Zertifizierungsschema Y03

# Compliance Management Systeme
## ISO 19600
## ONR 192050
## ISO 37001

Ausgabe 6.1: 2020-10-01

Medieninhaber und Hersteller
Austrian Standards plus GmbH Heinestraße 38, 1020 Wien

E-Mail: certification@austrian-standards.at
Internet: www.austrian-standards.at

# Inhaltsverzeichnis

# 1 Anwendungsbereich

Dieses Zertifizierungsschema legt die Vorgangsweise zur Zertifizierung eines Compliance Management Systems (CMS) durch die Zertifizierungsstelle von Austrian Standards (AS+C) fest.

Die Bewertung eines CMS erfolgt auf Basis der folgenden normativen Dokumente:

- ISO 19600:2014-12-15 Compliance management systems – Guidelines
- ONR 192050:2013-02-01 Compliance Management Systeme (CMS) – Anforderungen und Anleitung zur Anwendung
- ISO 37001:2016-10 Anti-Korruptions-Managementsysteme

Für die Durchführung eines Zertifizierungsverfahrens gelten die Anforderungen der Internationalen Norm ISO/IEC 17021-1[1].

Unsere Zertifizierungsstelle ist ISO/IEC 17021 akkreditiert für Managementsysteme zur Korruptionsbekämpfung (ISO 37001:2018).

Haftungsausschluss: Die Anwendung der obig genannten normativen Dokumente soll Organisationen dabei unterstützen, innerhalb einer Organisation ein wirksames Compliance Management System zu implementieren, welches die Wahrscheinlichkeit von Regelverstößen durch Organisationsmitglieder deutlich reduziert. Diese Anwendung, aber auch eine Zertifizierung nach dem vorliegenden Zertifizierungsschema stellt keine Garantie dafür dar, dass alle Mitglieder der zertifizierten Organisation stets rechtskonform handeln. Ein Compliance Management System und dessen Zertifizierung können vorsätzliches Fehlverhalten und kriminelle Handlungen von Mitgliedern einer Organisation nicht gänzlich verhindern. Eine Haftung der Austrian Standards plus GmbH und der Auditoren ist ausgeschlossen.

# 2 Kriterien für die Zertifizierung eines CMS

Für die Ausstellung eines Zertifikates gelten die Kriterien für ein Compliance Management Systems gemäß Anhang A und/oder Anhang B.

Antragsteller können ihr CMS entweder nach einer der internationalen Normen ISO 19600, ISO 37001 oder gemäß dem österreichischen Standard ONR 192050 oder einer beliebigen Kombination dieser Standards zertifizieren lassen.

# 3 Zertifizierungsprozess

## 3.1 Antragstellung

3.1.1 Der Antragsteller muss die Einleitung des Zertifizierungsverfahrens mittels eines von der Zertifizierungsstelle zur Verfügung gestellten Antragsformulars beantragen.

3.1.2 Der Antragsteller muss eine bevollmächtigte Kontaktperson für die Durchführung des Zertifizierungsverfahrens benennen.

3.1.3 Der Umfang eines beantragten Zertifizierungsverfahrens bestimmt sich durch folgende Parameter:

- Identifikation der juristischen Person, die Inhaber des Zertifikates ist,
- Geltungsbereich des angestrebten Zertifikates in Bezug auf die Organisation bzw. Untereinheiten der Organisation,

[1] ISO/IEC 17021-1:2015 Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren - Teil 1: Anforderungen

- Standorte der zu zertifizierenden Organisation,
- Compliance-Risikobereiche, die in den Geltungsbereich des Zertifikates aufgenommen werden sollen.

Zertifizierungsverfahren von mehreren, miteinander verbundenen juristischen Personen können gebündelt werden.

Zusammen mit dem Antrag muss der Antragsteller folgende Informationen über das zu zertifizierende Managementsystem dokumentieren. Diese Dokumentation muss das folgende umfassen:

a. den gewünschten Geltungsbereich der Zertifizierung;

b. die allgemeinen Merkmale der antragstellenden Organisation, einschließlich deren Name sowie die Anschrift(en) ihres/ihrer physischen Standort(e)s, bedeutsame Aspekte ihrer Prozesse und Tätigkeiten sowie alle maßgeblichen rechtlichen Verpflichtungen;

c. allgemeine Informationen bezüglich der antragstellenden Organisation, die für den beantragten Zertifizierungsbereich relevant sind, wie z. B. ihre Tätigkeiten, personelle und technische Ressourcen, Funktionen und Beziehungen in einer größeren Körperschaft, falls gegeben;

d. Informationen bezüglich aller ausgegliederten Prozesse, die von der Organisation genutzt werden und die Konformität mit den Anforderungen beeinflussen;

e. Informationen über das CMS betreffende Beratungsleistungen, die von der Organisation in Anspruch genommen wurden, und durch wen diese Leistungen durchgeführt wurden.

## 3.2 Prüfung des Antrags

3.2.1 Vor Durchführung des Audits prüft die Zertifizierungsstelle den Antrag um sicherzustellen, dass

- die Informationen über die antragstellende Organisation ausreichend für die Durchführung des Audits sind,
- alle bekannten Differenzen im Verständnis zwischen der Zertifizierungsstelle und der antragstellenden Organisation geklärt werden,
- der Geltungsbereich der angestrebten Zertifizierung, der/die Standort(e) der Tätigkeiten der antragstellenden Organisation, die zur Ausführung der Audits erforderliche Zeit sowie alle andere Aspekte, die die Zertifizierungstätigkeit beeinflussen, berücksichtigt werden.

3.2.2 Basierend auf dieser Prüfung wird die Zertifizierungsstelle die Kompetenzen ermitteln, die sie in ihrem Auditteam benötigt. Das Auditteam besteht zumindest aus einem Leitenden Auditor sowie aus Co-Auditoren nach Erfordernis.

3.2.3 Wird der Antrag von der Zertifizierungsstelle angenommen, erhält der Antragsteller eine diesbezügliche schriftliche Bestätigung.

## 3.3 Erstzertifizierung

### 3.3.1 Audit – Stufe 1

Das Audit der Stufe 1 wird durchgeführt um das eigentliche Zertifizierungsaudit (Audit der Stufe 2 gemäß Abschnitt 3.3.2) vorzubereiten. Das Audit der Stufe 1 muss vor Ort bei der zu zertifizierenden Organisation durchgeführt werden. Das Audit Stufe 1 kann in begründeten Ausnahmefällen als Fernaudit via Webkonferenztools durchgeführt werden.

Das Audit der Stufe 1 wird durchgeführt, um

a. die Dokumentation des Managementsystems der Organisation zu prüfen,

b. die Compliance Risikoanalyse und deren Scope zu überprüfen und daraus folgend die zu auditierenden Funktionen/Personengruppen für das Audit Stufe 2 zu identifizieren,

c. die spezifischen Bedingungen der Organisation zu beurteilen, sowie Gespräche mit Mitarbeitern zu führen, um die Reife des Systems für das Audit Stufe 2 zu ermitteln,

d. den Status der Organisation und dessen Verständnis bezüglich der Anforderungen der Normen zu bewerten,

e. notwendige Informationen bezüglich des Geltungsbereichs des CMS zu erfassen, der Prozesse und der Standorte der Organisation,

f. die Zuteilung der Ressourcen für das Audit der Stufe 2 zu bewerten sowie die Einzelheiten der Audits abzustimmen,

g. Schwerpunkte für die Planung des Audits der Stufe 2 festzulegen,

h. zu beurteilen, ob interne Audits und Managementbewertungen geplant und durchgeführt werden,

i. zu beurteilen, ob der Grad der Implementierung des Managementsystems belegt, dass die Organisation für das Audit der Stufe 2 reif ist.

Auditfeststellungen aus der Stufe 1 werden dokumentiert und dem Kunden mitgeteilt, einschließlich der Hinweise zu identifizierten Schwachstellen, die während des Audits der Stufe 2 als Nichtkonformität eingestuft werden könnten.

Der Leitende Auditor dokumentiert die Ergebnisse des Audits der Stufe 1 mittels der durch die Zertifizierungsstelle vorgegebenen Berichtsvorlage.

Die Zertifizierungsstelle entscheidet auf Basis des Berichts über die weitere Vorgehensweise. Der Abstand zwischen dem Audit der Stufe 1 und Audit der Stufe 2 (siehe 3.3.2) muss mindestens 2 Wochen und darf maximal 6 Monate betragen, wenn im Zuge des Audits der Stufe 1 Schwachstellen identifiziert werden, die im Zuge der Stufe 2 als Nichtkonformitäten eingestuft werden könnten. Werden die Schwachstellen innerhalb der Maximalfrist nicht in geeigneter Weise behoben, wird der Antrag abgewiesen.

### 3.3.2 Audit der Stufe 2

Der Zweck des Audits der Stufe 2 ist es, die Umsetzung einschließlich der Wirksamkeit des Managementsystems der Organisation zu bewerten und die Konformität des Managementsystems mit den Auditkriterien festzustellen.

Das Audit der Stufe 2 muss an dem/den Standort/en der zu zertifizierenden Organisation stattfinden.

Das Audit der Stufe muss zumindest das folgende umfassen:

a) Informationen und Nachweise über die Konformität mit allen Anforderungen des zutreffenden Bezugsdokumentes;

b) Überwachung der Leistung, Messung, Berichterstattung und Überprüfung in Bezug auf Ziele und Vorgaben im Rahmen des Geltungsbereichs des Compliance-Managementsystems;

c) die Fähigkeit und die Leistungsfähigkeit des Compliance-Managementsystems des Kunden im Hinblick auf die Erfüllung geltender gesetzlicher, behördlicher und vertraglicher Anforderungen;

d) Prüfung der operativen Lenkung der Prozesse des Kunden im Hinblick auf die Umsetzung der Vorgaben des Compliance-Managementsystems;

e) Prüfung des internen Audits und der Managementbewertung;

f) Verantwortlichkeit der Leitung für die Compliance-Politik des Kunden.

## 3.4 Durchführung von Audits

### 3.4.1 Allgemeines

Zur Durchführung eines Audits wird von der Zertifizierungsstelle das Auditteam bestellt. Die Zertifizierungsstelle informiert den Kunden über die Namen und relevante Informationen des Auditteams. Der Kunde hat die Möglichkeit, bis spätestens 3 Wochen vor dem Audit, der Bestellung von Auditteammitgliedern schriftlich zu widersprechen.

Zur Planung eines Audits in Kooperation mit dem Kunden wird der Auditplan dem Kunden sowie die Daten zum Audit mit dem Kunden abgestimmt.

Audits müssen eine Eröffnungsbesprechung zu Beginn des Audits und eine Abschlussbesprechung nach Beendigung des Audits umfassen.

Teile des Audits können mit elektronischen Mitteln erfolgen (Remote-Audits). Der Einsatz von Remote-Audits wird von der Zertifizierungsstelle im Rahmen der Festlegung des Auditprogrammes festgelegt. Der während eines solchen Remote-Audits erlangte Nachweis muss ausreichend sein, um den Auditor in die Lage zu versetzen, in Kenntnis der Sachlage eine begründete Entscheidung über die Konformität mit der jeweiligen Anforderung zu treffen.

Audits sind durch eine Begleitperson der Organisation zu begleiten, sofern nichts anderes mit der Organisation vereinbart wird. Die Auditoren haben das Recht, die Begleitperson von einzelnen Teilen (Interviews) auszuschließen, um etwaige Beeinflussungen zu verhindern.

### 3.4.2 Stichprobenprüfung an mehreren Standorten - Multi-site Audits

Für den Fall, dass eine Organisation mehr als einen Standort betreibt, die unter dem Geltungsbereich des Compliance Managementsystem abgedeckt werden, kann eine Stichprobe aus den bestehenden Standorten für die Audits herangezogen werden.

Die Zertifizierungsstelle legt die Anzahl und die Örtlichkeiten der zu auditierenden Standorte fest. Es müssen alle Funktionen der Organisation gemäß Abschnitt 3.4.3 durch das Audit abgedeckt werden können.

Standorte die von Unterauftragnehmern im Namen und Auftrag der Organisation betrieben werden, sind als eigene Standorte der Organisation zu betrachten. Diese Standorte sind in der Planung der Audits zu berücksichtigen.

### 3.4.3 Grundlegende Aufgaben des Auditteams

Die Aufgaben des Auditteams im Rahmen der Durchführung eines Audits umfassen zumindest das Folgende:

a) Struktur, grundsätzliche Regelungen, Prozesse, Verfahren, Aufzeichnungen und zugehörige Dokumente der Organisation bezüglich der zutreffenden Bezugsdokumente zu prüfen und zu verifizieren;

b) festzustellen, dass diese alle relevanten Anforderungen bezüglich des beabsichtigten Geltungsbereichs der Zertifizierung erfüllen;

c) festzustellen, dass die Prozesse und Verfahren wirksam eingeführt, umgesetzt und aufrechterhalten werden, um Grundlage für das Vertrauen in das Compliance-Managementsystem des Kunden zu schaffen;

d) dem Kunden in Bezug auf seine eigenen Maßnahmen etwaige Widersprüche zwischen seiner Politik, seinen Zielen und Vorgaben aufzuzeigen.

### 3.4.4 Zu auditierende Funktionen

Folgende Organisationseinheiten und Funktionen sind –sofern zutreffend– im Rahmen von Audits zumindest zu berücksichtigen und einzubinden:

A Funktionen, die im Rahmen der Etablierung und/oder Aufrechterhaltung des CMS Verantwortung tragen bzw. diesbezüglich relevant sind:

- Oberste Organe, z.B. Geschäftsleitung und Aufsichtsorgane
- Compliance Funktionen, regionale oder divisionale Compliance-Beauftragte
- Personalverantwortliche einschließlich Ausbildungsverantwortliche
- Interne Revision, Verantwortliche für interne Kontrollsysteme

B Alle Funktionen der Organisation die -gemäß dem Scope des CMS- einem relevanten Compliance-Risiko ausgesetzt sind, wie z.B.:

- Leiter und Mitarbeiter von Vertrieb, Einkauf, Produktion, Vertreter bei Behördenverfahren etc.
- alle im Rahmen des Audits Stufe 1 identifizierten Funktionen bzw. Personengruppen

Grundsätzlich gilt, dass sowohl Führungskräfte als auch betroffene Mitarbeiter in das Audit einzubeziehen sind.

### 3.4.5 Unterlagenprüfung

Folgende Unterlagen, Dokumente und Aufzeichnungen sind im Rahmen des Audits der Stufe 2 zumindest vom Auditteam zu prüfen und zu verifizieren:

- Compliance Handbuch und Handlungsanweisungen, Prozessbeschreibungen im Zusammenhang mit Compliance
- Leitbild, Code of Conduct
- schriftliche Dokumentation der Durchführung einer Compliance-Risiko-Bewertung und deren Ergebnisse
- Schulungsunterlagen
- Protokolle der Organisationsleitung bzw. des Aufsichtsorgans der Organisation, in welchen Compliance behandelt wird
- Berichte, welche Compliance zum Gegenstand haben, z.B. des Compliance Officers an die Organisationsleitung
- Compliance-Kommunikation an die Organisationsmitglieder
- Überprüfungsberichte, z.B. Auditreports
- Berichte über allfällige Compliance-Verstöße und Darstellung der daraus erfolgten Maßnahmen (sofern zutreffend).

### 3.4.6 Kommunikation während des Audits

Im Verlauf des Audits wird das Auditteam in regelmäßigen zeitlichen Abständen den Fortschritt des Audits bewerten und Informationen austauschen. Der Auditteamleiter wird bei Bedarf die Aufgaben unter den Mitgliedern des Auditteams neu zu ordnen und den Kunden in regelmäßigen zeitlichen Abständen über den Fortschritt des Audits und alle Bedenken unterrichten.

Falls die verfügbaren Auditnachweise anzeigen, dass die Auditziele nicht erreicht werden können oder ein unmittelbares und erhebliches Risiko bestehen kann, wird der Auditteamleiter dem Kunden und, falls möglich, der Zertifizierungsstelle darüber Bericht erstatten, um die entsprechenden Maßnahmen zu ermitteln. Zu diesen Maßnahmen können die erneute Bestätigung oder die Veränderung des Auditplans, Änderungen an den Auditzielen oder am Auditumfang oder auch der Abbruch des Audits gehören. Der Auditteamleiter wird der Zertifizierungsstelle über die Ergebnisse der ergriffenen Maßnahmen Bericht erstatten.

Der Auditteamleiter wird gemeinsam mit dem Kunden jeglichen Änderungsbedarf am Audit-umfang, der sich im Verlauf der Audittätigkeiten vor Ort herausstellt, überprüfen und der Zertifizierungsstelle darüber Bericht erstatten.

### 3.4.7 Auditschlussfolgerungen

Sollten im Rahmen eines Audits Nichtkonformitäten festgestellt werden, werden vom Auditteam entsprechende Auflagen zur Beseitigung der Abweichungen erteilt. Nichtkonformitäten werden wie folgt klassifiziert:

Untergeordnete Nichtkonformität: Nichtkonformität, die die Fähigkeit des Managementsystems, die beabsichtigten Ergebnisse zu erreichen, nicht beeinträchtigt.

Wesentliche Nichtkonformität: Nichtkonformität, die die Fähigkeit des Managementsystems, die beabsichtigten Ergebnisse zu erreichen, beeinträchtigt.

Anmerkung: In folgenden Fällen könnten Nichtkonformitäten als wesentlich eingestuft werden:

- wenn erheblicher Zweifel daran besteht, dass eine wirksame Prozesslenkung besteht oder dass Compliance Maßnahmen nicht umgesetzt werden;
- mehrere untergeordnete Nichtkonformitäten, die sich auf dieselbe Anforderung oder dasselbe Problem beziehen, könnten einen systembezogenen Fehler darstellen und somit eine wesentliche Nichtkonformität ergeben.

### 3.4.8 Korrekturmaßnahmen

Für alle untergeordneten Nichtkonformitäten muss die Organisation

1. eine Ursachenanalyse durchführen sowie
2. einen Plan zur Implementierung von Korrekturmaßnahmen erstellen.

Die effektive Implementierung der Korrekturmaßnahmen zu untergeordneten Nichtkonformitäten wird im Rahmen des nachfolgenden regulären Überwachungs- oder Rezertifizierungsaudit verifiziert.

Für alle wesentlichen Nichtkonformitäten muss die Organisation

1. eine Ursachenanalyse durchführen sowie
2. entsprechende Korrekturmaßnahmen implementieren.

Die effektive Implementierung der Korrekturmaßnahmen zu wesentlichen Nichtkonformitäten wird entweder

- durch eine Überprüfung von der Organisation bereitgestellter Unterlagen und Dokumentation oder
- im Rahmen eines teilweisen oder vollständigen Nachaudits verifiziert.

Sollte es nicht möglich sein, die Implementierung von Korrekturmaßnahmen zu einer oder mehrerer wesentlicher Nichtkonformitäten innerhalb von 6 Monaten nach dem letzten Tag des Audits Stufe 2 zu verifizieren, muss in jedem Fall ein erneutes Audit der Stufe 2 durchgeführt werden.

### 3.4.9 Empfehlungen zur Wirksamkeit des Managementsystems

Über die Feststellung der Konformität hinaus können die Auditoren auch Empfehlungen in Bezug auf die Wirksamkeit und Verbesserungsmöglichkeiten in Bezug auf das Managementsystem abgeben. Diese werden im Auditbericht dokumentiert haben aber keinen Einfluss auf die Ausstellung des Zertifikates gemäß Abschnitt 3.6.

### 3.4.10 Abschlussbesprechung

Am Ende des Audits wird eine Abschlussbesprechung gemeinsam mit dem zuständigen Management des Kunden und gegebenenfalls mit den Personen, die die Verantwortung für die zu auditierenden Funktionen oder Prozesse tragen, durchgeführt werden. Die Anwesenheit bei dieser Abschlussbesprechung wird aufgezeichnet.

Der Zweck der Abschlussbesprechung besteht darin, die aus dem Audit gezogenen Schlussfolgerungen einschließlich der Empfehlung hinsichtlich der Zertifizierung vorzustellen. Alle Nichtkonformitäten werden vom Auditteam erläutert sodass sie verstanden werden. Weiters wird folgendes erläutert bzw. vereinbart:

- weitere Vorgehensweise der Zertifizierungsstelle inkl. Behandlung von Nichtkonformitäten einschließlich aller Konsequenzen, die den Status der Zertifizierung des Kunden betreffen;
- Zeitrahmen, innerhalb dessen der Kunde einen Plan für Korrekturen und Korrekturmaßnahmen in Bezug auf die im Verlauf des Audits ermittelten Nichtkonformitäten vorlegen muss;
- Informationen zu den Prozessen für die Behandlung von Beschwerden und Einsprüchen.

Der Kunde erhält die Möglichkeit, Fragen zu stellen. Alle Meinungsverschiedenheiten zwischen dem Auditteam und dem Kunden in Bezug auf die Auditfeststellungen oder die aus dem Audit gezogenen Schlüsse werden erörtert und wenn möglich ausgeräumt. Alle nicht gelösten Meinungsverschiedenheiten werden dokumentiert und an die Zertifizierungsstelle weitergeleitet.

## 3.5 Auditbericht zur Erstzertifizierung

Das Auditteam analysiert und bewertet alle während der Audits der Stufe 1 und der Stufe 2 erfassten Informationen und Auditnachweise, trifft Auditfeststellungen und Auditschlussfolgerungen.

Die Informationen, die das Auditteam der Zertifizierungsstelle für die Zertifizierungsentscheidung bereitstellt, müssen mindestens enthalten:

a. die Auditberichte einschließlich Aufstellung der untergeordneten und wesentlichen Nichtkonformitäten und, wo zutreffend, zu Korrekturen und Korrekturmaßnahmen, die von der Organisation ergriffen wurden;

b. Dokumentation der Empfehlungen;

c. eine Empfehlung, ob die Zertifizierung gewährt werden soll oder nicht, sowie –wenn zutreffend- die Bedingungen hierfür.

## 3.6 Entscheidung über die Zertifizierung

### 3.6.1 Bewertungsprozess

Vor der Entscheidung über die Zertifizierung, wird durch die Zertifizierungsstelle eine Bewertung wie folgt durchgeführt:

a) Prüfung der durch das Auditteam bereitgestellten Informationen im Hinblick auf die Zertifizierungsanforderungen und den Geltungsbereich;

b) Bewertung, Verifizierung und Freigabe der Korrekturmaßnahmen für alle wesentlichen Nichtkonformitäten;

c) Bewertung und Freigabe des Plans der Organisation in Bezug auf Korrekturmaßnahmen für alle untergeordneten Nichtkonformitäten.

### 3.6.2 Ausstellung des Zertifikates

Basierend auf den Ergebnissen der Bewertung gemäß Abschnitt 4.5.2 entscheidet die Zertifizierungsstelle über die Ausstellung des Zertifikates. Der Geltungsbereich eines Zertifikates wird durch die folgenden Angaben bestimmt:

- Identifikation der juristischen Person (einschließlich der Adresse), die Inhaber des Zertifikates ist,
- Geltungsbereich in Bezug auf die Organisation bzw. fallweise Untereinheiten der Organisation in Abhängigkeit von den Ergebnissen des/der Audits,
- Angabe der geographischen Orte der Organisationseinheit(en),
- Compliancerisiken innerhalb des Geltungsbereiches.

Das Zertifikat hat eine Gültigkeit von 3 Jahren vorausgesetzt, dass die Bedingungen zur Aufrechterhaltung des Zertifikates gegeben sind.

## 3.7 Überwachungsaktivitäten

### 3.7.1 Überwachungsaudits

Zur Aufrechterhaltung des Zertifikates sind Überwachungsaudits und andere Überwachungsaktivitäten im Abstand von 1 Jahr durchzuführen.

Änderungen bzgl. der zertifizierten Organisation (Struktur, Rechtspersonen, Standorte u.dgl.) sind im Rahmen von Überwachungsaktivitäten zu berücksichtigen und sind entsprechend zu planen. In Abhängigkeit der Art und

des Umfanges der Änderungen wird die Zertifizierungsstelle die erforderlichen Überwachungsmaßnahmen festlegen.

Überwachungsaudits sind Vor-Ort-Audits, stellen aber nicht notwendigerweise vollständige Systemaudits dar, sodass die Zertifizierungsstelle das Vertrauen aufrechterhalten kann, dass das zertifizierte Managementsystem zwischen den Re-Zertifizierungsaudits weiterhin die Anforderungen erfüllt. Das Überwachungsauditprogramm muss mindestens umfassen:

a. interne Audits und Managementbewertung;
b. eine Bewertung der ergriffenen Maßnahmen zu Nichtkonformitäten, die im Rahmen des vorhergehenden Audits festgestellt wurden;
c. Umgang mit Compliancevorfällen und/oder diesbezüglichen Hinweisen
d. Wirksamkeit des Managementsystems im Hinblick auf das Erreichen der Ziele der zertifizierten Organisation;
e. Fortschritt bei geplanten Tätigkeiten, die auf eine ständige Verbesserung zielen;
f. Bewertung von Änderungen und
g. Nutzung von Zeichen und/oder andere Verweise auf die Zertifizierung.

Über die Durchführung des Überwachungsaudits wird vom Leitenden Auditor ein Bericht erstellt.

### 3.7.2 Bewertung durch die Zertifizierungsstelle

Dieser Bericht bildet die Basis für die Entscheidung der Zertifizierungsstelle, das Zertifikat aufrechtzuerhalten. In Abhängigkeit der Ergebnisse der Überwachung kann der Geltungsbereich eines Zertifikates erweitert oder eingeschränkt werden.

## 3.8 Rezertifizierung

### 3.8.1 Rezertifizierungsprozess

Zur Verlängerung des Zertifikates werden die folgenden Aktivitäten durchzuführen:

1. Prüfung der Überwachungsberichte des vorangegangenen Zertifizierungszyklus und einer Bewertung der Leistung des Managementsystems,
2. die Durchführung eines Rezertifizierungsaudits gemäß 3.8.2.

Für den Fall signifikanter Änderungen der Organisation, des Managementsystems oder des Umfeldes der Organisation, kann die Zertifizierungsstelle auch die Durchführung eines weiteren Audits der Stufe 1 gemäß 3.3.1 anordnen.

### 3.8.2 Rezertifizierungsaudit

Das Rezertifizierungsaudit muss ein Vor-Ort-Audit beinhalten, welches Folgendes behandelt:

a. die Wirksamkeit des Managementsystems in seiner Gesamtheit angesichts interner oder externer Änderungen und seine fortgesetzte Bedeutung und Anwendbarkeit im Geltungsbereich der Zertifizierung;
b. die dargelegte Verpflichtung zur Aufrechterhaltung der Wirksamkeit und Verbesserung des Managementsystems, um die gesamte Leistungsfähigkeit zu steigern;
c. ob das Betreiben des zertifizierten Managementsystems zum Erreichen von Politik und Zielstellungen der Organisation beiträgt.

Für jede festgestellte wesentliche Nichtkonformität, wird die Zertifizierungsstelle Fristen für umzusetzende Korrekturen und Korrekturmaßnahmen noch vor Ablauf der Zertifizierung festlegen. Solche Korrekturmaßnahmen müssen noch vor dem Ablauf des Zertifikates von der Organisation implementiert und von der Zertifizierungsstelle verifiziert werden.

### 3.8.3 Auditbericht zum Rezertifizierungsaudit

Die Zertifizierungsstelle trifft die Entscheidungen über die Erneuerung der Zertifizierung auf der Grundlage der Ergebnisse des Rezertifizierungsaudits sowie der Ergebnisse aus der Bewertung des Systems über den Zeitraum der Zertifizierung.

### 3.8.4 Zertifikatsausstellung

In Abhängigkeit der Ergebnisse der Rezertifizierung kann der Geltungsbereich eines Zertifikates erweitert oder eingeschränkt werden.

Wenn alle Rezertifizierungsaktivitäten vor Ablauf der bestehenden Zertifizierung erfolgreich abgeschlossen werden, dann kann das Ablaufdatum der neuen Zertifizierung auf dem Ablaufdatum der bestehenden Zertifizierung beruhen. Das Ausgabedatum des neuen Zertifikats entspricht dem Tag der Rezertifizierungsentscheidung.

Für den Fall, dass vor Ablauf des Zertifizierungsdatums das Rezertifizierungsaudit nicht abgeschlossen wurde oder es nicht möglich ist, die Umsetzung von Korrekturmaßnahmen für eine wesentliche Nichtkonformität zu verifizieren, dann wird keine Empfehlung für die Rezertifizierung ausgesprochen und die Gültigkeit der Zertifizierung nicht verlängert.

Unter der Voraussetzung, dass die ausstehenden Rezertifizierungstätigkeiten abgeschlossen worden sind, kann innerhalb von 6 Monaten nach Ablauf der Zertifizierung, das Zertifikat wieder ausgestellt werden; andernfalls ist mindestens ein Audit der Stufe 2 (gemäß 3.3.2) durchzuführen. Das Gültigkeitsdatum des Zertifikats muss dem Tag der Re-Zertifizierungsentscheidung oder einem späteren entsprechen und das Ablaufdatum muss auf dem vorangegangenen Zertifizierungszyklus basieren.

## 3.9 Außerordentliche Audits

Auf Basis der Ergebnisse eines Erst- oder Rezertifizierungsaudits, eines Überwachungsaudits und/oder auf Basis einer sonstigen Information der Zertifizierungsstelle, kann es erforderlich sein kurzfristig, anlassbezogen ein Audit zur Überprüfung der Normkonformität des Managementsystems durchzuführen. Solche außerordentlichen Audits sind wie unter den folgenden Voraussetzungen durchzuführen.

- es gibt eine Vereinbarung mit dem Kunden den zu vereinbaren;
- der Geltungsbereich und Zweck des Audits ist klar definiert und dem Kunden kommuniziert;
- das Auditteam ist bestimmt und dem Kunden kommuniziert.

Darüber hinaus gelten für die Durchführung dieser Audits und die Festlegung von Ergebnissen analog die Bestimmungen gemäß 3.4, sofern anwendbar.

## 3.10 Änderungen der Zertifizierungsgrundlagen

Änderungen in den der Zertifizierung zu Grunde liegenden normativen Dokumenten werden von der Zertifizierungsstelle den Zertifikatsinhabern umgehend mitgeteilt.

Dem Zertifikatsinhaber wird bei veränderten Anforderungen an das CMS eine Frist von 12 Monaten zur Anpassung an die geänderten Anforderungen eingeräumt. Der Nachweis der Erfüllung der Anforderungen ist im Rahmen eines Überwachungsaudits, zu erbringen. Nach Erbringung des Nachweises wird das Zertifikat mit einer neuen Referenz auf die geänderten normativen Dokumente bzw. dieses Zertifizierungsschema ausgestellt.

## 3.11 Änderungen im Geltungsbereich von Zertifikaten

Sollte der Zertifikatsinhaber die Erweiterung des Geltungsbereichs in Bezug auf weitere Organisationseinheiten bzw. Compliance relevante Risiken wünschen, muss er dies bei der Zertifizierungsstelle schriftlich beantragen. Die Zertifizierungsstelle wird nach Prüfung der Sachlage die für die Erweiterung des Geltungsbereiches des Zertifikates erforderlichen Prüfungen von Unterlagen und/oder Audits festlegen.

Sollte der Zertifikatsinhaber die Einschränkung des Geltungsbereichs in Bezug auf die zertifizierten Organisationseinheiten bzw. Compliance relevante Risiken wünschen, muss er dies der Zertifizierungsstelle schriftlich mitteilen. Die Zertifizierungsstelle reduziert den Anwendungsbereich des Zertifikates entsprechend. Ab diesem

Zeitpunkt darf die Organisation keinerlei Aussagen in Bezug auf die Zertifizierung Ihres CMS diesbezüglich mehr tätigen. Die Verifizierung der diesbezüglichen Verpflichtungen des Zertifikatsinhabers findet in jedem Fall im Rahmen der folgenden Überwachungsaudits statt.

Änderungen der Zertifikate in Bezug auf formale Angaben des Zertifikatsinhabers (wie z.B. Änderungen im Firmennamen oder der Adresse) sind der Zertifizierungsstelle schriftlich mitzuteilen. Die Zertifizierungsstelle stellt ohne fachliche Prüfung ein geändertes Zertifikat aus.

Jegliche Änderungen in der juristischen Person des Zertifikatsinhabers, bedingen einen neuen Antrag auf Zertifizierung und die Durchführung eines neuen Zertifizierungsverfahrens.

## 3.12 Zurückziehung von Zertifikaten

Es gelten die Allgemeinen Geschäftsbedingungen der Zertifizierungsstelle in der jeweils gültigen Fassung.

## 3.13 Vorgehensweise bei der Übernahme von Zertifikaten

Im Fall eines Wechsels eines Kunden von einer anderen Zertifizierungsstelle zu AS+C ist grundsätzlich im Sinne einer Erstzertifizierung gemäß Abschnitt 3.3 vorzugehen.

AS+C prüft -sofern durch den Kunden bereitgestellt- Auditberichte vorangegangener Audits. Auf Basis des Ergebnisses der Prüfung dieser Auditberichte kann AS+C gegebenenfalls entscheiden, auf die Durchführung eines Audits der Stufe 1 (gemäß Abschnitt 3.3.1) zu verzichten.

# Anhang A Kriterien nach ISO 19600 und ISO 37001

## ISO 19600 Abschnitt 4 Kontext der Organisation

### ISO 19600 Abschnitt 4.1 Verstehen der Organisation und ihres Kontextes

A.4.1 Die Organisation hat die für ihre strategische Ausrichtung relevanten externen und internen Angelegenheiten und Problemstellungen bestimmt, sofern diese Auswirkung auf die beabsichtigte Leistungsfähigkeit ihres Compliance-Managementsystems haben.

### ISO 19600 Abschnitt 4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

A.4.2 Die Organisation hat:

- die für ihr CMS relevanten interessierten Parteien, und
- die Anforderungen dieser interessierten Parteien,

bestimmt.

### ISO 19600 Abschnitt 4.3 Bestimmung des Geltungsbereiches des Compliance Management Systems

A.4.3 Die Organisation hat die Grenzen und die Anwendbarkeit ihres CMS bestimmt und dessen Geltungsbereich festgelegt.

> ANMERKUNG: Der Geltungsbereich des Compliance-Management-System wird bestimmt durch die geographischen und/oder die organisatorische Abgrenzungen sowie durch die Compliance-Risiken, in Bezug auf die das Compliance-Management-System zur Anwendung kommt.

A.4.4 Der Geltungsbereich ist als dokumentierte Information verfügbar.

### ISO 19600 Abschnitt 4.4 Prinzipien der guten Unternehmensführung (Good governance)

A.4.5 Die Organisation hat ein CMS eingeführt, welches den folgenden Prinzipien genügt:

1. direkter Zugang der Compliance-Funktion zum Aufsichtsorgan;
2. Unabhängigkeit der Compliance-Funktion;
3. entsprechende Befugnisse und ausreichende Ressourcen für die Compliance-Funktion.

### ISO 19600 Abschnitt 4.5 Compliance-Verpflichtungen

A.4.6 Die Organisation identifiziert systematisch ihre Compliance-Verpflichtungen und deren Auswirkungen auf ihre Aktivitäten.

A.4.7 Die Organisation dokumentiert ihre Compliance-Verpflichtungen.

A.4.8 Es existieren Verfahren, um neue und geänderte Gesetze, Vorschriften, Bestimmungen und andere Compliance-Verpflichtungen zu identifizieren.

A.4.9 Es existieren Verfahren, um die Auswirkungen der festgestellten Änderungen zu bewerten und um erforderliche Änderungen im Management der Compliance-Verpflichtungen zu implementieren.

### ISO 19600 Abschnitt 4.6 Identifikation, Analyse und Bewertung von Compliance-Risiken

A.4.10 Die Organisation identifiziert und bewertet ihre Compliance-Risiken, indem sie ihre Compliance-Verpflichtungen mit ihren Aktivitäten, Produkten, Dienstleistungen und relevanten Aspekten ihres Betriebs in Beziehung setzt.

A.4.11 Die Organisation analysiert Compliance-Risiken in Bezug auf Ursachen von Compliance-Verstößen, der Schwere der Folgen sowie der Wahrscheinlichkeit des Auftretens und der Konsequenzen eines Compliance-Verstoßes.

A.4.12 Compliance-Risiken werden in regelmäßigen Abständen überprüft und neubewertet sowie im Falle von:

- neuen oder geänderte Aktivitäten, Produkten oder Dienstleistungen;

- Änderungen an der Struktur oder Strategie der Organisation;
- signifikanten Veränderungen im Umfeld der Organisation;
- Änderungen der Compliance-Verpflichtungen; und
- bei Verstößen gegen der Compliance-Verpflichtungen.

## ISO 19600 Abschnitt 5 Führung

### ISO 19600 Abschnitt 5.1 Führung und Verpflichtung

A.5.1 Das Aufsichtsorgan und das Top-Management zeigen Führung und Engagement in Bezug auf das Compliance Management System durch:

1. die Schaffung und Wahrung der Grundwerte der Organisation;
2. die Kommunikation der Bedeutung eines Compliance Management System und dessen Einhaltung.

### ISO 19600 Abschnitt 5.2 Compliance-Politik

A.5.2 Das Aufsichtsorgan und das Top-Management haben eine Compliance-Politik festlegt.

A.5.3 Die Compliance-Politik bringt folgendes zum Ausdruck:

- den Umfang des Compliance Management Systems;
- die Anwendung und Kontext des Systems;
- die Verantwortung für die Administration und die Meldung von Compliance-Problemen;
- das erforderliche Niveau der Durchführung und die Rechenschaftspflicht; und
- die Folgen von Compliance-Verstößen.

A.5.4 Die Compliance-Politik

- ist dokumentiert und verfügbar;
- wird innerhalb der Organisation klar kommuniziert und ist für alle Mitarbeiter leicht zugänglich;
- wird -wenn erforderlich- aktualisiert.

### ISO 19600 Abschnitt 5.3 Rollen, Verantwortlichkeiten und Zuständigkeiten in der Organisation

#### Aufsichtsorgan und Top-Management

A.5.5 Das Aufsichtsorgan und das Top-Management stellen sicher, dass die Verpflichtung zu Compliance aufrechterhalten wird und dass Compliance-Verstöße und nicht regelkonformes Verhalten entsprechend verfolgt werden.

A.5.6 Die Verantwortung für Compliance bildet Teil der Stellenbeschreibungen für das Top-Management.

A.5.7 Eine Compliance-Funktion wurde benannt.

#### Top-Management

A.5.8 Angemessene und geeignete Ressourcen sind für das Compliance Management System bereitgestellt.

A.5.9 Verantwortlichkeiten und Befugnisse für die relevanten Funktionen wurden benannt und innerhalb der Organisation kommuniziert.

A.5.10 Das Top-Management wird nach Compliance bezogenen Leistungskriterien bzw. Ergebnissen gemessen.

#### Compliance-Funktion

A.5.11 Die Compliance-Funktion hat die Befugnis und die Verantwortung für das Compliance-Management-System.

A.5.12 Die Compliance-Funktion hat die Befugnis, unabhängig zu handeln.

A.5.13 Die Compliance-Funktion unterliegt keinen Interessenkonflikten und verfügt über folgendes:

1. die Fähigkeit zur effektiven Kommunikation und Einflussnahme;
2. die erforderliche Kompetenz.

A.5.14 Die Compliance-Funktion hat Unterstützung durch und direkten Zugang zum Aufsichtsorgan und dem Top-Management.

A.5.15 Die Compliance-Funktion hat Zugang zu:

1. Führungskräften und die Möglichkeit, frühzeitig in Entscheidungsprozesse eingebunden zu sein;
2. allen Ebenen der Organisation;
3. allen erforderlichen Informationen und Daten, um ihre Compliance-Aufgaben wahrzunehmen; und
4. kompetenter Beratung/Expertise in Bezug auf relevante Gesetze, Regelungen, Bestimmungen und Standards der Organisation.

A.5.16 Die Compliance-Funktion ist zuständig für die Festlegung von Compliance relevanten Leistungsindikatoren sowie die Überprüfung der Einhaltung und Überwachung der Leistungsindikatoren.

### Verantwortung der Führungskräfte

A.5.17 Führungskräfte sind innerhalb ihres Verantwortungsbereiches verantwortlich für Compliance.

### Verantwortung der Mitarbeiter

A.5.18 Die Mitarbeiter erfüllen ihre Verpflichtungen innerhalb des CMS.

### ISO 37001 Abschnitt 5.3.3 Delegierung von Entscheidungen

AB.5.1 Für den Fall, dass das Topmanagement Entscheidungsbefugnisse an Mitarbeiter delegiert, muss die Organisation, in allen Fällen eines höheren Korruptionsrisikos, sicherstellen, dass entweder

- ein Entscheidungsprozess etabliert und aufrechterhalten wird

oder

- Steuerungsmaßnahmen implementiert sind, die sicherstellen, dass Entscheidungsabläufe sowie die Befugnis der Personen, die Entscheidungen treffen, adäquat und frei von Interessenskonflikten sind.

AB.5.2 Das Top Management stellt sicher, dass diese Prozesse regelmäßig überprüft werden.

## ISO 19600 Abschnitt 6 Planung

### ISO 19600 Abschnitt 6.1 Maßnahmen in Bezug auf Compliance-Risiken

A.6.1 Die Organisation plant ihr CMS:

1. um sicherzustellen, dass die intendierten Zielsetzungen des CMS erreicht werden;
2. zur Verhinderung, Entdeckung und Verminderung von ungeplanten Effekten;
3. um eine kontinuierliche Verbesserung zu erreichen.

A.6.2 Die Organisation plant:

1) Maßnahmen, um auf Compliance-Risiken zu reagieren und
2) wie sie:
   — die Maßnahmen in die Prozesse des CMS integriert und implementiert;
   — die Effektivität der Maßnahmen evaluiert.

### ISO 19600 Abschnitt 6.2 Compliance-Ziele

A.6.3 Die Organisation hat Compliance-Ziele für relevante Funktionen und Ebenen festgelegt.

A.6.4 Die Compliance-Ziele:

1) sind konsistent mit der Compliance-Politik;
2) sind messbar (sofern praktikabel);
3) berücksichtigen zutreffende Anforderungen;
4) werden überwacht;
5) werden kommuniziert;
6) werden auf Stand gehalten und, wenn erforderlich, überarbeitet.

## ISO 19600 Abschnitt 7 Unterstützende Prozesse

### ISO 19600 Abschnitt 7.2 Kompetenz und Training

A.7.1 Die Organisation hat

1. die erforderlichen Kompetenzen für jene Personen bestimmt, die Tätigkeiten unter der Kontrolle der Organisation verrichten, und welche die Leistung der Organisation in Bezug auf Compliance beeinflussen;
2. sichergestellt, dass diese Personen auf Grundlage angemessener Ausbildung, Schulung oder Erfahrung kompetent sind.

A.7.2 Die Organisation bewahrt angemessene dokumentierte Informationen als Nachweis der Kompetenz auf.

A.7.3 Die Aus-und Weiterbildung der Mitarbeiter:

1. ist auf die Compliance-Verpflichtungen und Compliance-Risiken der jeweiligen Funktionen und Verantwortlichkeiten der Mitarbeiter ausgerichtet;
2. wird zu Beginn der Tätigkeit eines Mitarbeiters sowie fortlaufend durchgeführt;
3. wird in Bezug auf deren Wirksamkeit bewertet;
4. wird bei Bedarf aktualisiert; und
5. ist dokumentiert.

A.7.4 Weiterführende Compliance-Schulungsmaßnahmen werden in Betracht gezogen im Fall:

1. einer Änderung der Position oder Verantwortlichkeiten;
2. von Änderungen in der internen Prozesse, Richtlinien und Verfahren;
3. von Veränderungen in der Organisationsstruktur;
4. von Änderungen der Compliance-Verpflichtungen;
5. von Veränderungen bei den Tätigkeiten der Organisation, Produkten oder Dienstleistungen; und
6. von Problemstellungen, die sich aus der Überwachung, Prüfung, Bewertungen, Beschwerden und Compliance-Verstößen ergeben.

### ISO 37001 Abschnitt 7.2.2 Einstellungsprozess

AB.7.1 Die Organisation hat für alle ihre Mitarbeiter Verfahren wie folgt implementiert:

a) die Bedingungen der Anstellung verlangen vom Personal die Einhaltung der Anti-Korruptionspolitik sowie der Festlegungen des Managementsystems und geben der Organisation das Recht, Verstöße disziplinär zu verfolgen;

b) innerhalb eines vernünftigen Zeitrahmens nach der Einstellung erhalten die Mitarbeiter eine Kopie der Anti-Korruptionspolitik, bzw. erhalten Zugriff darauf, und erhalten ein diesbezügliches Training;

c) die Organisation hat Verfahren eingerichtet, die eine angemessene disziplinarische Verfolgung von Personen, die gegen die Anti-Korruptionspolitik oder die Festlegungen des Managementsystems verstoßen, ermöglichen.

d) Mitarbeiter erleiden keine Verfolgung, Diskriminierung oder disziplinarische Maßnahmen für den Fall:

1) der Verweigerung der Teilnahme in, oder die Zurückweisung jeglicher Aktivität in Fällen, die -in der Beurteilung des Mitarbeiters- ein erhöhtes Korruptionsrisiko darstellen und wo die Organisation keine Maßnahmen zur Verringerung des Risikos gesetzt hat oder

2) dass der Mitarbeiter einen Verdacht geäußert hat oder im guten Glauben über einen Fall berichtet hat oder, dass der Mitarbeiter selbst in Verdacht geraten ist, an einem versuchten, tatsächlichen und vermuteten Korruptionsfall beteiligt gewesen zu sein (mit der Ausnahme, dass der Mitarbeiter tatsächlich in einen Fall beteiligt ist).

AB.7.2 In Bezug auf alle Positionen (einschließlich der Anti-Korruptions-Compliance Funktion), die gemäß der Korruptions-Risikoanalyse, einem erhöhten Korruptionsrisiko ausgesetzt sind, hat die Organisation Verfahren implementiert die sicherstellen, dass:

a) eine sorgfältige Überprüfung von Personen vor ihrer Anstellung stattfindet sowie vor jeder Versetzung oder Beförderung. Das Verfahren stellt sicher, dass davon ausgegangen werden darf, dass die betreffende Person den Anforderungen der Anti-Korruptionspolitik und des Managementsystems entspricht.

b) Leistungsprämien, Leistungsziele und andere Anreizsysteme für die Vergütung regelmäßig überprüft werden, um zu verifizieren, dass ausreichende Sicherungsmaßnahmen getroffen wurden, die verhindern, dass diese Anreize Korruption befördern;

c) solche Mitarbeiter, das Top Management sowie Mitglieder des Aufsichtsorgans in regelmäßigen Abständen eine Erklärung über die Einhaltung der Anti-Korruptionspolitik abgeben.

### ISO 19600 Abschnitt 7.3 Bewusstseinsbildung

A.7.5 Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten, sind sich

1. der Compliance-Politik;
2. ihrer Rolle und ihres Beitrags zur Wirksamkeit des Compliance-Managementsystems;
3. der Folgen einer Nichterfüllung der Anforderungen des Compliance-Managementsystems

bewusst.

A.7.6 Das Top-Management nimmt seine Verantwortung für:

1. die Förderung der Akzeptanz der Mitarbeiter in Bezug auf die Bedeutung der Erreichung der Compliance-Ziele;
2. die Förderung von Vorschlägen durch die Mitarbeiter zur kontinuierlichen Verbesserung der Compliance-Leistung;
3. die Sicherstellung, dass die operativen Ziele und Vorgaben Compliance-konformes Verhalten nicht gefährden

wahr.

### ISO 37001 7.3 Bewusstseinsbildung und Training

AB.7.3 Die Organisation führt angemessene und ausreichende Maßnahmen zur Bewusstseinsbildung sowie Anti-Korruptionsschulungen für die Mitarbeiter durch. Diese Schulungen behandeln die folgenden Fragen unter Berücksichtigung der Ergebnisse der Korruptions-Risikobewertung:

a) die Anti-Korruptionspolitik, Verfahren und die Festlegungen des Managementsystem und die Verpflichtung der Mitarbeiter diese einzuhalten;

b) das Korruptionsrisiko, der Schaden der für den Mitarbeiter sowie die Organisation durch Korruption entstehen kann;

c) die Umstände unter denen Korruption entstehen kann in Bezug auf die Tätigkeiten und Pflichten des Mitarbeiters und wie diese erkannt werden können;

d) wie Aufforderungen oder Angebote von Bestechungsgeldern erkannt werden können und wie der Mitarbeiter darauf zu regieren hat;

e) wie die Mitarbeiter dazu beitragen können, Korruption zu verhindern und wie sie Indikatoren für Korruptionsrisiken erkennen können;

f) den Beitrag des Mitarbeiters zur Effektivität des Managementsystems, einschließlich die Vorteile einer verbesserten Anti-Korruptionsperformance und der Meldung von Verdachtsfällen;

g) die Implikationen und möglichen Konsequenzen der Nichteinhaltung der Festlegungen des Managementsystems;

h) wie und an wen sie jegliche Verdachtsfälle berichten können;

i) Informationen über angebotene Schulungen und Ressourcen.

AB.7.4 Die Organisation hat Verfahren implementiert zur Schulung und Bewusstseinsbildung von Geschäftspartnern, die im Auftrag und im Namen der Organisation handeln, und die ein erhöhtes Korruptionsrisiko darstellen könnten. Diese Verfahren identifizieren die Geschäftspartner für die solche Bewusstsein bildende Maßnahmen und Schulungen erforderlich sind, legen Inhalte und Methoden der Schulungen fest.

### ISO 19600 Abschnitt 7.4 Kommunikation

A.7.7 Die Organisation hat geeignete Methoden festgelegt, um sicherzustellen, dass die Wichtigkeit von Compliance allen Mitarbeitern kontinuierlich kommuniziert und von diesen verstanden wird.

A.7.8 Die Kommunikation transportiert klar die Erwartung an die Mitarbeiter und hebt jene Compliance-Verstöße hervor, in Bezug auf die Eskalationsmaßnahmen vorgesehen sind.

A.7.9 Ein praktikabler Ansatz für die externe Kommunikation an alle Stakeholder wurde implementiert.

### ISO 19600 Abschnitt 7.5 Dokumentation

A.7.10 Bei der Erstellung und Aktualisierung dokumentierter Information hat die Organisation

1. eine angemessene Kennzeichnung und Beschreibung;
2. ein angemessenes Format und Medium;
3. eine angemessene Überprüfung und Genehmigung im Hinblick auf Eignung der Dokumentation

sichergestellt.

A.7.11 Dokumentierte Information ist gelenkt, um sicherzustellen, dass die Information

1. verfügbar und für die Verwendung geeignet ist, und
2. angemessen geschützt ist.

## ISO 19600 Abschnitt 8 Betrieb

### ISO 19600 Abschnitt 8.1 Betriebliche Planung und Steuerung

A.8.1 Die Organisation hat die erforderlichen Prozesse zur Erfüllung der Compliance-Verpflichtungen implementiert und steuert diese indem sie:

1. Ziele für die Prozesse festlegt;
2. Kriterien für die Prozesse festlegt;
3. die Steuerung der Prozesse in Übereinstimmung mit den Kriterien durchführt;

4. dokumentierte Information im erforderlichen Umfang bereithält, so dass man darauf vertrauen kann, dass die Prozesse wie geplant durchgeführt wurden.

### ISO 19600 Abschnitt 8.2 Kontroll- und Steuerungsmaßnahmen

A.8.2 Kontroll- und Steuerungsmaßnahmen sind implementiert, um die festgestellten Compliance-Verpflichtungen und die damit verbundenen Compliance-Risiken zu managen.

A.8.3 Kontroll- und Steuerungsmaßnahmen werden in regelmäßigen Abständen evaluiert und überprüft, um ihre anhaltende Wirksamkeit zu gewährleisten.

### ISO 19600 Abschnitt 8.3 Fremdvergebene Prozesse

A.8.4 Fremdvergebene Prozesse werden gesteuert und überwacht.

A.8.5 Im Fall der Auslagerung von Aktivitäten, führt die Organisation eine Überprüfung (due diligence) durch, um sicherzustellen, dass die Compliance-Standards der Organisation nicht gemindert werden.

A.8.6 Die Organisation berücksichtigt Compliance-Risiken in Bezug auf Prozesse, die Drittparteien involvieren, wie zum Beispiel die Lieferung von Waren und Dienstleistungen und den Vertrieb von Produkten, und legt –falls erforderlich- Kontroll- und Steuerungsmaßnahmen fest.

### ISO 37001 Abschnitt 8.2 Sorgfältige Überprüfung (Due diligence)

AB.8.1 In Fall, dass die Korruptions-Risikobewertung ein erhöhtes Korruptionsrisiko in Bezug auf:

a) spezifische Kategorien von Transaktionen, Projekten oder Aktivitäten,

b) geplante oder laufende Beziehungen zu bestimmten Kategorien von Geschäftspartnern, oder

c) spezifische Kategorien von Mitarbeitern in bestimmten Positionen,

ergeben hat, hat die Organisation die Art und das Ausmaß des Korruptionsrisikos in Bezug auf diese spezifische Transaktionen, Projekte, Aktivitäten, Geschäftspartner und Mitarbeiter, die unter diese Kategorien fallen, bewertet.

AB.8.2 Diese Bewertung umfasst jegliche erforderliche Prüfung, um ausreichend Informationen zur Beurteilung des Korruptionsrisikos zu erhalten.

AB.8.3 Die Due Diligence wird mit einer festgelegten Häufigkeit aktualisiert, so dass Änderungen und neue Informationen berücksichtigt werden können.

### ISO 37001 Abschnitt 8.3 Finanzielle Steuerungsmaßnahmen

AB.8.4 Die Organisation hat finanzielle Steuerungsmaßnahmen zur Kontrolle des Korruptionsrisikos implementiert.

### ISO 37001 Abschnitt 8.4 Nicht-finanzielle Steuerungsmaßnahmen

AB.8.5 Die Organisation hat nicht-finanzielle Steuerungsmaßnahmen zur Kontrolle des Korruptionsrisikos in Bezug auf die Bereiche Beschaffung, Betrieb, Vertrieb, Handel, Personalwesen, Rechtsangelegenheiten implementiert.

### ISO 37001 Abschnitt 8.5 Anti-Korruptions-Maßnahmen bei kontrollierten Organisationen und Geschäftspartnern

AB.8.6 Die Organisation hat Verfahren implementiert, die festlegen, dass anderen Organisationen, über die die Organisation die Kontrolle hat, entweder:

a) das Managementsystem der Organisation umsetzen oder

b) ihre eigenen Anti-Korruptions Steuerungsmaßnahmen implementieren.

AB.8.7 In Bezug auf Geschäftspartner, die nicht durch die Organisation gesteuert werden, für die die Beurteilung des Korruptionsrisikos oder die sorgfältige Überprüfung ein höheres Korruptionsrisiko identifiziert hat, hat die Organisation Verfahren wie folgt implementiert:

a) Organisation hat bestimmt, ob der Geschäftspartner Steuerungsmaßnahmen zur Kontrolle der relevanten Korruptionsrisiken implementiert hat;

b) für den Fall, dass der Geschäftspartner keine Steuerungsmaßnahmen zur Kontrolle der relevanten Korruptionsrisiken implementiert hat, oder für den Fall, dass die Verifizierung solcher Maßnahmen nicht möglich ist:

1) sofern praktikabel: die Organisation hat die Geschäftspartner verpflichtet, Steuerungsmaßnahmen zur Kontrolle der Korruption in Bezug auf die relevante Transaktion, Projekt oder Tätigkeit zu implementieren; oder

2) sofern dies nicht praktikabel: die Organisation hat diesen Faktor bei der Beurteilung der Korruptionsrisiken, welche die Geschäftspartner darstellen, und die Art und Weise, in der die Organisation solche Risiken steuert, berücksichtigt.

### ISO 37001 Abschnitt 8.6 Verpflichtungen zur Korruptionsbekämpfung

AB.8.8 Für Geschäftspartner, die ein erhöhtes Korruptionsrisiko darstellen, hat die Organisation Verfahren implementiert, die, soweit durchführbar, erfordern:

a) die Geschäftspartner verpflichten sich, Korruption durch oder im Auftrag oder zum Vorteil des Geschäftspartners in Verbindung mit der relevanten Transaktion, dem relevanten Projekt, der relevanten Tätigkeit oder Beziehung zu verhindern;

b) die Organisation ist in der Position, die Beziehung mit dem Geschäftspartner im Fall von Korruption durch oder im Auftrag oder zum Vorteil des Geschäftspartners in Verbindung mit der relevanten Transaktion, dem relevanten Projekt, der relevanten Tätigkeit oder Beziehung zu beenden.

### ISO 37001 Abschnitt 8.7 Geschenke, Bewirtung, Spenden und ähnliche Vorteile

AB.8.9 Die Organisation hat Verfahren implementiert, die das Anbieten, die Bereitstellung oder die Annahme von Geschenken, Bewirtung, Spenden und ähnlicher Vorteile verhindern, für den Fall, dass ein solches Anbieten, die Bereitstellung oder die Annahme Korruption darstellt oder berechtigterweise als solche wahrgenommen werden könnte.

### ISO 37001 Abschnitt 8.8 Management unzureichender Anti-Korruptions Steuerungsmaßnahmen

AB.8.10 Wenn die an einer spezifischen Transaktion, Projekt, Tätigkeit oder Beziehung mit einem Geschäftspartner durchgeführte sorgfältige Prüfung (Due Diligence) festlegt, dass die Korruptionsrisiken nicht mit den vorhandenen Maßnahmen zur Korruptionsbekämpfung gesteuert werden können und die Organisation zusätzliche Steuerungsmaßnahmen zur Korruptionsbekämpfung nicht verwirklichen kann oder hierzu nicht bereit ist, hat die Organisation:

a) für den Fall einer bestehenden Transaktion, Projekt, Tätigkeit oder Beziehung Schritte unternommen, um sie so schnell wie möglich abzubrechen, zu beenden, einzustellen, sich aus ihr zurückzuziehen;

b) für den Fall einer neuen Transaktion, Projekt, Tätigkeit oder Beziehung diese verschoben oder die Fortsetzung abgelehnt.

### ISO 37001 Abschnitt 8.9 Äußern von Bedenken

AB.8.11 Die Organisation hat Verfahren implementiert, die:

a) Personen ermutigen und ihnen ermöglichen versuchte, mutmaßliche oder tatsächliche Korruption oder alle Verstöße gegen oder Schwächen im Managementsystem an die Compliance Funktion oder anderes geeignetes Personal zu berichten (entweder direkt oder über eine geeignete dritte Partei);

b) die Organisation verpflichten, Berichte vertraulich zu behandeln, um die Identität des Berichterstatters und anderer mit dem Bericht in Zusammenhang stehender oder in dem Bericht genannter Personen zu schützen;

c) ein anonymes Melden erlauben;

d) Vergeltung nicht erlauben and jene Personen vor Vergeltung schützen, die im guten Glauben über einen versuchten, tatsächlichen oder einen vermuteten Korruptionsfall oder einen Verstoß gegen die Anti-Korruptionspolitik oder das Managementsystem berichtet haben;

e) es dem Personal ermöglichen, Rat von einer geeigneten Person zu erhalten was zu tun ist, wenn es einer Situation gegenübersteht, die Korruption beinhalten könnte.

AB.8.12 Die Organisation hat sichergestellt, dass alle Mitarbeiter über die Meldeverfahren informiert sind, in der Lage sind, diese zu nutzen und sich ihrer Rechte und Schutzmaßnahmen im Rahmen der Verfahren bewusst sind.

### ISO 37001 Abschnitt 8.10 Untersuchung von und Umgang mit Korruption

AB.8.13 Die Organisation hat Verfahren implementiert, die:

a) die Bewertung, und sofern angebracht, die Untersuchung jedes Korruptionsfalls oder Verstöße gegen die Anti-Korruptionspolitik oder das Managementsystem erfordern;

b) geeignete Maßnahmen für den Fall erfordern, dass eine Untersuchung einen Fall von Korruption oder einen Verstoß gegen die Anti-Korruptionspolitik oder das Managementsystem offenbart;

c) Ermittler ermächtigen und befähigen;

d) Kooperation bei der Untersuchung durch das relevante Personal erfordern;

e) festlegen, dass der Status und die Resultate von Untersuchungen an die Compliance Funktion berichtet werden;

f) festlegen, dass Untersuchungen vertraulich durchgeführt werden und, dass Ergebnisse von Untersuchungen vertraulich behandelt werden.

AB.8.14 Untersuchungen werden von Personen durchgeführt und werden an Personen berichtet, die nicht Teil der untersuchten Rolle oder Funktion sind.

## ISO 19600 Abschnitt 9 Bewertung der Leistung

### ISO 19600 Abschnitt 9.1 Überwachung, Messungen, Analysen und Bewertungen

A.9.1 Das Compliance Management System wird zur Sicherstellung der Compliance-Leistung überwacht.

A.9.2 Ein Plan für eine laufende Überwachung ist festgelegt.

A.9.3 Die Organisation bewahrt dokumentierte Informationen als Nachweis der Ergebnisse der Überwachungen auf.

A.9.4 Verfahren für die Erfassung von Rückmeldungen über die Compliance-Leistung der Organisation sind implementiert.

A.9.5 Es existieren messbare Indikatoren zur Quantifizierung der Compliance-Leistung der Organisation.

A.9.6 Es ist sichergestellt, dass das Aufsichtsgremium, das Top-Management und die Compliance-Funktion über die Leistung des Compliance-Management-Systems und über dessen andauernde Angemessenheit informiert sind.

A.9.7 Das interne Berichtswesen stellt sicher, dass:

1. geeignete Kriterien und Verpflichtungen für die Berichterstattung festgelegt sind;

2. Fristen für die regelmäßige Berichterstattung etabliert sind;
3. ein Berichtswesen für Ausnahmefälle eingerichtet ist, zur Ermöglichung von ad-hoc-Meldungen im Falle von aufgetretenen Compliance-Verstößen;
4. Systeme und Prozesse vorhanden sind, um die Richtigkeit und Vollständigkeit der Informationen zu gewährleisten;
5. Informationen an die relevanten Funktionen oder Bereiche der Organisation zur Verfügung gestellt werden, um Vorbeugungs-, Korrektur-und Abhilfemaßnahmen ergreifen zu können; und
6. Unterschriftenregelungen (die die Compliance Funktion einschließen) existieren, zur Bestätigung der Richtigkeit der Berichte an das Aufsichtsgremium.

A.9.8 Compliance-Verstöße werden entsprechend gemeldet.

A.9.9 Die Mitarbeiter werden ermutigt, auf Compliance-Verstöße zu reagieren und diese zu melden.

A.9.10 Aufzeichnungen über die Compliance-Aktivitäten der Organisation werden geführt. Aufzeichnungen werden in Bezug auf Beschwerden und deren Klassifizierung, auf Streitfälle sowie in Bezug auf mutmaßliche Compliance-Verstöße (einschließlich unternommener Schritte zu deren Lösung) geführt.

A.9.11 Aufzeichnungen werden derart gespeichert, dass deren Lesbarkeit, Identifizierbarkeit und Wiederherstellung sichergestellt ist.

A.9.12 Aufzeichnungen werden gegen jedes Hinzufügen, Löschen, Änderung, unberechtigte Nutzung oder Unterdrückung von Informationen geschützt.

### ISO 19600 Abschnitt 9.2 Audit

A.9.13 Die Organisation führt Audits in geplanten Abständen durch, um Informationen darüber zu erhalten, ob das Compliance Management System

1. die eigenen Anforderungen erfüllt und den Kriterien der ISO 19600 entspricht,
2. wirksam implementiert und aufrechterhalten wird.

A.9.14 Die Organisation:

1. hat ein oder mehrere Auditprogramme implementiert; die Auditprogramme legen die Häufigkeit von Audits, Methoden, Verantwortlichkeiten sowie Berichterstattung fest;
2. hat für jedes Audit die Auditkriterien sowie den Umfang festgelegt,
3. wählt Auditoren aus und führt Audits auf eine Weise durch, dass die Objektivität und Unparteilichkeit des Auditprozesses sichergestellt ist,
4. hat sichergestellt, dass die Ergebnisse des Audits gegenüber der zuständigen Leitung berichtet werden,
5. bewahrt dokumentierte Information als Nachweis der Verwirklichung des Auditprogramms und der Ergebnisse des Audits auf.

### ISO 19600 Abschnitt 9.3 Managementbewertung

A.9.15 Die oberste Leitung bewertet das Compliance Management System in geplanten Abständen.

A.9.16 Dokumentierte Informationen als Nachweis der Ergebnisse der Managementbewertung werden aufbewahrt.

### ISO 37001 Abschnitt 9.4 Bewertung durch die Anti-Korruptions Compliance Funktion

**AB.9.1** Die Anti-Korruptions Compliance Funktion bewertet, auf kontinuierlichen Basis, ob das Managementsystem:

a) adäquat in Bezug auf die Korruptionsrisiken der Organisation ist;

b) effektiv implementiert ist.

AB.9.2 Die Anti-Korruptions Compliance Funktion berichtet in geplanten Zeitabständen, sowie -sofern erforderlich- auf einer ad-hoc Basis, an das Aufsichtsgremium und das Top-Management über die Eignung und die Implementierung des Managementsystems, einschließlich der Ergebnisse von Untersuchungen und Audits.

## ISO 19600 Abschnitt 10 Verbesserung

A.10.1 Für den Fall des Auftretens eines Compliance-Verstoßes:

1. reagiert die Organisation entsprechend auf den Compliance-Verstoß;
2. wird die Notwendigkeit von Maßnahmen zur Beseitigung der Ursachen für den Compliance-Verstoß evaluiert;
3. werden die erforderlichen Maßnahmen durchgeführt;
4. wird die Wirksamkeit der ergriffenen Korrekturmaßnahmen überprüft, und
5. falls erforderlich, werden Änderungen am Compliance Management System vorgenehmen.

A.10.2 Dokumentierte Informationen werden aufbewahrt, als Nachweis über:

1. die Art des Compliance-Verstoßes und die daraus folgenden, ergriffenen Maßnahmen; und
2. die Ergebnisse der Korrekturmaßnahmen.

A.10.3 Ein Eskalationsprozess ist eingerichtet und kommuniziert, um sicherzustellen, dass alle Compliance-Verstöße erhoben, gemeldet und schlussendlich an die zuständigen Führungskräfte eskaliert werden und die Compliance-Funktion informiert wird.

A.10.4 Es existiert ein Mechanismus für die Mitarbeiter und/oder Dritte, um vermutetes oder tatsächliches Fehlverhalten oder Verstöße gegen Compliance-Verpflichtungen auf vertraulicher Basis und ohne Angst vor Vergeltungsmaßnahmen, zu melden.

# Anhang B Kriterien nach ONR 192050

## B.1 Rolle der Leitung der Organisation

B.1.1 Das Verhalten der Leitung der Organisation muss im Einklang mit dem CMS stehen.

B.1.2 Die Leitung der Organisation muss sicherstellen, dass das CMS entwickelt, eingeführt, aufrechterhalten, regelmäßig überprüft und bei Bedarf verbessert wird. Das CMS muss dokumentiert werden.

B.1.3 Die Leitung der Organisation muss sicherstellen, dass die erforderlichen Voraussetzungen für das CMS, im Rahmen sowohl der Aufbau- als auch der Ablauforganisation, geschaffen werden.

B.1.4 Die Leitung der Organisation muss sicherstellen, dass die erforderlichen Ressourcen für das CMS in Abhängigkeit der Ergebnisse der Compliance-Risiko-Bewertung zur Verfügung stehen.

B.1.5 Die Leitung der Organisation muss sicherstellen, dass auf Basis der Ergebnisse der Compliance-Risiko-Bewertung Maßnahmen zur Verminderung der Compliance-Risiken getroffen und umgesetzt werden.

B.1.6 Die Leitung der Organisation muss das CMS und dessen Inhalte den Organisationsmitgliedern im erforderlichen Umfang nachweislich zur Kenntnis bringen. Hierzu müssen den Organisationsmitgliedern die relevanten Unterlagen und Dokumente zugänglich gemacht werden.

## B.2 Compliance Officer (CO)

B.2.1 Die Aufgaben eines CO müssen entweder von der Leitung der Organisation oder von einem anderen Organisationsmitglied oder mehreren anderen Organisationsmitgliedern wahrgenommen werden.

B.2.2 Der CO muss die Leitung der Organisation bei der Entwicklung, der Einführung, der Aufrechterhaltung, der regelmäßigen Überprüfung und bei der Verbesserung des CMS beraten und unterstützen.

B.2.3 Der CO muss schriftlich durch die Leitung der Organisation berufen werden und seiner Berufung zustimmen. Die Berufung hat eine Beschreibung seiner Aufgaben zu enthalten.

B.2.4 Der CO muss mit den Befugnissen ausgestattet sein, die er für die Erfüllung seiner Aufgaben benötigt.

B.2.5 Der CO muss in Bezug auf seine Aufgaben weisungsfrei sein.

B.2.6 Der CO muss die Möglichkeit zur direkten Kommunikation mit der Leitung der Organisation haben.

B.2.7 Der CO muss über die für seine Tätigkeit erforderlichen Kenntnisse verfügen und mit den Tätigkeiten der Organisation grundsätzlich vertraut sein.

B.2.8 Der CO muss auf die Organisation bezogene Kenntnisse über Compliance-relevante Vorgänge, Regeln, Compliance-Risiko-Bewertung, Monitoring und Auditing haben.

B.2.9 Der CO muss regelmäßig – mindestens einmal jährlich – einen Compliance-Report erstellen. Dieser Report muss der Leitung der Organisation zur Kenntnis gebracht werden.

## B.3 Compliance-Risiko-Bewertung und Maßnahmen

B.3.1 Im Rahmen des CMS muss eine Compliance-Risiko-Bewertung nach einem festgelegten Verfahren erfolgen und dokumentiert werden.

B.3.2 Dieses Verfahren muss zumindest folgende Schritte enthalten:

- die Identifikation der Compliance-relevanten Vorgänge im Hinblick auf die Regeln;
- die Identifikation von Compliance-Risiken und Bewertung nach ihrer Eintrittswahrscheinlichkeit und ihren Konsequenzen;
- die Priorisierung und daraus abgeleitet das Treffen von Maßnahmen.

B.3.3 Die Compliance-Risiko-Bewertung muss sich auf alle Organisationsmitglieder erstrecken.

B.3.4 Die Ergebnisse der Compliance-Risiko-Bewertung müssen dokumentiert und der Leitung der Organisation zur Kenntnis gebracht werden.

**B.3.5** Die Compliance-Risiko-Bewertung muss regelmäßig – mindestens einmal jährlich – erfolgen.

## B.4 Handlungsanweisungen

B.4.1 Das CMS muss schriftlich dokumentierte und verbindliche Handlungsanweisungen umfassen mit dem Zweck, Regel-Verstöße zu verhindern beziehungsweise gegebenenfalls aufzudecken.

B.4.2 Die Handlungsanweisungen müssen aus den Ergebnissen der Compliance-Risiko-Bewertung abgeleitet werden.

B.4.3 Die Handlungsanweisungen müssen regeln, wie mit Compliance-relevanten Vorgängen umgegangen wird.

B.4.4 Vor der Besetzung von Schlüssel-Positionen, die auf Basis der Compliance-Risiko-Bewertung identifiziert wurden, müssen die Kandidaten in Hinblick auf Compliance überprüft werden.

## B.5 Training

B.5.1 Im Rahmen des CMS muss sichergestellt werden, dass die Organisationsmitglieder auf Basis der Ergebnisse der Compliance-Risiko-Bewertung regelmäßig trainiert werden.

B.5.2 Die Methode, der Umfang und die Intensität des Trainings müssen dem Aufgabenbereich der jeweiligen Organisationsmitglieder angepasst sein.

B.5.3 Organisationsmitglieder in Schlüsselposition müssen im Rahmen von Präsenzschulungen trainiert werden.

B.5.4 Das Training muss dokumentiert werden. Diese Dokumentation muss zumindest beinhalten: Teilnehmer, Zeitpunkt, Dauer und Inhalt der Trainingsmaßnahmen.

## B.6 Wirksamkeit des CMS

B.6.1 Das CMS muss die Überwachung der Einhaltung von Handlungsanweisungen in der jeweils erforderlichen Frequenz beinhalten.

B.6.2 Das CMS muss stichprobenartige oder anlassbezogene Überprüfungen von Compliance-relevanten Vorgängen beinhalten.

B.6.3 Die Angemessenheit, Eignung und Wirksamkeit des CMS müssen regelmäßig überprüft werden, unter anderem durch Überprüfung der Einhaltung von Handlungsanweisungen und durch Überprüfung der Durchführung von Trainings. Die Überprüfung muss objektiv und unparteilich erfolgen.

B.6.4 Es muss für Organisationsmitglieder die Möglichkeit zur Meldung von Regel-Verstößen geben.

- Die Identität des Meldenden muss auf dessen Wunsch vertraulich behandelt werden, mit Ausnahme von gesetzlichen Offenlegungspflichten.
- Die Meldung muss auch anonym erfolgen können.
- Sanktionen gegen gutgläubig Meldende müssen ausgeschlossen werden, sofern sie nicht am Regel-Verstoß beteiligt waren.
- Die Möglichkeit der Meldung muss den Organisationsmitgliedern zur Kenntnis gebracht werden.
- Alle Meldungen müssen behandelt werden.

B.6.5 Zur Behandlung von aufgedeckten Regel-Verstößen muss ein Verfahren festgelegt werden.

B.6.6 Bei aufgedeckten Regel-Verstößen müssen Sanktionen und erforderlichenfalls Verbesserungsmaßnahmen des CMS festgelegt, umgesetzt und dokumentiert werden. Dies muss an die Leitung der Organisation zeitnah gemeldet werden.

## B.7 Kommunikation

B.7.1 Die Leitung der Organisation muss regelmäßig ihr Engagement für Compliance bekunden und über die für die Organisation adäquaten Kanäle kommunizieren.

B.7.2 Die Organisationsmitglieder müssen regelmäßig über die für sie relevanten Änderungen im CMS informiert werden.