

zu erreichendes Ergebnis

Anmerkung 1 zum Begriff: Ein Ziel kann strategisch, taktisch und/oder operativ sein.

Anmerkung 2 zum Begriff: Ziele können sich auf verschiedene Disziplinen beziehen (z. B. finanzielle, gesundheits- und sicherheitsbezogene sowie umweltbezogene Ziele) und für verschiedene Ebenen gelten (z. B. strategisch, organisationsweit, projekt-, produkt-, prozessbezogen).

Anmerkung 3 zum Begriff: Ein Ziel kann auf andere Weise ausgedrückt werden, z. B. als beabsichtigtes Ergebnis, als Zweck, als betriebliches Kriterium, als Compliance-Ziel oder durch andere Wörter mit ähnlicher Bedeutung (en: aim, goal, target).

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

3.10

Prozess

Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt

3.11

Risiko

Auswirkung von Ungewissheit auf die *Ziele* (3.9)

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 73:2009, 3.5.1.3) und „Folgen“ (definiert in ISO Guide 73:2009, 3.6.1.3), 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“ (ISO Guide 73:2009, 3.6.1.1) seines Eintretens beschrieben.

3.12

Compliance-Risiko

Auswirkung von Ungewissheit auf die *Compliance-Ziele* (3.9)

Anmerkung 1 zum Begriff: Compliance-Risiko kann durch Eintrittswahrscheinlichkeit und die Folgen von *Non-Compliance* (3.18) mit den bindenden Verpflichtungen der Organisation charakterisiert werden.

3.13

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 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 beispielsweise in dokumentierter Information enthalten ist.

3.14

Compliance-Anforderung

Anforderung (3.13), die eine *Organisation* (3.1) erfüllen muss

3.15

Compliance-Verpflichtung

Anforderung (3.13), der sich eine *Organisation* (3.1) freiwillig unterwirft

3.16

bindende Verpflichtung

Compliance-Anforderung (3.14) oder *Compliance-Verpflichtung* (3.15)

3.17

Compliance

Einhalten aller *bindenden Verpflichtungen* (3.16) der *Organisation*

Anmerkung 1 zum Begriff: Compliance wird nachhaltig gestaltet, indem sie in der Kultur einer *Organisation* (3.1) und in dem Verhalten und der Grundhaltung der für sie arbeitenden Personen verankert wird.

3.18

Non-Compliance

Nichteinhalten einer *bindenden Verpflichtung* (3.16)

Anmerkung 1 zum Begriff: Non-Compliance kann ein einzelnes oder ein wiederkehrendes Ereignis sein und kann, muss aber nicht, das Ergebnis einer *Nichtkonformität* (3.33) sein.

3.19

Compliance-Kultur

ethische Werte und Überzeugungen, die in einer *Organisation* (3.1) durchgehend bestehen und im Zusammenspiel mit den Strukturen und Kontrollmechanismen einer Organisation einen Verhaltensstandard schaffen, der die *Compliance* (3.17) fördert

3.20

Kodex

Bezeichnung von Praktiken, die intern oder von einer internationalen, nationalen oder Branchen-Organisation entwickelt wurden

Anmerkung 1 zum Begriff: Der Kodex kann obligatorisch oder freiwillig sein.

3.21

Organisations- und Industriestandards

dokumentierte *Kodizes* (3.20), bewährte Praktiken, Chartas, technische und Branchenstandards, die von einer *Organisation* (3.1) als maßgeblich erachtet werden

3.22

Regulierungsbehörde

Organisation (3.1), die für die Regulierung oder die Durchsetzung von *Compliance* (3.17) mit gesetzgeberischen oder sonstigen *Anforderungen* (3.13) verantwortlich ist

3.23

Kompetenz

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

3.24

dokumentierte Information

Information, die von einer *Organisation* (3.1) gelenkt 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: Dokumentierte Information kann sich beziehen auf:

- das *Managementsystem* (3.7), einschließlich damit verbundener *Prozesse* (3.10);
- Informationen, die für den Betrieb der Organisation geschaffen wurden (Dokumentation);
- Nachweise erreichter Ergebnisse (Aufzeichnungen).

3.25

Verfahren

festgelegter Weg zur Durchführung einer Tätigkeit oder eines *Prozesses* (3.10)

3.26

Leistung

messbares Ergebnis

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

Anmerkung 2 zum Begriff: Leistung kann sich auf das Führen und Steuern von Tätigkeiten, *Prozessen* (3.10), Produkten (einschließlich Dienstleistungen), Systemen oder *Organisationen* (3.1) beziehen.

3.27

fortlaufende Verbesserung

wiederkehrende Tätigkeit oder wiederkehrender *Prozess* (3.10) zum Steigern der *Leistung* (3.26)

3.28**ausgliedern (Verb)**

eine Vereinbarung treffen, bei der eine externe *Organisation* (3.1) einen Teil einer Funktion oder eines *Prozesses* (3.10) einer Organisation wahrnimmt bzw. durchführt

Anmerkung 1 zum Begriff: Eine externe Organisation befindet sich außerhalb des Anwendungsbereichs des *Managementsystems* (3.7), obwohl die ausgegliederte Funktion oder der ausgegliederte Prozess im Rahmen des Anwendungsbereichs liegen.

3.29**Überwachung**

Bestimmung des Zustands eines Systems, eines *Prozesses* (3.10) oder einer Tätigkeit

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

Anmerkung 2 zum Begriff: Überwachung ist keine einmalige Tätigkeit, sondern ist ein Prozess der regelmäßigen oder fortlaufenden Überwachung einer Situation.

3.30**Messung**

Prozess (3.10) zum Bestimmen eines Wertes

3.31**Audit**

systematischer, unabhängiger und dokumentierter *Prozess* (3.10) 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 (Erstparteien-Audit) oder externes (Zweitparteien- oder Drittparteien-Audit) Audit sein und es kann ein kombiniertes Audit sein (Verbindung zweier oder mehrerer Disziplinen).

Anmerkung 2 zum Begriff: „Auditnachweise“ und „Auditkriterien“ sind in ISO 19011 definiert.

Anmerkung 3 zum Begriff: Unabhängigkeit lässt sich dadurch nachweisen, dass keine Verantwortlichkeit für die zu auditierenden Tätigkeiten besteht oder keine Vorurteile oder Interessenkonflikte vorliegen.

3.32**Konformität**

Erfüllung einer *Anforderung* (3.13) eines Managementsystems

3.33**Nichtkonformität**

Fehler

Nichterfüllung einer *Anforderung* (3.13) eines Managementsystems

Anmerkung 1 zum Begriff: Nichtkonformität ist nicht gleichzusetzen mit *Non-Compliance* (3.18).

3.34**Korrektur**

Maßnahme zum Beseitigen einer erkannten *Nichtkonformität* (3.33) oder einer *Non-Compliance* (3.18)

3.35**Korrekturmaßnahme**

Maßnahme zum Beseitigen der Ursache einer *Nichtkonformität* (3.33) oder einer *Non-Compliance* (3.18) und zum Verhindern des erneuten Auftretens

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes

Die Organisation sollte externe und interne Themen bestimmen, wie beispielsweise auf Compliance-Risiken bezogene Themen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Compliance-Managementsystems zu erreichen. Dabei sollte die Organisation eine breite Palette an externen und internen Aspekten berücksichtigen, wie beispielsweise gesetzliche, soziale und kulturelle Zusammenhänge, die wirtschaftliche Situation und die internen Richtlinien, Verfahren, Prozesse und Ressourcen.

4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Die Organisation sollte

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

bestimmen.

4.3 Festlegen des Anwendungsbereichs des Compliance-Managementsystems

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

ANMERKUNG Der Anwendungsbereich des Compliance-Managementsystems soll die geographischen und/oder betrieblichen Bereiche festlegen, in denen das Compliance-Managementsystem gilt, besonders wenn die Organisation Teil einer größeren Organisation an einem bestimmten Ort ist.

Bei der Festlegung des Anwendungsbereichs sollte die Organisation

- die unter 4.1 genannten externen und internen Themen,
- die unter 4.2 und 4.5.1 genannten Anforderungen

berücksichtigen.

Der Anwendungsbereich sollte jederzeit als dokumentierte Information verfügbar sein.

4.4 Compliance-Managementsystem und Grundsätze der Good Governance

Die Organisation sollte ein Compliance-Managementsystem, einschließlich der erforderlichen Prozesse und deren Wechselwirkungen, nach der vorliegenden Internationalen Norm unter Berücksichtigung der folgenden Governance-Grundsätze aufbauen, entwickeln, verwirklichen, bewerten, aufrechterhalten und fortlaufend verbessern:

- direkter Zugang der Compliance-Funktion zum obersten Organ;
- Unabhängigkeit der Compliance-Funktion;
- Gewährleistung der erforderlichen Autorität und Befugnisse sowie adäquater Ressourcen der Compliance-Funktion.

Das Compliance-Managementsystem sollte die Werte, Ziele, Strategie und Compliance-Risiken einer Organisation widerspiegeln.