TR CMS 101:2011

Standard für Compliance Management Systeme (CMS)

des TÜV Rheinland, Köln

TÜVRheinland®
Genau. Richtig.

Gesamtumfang: 22 Seiten

TÜVRheinland®
Genau. Richtig.

Inhaltsverzeichnis

Vorwort

Die oberste Leitung ist für die Einrichtung, Aufrechterhaltung und ständige Verbesserung eines Management Systems zur Erfüllung der Compliance-Anforderungen verantwortlich. Als Querschnittsthema betrifft Compliance alle Bereiche und Funktionen einer Organisation. Compliance-Maßnahmen erfolgen nicht isoliert, sondern müssen in die administrativen und operativen Abläufe der Organisation integriert werden. Dies bedingt eine systematische Herangehensweise, um die Erfüllung der Compliance-Anforderungen in der gesamten Organisation zu erreichen.

Angesichts der Bedeutung von Compliance und der möglichen Folgen von Verstößen gegen Compliance-Anforderungen handelt es sich beim Compliance Management System um ein eigenständiges Manangement-System. Das Compliance Management System weist Berührungspunkte zu anderen Management-Systemen und Regelwerken auf (z.B. Corporate Governance, Risikomanagement, Qualitätsmanagement, Umweltmanagement, Betriebliches Kontinuitätsmanagement, Nachhaltigkeitsmanagement).

Compliance-Anforderungen sind nicht statisch, sondern unterliegen häufigen Änderungen (z.B. aufgrund von gesetzlichen Änderungen, der Aufnahme neuer Tätigkeiten oder der Erstreckung von Aktivitäten in neue Regionen). Für die Realisierung und eine ständige Verbesserung des Compliance Management Systems ist ein iterativer Prozess erforderlich, der in folgender Übersicht dargestellt wird:

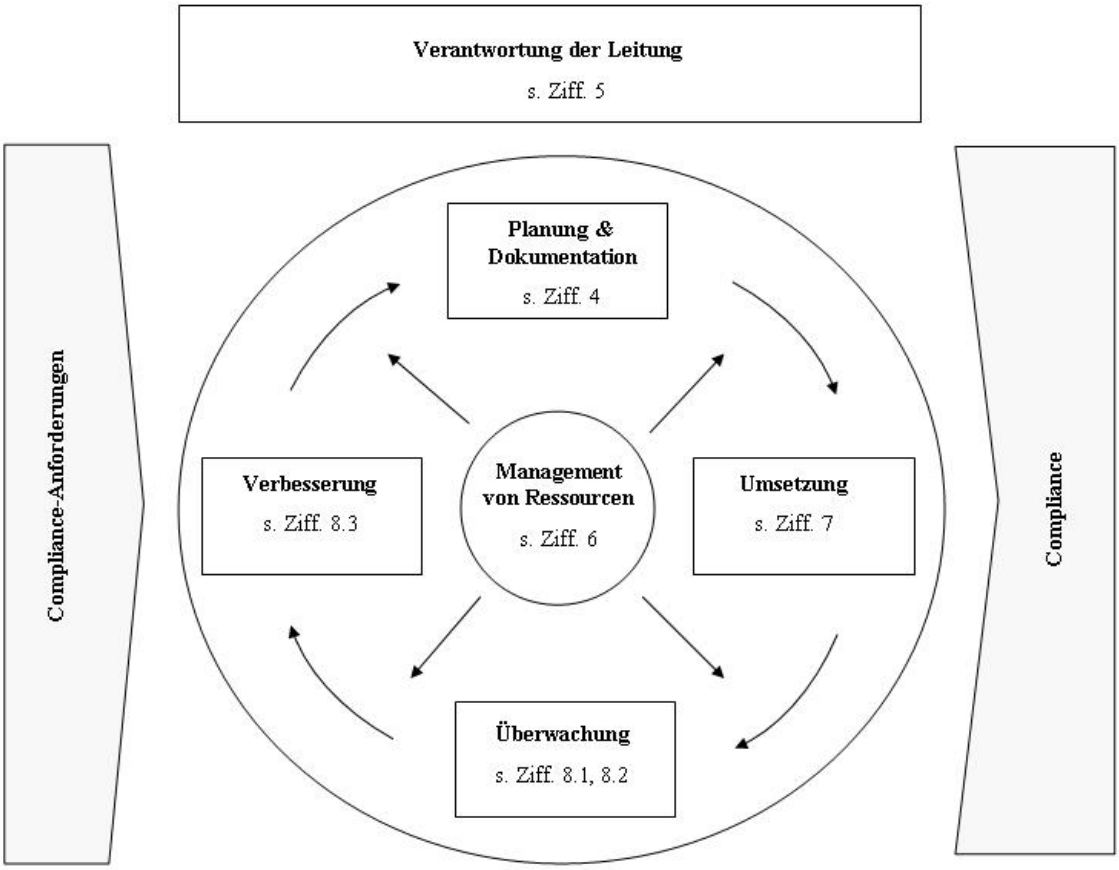

Bild 1 - Modell eines prozessorientierten Compliance Management Systems (CMS)®

Die Dokumentation des Compliance Management Systems ermöglicht dessen unabhängige Umsetzung und Aufrechterhaltung.

Aus der wirksamen Umsetzung und Aufrechterhaltung eines Compliance Management Systems und dessen Kommunikation innerhalb der Organisation und nach außen ergeben sich für die Organisation zusätzliche Chancen. Das hierdurch erzeugte Vertrauen bei Stakeholdern (z.B. Mitarbeitern, Kunden, Behörden, Gesellschaftern, Investoren) kann sich in nachhaltigeren Beziehungen auswirken (z.B. stärkere Kundenbindung, langfristige Geschäftsbeziehungen, höhere Motivation der Beschäftigten). Darüber hinaus kann die Organisation von niedrigeren Kosten für Korrekturmaßnahmen, günstigeren Finanzierungskonditionen und Versicherungsprämien profitieren.

0 Einleitung

Dieser Standard zeigt die Grundelemente auf, die ein Management System zur Erfüllung der für die Organisation anwendbaren Compliance-Anforderungen enthalten muss; die konkrete Ausgestaltung und Umsetzung des Compliance Management Systems ist organisationsabhängig und liegt in der Verantwortung der obersten Leitung.

Die in diesem Standard aufgezeigten Elemente des Compliance Management Systems sind überprüfbar und nachweisbar, um festzustellen, ob und in welchen Punkten eine Organisation über ein Compliance Management System verfügt, das die in Kapitel 2 beschriebenen Ziele erfüllt. Compliance Management Systeme können organisationsspezifisch unterschiedlich strukturiert oder dokumentiert sein.

Der Standard TR CMS 101:2011 für Compliance Management Systeme ermöglicht es, einer Organisation nach erfolgreicher Durchführung des Systemaudits in einem Zertifikat zu bescheinigen, dass sie nachweislich

a) ein wirksames Compliance Management System aufrecht erhält,

b) die Mindestanforderungen an ein Compliance Management System erfüllt, und

c) in der Lage ist, präventive wie korrigierende Maßnahmen umzusetzen.

Mit der Zertifizierung des Compliance Management Systems wird keine Aussage darüber getroffen, dass die Organisation tatsächlich alle geltenden Compliance-Anforderungen erfüllt; die Durchführung des Zertifizierungsaudits stellt keine Beratung hinsichtlich der anwendbaren Regeln bzw. Rechtsberatung dar. Ein Zertifizierungsaudit bzw. eine Zertifizierung entbindet die Organisation nicht grundsätzlich von einer Haftung bei Organisationsverschulden oder Aufsichtspflichtverletzungen. Vorgaben für das Audit und Prüfanleitungen sind in einem separaten Leitfaden des TÜV Rheinland niedergelegt.

1 Anwendungsbereich

Der vorliegende Standard legt die grundlegenden Elemente fest, die zu einem Compliance Management System gehören. Er ist auf alle Organisationen sowohl national als auch international anwendbar.

Die Ausgestaltung und Verwirklichung des Compliance Management Systems wird beeinflusst durch

a) Größe und Struktur der Organisation, Art ihrer Tätigkeit,

b) Regionen, in denen die Organisation tätig ist,

c) bereitgestellte Produkte,

d) angewendete Prozesse,

e) Umfeld, sich verändernde Erfordernisse,

f) spezifische Risiken der Organisation und

g) besondere Ziele der Organisation.

Elemente des Compliance Management Systems sind so festzulegen, dass sie nachgewiesen und überprüft werden können. Damit lässt sich feststellen, ob die Organisation über ein wirksames Compliance Management System verfügt.

2 Ziele des Compliance Management Systems

Ziel des Compliance Management Systems ist es, systematisch die Voraussetzungen in der Organisation dafür zu schaffen, dass Verstöße gegen Compliance-Anforderungen vermieden bzw. wesentlich erschwert und eingetretene Verstöße erkannt und behandelt werden können.

3 Begriffe

Ausgegliederte Compliance-Prozesse	Compliance-relevante Abläufe, die aufgrund einer Entscheidung der Organisation durch eine externe Stelle ausgeführt werden
Audit	Prüfung
Betriebliches Kontinuitätsmanagement	Sicherstellung der Aufrechterhaltung wesentlicher Abläufe in der Organisation beim Eintritt schwerwiegender Ereignisse (Business Continuity Management)
Compliance	Erfüllung der Compliance-Anforderungen (s. dort)
Compliance-Anforderungen	Alle Regeln, die von der Organisation und den dort tätigen Personen zu beachten sind, unabhängig davon, ob es sich um gesetzliche oder behördliche Compliance-Anforderungen handelt oder solche, deren verbindliche Anwendbarkeit die Organisation

	für sich selbst oder eine andere Organisation für seine Mitglieder festgelegt hat
Compliance-Beauftragter	Beauftragter der obersten Leitung für die Umsetzung der Elemente des Compliance Management Systems
Compliance-Kultur	Innere Akzeptanz der Compliance-Anforderungen, gelebtes Verhalten und tatsächliche Berücksichtigung der Compliance-Anforderungen in der Organisation
Hinweisgebersystem	Möglichkeit, sich auch außerhalb der sonst geltenden Berichtswege mit compliance-relevanten Hinweisen an eine (interne oder externe) Anlaufsstelle wenden zu können
Kennzahlen zur Messung von Compliance	Messbare Kenngrößen, die zahlenmäßig Rückschlüsse auf die Wirksamkeit des Compliance Management Systems zulassen (z.B. Anzahl der erkannten Verstöße gegen Compliance-Anforderungen)

4 Compliance Management System

4.1 Allgemeine Anforderungen

Die Organisation muss ein Compliance Management System einführen, dokumentieren, verwirklichen, aufrechterhalten und dessen Wirksamkeit ständig verbessern.

Die Organisation muss

a) die für das Compliance Management System erforderlichen Prozesse und ihre Anwendung in der gesamten Organisation festlegen,

b) die Abfolge und Wechselwirkung dieser Prozesse festlegen,

c) die erforderlichen Kriterien und Methoden festlegen, um das wirksame Durchführen und Lenken dieser Prozesse sicherzustellen,

d) die Verfügbarkeit von Ressourcen und Informationen sicherstellen, die zur Durchführung und Überwachung dieser Prozesse benötigt werden,

e) diese Prozesse überwachen, soweit zutreffend messen und analysieren und

f) die erforderlichen Maßnahmen treffen, um die geplanten Ergebnisse sowie eine ständige Verbesserung dieser Prozesse zu erreichen.

Die Organisation muss diese Prozesse in Übereinstimmung mit den Anforderungen dieses Standards leiten und lenken.

Wenn sich die Organisation entscheidet, compliance-relevante Prozesse auszugliedern, muss sie die Lenkung derartiger Prozesse sicherstellen. Die Art und der Umfang der Lenkung derartiger ausgegliederter Prozesse müssen im Compliance Management System festgelegt sein.

ANMERKUNG Die Ausgliederung von compliance-relevanten Prozessen entbindet die Organisation nicht von der Pflicht zur Erfüllung der für sie geltenden Compliance-Anforderungen.

4.2 Dokumentationsanforderungen

4.2.1 Allgemeines

Die Dokumentation zum Compliance Management System muss die notwendigen Vorgabe- und Nachweisdokumente enthalten.

Übliche Vorgabedokumente sind:

a) Rechtsquellen; darunter Gesetze, Verordnungen, Verwaltungsakte, Satzungen, verbindliche Standards oder Kodizes,

b) Aufstellung der spezifischen, für die Organisation anwendbaren Compliance-Anforderungen (Handbücher, Richtlinien),

c) Beschreibung des Compliance Management Systems,

d) dokumentierte Verfahren und Prozesse oder Arbeitsanweisungen zur Sicherstellung der Erfüllung von Compliance-Anforderungen und zur Vernetzung von compliance-relevanten Prozessen mit anderen Prozessen und

e) dokumentierte Verfahren, die von diesem Standard gefordert werden.

Übliche Nachweisdokumente sind:

a) Aufzeichnungen über Ergebnisse von Compliance-Audits und Korrekturmaßnahmen,

b) Compliance-Berichte,

c) Risikoanalysen und -bewertungen

d) Aufzeichnungen über Kennzahlen zur Messung von Compliance,

e) Protokolle der Befassung der obersten Leitung mit Compliance-Angelegenheiten,

f) Dokumente über die Durchführung von Compliance-Schulungen,

g) Dokumente über Verstöße gegen Compliance-Anforderungen und die in diesen Fällen ergriffenen Maßnahmen und Sanktionen,

h) Aufzeichnungen, die die Organisation zur Sicherstellung der wirksamen Planung, Durchführung und Lenkung ihrer Prozesse als notwendig eingestuft hat, und

i) rechtlich vorgeschriebene Nachweisdokumente.

4.2.2 Lenkung von Vorgabedokumenten

Die vom Compliance Management System geforderten Vorgabedokumente müssen gelenkt werden. Ein dokumentiertes Verfahren zur Festlegung der erforderlichen Lenkungsmaßnahmen muss eingeführt werden, um

a) Dokumente vor ihrer Herausgabe zu genehmigen,

b) Dokumente in geplanten Abständen zu bewerten, bei Bedarf zu aktualisieren und erneut zu genehmigen,

c) sicherzustellen, dass Änderungen und der aktuelle Überarbeitungsstatus von Dokumenten gekennzeichnet werden,

d) sicherzustellen, dass gültige Fassungen zutreffender Dokumente an den jeweiligen Einsatzorten verfügbar sind,

e) sicherzustellen, dass Dokumente für die Betroffenen lesbar und verständlich sind,

g) die unbeabsichtigte Verwendung veralteter Dokumente zu verhindern und diese in geeigneter Weise zu kennzeichnen, falls sie aufbewahrt werden,

h) sicherzustellen, dass gesetzliche Aushang- oder Auslegungspflichten eingehalten werden und

i) sicherzustellen, dass Dokumente und Aufzeichnungen für die Dauer der gesetzlichen oder sonst festgelegten Aufbewahrungspflicht in geeigneter Weise aufbewahrt und geschützt werden und lesbar, leicht erkennbar und wieder auffindbar bleiben.

4.2.3 Lenkung von Nachweisdokumenten

Nachweisdokumente über die Einhaltung der Compliance-Anforderungen müssen gelenkt werden.

Die Organisation muss ein dokumentiertes Verfahren einführen, um die Lenkungsmaßnahmen festzulegen, die für die Kennzeichnung, die Aufbewahrung, den Schutz, die Wiederauffindbarkeit von Nachweisdokumenten, die Einhaltung der Aufbewahrungsfrist sowie die Verfügung über Nachweisdokumente erforderlich sind.

Nachweisdokumente müssen lesbar, leicht erkennbar und wieder auffindbar verwahrt werden.

5 Verantwortung der Leitung

5.1 Verpflichtung der Leitung

Die oberste Leitung muss die Entwicklung und Verwirklichung des Compliance Management Systems und die ständige Verbesserung von dessen Wirksamkeit nachweisen, indem sie

a) der Organisation die Verbindlichkeit der Compliance-Anforderungen und die Bedeutung der Einhaltung der Compliance-Anforderungen vermittelt,

b) ein Bekenntnis zur Schaffung einer Compliance-Kultur abgibt, insbesondere ihre Erwartung zum Ausdruck bringt, dass die Compliance-Anforderungen tatsächlich eingehalten werden,

c) die Ziele und Werte der Organisation mit den Compliance-Anforderungen in Einklang bringt,

d) regelmäßig die Compliance-Risikoanalyse hinsichtlich der tatsächlichen Risiken überprüft und ggf. anpasst,

d) planmäßig Managementbewertungen des Compliance Management Systems durchführt,

e) die Verfügbarkeit von Ressourcen sicherstellt und

f) die fortdauernde Angemessenheit und Funktionsfähigkeit des Compliance Management Systems überwacht.

5.2 Verantwortung, Befugnis und Kommunikation

5.2.1 Verantwortung und Befugnis

Die oberste Leitung muss sicherstellen, dass die Verantwortungen und Befugnisse festgelegt und innerhalb der Organisation bekannt gemacht werden.

5.2.2 Compliance-Beauftragter

Die oberste Leitung muss ein Mitglied der Leitung der Organisation sorgfältig auswählen und benennen, das selbständig oder in Zusammenarbeit mit anderen die Verantwortung und Befugnis hat:

a) darauf hinzuwirken, dass die für das Compliance Management System erforderlichen Prozesse eingeführt, verwirklicht und aufrechterhalten werden,

b) der obersten Leitung über die Leistung und Wirksamkeit des Compliance Management Systems und jegliche Notwendigkeit für Verbesserungen zu berichten,

c) das Bewusstsein und die Kommunikation über die Compliance-Anforderungen in der gesamten Organisation sicherzustellen und

d) eigeninitiativ compliance-relevante Vorgänge aufzugreifen, zu dokumentieren und an die oberste Leitung zu berichten.

Die oberste Leitung ermöglicht dem Compliance-Beauftragten eine unabhängige Wahrnehmung der Compliance-Aufgaben. Sie weist dem Compliance-Beauftragten keine weiteren Aufgaben zu, die Zielkonflikte mit der Erfüllung der Compliance-Aufgaben mit sich bringen.

5.2.3 Interne Kommunikation

Die oberste Leitung muss sicherstellen, dass geeignete Prozesse der Kommunikation innerhalb der gesamten Organisation eingeführt und aufrechterhalten werden und eine Kommunikation über die Wirksamkeit des Compliance Management Systems stattfindet. Die Kommunikation muss die Unterrichtung aller Personen über die sie betreffenden Compliance-Anforderungen beinhalten und auf mögliche Folgen von Compliance-Verstößen hinweisen. Die oberste Leitung muss sicherstellen, dass erkannte Verstöße gegen Compliance-Anforderungen unverzüglich berichtet werden.

Die oberste Leitung muss die Einhaltung ihrer Informations- und Berichtspflichten zu Compliance-Angelegenheiten gegenüber den internen Aufsichtsgremien und -organen sicherstellen. Die internen Aufsichtsgremien und -organe befassen sich entsprechend ihren gesetzlichen Aufsichts- bzw. Sorgfaltspflichten mit Compliance-Angelegenheiten der Organisation.

5.3 Managementbewertung

5.3.1 Allgemeines

Die oberste Leitung muss das Compliance Management System der Organisation planmäßig in angemessenen Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen. Diese Bewertung muss die Bewertung von Möglichkeiten für Verbesserungen und den Änderungsbedarf bezüglich des Compliance Management System enthalten.

Aufzeichnungen über die Managementbewertung müssen aufrechterhalten werden.

5.3.2 Eingaben für die Bewertung

Eingaben für die Managementbewertung müssen Informationen zu Folgendem enthalten:

a) Ergebnisse von Audits,

b) Hinweise zu compliance-relevanten Angelegenheiten von Mitarbeitern, Geschäftspartnern, Kunden, Nutzern, Behörden, Verbänden etc.,

c) Meldungen über erkannte Verstöße gegen Compliance-Anforderungen,

d) Status und Wirksamkeit von Vorbeugungs- und Korrekturmaßnahmen sowie Aufwand für ergriffene Korrekturmaßnahmen,

e) Folgemaßnahmen vorangegangener Managementbewertungen und Ergebnisse von Folgemaßnahmen vorausgegangener Überwachungen,

f) Änderungen, die sich auf das Compliance Management System auswirken könnten (z.B. Gesetzesänderungen, veränderte Risikolage),

g) Empfehlungen für Verbesserungen und

h) Kennzahlen zur Messung von Compliance.

5.3.3 Ergebnisse der Bewertung

Die Ergebnisse der Managementbewertung müssen Entscheidungen und Maßnahmen zu Folgendem enthalten:

a) Verbesserung der Wirksamkeit des Compliance Management Systems und seiner Prozesse,

b) Bedarf an Ressourcen und

c) Abdeckung des ermittelten Schulungsbedarfs zu compliance-relevanten Themen.

6 Management von Ressourcen

6.1 Bereitstellung von Ressourcen

Die Organisation muss die erforderlichen Ressourcen ermitteln und bereitstellen, um das Compliance Management System zu verwirklichen, aufrechtzuerhalten und seine Wirksamkeit ständig zu verbessern.

6.2 Personelle Ressourcen

6.2.1 Allgemeines

Personen, die für ihre Tätigkeit Compliance-Anforderungen zu beachten haben, müssen über die zur Erfüllung dieser Anforderungen erforderliche Ausbildung, Schulung, Fertigkeiten und Erfahrungen verfügen.

6.2.2 Kompetenz, Schulung und Bewusstsein

Die Organisation muss

a) den Schulungsbedarf systematisch ermitteln und auswerten, der für die Erlangung der notwendigen Kompetenzen zur Erfüllung der Compliance-Anforderungen erforderlich ist,

b) erforderliche Compliance-Schulungen oder andere Maßnahmen durchführen, um diese Kompetenzen zu vermitteln,

c) die Wirksamkeit der ergriffenen Maßnahmen beurteilen,

d) das Verständnis für die Bedeutung der Erfüllung der Compliance-Anforderungen und das Bewusstsein für die möglichen Folgen von Compliance-Verstößen erzeugen und

e) geeignete Aufzeichnungen zu Ausbildung, Schulung, Fertigkeiten und Erfahrung sowie den anderen Maßnahmen zur Förderung der notwendigen Kompetenz führen.

6.3 Infrastruktur

Die Organisation muss die Infrastruktur ermitteln, bereitstellen und aufrechterhalten, die zur Erfüllung der Compliance-Anforderungen erforderlich ist.

Die Organisation muss bei Bedarf Zugang zu (internen oder externen) Rechtsauskünften hinsichtlich des Umfangs, der Anwendbarkeit, der Geltung und der Reichweite von Compliance-Anforderungen ermöglichen.

7 Compliance-Prozesse und Umsetzung

7.1 Spezifische Compliance-Risiken der Organisation

Die Organisation muss Compliance-Risiken, die sich aus ihrer Größe, Struktur, der Art ihrer Tätigkeit sowie den Regionen, in denen sie tätig ist, ergeben, systematisch analysieren und identifizieren.

Die oberste Leitung muss

a) sicherstellen, dass ihr regelmäßig über die Compliance-Risiken der Organisation berichtet wird, und

b) die spezifischen Compliance-Risiken der Organisation regelmäßig bewerten und angemessene Vorbeugungsmaßnahmen ergreifen.

7.2 Anwendbare Compliance-Anforderungen

Die Organisation muss

a) die für sie aufgrund ihrer Aktivitäten (z.B. Dienstleistungen, Produkte, geographische Regionen) spezifisch anwendbaren Compliance-Anforderungen systematisch analysieren und identifizieren und das Verfahren hierfür dokumentieren,

b) Änderungen der spezifisch anwendbaren Compliance-Anforderungen sowie die Auswirkungen dieser Änderungen auf die Organisation laufend überwachen,

c) über die Einführung von verbindlichen Compliance-Vorgaben, die nicht bereits kraft Gesetzes oder behördlicher Anordnung gelten, entscheiden,

d) die für sie spezifisch anwendbaren Compliance-Anforderungen dokumentieren und verfügbar machen und

e) sicherstellen, dass alle Betroffenen über die anwendbaren Compliance-Anforderungen informiert sind, und

f) die Dokumentation der für sie spezifisch anwendbaren Compliance-Anforderungen laufend aktualisieren.

7.3 Entscheidung über die angemessenen Maßnahmen zur Erfüllung der Compliance-Anforderungen

Die Organisation muss über Abläufe verfügen, mit denen sichergestellt werden kann, dass die zur Erfüllung der Compliance-Anforderungen angemessenen Maßnahmen getroffen und die der Größe und Struktur der Organisation, der Art ihrer Tätigkeit sowie den Regionen, in denen sie tätig ist, angemessen Prozesse eingeführt werden.

7.4 Integration der Compliance-Anforderungen in die Arbeitsabläufe

Arbeitsabläufe müssen so gestaltet werden, dass die Erfüllung der Compliance-Anforderungen erleichtert und ermöglicht wird.

7.5 Umgang mit compliance-relevanten Interessenskonflikten

Die Organisation muss über Prozesse verfügen, mit denen mögliche und aufgetretene compliance-relevante Interessenskonflikte identifiziert werden können.

Sie muss Betroffenen Maßgaben an die Hand geben, wie mit möglichen oder aufgetretenen, compliance-relevanten Interessenskonflikten umzugehen ist. Dies gilt auch hinsichtlich von Konflikten zwischen den Interessen der Organisation einerseits und den Interessen von Kunden oder Nutzern andererseits.

Die Organisation muss sicherstellen, dass angemessene Funktionstrennungen bestehen, die zur Vermeidung von compliance-relevanten Interessenskonflikten erforderlich sind.

7.6 System von Freigaben, Genehmigungen und Berechtigungen

Die Organisation muss über ein System von Berechtigungen für Freigaben und Genehmigungen verfügen, das geeignet ist, Verstöße gegen Compliance-Anforderungen zu vermeiden.

Die geltenden Freigabegrenzen, Genehmigungserfordernisse und die Notwendigkeit des Zusammenwirkens mehrerer Personen für die Durchführung compliance-relevanter Vorgänge müssen dokumentiert und innerhalb der Organisation bekannt gemacht werden.

7.7 Hinweisgebersystem

Die Organisation muss eine (interne oder externe) Anlaufsstelle einrichten und innerhalb der Organisation bekanntmachen, die es Personen ermöglicht, compliance-relevante Hinweise (z.B. zu erkannten Verstößen gegen Compliance-Anforderungen) – gegebenenfalls anonym – zu geben oder Vorschläge einzubringen.

Die Abläufe im Umgang mit compliance-relevanten Hinweisen und Vorschlägen, die bei der Anlaufstelle eingehen, müssen dokumentiert werden. Hinweisgeber erhalten eine Rückmeldung über die Behandlung ihrer Hinweise und Vorschläge, sofern diese nicht anonym erfolgen.

ANMERKUNG Für das Hinweisgebersystem muss nicht notwendigerweise eine neue Funktion geschaffen werden; das Hinweisgebersystem muss jedoch Personen ermöglichen, sich auch außerhalb der sonst in der Organisation geltenden Berichtswege mit compliance-relevanten Hinweisen an eine Anlaufsstelle wenden zu können.

7.8 Beratung, Unterstützung

Die Organisation muss sicherstellen, dass Betroffene bei Fragen zu compliance-relevanten Angelegenheiten und zum Umgang mit Interessenskonflikten Beratung und Hilfestellung erhalten.

7.9 Umgang mit compliance-relevanten Vorgängen

Die Organisation muss über ein dokumentiertes Verfahren für den Umgang mit compliance-relevanten Vorgängen, einschließlich Zuständigkeiten und Berichtswegen, verfügen.

Die Organisation muss die rechtlich vorgeschriebene Kommunikation nach außen (z.B. Berichts-, Melde-, Informations- und Warnpflichten gegenüber Behörden, Kapitalmarkt, Kunden etc.) sicherstellen.

Alle relevanten Compliance-Vorgänge sowie ihre Behandlung und Lösung müssen dokumentiert werden.

7.10 Externe Dienstleister

Die Organisation muss sicherstellen, dass für externe Dienstleister, derer sie sich für die Erfüllung ihrer Compliance-Anforderungen bedient oder die sie in compliance-relevante Vorgänge einbindet, zumindest dieselben Compliance-Anforderungen gelten wie für die Organisation selbst.

8 Systemüberwachung, -analyse und -verbesserung

Die Organisation muss die Überwachungs-, Analyse- und Verbesserungsprozesse planen und verwirklichen, die erforderlich sind, um die Wirksamkeit des Compliance Management Systems sicherzustellen.

8.1 Interne Audits

Die Organisation muss in geplanten Abständen interne Audits durchführen, um zu ermitteln, ob das Compliance Management System

a) die Compliance-Anforderungen und die in diesem Standard beschriebenen Anforderungen an das Compliance Management System erfüllt und

b) wirksam verwirklicht und aufrechterhalten wird.

Ein Auditprogramm muss geplant werden, wobei der Status und die Bedeutung der zu auditierenden Prozesse und Bereiche sowie die Ergebnisse früherer Audits berücksichtigt werden müssen. Die Auditkriterien, der Auditumfang, die Audithäufigkeit und die Auditmethoden müssen festgelegt werden. Die Auswahl der Auditoren und die Durchführung der Audits müssen Objektivität und Unparteilichkeit des Auditprozesses sicherstellen. Auditoren dürfen ihre eigene Tätigkeit nicht auditieren.

Die Organisation entscheidet über die Verantwortungen und über die Durchführung von Audits sowie über die Berichterstattung über die Ergebnisse und über die Führung von Aufzeichnungen. Die wesentlichen Ergebnisse der Compliance-Audits müssen an die oberste Leitung berichtet werden.

Aufzeichnungen über Audits und deren Ergebnisse müssen aufrechterhalten werden.

Die für den auditierten Bereich verantwortliche Leitung muss sicherstellen, dass jegliche notwendigen Korrekturen und Korrekturmaßnahmen ohne ungerechtfertigte Verzögerung zur Behebung von erkannten Abweichungen und ihrer Ursachen ergriffen werden. Folgemaßnahmen müssen die

Verifizierung der ergriffenen Maßnahmen und die Berichterstattung über die Verifizierungsergebnisse enthalten.

8.2 Überwachung

Die Organisation muss geeignete Methoden zur Überwachung des Compliance Management Systems anwenden und die Ergebnisse der Überwachung des Compliance Management Systems dokumentieren. Diese Methoden müssen darlegen, dass die eingeführten Prozesse in der Lage sind, die Compliance-Anforderungen zu erfüllen.

Die Überwachung muss sich auch auf die von der Organisation ausgegliederten compliance-relevanten Prozesse und auf die zur Durchführung dieser Prozesse herangezogenen externen Stellen beziehen.

Wo anwendbar, werden Kennzahlen zur Messung von Compliance zur Ermittlung der Wirksamkeit der Prozesse zur Erfüllung der Compliance-Anforderungen eingeführt und verwendet.

Eingehende Meldungen oder Berichte über compliance-relevante Vorkommnisse oder Ereignisse (einschließlich Verstößen gegen Compliance-Anforderungen) werden umgehend und planmäßig aufgegriffen und an die definierten Stellen berichtet.

Werden die geplanten Ergebnisse nicht erreicht, müssen, soweit angemessen, Korrekturen und Korrekturmaßnahmen ergriffen werden.

Der Status von Korrekturmaßnahmen muss laufend durch die von der Organisation bestimmten Verantwortlichen nachgehalten werden.

8.3 Verbesserung

8.3.1 Ständige Verbesserung

Die Organisation muss die Wirksamkeit des Compliance Management Systems ständig aufgrund der Ergebnisse aus der Überwachung einschließlich der Auditergebnisse, der Compliance-Kennzahlen und den Managementbewertungen verbessern.

8.3.2 Korrekturmaßnahmen

Die Organisation muss angemessene Korrekturmaßnahmen zur Beseitigung der Ursachen von erkannten Verstößen gegen Compliance-Anforderungen ergreifen, um deren erneutes Auftreten zu verhindern.

Ein dokumentiertes Verfahren muss eingeführt werden, um Anforderungen festzulegen zur

a) Bewertung von Verstößen gegen Compliance-Anforderungen,

b) Ermittlung der Ursachen von Verstößen gegen Compliance-Anforderungen,

c) Beurteilung des Handlungsbedarfs, um das erneute Auftreten von Verstößen gegen Compliance-Anforderungen zu verhindern,

d) Ermittlung und Verwirklichung der erforderlichen Maßnahmen,

e) Aufzeichnung der Ergebnisse der ergriffenen Maßnahmen,

f) Bewertung der Wirksamkeit der ergriffenen Korrekturmaßnahmen und

g) Bewertung der Wirksamkeit der durchgeführten Überwachungsmaßnahmen.

8.3.3 Vorbeugungsmaßnahmen

Die Organisation muss angemessene Maßnahmen zur Beseitigung der Ursachen für mögliche Verstöße gegen Compliance-Anforderungen festlegen, um deren Auftreten zu verhindern.

Ein dokumentiertes Verfahren muss eingeführt werden, um Anforderungen festzulegen zur

a) Ermittlung möglicher künftiger Verstöße gegen Compliance-Anforderungen und ihrer Ursachen,

b) Beurteilung des Handlungsbedarfs, um das Auftreten von Verstößen gegen Compliance-Anforderungen zu verhindern,

c) Ermittlung und Verwirklichung der erforderlichen Maßnahmen,

d) Aufzeichnung der Ergebnisse der ergriffenen Maßnahmen und

e) Bewertung der Wirksamkeit der ergriffenen Vorbeugungsmaßnahmen.

Literaturhinweise

ISO 9001:2008

ONR 49001:2004

BS 25999

AS 3806-2006

ISO 26000:2010