

ICS 03.100.02; 03.100.70

Leitfaden für Compliance-Management-Systeme in kleinen und mittleren Unternehmen

Guide for compliance management systems in small and medium enterprises

Guide pour les systèmes de gestion de la conformité dans les petites et moyennes entreprises

Gesamtumfang 51 Seiten

Dieses Dokument wurde durch die im Vorwort genannten Verfasser erarbeitet und verabschiedet.



Inhalt

	Seite
Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Allgemeines	9
4.1 Einleitung	9
4.2 Ziele des Selbst-Checks	9
4.3 Grundsätze für den Selbst-Check	9
4.4 Identifikation der vorhandenen Prozesse im Unternehmen	10
4.4.1 Allgemeines	10
4.4.2 Steuerungsprozess/Managementprozess	10
4.4.3 Wertschöpfungsprozess	10
4.4.4 Unterstützungsprozesse	11
4.5 Auswertung der Ergebnisse des Compliance-Selbst-Checks	12
5 Empfehlungen an ein Compliance-Management-System für kleine und mittelständische Unternehmen	13
6 Risikoanalyse/Scoping des Unternehmens — Beschreibung der relevanten Risiken	13
6.1 Allgemeines	13
6.2 Arbeitsstrafrecht	13
6.3 Außenwirtschaftsstrafrechtliche Risiken	14
6.4 Datenschutzrechtliche Risiken	14
6.5 Geheimnisschutzstrafrecht	15
6.6 Risiken in Bezug auf Geldwäsche	15
6.7 Cyber-Strafrecht	15
6.8 Korruptionsrisiken	15
6.9 Lieferkettenhaftung	16
6.10 Umweltstrafrecht	17
6.11 Wettbewerbsstrafrechtliche Risiken/Kartellordnungswidrigkeiten	17
7 Handlungsempfehlungen für die Verbesserung des Compliance-Management-Systems (CMS)	18
7.1 Allgemeines	18
7.2 Prävention	18
7.2.1 Kommunikation	18
7.2.2 Tone from the top	19
7.2.3 Erarbeitung Verhaltenskodex	19
7.2.4 Stärkung der Mitarbeitendenbindung/-identifikation und Unternehmenskultur	20
7.2.5 Lieferantenkodex	20
7.2.6 Festlegung von Zuständigkeiten und Kompetenzen	21
7.2.7 Delegation	21
7.2.8 Schulungen	21
7.2.9 Richtlinien	22
7.2.10 Identifizierung unternehmenseigener/fremder Geschäftsgeheimnisse	23
7.2.11 Offboarding-Prozess	23
7.2.12 IT-Vorkehrungen	24
7.2.13 Vermeidung von Bargeld	24
7.2.14 Technische und organisatorische Maßnahmen (TOMs)	24
7.2.15 Arbeitszeiterfassung	25
7.3 Detektion	25
7.3.1 Kommunikation	25
7.3.2 Regelmäßige Kontrollen	26

7.3.3	Regelmäßige Prozesskontrollen	26
7.3.4	Regelmäßige (interne) Kontrollen	26
7.3.5	Funktionstrennung	27
7.3.6	Aufsicht und Überprüfung	27
7.3.7	Festlegung von Budgets und Budgetkontrollen	27
7.3.8	Vier-Augen-Prinzip	28
7.3.9	Hinweisgebersystem	28
7.3.10	Dokumentation (Verarbeitungsverzeichnis) — Einführung zentrales Dokumentationsmanagement	29
7.3.11	Vorfalldokumentation	29
7.4	Reaktion	29
7.4.1	Kommunikation	29
7.4.2	Durchführung von Audits	30
7.4.3	Durchsetzbarkeit und Sanktionen	31
	Anhang A (informativ) Compliance-Selbst-Check	32
	Literaturhinweise	49

Tabellen

Tabelle A.1	— Compliance-Selbst-Check — Einführung	32
Tabelle A.2	— Compliance-Selbst-Check — Allgemeine Fragen	33
Tabelle A.3	— Compliance-Selbst-Check — Managementprozess	37
Tabelle A.4	— Compliance-Selbst-Check — Einkaufsprozess	39
Tabelle A.5	— Compliance-Selbst-Check — Vertriebsprozess	41
Tabelle A.6	— Compliance-Selbst-Check — Wertschöpfungsprozess	43
Tabelle A.7	— Compliance-Selbst-Check — Personalprozess	45
Tabelle A.8	— Compliance-Selbst-Check — IT-Prozess	46
Tabelle A.9	— Compliance-Selbst-Check — Logistikprozess	47
Tabelle A.10	— Compliance-Selbst-Check — Finanzprozess	48

Vorwort

Diese DIN SPEC wurde nach dem PAS-Verfahren erarbeitet. Die Erarbeitung von DIN SPEC nach dem PAS-Verfahren erfolgt in DIN-SPEC-Konsortien und nicht zwingend unter Einbeziehung aller interessierten Kreise.

Die vorliegende DIN SPEC ging aus dem Projekt „Empirische Entwicklung und Prüfung eines Compliance-Standards für den Mittelstand — MiCo“ im Rahmen der vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) geförderten Initiative „Wissens- und Technologietransfer durch Patente und Normen — WIPANO“ (Förderkennzeichen FKZ 03TN0043C) hervor.

Die Erarbeitung und Verabschiedung des Dokuments erfolgten durch die nachfolgend genannten Initiator(en) und Verfasser:

— DIKOIN GmbH

Prof. Dr. Andreas Hoffjan

— Expertenrat Mittelstands-Compliance e.V.

Michael Adel, Dr. Johann Ante, Björn Baltés, Ralf Damberg, Prof. Dr. Michael Lindemann, Christina Ritzenhoff, Nora Schröder, Andreas Seepe, Jannik Zahlten

— PARK Compliance Services GmbH

Dr. Tobias Eggers

Für dieses Thema bestehen derzeit keine Normen im Deutschen Normenwerk.

DIN SPEC sind nicht Teil des Deutschen Normenwerks.

Für diese DIN SPEC wurde kein Entwurf veröffentlicht.

Trotz großer Anstrengungen zur Sicherstellung der Korrektheit, Verlässlichkeit und Präzision technischer und nicht-technischer Beschreibungen kann das DIN-SPEC-Konsortium weder eine explizite noch eine implizite Gewährleistung für die Korrektheit des Dokuments übernehmen. Die Anwendung dieses Dokuments geschieht in dem Bewusstsein, dass das DIN-SPEC-Konsortium für Schäden oder Verluste jeglicher Art nicht haftbar gemacht werden kann. Die Anwendung der vorliegenden DIN SPEC entbindet den Nutzer nicht von der Verantwortung für eigenes Handeln und geschieht damit auf eigene Gefahr.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Die kostenfreie Bereitstellung dieses Dokuments als PDF-Version über den DIN Media Webshop wurde im Vorfeld finanziert.

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

Einleitung

Dieses Dokument hat das Ziel, die Implementierung eines Compliance-Management-Systems in kleinen und mittelständischen Unternehmen unter Beachtung ihrer Ressourcen und Möglichkeiten zu unterstützen und voranzutreiben. Es legt Anforderungen für einen standardisierten Managementprozess in dieser Zielgruppe fest, die ggf. nur partiell oder in geringem Umfang in die Unternehmensstruktur der Zielgruppen integriert sind. Kleine und mittelständische Unternehmen sind in diesem Kontext Betriebe, die inhabergeführt sind, durch eine von der Familie berufene Geschäftsführung vertreten werden und/oder der Eigenkapitalhaftung unterliegen. Oft ist diesen Unternehmern ihr Gefährdungspotential nur unzureichend bekannt und nur wenige Maßnahmen, die von den Aufsichtsbehörden regelmäßig kontrolliert werden, werden von ihnen umgesetzt. Ein Managementsystem scheidet oftmals an den im Tagesgeschäft benötigten Ressourcen, die in der Praxis sowohl zeitlich als auch monetär begrenzt sind. Zudem verfügen diese Unternehmen oftmals über kein oder nur über unzureichendes Compliance-Know-how. Sie sind deshalb auf Unterstützung durch handhabbare pragmatische Instrumente und/oder bezahlbare externe Beratungsdienstleistungen angewiesen. Auf Basis der erfassten Betriebsabläufe und -prozesse soll dieses Dokument die Unternehmen dabei unterstützen, die eigenen Voraussetzungen für ein Compliance-Management-System zu analysieren, Maßnahmen zu initiieren und systemimmanenten Risiken zeit- und kosteneffizient entgegenzuwirken.

Dabei liegt es in der Verantwortung der Unternehmensführung zu entscheiden, welche Schwerpunkte zum Aufbau eines Compliance-Management-Systems gesetzt werden sollen, bzw. anhand der Ausgangssituation den für das jeweilige Unternehmen passenden Maßnahmenkatalog zu erarbeiten. Neben den externen Anforderungen des firmenspezifischen Umfelds und der involvierten Parteien liefert der Blick auf interne förderliche und hinderliche Einflussfaktoren wichtige Hinweise auf den aktiven und zielgerichteten Aufbau eines Compliance-Management-Systems. Insbesondere für die Unternehmensführung ist es wichtig sich mit den verabschiedeten Maßnahmen zu identifizieren, ein Compliance konformes Verhalten vorzuleben, Kernaktivitäten über alle Unternehmensebenen zu kommunizieren und Instrumente zu erarbeiten, die ein nichtkonformes Verhalten Einzelner sanktionieren. Eine regelmäßige Bewertung des Zielerreichungsgrades einer verabschiedeten Maßnahme, aber auch die damit erfolgende Weiterentwicklung dieses Managementsystems im Sinne der Unternehmensziele und die Schaffung förderlicher Rahmenbedingungen sind die Grundlage der Vorgehensweise. Dazu gehört unter anderem das Etablieren von Strukturen und Anreizen, damit Mitarbeitende in der täglichen Arbeit Compliance-konformes Verhalten aufbauen, teilen und auch zielgerichtet anwenden können.

Strukturen und Anreize sollen Compliance-Anwendungen explizit bei kleinen und mittelständischen Unternehmen fördern sowie Wege zu einer ressourcenadäquaten Umsetzung aufzeigen.

Im Anhang A befindet sich ein praxisorientierter Maßnahmenkatalog, der sowohl bei der ersten Bewertung der Ausgangssituation Anwendung findet, aber auch Maßnahmen und Gesetzesgrundlagen aufzeigt, die für ein Compliance-Management-System bei der angestrebten Zielgruppe relevant sind.

Für die spezifischen Compliance Rahmenbedingungen bei klein- und mittelständischen Betrieben bestehen derzeit keine hierauf zugeschnittenen Normen im deutschen Normenwerk. Für größere Unternehmen und Konzerne wurde das Compliance-Management-System nach DIN ISO 37301 erarbeitet. Weitere Normen für diesen Themenbereich sind DIN ISO 37001 und DIN ISO 37002. Auch DIN SPEC 91443 sowie DIN SPEC 27076 geben wichtige Impulse für die Compliance in kleinen und mittelständischen Unternehmen (KMU).

1 Anwendungsbereich

Dieses Dokument dient als Leitfaden für ein Compliance-Management-System kleiner und mittelständischer Unternehmen (KMUs). Dieses Dokument gibt Anleitung für die Durchführung eines Selbst-Checks zur Ermittlung des aktuellen Stands des vorhandenen Compliance-Management-Systems sowie die Ermittlung der größten Risikobereiche. Darüber hinaus werden konkrete Handlungsempfehlungen für die Verbesserung des eigenen Compliance-Management-Systems gegeben. Es werden keine Anforderungen an Compliance definiert.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

DIN ISO 37301:2021-11, *Compliance-Managementsysteme — Anforderungen mit Leitlinien zur Anwendung (ISO 37301:2021)*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

DIN und DKE stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- DIN-TERMinologieportal: verfügbar unter <https://www.din.de/go/din-term>
- DKE-IEV: verfügbar unter <https://www.dke.de/DKE-IEV>

3.1

Organisation

Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre *Ziele* (3.10) zu erreichen

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

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

[QUELLE: DIN ISO 37301:2021-11, 3.1]

3.2

Unternehmen

Einzelperson oder Personengruppe, die als Einzelunternehmer, Kapitalgesellschaft, Unternehmen, Joint Venture, gemeinnützige Organisation, Firma, Betrieb, Behörde, Partnerschaft, Wohltätigkeitsorganisation oder Institution oder als Teil oder Kombination davon strukturiert ist, ob eingetragen oder nicht, öffentlich oder privat, die die rechtliche Eigentümerschaft oder vertraglich autorisierte Rechte zur Nutzung und/oder Förderung einer Marke in der Kategorie zum wirtschaftlichen oder gesellschaftlichen Nutzen besitzt und/oder hat

[QUELLE: ISO 20671-1:2021, 3.1.1, modifiziert – ins Deutsche übersetzt]

3.3

kleines und mittleres Unternehmen

KMU

Organisationen von kleiner oder mittlerer Größe, wie durch die anerkannte Behörde in dem Land oder der Region festgelegt

Anmerkung 1 zum Begriff: Für die Klassifikation in ein kleines und mittleres Unternehmen wird die Einheit von Eigentum und Leitung vorausgesetzt. Diese ist nach Ansicht des Instituts für Mittelstandsforschung (IfM) gegeben, wenn bis zu zwei natürliche Personen oder deren Familienangehörige mindestens 50 % der Anteile eines Unternehmens halten und zeitgleich der Geschäftsführung angehören.

Anmerkung 2 zum Begriff: Erfüllt ein Unternehmen die nachstehenden Kriterien, so ist es als KMU laut Definition der Europäischen Kommission zu klassifizieren: Anzahl der Beschäftigten: < 250 und Jahresumsatz: ≤ 50 Mio. € oder Bilanzsumme: ≤ 43 Mio. €.

[QUELLE: DIN ISO 30414:2019-06, 3.4, modifiziert – Anmerkung 1 zum Begriff wurde durch neue Anmerkung 1 und Anmerkung 2 zum Begriff ersetzt]

3.4

Compliance

Erfüllen aller *Compliance-Verpflichtungen* (3.7) einer *Organisation* (3.1)

[QUELLE: DIN ISO 37301:2021-11, 3.26]

3.5

Non-Compliance

Nichterfüllung von *Compliance-Verpflichtungen* (3.7)

[QUELLE: DIN ISO 37301:2021-11, 3.27]

3.6

Compliance-Risiko

Wahrscheinlichkeit des Auftretens und die Folgen von *Non-Compliance* (3.5) mit den *Compliance-Verpflichtungen* (3.7) der *Organisation* (3.1)

[QUELLE: DIN ISO 37301:2021-11, 3.24]

3.7

Compliance-Verpflichtungen

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

Anmerkung 1 zum Begriff: Dabei beinhalten die Anforderungen die Einhaltung der gesetzlichen Bestimmungen, regulatorischer Standards, Stakeholder-Forderungen sowie weitere interne Vorgaben.

[QUELLE: DIN ISO 37301:2021-11, 3.25, modifiziert – Anmerkung 1 zum Begriff wurde hinzugefügt]

3.8

Managementsystem

Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer *Organisation* (3.1), um Politiken, *Ziele* (3.10) und *Prozesse* (3.12) zum Erreichen dieser Ziele festzulegen

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

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

[QUELLE: DIN ISO 37301:2021-11, 3.4]

3.9

Compliance-Managementsystem

CMS

Einhaltung der *Compliance-Verpflichtungen* (3.7) einer *Organisation* (3.1) durch ein operationalisiertes *Managementsystem* (3.8)

Anmerkung 1 zum Begriff: Hauptziel ist die Vermeidung von Regelverstößen und die Minimierung von Haftungs- und Schadensrisiken sowie die Sicherstellung regelkonformen Verhaltens aller Mitarbeitenden des Unternehmens durch organisatorische Maßnahmen.

3.10

Ziel

zu erreichendes Ergebnis

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

Anmerkung 2 zum Begriff: Ziele können sich auf verschiedene Disziplinen (wie beispielsweise Finanzen, Gesundheit und Sicherheit, Umwelt) beziehen.

Anmerkung 3 zum Begriff: Ein Ziel kann auf andere Weise ausgedrückt werden, z. B. als beabsichtigtes Ergebnis, als Zweck, als betriebstechnisches Kriterium, als *Compliance-* (3.4) Ziel oder durch Verwendung anderer Worte mit ähnlicher Bedeutung (z. B. Zielvorgabe, Zielstellung oder Einzelziel).

Anmerkung 4 zum Begriff: Im Kontext von *Compliance-Managementsystemen* (3.9) werden Compliance-Ziele von *Organisationen* (3.1) im Einklang mit ihrer Compliance-Politik gesetzt, um bestimmte Ergebnisse zu erreichen.

[QUELLE: DIN ISO 37301:2021-11, 3.6, modifiziert – Anmerkung 2 zum Begriff geändert]

3.11

Risiko

Auswirkung von Ungewissheit auf *Ziele* (3.10)

Anmerkung 1 zum Begriff: Eine Auswirkung ist eine Abweichung vom Erwarteten – in positiver oder negativer Hinsicht.

Anmerkung 2 zum Begriff: Ungewissheit ist der Zustand des auch teilweisen Fehlens von Informationen im Hinblick auf das Verständnis eines Ereignisses oder Wissen über ein Ereignis, seine Folgen oder seine Wahrscheinlichkeit.

Anmerkung 3 zum Begriff: Risiko wird häufig durch Bezugnahme auf mögliche „Ereignisse“ (definiert in ISO 31073) und „Folgen“ (definiert in ISO 31073), oder durch eine Kombination beider charakterisiert.

Anmerkung 4 zum Begriff: Risiko wird häufig mittels der Folgen eines Ereignisses (einschließlich Veränderungen der Umstände) in Verbindung mit der „Wahrscheinlichkeit“ (definiert in ISO 31073) seines Eintretens beschrieben.

[QUELLE: DIN ISO 37301:2021-11, 3.7]

3.12

Prozess

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

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

[QUELLE: DIN ISO 37301:2021-11, 3.8]

3.13**Risikoanalyse**

Prozess (3.12) der Untersuchung identifizierter Risiko(3.11)-Faktoren hinsichtlich Eintrittswahrscheinlichkeit, potenziellem Verlust und möglichen Risikomanagementstrategien

[QUELLE: ISO/IEC/IEEE 24765:2017, 3.3514, modifiziert – ins Deutsche übersetzt]

4 Allgemeines**4.1 Einleitung**

Dieses Dokument gibt einen Leitfaden für eine klare Struktur zum Aufbau oder zur Implementierung eines Compliance-Management-Systems. Es beginnt mit der Erläuterung der Compliance-relevanten Risikobereiche, führt durch die betriebsspezifischen Prozesse des Unternehmens und endet mit der Beschreibung konkreter Handlungsempfehlungen für die Einrichtung und Fortentwicklung eines umfassenden Compliance-Management-Systems, das auf die Bedürfnisse des Unternehmens abgestimmt ist. Dieser Abschnitt beschreibt die Ziele dieses Dokuments sowie die konkrete Durchführung des in Anhang A beigefügten Selbst-Checks.

4.2 Ziele des Selbst-Checks

Die zentralen Ziele des Selbst-Checks für Compliance in KMUs sind:

- 1) Die Sensibilisierung der Unternehmensverantwortlichen und -mitarbeitenden für die relevanten Compliance-Risiken des Unternehmens:

Aufgabe des Compliance Selbst-Checks ist es, die Stärken und Schwächen der Unternehmensstruktur bzw. des Compliance-Management-Systems zu identifizieren und konkrete Folgemaßnahmen für risikobehaftete Unternehmensbereiche und Prozesse zu definieren.

- 2) Die Ermittlung des IST-Zustandes des bestehenden Compliance-Management-Systems des Unternehmens:

Dazu empfiehlt es sich, sich schrittweise einen Überblick über die bereits bestehenden Compliance-Strukturen des Unternehmens zu verschaffen, bereits vorhandene Compliance-Maßnahmen zu identifizieren und auf diese Weise den aktuellen Stand der Compliance-Organisation zu erheben.

- 3) Die Identifikation der aktuell größten Compliance-relevanten Risiken des Unternehmens:

Zu diesem Zweck werden die unterschiedlichen Bereiche bzw. Prozesse des Unternehmens betrachtet und deren immanente Risiken für das Unternehmen identifiziert. Dabei erfolgt eine Identifikation der Compliance-relevanten Schwachstellen im Unternehmen, die akuten Handlungsbedarf auslösen.

- 4) Die Unterbreitung von individuellen Handlungsempfehlungen:

Dieses Dokument unterbreitet konkrete Handlungsempfehlungen für den Aufbau und die Fortentwicklung eines Compliance-Management-Systems. Neben den Maßnahmenvorschlägen im Selbst-Check befinden sich in diesem Dokument nähere Hinweise für die Umsetzung der einzelnen Maßnahmen.

4.3 Grundsätze für den Selbst-Check

Bei der Anwendung dieses Dokuments müssen folgende Grundsätze beachtet werden:

- Die durchführende Person agiert unabhängig im Unternehmen und begleitet das Compliance-Management-System federführend.
- Die im Zuge des Selbst-Checks erfragten Informationen sollten nach bestem Wissen und Gewissen angegeben werden. Üblicherweise sind die Daten für den Selbst-Check nicht in einem zentralen Dokumentenma-

nagement abgelegt, sondern lagern in unterschiedlichen Abteilungen. Bei Erhebung der erfragten Informationen kann es daher notwendig werden, weitere Mitarbeitende des Unternehmens einzubeziehen.

- Der Selbst-Check darf nicht dazu verwendet werden, Dritte über den aktuellen Stand des Compliance-Management-Systems zu täuschen.
- Die Einhaltung der Grundsätze dieses Dokuments wird mit einer Unterschrift bestätigt.

4.4 Identifikation der vorhandenen Prozesse im Unternehmen

4.4.1 Allgemeines

Bevor mit der Ermittlung konkreter Compliance-Risiken begonnen werden kann, ist es von zentraler Bedeutung, die aktuellen Prozesse (siehe 3.12) des Unternehmens zu betrachten.

In Unternehmen laufen zahlreiche unterschiedliche Prozesse ab. Diese werden typischerweise nach der Art der jeweiligen Tätigkeit unterschieden. Operative Prozesse (Geschäftsprozesse, Wertschöpfungsprozesse, Kernprozesse) bilden die primäre Geschäftstätigkeit eines Unternehmens ab und sind auf die Organisationsziele ausgerichtet. Bezeichnend für operative Prozesse sind der hohe Wertschöpfungsanteil, die direkte Ausrichtung auf den externen Kunden und die wettbewerbskritische Abgrenzung zur direkten Konkurrenz. Damit operative Prozesse im Unternehmen gut funktionieren, gibt es die sogenannten Unterstützungsprozesse (Supportprozess, Serviceprozess), welche zwar keinen oder nur einen sehr geringen Anteil an der Wertschöpfung des Unternehmens haben, aber dafür zentrale Schnittstellen zu anderen Prozessen darstellen. Ohne sie kann das Unternehmen keinen Mehrwert generieren. Die Effektivität und Effizienz von operativen Prozessen ist stark von der Ausgestaltung der Unterstützungsprozesse abhängig, da diese u. a. die Ressourcen zur Verfügung stellen und die Betriebsbereitschaft im Unternehmen sicherstellen. Je nach Unternehmen kann zwischen Unterstützungs- und Kernprozessen nicht immer eindeutig unterschieden werden, da die Wertschöpfung immer individuell vom Unternehmensziel abhängig ist. Deshalb ist es möglich, dass bei unterschiedlichen Unternehmen der gleiche Prozess auf der einen Seite direkt wertschöpfend ist und auf der anderen Seite lediglich indirekt zur Wertschöpfung beiträgt. Ein Beispiel dafür ist die Personalbeschaffung für einen Personaldienstleister im Vergleich zu einem Industrieunternehmen. Ein konstruktives Zusammenspiel aller Prozesse kann ausschließlich durch aktive Steuerungsprozesse sichergestellt werden. Alle Planungs- und Kontrollaufgaben im Unternehmen werden durch Steuerungsprozesse (Managementprozesse, Führungsprozesse) initiiert und liefern Anweisungen, Regeln und Praktiken für die Kern- und Unterstützungsprozesse des Unternehmens. Im Folgenden werden alle Prozesse kurz vorgestellt. Bei den hier vorgestellten Prozessen handelt es sich um exemplarische Musterprozesse, die von der eigenen Unternehmenspraxis abweichen können. Allgemeine Fragestellungen werden in Tabelle A.2 des Selbst-Checks in Bezug genommen. Eine allgemeine Einführung wird in Tabelle A.1 gegeben.

4.4.2 Steuerungsprozess/Managementprozess

Steuerungsprozesse regeln das Zusammenspiel aller Geschäftsprozesse. Sie sind die unternehmerische Klammer über alle leistungserstellenden und unterstützenden Prozesse. Sie sorgen für eine zielorientierte Struktur des gesamten Unternehmens. Ein klassischer Steuerungsprozess – auch Managementprozess genannt – setzt sich dabei aus unterschiedlichen Funktionen zusammen. Diese zentralen Funktionen sind die Unternehmensplanung, die Organisation innerhalb des Unternehmens, die Personaleinsatzplanung sowie die Führung und Kontrolle. Aber auch Themengebiete wie eine Vertriebsstrategie, die Budgetierung, das Risikomanagement und Compliance fallen in den Bereich der Steuerungsprozesse. Da die Steuerungsprozesse innerhalb des Unternehmens sehr vielfältig und individuell sind, wird an dieser Stelle auf eine weitere Ausdifferenzierung verzichtet. Managementprozesse werden in Tabelle A.3 des Selbst-Checks in Bezug genommen.

4.4.3 Wertschöpfungsprozess

4.4.3.1 Allgemeines

Mit einem **Wertschöpfungsprozess** wird das Ziel verfolgt, einen Mehrwert für das Unternehmen zu generieren. Den Mehrwert bietet dabei die zielgerichtete Erstellung eines vorher definierten Produktes. Produkte können dabei sowohl Waren als auch Dienstleistungen sein, dies ist abhängig von der Branche des Unternehmens.

Der Wertschöpfungsprozess sollte nach klar definierten Abläufen mit klar beschriebenen Aufgaben stattfinden. Diese Prozesse kennzeichnen das Wesen des Unternehmens. Sie sind in der Regel wettbewerbskritisch und bilden Leistungserstellungsprozesse ausgehend von den Wünschen der Kundschaft bis hin zu der von der Kundschaft wahrgenommenen Auslieferung bzw. Leistungserbringung ab. Wertschöpfungsprozesse werden in Tabelle A.6 des Selbst-Checks in Bezug genommen.

BEISPIEL Wertschöpfungsprozesse können die Auftragsbearbeitung, Produktentwicklung, Produktion sowie Distribution der dazugehörigen Services sein.

4.4.3.2 Einkaufsprozess

Der **Beschaffungs- oder Einkaufsprozess** ist eine Funktion im Unternehmen, die sich mit dem Einkauf und der Beschaffungslogistik von Materialien für den Wertschöpfungsprozess befasst. Dabei ist das Ziel, eine bedarfsgerechte und wirtschaftliche Versorgung mit Waren für das Unternehmen sicherzustellen. Am Ende des Beschaffungsprozesses ist die richtige Ware (das Beschaffungsobjekt) in der korrekten Menge, in einer zufriedenstellenden Qualität und zu wirtschaftlichen Kosten, zum passenden Zeitpunkt am richtigen Ort. Bei einem Handelsunternehmen handelt es sich bei diesem Prozess um die Beschaffung der Waren, die für den Weiterverkauf gebraucht werden. Ein Beschaffungsprozess umfasst dabei im Wesentlichen die vorangehende Recherche der zu beschaffenden Produkte, die Ausschreibung und Prüfung der Angebote, die Preisverhandlungen und die Auswahl des Lieferanten für das Unternehmen. Einkaufsprozesse werden in Tabelle A.4 des Selbst-Checks in Bezug genommen.

4.4.3.3 Produktionsprozess

Ein **Produktionsprozess** ist der Vorgang der betrieblichen Leistungserstellung und damit Kern der Wertschöpfung eines Unternehmens. Formal wirken dabei technologisch, zeitlich und örtlich bestimmte Produktionsfaktoren in einer Kombination zur effizienten Herstellung einer bestimmten Gütermenge in bestimmter Qualität zusammen. Durch einen festgelegten Ablauf werden Rohstoffe verarbeitet und direkt oder über Zwischenprodukte zu einem verkaufsfähigen Produkt. Der Produktionsprozess steht im engen Zusammenhang mit den Beschaffungsprozessen, den logistischen Prozessen des Unternehmens sowie den Vertriebsprozessen, aber auch den vorgelagerten Prozessen wie Forschung und Entwicklung, sowie einer umfassenden Planung durch das Management.

4.4.3.4 Vertriebsprozess

Der **Vertriebsprozess** beschreibt den Verkauf der Produkte oder Dienstleistungen vor und nach dem Produktionsprozess. Dabei umfasst er unterschiedliche Schritte, wie die Akquisition von Kundschaft, die Auswahl geeigneter Vertriebskanäle, aber auch die Stärkung der Bindung sowie Rückgewinnung ehemaliger Kundschaft. Vertriebsprozesse werden in Tabelle A.5 des Selbst-Checks in Bezug genommen.

4.4.4 Unterstützungsprozesse

4.4.4.1 Allgemeines

Unterstützungsprozesse oder auch Service- oder Supportprozesse haben keinen oder nur einen sehr geringen Wertschöpfungsanteil. Sie offerieren Querschnittsleistungen für andere Prozesse. Die Wertschöpfung des Unternehmens ist ohne sie nicht durchführbar. Diese Prozesse tragen zwar nicht aktiv zur Wertschöpfung bei und werden von der Kundschaft nicht aktiv wahrgenommen, sind aber dennoch wichtiger Bestandteil des Unternehmens und dürfen daher nicht vernachlässigt werden. Obwohl die Kundschaft die Unterstützungsprozesse nicht erkennen kann, haben sie in der Regel einen großen Einfluss auf die Zufriedenheit.

BEISPIEL Als Unterstützungsprozesse sind die Finanzbuchhaltung, die Kostenrechnung, das Berichtswesen oder das Personalwesen sowie das Marketing anzuführen.

4.4.4.2 Personalprozess

Ein **Personalprozess** ist auf das betriebliche Personalwesen ausgerichtet. Der Personalprozess eines Unternehmens umfasst ganz unterschiedliche Bereiche. Es sind verschiedene kleine Abläufe notwendig,

die den gesamten Personalprozess des Unternehmens vervollständigen. So kann dieser Prozess aus den Funktionen Personalbedarfsplanung, Personalbeschaffung, Personaleinsatz, Personalbindung und Personalfreisetzung bestehen. Der Personalprozess ist keine reine Verwaltungsfunktion, sondern vielmehr leistet der Personalprozess einen zentralen Beitrag zum Unternehmenserfolg. Der Personalprozess wird in Tabelle A.7 des Selbst-Checks in Bezug genommen.

4.4.4.3 Logistikprozess

Der **Logistikprozess** beschreibt zum einen den Weg der Ware vom Abschluss der Produktion bis zur Kundschaft mit anschließender Kontrolle. Zum anderen sind der Wareneingang, die Anlieferung, die Einlagerung, die Zulieferung (der interne Warenfluss) und die Lagerhaltung Teil dieses Prozesses. Um Waren effizient bereitstellen zu können und die Wünsche der Kundschaft zu erfüllen, benötigt das Unternehmen einen gut strukturierten Logistikprozess. Logistikprozesse werden in Tabelle A.9 des Selbst-Checks in Bezug genommen.

4.4.4.4 Prozesse einer Finanzabteilung

Auch wenn die **Finanzprozesse** des Unternehmens als Unterstützungsprozesse definiert werden, gelten sie als das Rückgrat des Unternehmens. Dabei werden alle Einnahmen und Ausgaben des Unternehmens vollständig erfasst. Es werden Budgets für die unterschiedlichen Unternehmensbereiche erstellt sowie kontrolliert. Zwei Finanzprozesse sind hier besonders wichtig. Die Debitorenbuchhaltung ist ein wesentlicher Teilbereich der Finanzbuchhaltung von Unternehmen. Diese beschäftigt sich mit der Erfassung und Verwaltung der Forderungen und Gutschriften sowie der Begleichung der offenen Posten aus den Lieferungen und sonstigen Leistungen des Unternehmens. Dieser Teil der Finanzbuchhaltung bearbeitet also die Kundschaft betreffende Geschäftsvorfälle. Die Hauptaufgabe der Kreditorenbuchhaltung ist hingegen die Bearbeitung der kreditorischen Eingangrechnungen. Finanzprozesse werden in Tabelle A.10 des Selbst-Checks in Bezug genommen.

BEISPIEL Zur Kreditorenbuchhaltung zählen Tätigkeiten wie Kreditorenstammsatzpflege, Rechnungsprüfung und Kontierung, Erfassung (Buchung) der eingehenden Rechnungen und Gutschriften, die Offene-Posten-Verwaltung, die Veranlassung der Zahlung (unter anderem auch Anzahlung und Vorauszahlung), die Archivierung sowie auch das allgemeine Berichtswesen im Kreditorenbereich.

4.4.4.5 IT-Prozess

Der **IT-Prozess** vereint alle Prozesse des Unternehmens digital. Zudem bietet dieser eine wichtige Schnittstelle zu Kundschaft und Lieferanten. Der übergeordnete IT-Prozess umfasst demnach viele einzelne Prozesse. Dabei stehen beispielsweise die Beschaffung von Technologie, die Auswahl und Bewertung der Technologien, die Prozessstrukturierung und -verbesserung, die Sicherheit sowie das Einhalten von Richtlinien und Normen im Fokus. Daher ist es von zentraler Bedeutung, die IT-Prozesse des Unternehmens regelmäßig zu betrachten und eventuelle Anpassungen vorzunehmen. IT-Prozesse werden in Tabelle A.8 des Selbst-Checks in Bezug genommen.

4.5 Auswertung der Ergebnisse des Compliance-Selbst-Checks

Bei der Beantwortung der insgesamt 31 Fragen zu dem eigenen Unternehmen und den vorhandenen Compliance-Maßnahmen innerhalb des Unternehmens sollen die wesentlichen Schwachstellen des Unternehmens im Bereich Compliance ermittelt werden. Die Fragen beginnen mit der grundsätzlichen Unternehmensstruktur und folgen dann den unterschiedlichen Prozessen innerhalb des Unternehmens. Jede Frage wird auf einer Skala von 1 bis 10 beantwortet. Je höher die Punktzahl bei einer Frage, desto mehr Handlungsbedarf besteht in diesem Bereich. Die entsprechenden Maßnahmen sind neben der entsprechenden Frage stichpunktartig angeführt. In Abschnitt 7 sind die Maßnahmen ausführlich aufgeführt und es werden erste Handlungsempfehlungen gegeben. Ebenfalls gibt es bei jeder Frage Hinweise, welche Risiken es bei den entsprechenden Fragen zu beachten gibt. Die Antwortoptionen sind Richtwerte, um einen ersten Eindruck von der aktuellen Situation des Unternehmens zu erhalten. Es können mittels des Compliance-Selbst-Checks erste Schritte bei dem Ausbau und der Verbesserung des eigenen Compliance-Management-Systems vorgenommen werden, dieser darf aber nicht als vollständige Absicherung betrachtet werden.

Unternehmen, die im Zuge der Beantwortung des Selbst-Checks positive Ergebnisse in Bezug auf das Compliance-Management-System erzielen konnten und denen daher keine konkreten Handlungsemp-

fehlungen in Form von Maßnahmen unterbreitet werden, sollten kontinuierlich an dem erreichten Level weiterarbeiten.

Dieser Selbst-Check für Unternehmen trägt dem Gedanken Rechnung, dass die Einrichtung und Pflege eines Compliance-Management-Systems Daueraufgaben sind. Mit der einmaligen Bewertung des Systems ist es nicht getan. Vielmehr sind Compliance-Management-Systeme kontinuierlich auf ihre Angemessenheit zu überprüfen, anzupassen und weiterzuentwickeln.

5 Empfehlungen an ein Compliance-Management-System für kleine und mittelständische Unternehmen

Kleine und mittelständische Unternehmen zeichnen sich durch typisierbare interne Prozesse aus. Aus diesen Prozessen lassen sich die für das Unternehmen relevanten Compliance-Risiken ableiten. Darauf aufbauend lassen sich zahlreiche typische, in den Prozessen des Unternehmens wurzelnde Compliance-Risiken mit Hilfe konkreter Compliance-Maßnahmen angemessen adressieren. Diese Analyse wird durch den Compliance-Selbst-Check unterstützt.

Kleine und mittelständische Unternehmen zeichnen sich gegenüber Großunternehmen und Konzernen durch eine Besonderheit aus, die sich insbesondere auf die Compliance-Anforderungen auswirkt. In mittelständischen Unternehmen lebt die Unternehmensleitung bestimmte „Werte“ – nicht harte „Verhaltensregeln“ – vor und „transportiert“ diese direkt in die Belegschaft. Deshalb ist es wichtig, dass Compliance-Regelwerke für kleine und mittelständische Unternehmen einfache und praktikable Lösungen vorhalten, die dieser unmittelbaren Kommunikation und Unternehmenskultur gerecht werden. Regelwerke sind deshalb nach Möglichkeit konkret und einfach zu halten. Sie müssen sich schnell und unkompliziert vermitteln lassen und der Unternehmenskultur in Form und Tonalität entsprechen.

Aus diesem Grund sollten Compliance-Richtlinien bei KMUs nach Möglichkeit nur die „Leitplanken“ skizzieren und keine allzu differenzierten Verhaltensanforderungen definieren. Vielmehr sollte das gebotene Verhalten plakativ und in einfachen, wenigen Worten auf den Punkt gebracht werden. Der Fokus sollte darauf gelegt werden, ein angemessenes „Compliance-Bauchgefühl“ bei den Mitarbeitenden zu fördern. Der Schwerpunkt der Compliance-Maßnahmen liegt daher auf kommunikativen und weniger auf regulatorischen Elementen, wie man sie in Konzernstrukturen findet. Mittelstands-Compliance verträgt im Gegensatz zu Compliance-Organisationen in Groß- und Konzernunternehmen nur ein geringes Maß an Komplexität. Bei der Einrichtung der Compliance-Organisation ist daher darauf zu achten, dass die Arbeitsfähigkeit des Unternehmens nicht eingeschränkt wird.

6 Risikoanalyse/Scoping des Unternehmens — Beschreibung der relevanten Risiken

6.1 Allgemeines

Ein Unternehmen ist unterschiedlichen Risiken ausgesetzt. Diese können je nach Branche variieren. Um ein effektives Compliance-Management-System implementieren zu können, sollte das Unternehmen sich seiner einzelnen Risikobereiche bewusst sein. Übergeordnet unterliegt die Geschäftsleitung Aufsichts- und Organisationspflichten. Die Aufsichts- und Organisationspflichten umfassen die Auswahl und Überwachung von Aufsichtspersonen, die Durchführung von Kontrollen/Stichproben, die Erhaltung des funktionsgerechten Zustandes von Betriebsmitteln und die genaue Verteilung von Verantwortlichkeiten. Ziel der Aufsichts- und Organisationspflichten ist die Erreichung eines gefahrlosen Ablaufs der betrieblichen Prozesse.

6.2 Arbeitsstrafrecht

Arbeits- und Betriebssicherheit betrifft die Sicherstellung einer sicheren Arbeitsumgebung und den Schutz der Gesundheit der Beschäftigten. Dazu gehören Aspekte wie die Regelung von Arbeitszeiten, Pausenzeiten und der Umgang mit besonders schutzbedürftigen Arbeitnehmern. Die Betriebssicherheit bezieht sich auf den sicheren Umgang mit Arbeitsmitteln wie Werkzeugen, Geräten und Maschinen. Illegale Beschäftigung umfasst die Beschäftigung von Arbeitnehmern ohne erforderliche Arbeits- oder Aufenthaltserlaubnis sowie die nachhaltige Beauftragung solcher Personen mit Arbeiten. Unter sozialen Schutz fallen die ordnungsgemäße Anmel-

derung von Arbeitnehmern und die Erfüllung sozial- und steuerrechtlicher Pflichten. Dies schließt auch den Umgang mit Scheinselbständigkeit und die korrekte Abführung von Sozialversicherungsbeiträgen ein. Beispielsweise das Strafgesetzbuch (StGB) und die Abgabenordnung (AO) sehen strafrechtliche Sanktionen für die nicht ordnungsgemäße Abführung von Sozialversicherungsbeiträgen sowie für die Hinterziehung von Steuern im Zusammenhang mit Arbeitsentgelt vor.

Zudem umfasst dieser Bereich die Einhaltung von Mindestlohnvorschriften und Regelungen zur Arbeitnehmerüberlassung. Für die Nichteinhaltung von Mindestlohnvorschriften und die Missachtung von Pflichten im Rahmen der Arbeitnehmerüberlassung sehen das Mindestlohngesetz (MiLoG) sowie das Arbeitnehmerentwengesetz (AEntG) entsprechende Bußgeldtatbestände vor.

Der Schutz von Betriebsverfassungsorganen beinhaltet den Schutz von Betriebsräten und anderen Vertretungsorganen der Arbeitnehmer. Es geht darum, deren Wahl und Tätigkeit vor Beeinträchtigungen zu schützen und Benachteiligungen oder unzulässige Begünstigungen zu verhindern. Der Arbeitnehmerdatenschutz behandelt den korrekten Umgang mit personenbezogenen Daten von Arbeitnehmern. Er umfasst die Grenzen von Überwachungs- und Kontrollmaßnahmen am Arbeitsplatz, wie etwa die auditive oder optische Überwachung, Standortüberwachung oder Kontrolle der Kommunikation von Arbeitnehmern. Diese Bereiche stellen typische Risikofelder im Arbeitsstrafrecht dar, mit denen sich Unternehmen auseinandersetzen sollten, um mögliche rechtliche Konsequenzen zu vermeiden.

BEISPIEL Das Arbeitszeitgesetz (ArbZG) sieht zum Schutz der Belegschaft/des Personals klare Regelungen für die werktägliche (Nacht-)Arbeitszeit einschließlich Pausenregelungen sowie die Sonn- und Feiertagsbeschäftigung vor. Auch sind besonders Schutzbedürftige, wie Schwangere oder Schwerbehinderte im ArbZG besonders geschützt. Im ArbZG ist zudem geregelt, dass eine Missachtung ein Bußgeld zur Folge haben kann.

Die Betriebssicherheit beschreibt als spezielle Überwachungs- und Schutzpflicht den sicheren Umgang der Beschäftigten mit Arbeitsmitteln (Werkzeuge, Geräte, Maschinen oder Anlagen). Beispielsweise sehen das Arbeitsschutzgesetz (ArbSchG) und die Betriebssicherheitsverordnung (BetrSichV) für eine Missachtung der Schutzpflichten strafrechtliche Sanktionen und Bußgelder vor.

6.3 Außenwirtschaftsstrafrechtliche Risiken

Die außenwirtschaftlichen Risiken eines Unternehmens beziehen sich im Wesentlichen auf Verstöße gegen das Exportkontrollrecht. Das Exportkontrollrecht umfasst überwiegend zoll- und steuerrechtliche Vorgaben zum Export von Wissen, Waren und Dienstleistungen sowie Regelungen des Kapital- und Zahlungsverkehrs. Ziel ist es, die nationalen Interessen auch im internationalen Handelsverkehr zu schützen. Verstöße gegen außenwirtschaftliche Vorgaben sind beispielsweise im Außenwirtschaftsgesetz (AWG) sowie in der Außenwirtschaftsverordnung (AWV) mit straf- und ordnungswidrigkeitsrechtlichen Sanktionen belegt.

6.4 Datenschutzrechtliche Risiken

Das Datenschutzstrafrecht umfasst die rechtlichen Risiken, die mit der Verarbeitung personenbezogener Daten in Unternehmen verbunden sind. Es betrifft insbesondere folgende Bereiche:

Bei der Datenverarbeitung verarbeiten Unternehmen in der Regel Daten ihrer Mitarbeitenden, Kunden und Geschäftspartner. Diese Verarbeitung erfolgt zunehmend nicht mehr in unternehmenseigenen Rechenzentren, sondern durch Nutzung von Cloud-Computing-Diensten.

Im Rahmen der internationalen Datenübertragung speichern und verarbeiten Cloud-Dienste Daten oft in verschiedenen Ländern, was zu unterschiedlichen Datenschutzstandards führen kann. In vielen Ländern gibt es gesetzliche Mindestanforderungen an den Datenschutz. Diese Standards zielen in der Regel darauf ab, die personenbezogenen Daten aller Stakeholder angemessen zu schützen. Bei Nichteinhaltung der geltenden Datenschutzstandards können Unternehmen mit verschiedenen Sanktionen konfrontiert werden: Im Bundesdatenschutzgesetz (BDSG) sowie in der Datenschutz-Grundverordnung (DSGVO) sind beispielsweise verschiedene Straf- und Ordnungswidrigkeitentatbestände normiert. Die Implementierung angemessener IT-Sicherheitssysteme ist ein wesentlicher Bestandteil des Datenschutzes. Unternehmen, die es versäumen, ausreichende Sicherheitsmaßnahmen zu ergreifen, können nicht nur gegen allgemeine Organisations- und Aufsichtspflichten verstoßen, sondern verwirklichen möglicherweise auch im Strafgesetzbuch (StGB) normierte Tatbestände.

Die Unternehmensleitung trägt in der Regel die Verantwortung für die Einhaltung der Datenschutzbestimmungen. Diese Aspekte stellen typische Risikofelder im Datenschutzstrafrecht dar.

6.5 Geheimnisschutzstrafrecht

Der Schutz von unternehmenseigenen und unternehmensfremden Geheimnissen ist unter anderem für die Sicherung des unternehmerischen Know-hows und dadurch des Unternehmensvermögens ein wichtiger Bestandteil eines Compliance-Management-Systems. Geschützt sind Geschäftsgeheimnisse vor unerlaubter Erlangung, Nutzung oder Offenlegung von Geschäftsgeheimnissen. Das Geschäftsgeheimnisgesetz (GeschGehG) sieht strafrechtliche Sanktionen für Zuwiderhandlungen vor.

Insbesondere Unternehmen mit einer hohen Fluktuation von Mitarbeitenden oder einem hohen Innovationspotential sind von den Risiken im Bereich der Geschäftsgeheimnisse betroffen. Eine ständig wechselnde Belegschaft führt zu einer wachsenden Zahl der Informierten und somit zu einem erhöhten Risiko der Informationsoffenbarung.

6.6 Risiken in Bezug auf Geldwäsche

Geldwäsche bezieht sich im Allgemeinen auf Aktivitäten, die darauf abzielen, die illegale Herkunft von Vermögenswerten zu verschleiern. Dies kann das Verbergen, Verschaffen, Verwahren oder mit Vereitelungsabsicht ausgeführte Umtauschen, Übertragen oder Verbringen von rechtswidrig erlangten Vermögenswerten umfassen. Unternehmen mit vielen unterschiedlichen Transaktionen, insbesondere solche mit einem großen Anteil an Bargeldgeschäften, weisen ein erhöhtes Risikopotenzial auf. Im Bereich der Geldwäsche existieren besondere Organisationsanforderungen.

BEISPIEL Zu den organisatorischen Maßnahmen zählen beispielsweise die Durchführung einer regelmäßigen Risikoanalyse sowie die Bestimmung eines Geldwäschebeauftragten.

Bei Nichteinhaltung der Verpflichtungen zur Geldwäscheprävention können Unternehmen mit verschiedenen Sanktionen konfrontiert werden. Im Geldwäschegesetz (GwG) werden Bußgeldvorschriften sowie Verwaltungssanktionen wie Einschränkung oder Entzug von Lizenzen geregelt, sofern gegen Verpflichtungen verstoßen wird. Zudem sieht das Strafgesetzbuch (StGB) in bestimmten Fällen strafrechtliche Sanktionen vor.

6.7 Cyber-Strafrecht

Computerkriminalität (Cybercrime) umfasst unterschiedlichste Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik des Unternehmens oder gegen diese begangen werden. Anders als im Bereich des Datenschutzes handelt es sich im Bereich des Cybercrimes vor allen Dingen um externe Compliance-Risiken.

Häufige Formen von Cyberangriffen umfassen Ransomware: Eine Form von Malware, die Unternehmenssysteme verschlüsselt und Lösegeld fordert. Phishing sind Versuche, sensible Informationen durch gefälschte E-Mails oder Websites zu erlangen. Malware ist eine Schadsoftware, die über E-Mail-Anhänge oder infizierte Websites verbreitet wird. Begünstigende Faktoren sind die zunehmende Nutzung von Endgeräten für private und dienstliche Zwecke, was das Risiko von Cyberangriffen erhöhen kann. Neben Reputationsverlusten und Vermögensschäden durch die Veröffentlichung sensibler Daten durch unbefugte Dritte, sind u. a. im Strafgesetzbuch (StGB) sowie im speziellen IT-Sicherheitsrecht wie dem IT-Sicherheitsgesetz (IT-SiG) oder dem Gesetz über das Bundesamt für Sicherheit und Informationstechnik (BSIG) Sanktionsmöglichkeiten für Unternehmensverantwortliche geregelt.

6.8 Korruptionsrisiken

Die Reichweite der Korruptionsstrafbarkeit erstreckt sich sowohl auf nationale als auch internationale Handlungen. Unternehmen mit internationaler Tätigkeit sollten sich daher mit den geltenden Bestimmungen in den jeweiligen Zielländern vertraut machen. Hauptbereiche der Korruption umfassen den geschäftlichen Verkehr, das Gesundheitswesen, den öffentlichen Dienst sowie die Mandatsträgerkorruption.

Bei den Handlungsformen wird zwischen aktiver Korruption, also Handlungen des Vorteilsgebers wie Bestechung oder Vorteilsgewährung, und passiver Korruption, die Handlungen des Vorteilsnehmers wie Bestechlichkeit oder Vorteilsannahme umfasst, unterschieden. Strafbarkeitsrisiken können offenkundig sein, wie das Versprechen, Anbieten oder Gewähren von Vorteilen für rechtswidrige Handlungen. In manchen Bereichen, insbesondere im öffentlichen Dienst, kann jedoch auch die sogenannte „Klimapflege“ problematisch sein, bei der noch keine konkrete korruptive Austauschbeziehung beabsichtigt ist. Besondere Risikogruppen sind Personen in öffentlichen Funktionen wie Beamte, Richter oder Personen in öffentlich-rechtlichen Arbeitsverhältnissen, aber auch Personen in privatwirtschaftlichen Organisationen, die öffentliche Aufgaben wahrnehmen. Die Abgrenzung zwischen diesen Gruppen kann in der Praxis oft schwierig sein, was das Risiko einer Strafbarkeit erhöht. Neben den Korruptionsdelikten können auch andere Straftatbestände relevant sein, wie beispielsweise die im Strafgesetzbuch (StGB) nominierte Untreue. Im Strafgesetzbuch (StGB) ist etwa auch das Führen von verborgenen Geldbeständen (sog. „Schwarzen Kassen“) mit strafrechtlichen Konsequenzen belegt. Neben strafrechtlichen Sanktionen des Strafgesetzbuchs (StGB) können bei Korruption auch Bußgelder aus dem Ordnungswidrigkeitengesetz (OWiG) eingreifen.

6.9 Lieferkettenhaftung

Die Lieferkettenhaftung ist ein zunehmend wichtiger Aspekt der unternehmerischen Verantwortung, der darauf abzielt, wesentliche Schutzgüter entlang der gesamten Lieferkette zu wahren. Diese Schutzgüter umfassen insbesondere Menschenrechte, Umweltschutz und Rechte von Arbeitnehmenden. Regulatorische Maßnahmen in diesem Bereich betreffen in erster Linie größere Unternehmen, haben aber auch Auswirkungen auf kleinere Unternehmen in der Lieferkette. Für Unternehmen, die direkt von solchen Regelungen betroffen sind, existieren u. a. im Lieferkettensorgfaltspflichtengesetz (LkSG) eine Reihe von Sorgfaltspflichten. Dazu gehören typischerweise die Einrichtung eines funktionierenden Risikomanagements und die Durchführung regelmäßiger Risikoanalysen. Diese Analysen sollten potenzielle Verletzungen von Menschenrechten, negative Umweltauswirkungen und mögliche Verstöße gegen Arbeitnehmerrechte in der gesamten Lieferkette berücksichtigen. Auch die Verabschiedung einer Grundsatzerklärung zu diesen Sorgfaltspflichten sowie die Anwendung von Präventions- und Abhilfemaßnahmen können Teil dieser Pflichten gemäß LkSG sein.

Kleinere Unternehmen, die nicht direkt unter solche Regelungen fallen, können dennoch indirekt betroffen sein. Dies geschieht oft durch die Weitergabe von Anforderungen entlang der Lieferkette, sei es durch freiwillige Übernahme oder durch Verpflichtungen seitens ihrer größeren Geschäftspartner. Auch sie müssen sich daher mit Fragen des Schutzes von Menschenrechten, der Einhaltung von Umweltstandards und der Gewährleistung fairer Arbeitsbedingungen auseinandersetzen. Verstöße gegen Sorgfaltspflichten in der Lieferkette können erhebliche Konsequenzen haben. Im Lieferkettensorgfaltspflichtengesetz (LkSG) sind für die direkt betroffenen Unternehmen Sanktionen von Zwangsgeldern bis hin zu substanziellen Bußgeldern normiert, die sich am Jahresumsatz orientieren können. Indirekt betroffene Unternehmen müssen mit Umsatzeinbußen rechnen, die sich aus Benachteiligungen in Vergabeverfahren oder aus Kürzungen oder gar Abbrüchen von Kundenbeziehungen ergeben können.

Neben den Sorgfaltspflichtverletzungen in der Lieferkette ist für produzierende Unternehmen auch die strafrechtliche Produktverantwortung von Bedeutung. Im Strafgesetzbuch (StGB) sind Sanktionen für Verletzungen von Leib und Leben geregelt, die beispielsweise auch eingreifen können, wenn solche aufgrund von Produktfehlern eintreten. Hier zeigt sich die enge Verbindung zwischen Produktsicherheit und dem Schutz von Menschenrechten und Arbeitnehmerrechten.

Um diesen Risiken zu begegnen, ist es für Unternehmen aller Größen ratsam, sich mit den Anforderungen der Lieferkettenhaftung auseinanderzusetzen. Dies kann die Implementierung von Risikomanagementsystemen, die Durchführung von Lieferkettenaudits, die Schulung von Mitarbeitenden und die Entwicklung von Strategien zur Bewältigung von Menschenrechts-, Umwelt- und Arbeitnehmerrechtsrisiken in der Lieferkette umfassen.

BEISPIEL Besonderes Augenmerk liegt dabei auf Bereichen wie Kinderarbeit, Zwangsarbeit, Diskriminierung, faire Entlohnung, sichere Arbeitsbedingungen, Vereinigungsfreiheit sowie Umweltverschmutzung und nachhaltige Ressourcennutzung.

Eine proaktive Herangehensweise an diese Themen kann nicht nur rechtliche Risiken minimieren, sondern auch zur Verbesserung der Unternehmensreputation und zur Stärkung von Geschäftsbeziehungen beitragen.

Darüber hinaus kann sie einen positiven Beitrag zur nachhaltigen Entwicklung und zum Schutz grundlegender Rechte und Umweltressourcen leisten.

6.10 Umweltstrafrecht

Das Umweltstrafrecht stellt für Unternehmen ein bedeutendes Risikofeld dar, das eine Vielzahl von Aspekten umfasst und weitreichende Konsequenzen haben kann. Unternehmen unterliegen verschiedenen umweltrechtlichen Vorgaben.

BEISPIEL Zu den typischen Delikten im Bereich des Umweltstrafrechts gehören Verunreinigungen von Luft, Gewässern und Boden. Diese können durch verschiedene betriebliche Aktivitäten verursacht werden, sei es durch Emissionen aus Produktionsprozessen, unsachgemäße Lagerung von Materialien oder Unfällen bei der Handhabung von Chemikalien. Auch die unsachgemäße Entsorgung von Abfällen stellt ein häufiges Umweldelikt dar. Hierbei kann es sich um die falsche Trennung, die unerlaubte Ablagerung oder den illegalen Transport von Abfällen handeln. Beispielsweise im Strafgesetzbuch (StGB) sowie im Bundes-Immissionsschutzgesetz (BImSchG) sind ordnungswidrigkeitenrechtliche sowie strafrechtliche Sanktionen für solche Verhaltensweisen vorgesehen.

Ein weiterer wichtiger Aspekt des Umweltstrafrechts betrifft den Betrieb von Anlagen. Im Bundes-Immissionsschutzgesetz (BImSchG) und im Strafgesetzbuch (StGB) ist geregelt, dass das unerlaubte Betreiben von Anlagen, sei es ohne die erforderliche Genehmigung oder unter Missachtung von Auflagen, ordnungswidrigkeitenrechtliche sowie strafrechtliche Konsequenzen haben kann.

Darüber hinaus gibt es in anderen Rechtsordnungen verschiedene Anzeige- und Meldepflichten im Zusammenhang mit international umweltrelevanten Aktivitäten. Die Verletzung dieser Pflichten, sei es durch Unterlassung oder durch falsche Angaben, kann ebenfalls zu Bußgeldern führen. Je nach Branche und spezifischer Unternehmenstätigkeit können zusätzliche, spezielle Anforderungen gelten. Unternehmen, die mit Gefahrstoffen arbeiten unterliegen oft besonderen Vorschriften bezüglich der Handhabung, Lagerung und Entsorgung dieser Stoffe. Auch in Bereichen wie der Energieerzeugung, der Landwirtschaft oder der Bauindustrie können spezifische umweltrechtliche Bestimmungen relevant sein.

6.11 Wettbewerbsstrafrechtliche Risiken/Kartellordnungswidrigkeiten

Im Rahmen unternehmerischer Tätigkeit stellt das Wettbewerbsrecht ein bedeutendes Risikofeld dar, das verschiedene Aspekte des Marktverhaltens umfasst. Es zielt darauf ab, einen fairen und lautereren Wettbewerb sicherzustellen und schützt dabei nicht nur Konkurrenten, sondern auch Konsumenten und die Allgemeinheit.

Ein wesentlicher Bereich des Wettbewerbsrechts betrifft den unlauteren Wettbewerb. Dazu zählt auch, dass das Wettbewerbsverhalten von Unternehmen nicht durch unwahre oder irreführende Angaben geprägt ist. Dies kann sich auf verschiedene Aspekte der Geschäftstätigkeit beziehen, wie etwa Werbeaussagen, Produktbeschreibungen oder Preisangaben. Auch eine übermäßige Belästigung von Marktteilnehmern, sei es durch aggressive Werbemethoden oder aufdringliche Kundenansprache, kann als unlauterer Wettbewerb gelten.

Ein weiterer wichtiger Aspekt des Wettbewerbsrechts betrifft wettbewerbsbeschränkende Praktiken und Absprachen zwischen Unternehmen. Im Rahmen des Konkurrenzkampfes können Unternehmen versucht sein, Vereinbarungen zu treffen oder Verhaltensweisen zu koordinieren, die den Wettbewerb einschränken. Solche Praktiken können verschiedene Formen annehmen, wie etwa Preisabsprachen, Marktaufteilungen oder den Austausch wettbewerbsrelevanter Informationen. Das Gesetz gegen Wettbewerbsbeschränkungen (GWB) sieht Sanktionen für entsprechendes Verhalten vor.

Besondere Aufmerksamkeit verdient der Bereich der Werbung und Vermarktung.

BEISPIEL Im Gesetz gegen den unlauteren Wettbewerb (UWG) sind u. a. Bußgelder für irreführende Werbepraktiken normiert. Dies betrifft nicht nur offensichtlich falsche Aussagen, sondern auch subtilere Formen der Irreführung, wie etwa unvollständige Informationen oder irreführende Darstellungen.

Die Behauptung unwahrer Tatsachen über ein beworbenes Produkt kann nicht nur wettbewerbsrechtliche Konsequenzen haben, sondern ist unter bestimmten Voraussetzungen auch von der im Strafgesetzbuch (StGB) geregelten Betrugsstrafbarkeit erfasst. Die Konsequenzen von Verstößen gegen das Wettbewerbsrecht können erheblich sein. Je nach Schwere des Verstoßes und der jeweiligen Rechtsordnung können sie von Bußgeldern

über zivilrechtliche Schadenersatzforderungen bis hin zu strafrechtlichen Sanktionen reichen. Zudem kann ein Verstoß gegen wettbewerbsrechtliche Bestimmungen zu erheblichen Reputationsschäden für das Unternehmen führen.

7 Handlungsempfehlungen für die Verbesserung des Compliance-Management-Systems (CMS)

7.1 Allgemeines

Nach DIN ISO 37301:2021-11 ist eine vorherige Risikoanalyse des Unternehmens gefordert. Nur wenn die Verantwortlichen die risikoanfälligen Punkte des Unternehmens kennen, können mit Hilfe des CMS die relevanten Risiken gezielt minimiert werden. Hierfür ist es von entscheidender Bedeutung, dass branchenspezifische Risiken in der Analyse berücksichtigt werden.

Compliance-Management-Systeme verfolgen im Wesentlichen drei Schutzrichtungen:

- 1) Prävention (en: Prevent): Die Verhinderung von Compliance-Verstößen durch die Einführung bestimmter präventiv wirkender Maßnahmen und Mechanismen.
- 2) Detektion (en: Detect): Kein CMS ist in der Lage, jeden denkbaren Compliance-Verstoß zu verhindern. Aufgabe eines funktionierenden CMS ist es daher, Compliance-Verstöße aufzudecken.
- 3) Reaktion (en: React): Definition von adäquaten Folgemaßnahmen und Sanktionen für festgestellte Compliance-Verstöße.

Zur Prävention gehört klassischerweise eine passende Aufbauorganisation mit entsprechenden Delegationen sowie Compliance-Schulungen, ein Verhaltenskodex und die Festlegung der Risikoadressierten. Das Aufdecken von Verstößen im Unternehmen wird unterstützt durch ein implementiertes Hinweisgebersystem (siehe 7.3.9), die Einführung des Vier-Augen-Prinzips (siehe 7.3.8) bei risikogeneigten Prozessen sowie die lückenlose Dokumentation der einzelnen Prozesse innerhalb des Unternehmens. Die Reaktion des Unternehmens auf eventuelle Verstöße sollte vor allen Dingen durch regelmäßige Kontrollen des eigenen CMS und – falls notwendig – entsprechende Anpassungen geprägt sein. Zudem sind ein internes Berichtswesen sowie eine entsprechende Risikosteuerung und eine Dokumentation der getroffenen Maßnahmen empfehlenswert.

7.2 Prävention

7.2.1 Kommunikation

ANMERKUNG 1 Das Thema Kommunikation wird in den Fragen 2 und 17 des Selbst-Checks in Bezug genommen.

Kommunikation findet immer zugleich auf verschiedenen Ebenen und in verschiedenen Richtungen statt. Im Compliance-Management hat die interne Kommunikation eine besondere Rolle insbesondere bei der Prävention von Compliance-Verstößen.

ANMERKUNG 2 Die externe Kommunikation gewinnt (erst) in der Detektion von und Reaktion auf Compliance-Verstößen an Bedeutung. Dann geht es darum, Fehlverhalten oder Skandale gegenüber Stakeholdern zu kommunizieren, interne Untersuchungen oder solche der Polizei und Staatsanwaltschaft zu begleiten und schließlich Sanktionen bekannt zu machen und einzuordnen.

Ziel der internen Kommunikation zur Prävention von Compliance-Verstößen ist es, zum einen die Werte des Unternehmens und alle geltenden Regeln einschließlich möglicher Konsequenzen regelmäßig und wiederholend so an die Zielgruppen zu vermitteln, dass die Inhalte von allen Beteiligten verstanden und befolgt werden. Zum anderen gilt es, die in diesem Maßnahmenkatalog beschriebenen Compliance-Maßnahmen anzukündigen, ihren Zweck und ihre Funktionsweise zu erklären sowie in den Gesamtkontext der Compliance einzuordnen.

Um diese Kommunikation erfolgreich umzusetzen, wird empfohlen, sich vorher die folgenden Fragen zu stellen:

- 1) Was genau soll kommuniziert werden? Die genauen Inhalte der Compliance-Kommunikation sollten präzise definiert werden. Dazu gehört es auch zu überlegen, was nicht gesagt werden sollte.
- 2) Wer genau sind die Zielgruppen dieser Kommunikation? Dazu gehört es auch zu überlegen, welche Eigenschaften die Zielgruppe hat, die bei der Vermittlung der Inhalte eine Rolle spielen. Diese Eigenschaften zeigen, wie (siehe 7.2.1, Punkt 4), wann (siehe 7.2.1, Punkt 5) und über welchen Kanal (siehe 7.2.1, Punkt 6) die Inhalte kommuniziert werden müssen, damit sie von der Zielgruppe verstanden werden. Eigenschaften können z. B. Alter, Tätigkeit im Unternehmen (ausschlaggebend für die Relevanz der zu kommunizierenden Inhalte), Bildungsgrad, gesprochene Sprachen, Arbeitszeiten, Mediennutzungsverhalten, Aufenthaltsorte und Laufwege u. a. sein.
- 3) Wer sollte der Absender sein? Dazu gehört es zu klären, auf welcher hierarchischen Ebene der Absender stehen sollte, welche Glaubwürdigkeit er durch Rang und Persönlichkeit hat und welche Beziehung er zur Zielgruppe pflegt.
- 4) In welcher Tonalität soll kommuniziert werden? Handelt es sich bei den Kommunikationsinhalten um Handlungsanweisungen, Empfehlungen oder eine freundliche Erinnerung an die Schulung, an der noch teilgenommen werden muss? Entsprechend sollte die Kommunikation in ihrer Wortwahl und ihrem Duktus angepasst werden.
- 5) Wann sollen die Inhalte vermittelt werden? Neben den gesetzlichen Vorschriften zur rechtzeitigen Kommunikation von Regeln, wird empfohlen zu überlegen, wann der passende Zeitpunkt für die Kommunikation von Compliance-Inhalten gegeben ist. Im besten Fall wird ein Zeitpunkt gewählt, der es der Zielgruppe erlaubt, die Inhalte tatsächlich zu rezipieren, zu verstehen und im besten Fall auch zeitnah das gewünschte Verhalten zu zeigen. Es ist davon auszugehen, dass die stete Thematisierung und Wiederholung von Compliance-Inhalten, die die Zielgruppe nicht überfordert, die Wirkung der Kommunikation verstärkt. Das sog. Onboarding neuer Mitarbeitenden in das Unternehmen ist eine besondere Kommunikationssituation, die sorgfältig begleitet werden sollte, um die neuen Mitarbeitenden nicht zu überfordern, aber gleichzeitig rechtzeitig mit den Werten und Compliance-Regeln im Unternehmen vertraut zu machen.
- 6) Welche Kanäle sollen für die Kommunikation genutzt werden? Die Antwort auf diese Frage leitet sich aus den Fragen 1 bis 5 ab. Nach Überlegungen zu diesen Aspekten sollte deutlich sein, welche Kanäle sich für die Übermittlung der Compliance-Inhalte eignen. Es wird dabei empfohlen, vor allem bereits etablierte Kommunikationskanäle zu bespielen oder neue Kanäle sorgfältig auszuwählen sowie ihre Nutzung intensiv zu bewerben. Es ist bei allem sicherzustellen, dass die kommunizierten Inhalte dort ankommen, wo sie Compliance-Verstöße verhindern sollen.

7.2.2 Tone from the top

ANMERKUNG Das Thema Tone from the top wird in den Fragen 1, 2, 10 und 11 des Selbst-Checks in Bezug genommen.

Der Tone from the Top bezieht sich auf die Haltung und das Verhalten der Führungskräfte eines Unternehmens in Bezug auf Regeln, Vorschriften und ethische Standards. Die Führungsebene sollte ein klares Bekenntnis zu Compliance zeigen und diese Haltung durch ihr eigenes Handeln untermauern. Ein positives und unterstützendes Verhalten der Führungskräfte zum Thema Compliance sendet ein starkes Signal an die Mitarbeitenden, dass die Einhaltung von Regeln und Vorschriften ernst genommen wird und integraler Bestandteil der Unternehmenskultur ist. Das Thema Compliance sollte regelmäßig in Geschäftsführungssitzungen und anderen wichtigen Treffen der Geschäftsleitung aufgenommen werden, um die Relevanz der Thematik zu unterstreichen.

7.2.3 Erarbeitung Verhaltenskodex

ANMERKUNG Das Thema Verhaltenskodex wird in den Fragen 1, 2 und 11 des Selbst-Checks in Bezug genommen.

Ein Verhaltenskodex des Unternehmens definiert zentrale Regeln und Werte eines Unternehmens in schriftlicher Form auf Basis freiwilliger Selbstverpflichtung. Die konkreten Inhalte eines Verhaltenskodex können je nach Unternehmen variieren, aber typischerweise umfassen sie:

- Bestimmung des Geltungsbereichs (intern/extern, Mutter/Tochter);
- Verpflichtung der Geschäftsleitung;
- Unternehmenswerte und -prinzipien;
- Verhaltensregeln und -richtlinien;
- Verweise auf das Schulungswesen;
- Verweise auf das Hinweisgeberschutzsystem;
- Sanktionen;
- Beschreibung der Verantwortlichkeiten im System.

Es wird empfohlen, dass der Verhaltenskodex klar verständlich und relevant für die Mitarbeitenden ist. Er sollte möglichst kurz formuliert und optisch ansprechend gestaltet werden, um die Umsetzung und Einhaltung zu fördern. Zudem ist sicherzustellen, dass alle Mitarbeitenden des Unternehmens Zugriff auf die Inhalte des Dokumentes haben. Bei der Entwicklung wird empfohlen, zunächst den Zweck und die Ziele des Verhaltenskodexes festzulegen, um den Mehrwert für das Unternehmen sicherzustellen. Die Beteiligung relevanter Stakeholder, wie Führungskräfte und Mitarbeitende bei der Entwicklung eines Verhaltenskodex zur Sicherstellung aller Perspektiven ist unumgänglich, damit der Verhaltenskodex einen Mehrwert für das Unternehmen bietet.

7.2.4 Stärkung der Mitarbeitendenbindung/-identifikation und Unternehmenskultur

ANMERKUNG Das Thema Stärkung der Mitarbeitendenbindung/-identifikation und Unternehmenskultur wird in den Fragen 2 und 5 des Selbst-Checks in Bezug genommen.

Die Bindung der Mitarbeitenden an das Unternehmen ist ein zentrales Instrument zur Senkung der Fluktuation. Eine Stärkung dieser kann auf verschiedene Weisen geschehen: Eine offene und transparente Kommunikation zwischen Führungskräften und Mitarbeitenden sollte für eine starke Bindung angestrebt werden. Regelmäßige Meetings, Feedback-Gespräche und Informationsaustausch helfen dabei, ein Gefühl der Zugehörigkeit und Wertschätzung zu schaffen. Mitarbeitende sollten regelmäßig und angemessen für ihre Arbeit und ihren Beitrag zum Erfolg des Unternehmens wertgeschätzt werden. Die Förderung einer gesunden Work-Life-Balance durch flexible Arbeitszeiten, Homeoffice-Möglichkeiten und Urlaubsregelungen trägt dazu bei, dass sich Mitarbeitende wohlfühlen und langfristig mit dem Unternehmen verbunden bleiben. Ein insgesamt positives Betriebsklima, in dem Teamwork, Zusammenarbeit und gegenseitige Unterstützung gefördert werden, trägt dazu bei, dass sich Mitarbeitende mit dem Unternehmen identifizieren. Die Bereitstellung von Weiterbildungs- und Entwicklungsmöglichkeiten zeigt den Mitarbeitenden, dass das Unternehmen in ihre berufliche Entwicklung investiert und sie unterstützt. Karriereperspektiven und Aufstiegsmöglichkeiten innerhalb des Unternehmens motivieren Mitarbeitende dazu, langfristig im Unternehmen zu bleiben und sich weiterzuentwickeln.

7.2.5 Lieferantenkodex

ANMERKUNG Das Thema Lieferantenkodex wird in den Fragen 2 und 16 des Selbst-Checks in Bezug genommen.

Ein Lieferantenkodex ist ein Dokument, das die Erwartungen und Anforderungen eines Unternehmens an seine Lieferanten festlegt. Er dient dazu, sicherzustellen, dass die Zulieferer eines Unternehmens ethisch handeln, gesetzliche Vorschriften einhalten und qualitativ hochwertige Produkte oder Dienstleistungen liefern. Er kann dafür ethische Grundsätze und Verhaltensregeln enthalten.

BEISPIEL Korruption, Bestechung und Diskriminierung verbieten sowie die Einhaltung von Menschenrechten verlangen.

Mit einem Lieferantenkodex können Unternehmen sich dafür engagieren, dass ihre Lieferkette transparent, nachhaltig und verantwortungsbewusst ist. Mit dem Kodex können zu Informationszwecken auch gesetzliche Mindeststandards für Arbeitsbedingungen, wie z. B. die Einhaltung des Mindestlohns, angemessene Arbeitszeiten, Gesundheits- und Sicherheitsvorschriften am Arbeitsplatz oder Verbot von Zwangsarbeit, wiedergegeben werden.

7.2.6 Festlegung von Zuständigkeiten und Kompetenzen

ANMERKUNG Das Thema Festlegung von Zuständigkeiten und Kompetenzen wird in den Fragen 2, 7, 16, 21, 22, 24, 27, 28, 29 und 30 des Selbst-Checks in Bezug genommen.

Das Festlegen von Zuständigkeiten und Kompetenzen für die Compliance im Unternehmen ist entscheidend dafür, dass gesetzliche Vorschriften, Unternehmensrichtlinien und ethische Standards eingehalten werden. Dazu sollte klar definiert werden, wer im Unternehmen dafür verantwortlich ist, dass Compliance-Richtlinien festgelegt und eingehalten werden. Dies können speziell geschulte Mitarbeitende, Compliance-Beauftragte oder Führungskräfte sein. Durch die Festlegung klarer Zuständigkeiten und Kompetenzen im Bereich Compliance sowie durch Schulungen, Überwachung und regelmäßige Überprüfung können Unternehmen sicherstellen, dass sie rechtliche Risiken minimieren, Reputationsschäden vermeiden und langfristig erfolgreich agieren.

7.2.7 Delegation

ANMERKUNG Das Thema Delegation wird in den Fragen 1, 2, 5, 10 und 12 des Selbst-Checks in Bezug genommen.

Es kann sowohl zwischen horizontaler und vertikaler Delegation unterschieden werden als auch zwischen externer und interner Delegation. Die horizontale Delegation bedeutet die Übertragung von Aufgaben, Verantwortlichkeiten und Befugnissen auf Personen oder Teams auf derselben Hierarchieebene innerhalb des eigenen Unternehmens. Entscheidungsbefugnisse werden dabei auf Einzelpersonen oder Teams übertragen, die auf derselben Ebene in der Organisationsstruktur arbeiten. Horizontale Delegation kann dazu beitragen, die Effizienz, Zusammenarbeit und Flexibilität in einer Organisation zu erhöhen, da Entscheidungen schneller getroffen werden können und die Verantwortung auf mehrere Personen verteilt wird. Vertikale Delegation heißt, dass Aufgaben, Verantwortlichkeiten und Befugnisse von einer Hierarchieebene auf die nächste übertragen werden. Sie beschreibt Delegation von Entscheidungsbefugnissen von Führungskräften auf ihre direkten Unterebenen oder Teams.

Vertikale Delegation ist ein wichtiger Bestandteil der Organisationsstruktur, da sie dazu beiträgt, die Effizienz, Kontrolle und Kommunikation in einer Organisation sicherzustellen. Durch die vertikale Delegation können Führungskräfte ihre Aufgaben delegieren und sich auf strategische Entscheidungen konzentrieren, während ihre Mitarbeitende die täglichen operativen Aufgaben übernehmen.

Bei der internen Delegation werden Aufgaben und Verantwortlichkeiten innerhalb des Unternehmens an andere Mitarbeitende oder Abteilungen übertragen. Diese Art der Delegation erfolgt zwischen Mitarbeitenden auf verschiedenen Hierarchieebenen oder innerhalb derselben Abteilung. Sie fördert die Zusammenarbeit, den Wissensaustausch und die Effizienz im Unternehmen. Bei der externen Delegation werden Aufgaben und Verantwortlichkeiten an Externe (Bspw. Dienstleister oder Lieferanten außerhalb des Unternehmens) übertragen. Sie dient der Auslagerung von bestimmten Geschäftsprozessen, wie IT-Services oder Buchhaltung. Externe Delegation ermöglicht es dem Unternehmen, sich auf seine Kernkompetenzen zu konzentrieren, Kosten zu senken und flexibler auf Marktanforderungen zu reagieren.

7.2.8 Schulungen

ANMERKUNG Das Thema Schulungen wird primär in den Fragen 1, 2, 4, 9 und 24 des Selbst-Checks in Bezug genommen.

Schulungen dienen der Prävention von Verstößen, weil die Mitarbeitenden für Regeln sensibilisiert werden. Sie lernen, welche Regeln es gibt und wie sie einzuhalten sind. Auch werden in Schulungen mögliche Sanktionen bei Verstößen aufgezeigt. Ein plausibles Schulungs- oder Trainingskonzept vermittelt den Mitarbeitenden deshalb, was von ihnen erwartet wird. Die notwendigen Inhalte können von Unternehmen zu Unternehmen erheblich variieren. Anhand der Risikolage (vgl. die Ergebnisse der Risikoanalyse) des Unternehmens sollte

unterjährig entschieden werden, welche Gruppen zu welchen Themen geschult oder trainiert werden. Feedback und Fragen zu den Compliance-Regelungen in den Schulungen geben dem Unternehmen die Möglichkeit, auf mögliche Lücken und Missverständnisse zu reagieren und Regeln und Schulungen stetig zu verbessern.

Typische Schulungen/Trainings für die meisten Mitarbeitenden im mittelständischen Unternehmen sind:

- allgemeine Compliance-Bewusstseins Schulungen;
- Antikorruptionsschulung;
- Antikartellschulung;
- Arbeitssicherheitsschulung;
- Schulung zum Umgang mit IT und Daten;
- Durchsuchungsschulung.

Daneben wird empfohlen regelmäßig für einzelne operative Abteilungen Sonderschulungen, etwa Umweltschutz (insbes. REACH, BImSchG) oder finanzrechtliche Schulungen anzubieten. Diese können in Präsenz oder mittels EDV-Tools als Onlineschulung durchgeführt werden. Bei der Durchführung empfiehlt es sich darauf zu achten, eine mit entsprechenden Kompetenzen ausgestattete Ansprechperson zu wählen, die notwendigenfalls auch Rückfragen beantworten kann. Die Schulungsteilnahme der Mitarbeitenden sollte dokumentiert werden. Dies sollte in der Regel in Form von Unterschriftenlisten erfolgen. Schulungen sollten nicht einfach Gesetze darstellen, sondern die Compliance-Regelungen des Unternehmens sowie bestehende Risiken und mögliche unbewusste Verstöße anschaulich erläutern, damit sie in der Belegschaft wirken.

7.2.9 Richtlinien

ANMERKUNG Das Thema Richtlinien wird primär in den Fragen 2, 24 und 29 des Selbst-Checks in Bezug genommen.

Es ist notwendig, dass robuste Regeln auf Basis der Risikolage des Unternehmens erstellt werden. Sie müssen leicht verständlich und praktikabel sein, sollten sich auf das Notwendige beschränken und sollten nicht jeden möglichen Einzelfall regeln. Um einer Überregulierung vorzubeugen, sollten lediglich Sachverhalte geregelt werden, die dies unbedingt erfordern.

Typische Bereiche für Richtlinien in mittelständischen Unternehmen sind:

- Verhaltenskodex: Allgemeine Verhaltensrichtlinien für alle Mitarbeitenden;
- Antikorruptionsrichtlinie: Regeln zur Vermeidung und Meldung von Korruption;
- Antikartellrichtlinie: Regeln zur Verhinderung von Kartellverstößen;
- Datenschutzrichtlinie: Maßnahmen zum Schutz personenbezogener Daten;
- IT-Sicherheitsrichtlinie: Bestimmungen zur Nutzung von IT-Systemen und zum Schutz vor Cyberangriffen;
- Umweltschutzrichtlinie: Vorgaben zum Umweltschutz und zur Einhaltung umweltrechtlicher Bestimmungen;
- Arbeitssicherheitsrichtlinie: Regelungen zur Sicherheit am Arbeitsplatz.

Die Richtlinien müssen von der Geschäftsleitung genehmigt werden und allen betroffenen Mitarbeitenden zugänglich gemacht werden. Dies kann über das Intranet, E-Mail oder in gedruckter Form geschehen. Ein effektives Richtlinienwesen erfordert die regelmäßige Überprüfung und Aktualisierung der bestehenden Richtlinien (Anpassung an gesetzliche Änderungen). Empfehlenswert ist es, sich die Regelungen regelmäßig anzu-

schauen. Es empfiehlt sich, Feedback von den Mitarbeitenden der einzelnen Fachabteilungen einzuholen, um praktische Herausforderungen und Verbesserungspotenziale zu identifizieren. Eine klare Kommunikation und leichte Zugänglichkeit der Richtlinien sind entscheidend für ihre Wirksamkeit. Die Richtlinien sollten in einer für die Mitarbeitenden verständlichen Sprache verfasst werden.

7.2.10 Identifizierung unternehmenseigener/fremder Geschäftsgeheimnisse

ANMERKUNG Das Thema Identifizierung unternehmenseigener/fremder Geschäftsgeheimnisse wird in Frage 13 des Selbst-Checks in Bezug genommen.

Die Identifizierung und der Schutz von Geschäftsgeheimnissen sind für mittelständische Unternehmen von großer Bedeutung, um ihre Wettbewerbsfähigkeit zu erhalten und rechtliche Risiken zu minimieren. Geschäftsgeheimnisse können technische Informationen, Geschäftsstrategien, Kundenlisten oder spezielle Verfahren umfassen.

Wichtige Schritte zur Identifizierung und zum Schutz von Geschäftsgeheimnissen sind die Bestandsaufnahme durch eine systematische Erfassung aller potenziellen Geschäftsgeheimnisse im Unternehmen. Eine Klassifizierung erfolgt durch die Einstufung der identifizierten Informationen nach ihrer Wichtigkeit und Schutzbedürftigkeit. Eine rechtliche Prüfung sollte dann durch die Feststellung erfolgen, ob die Informationen die gesetzlichen Voraussetzungen für Geschäftsgeheimnisse erfüllen. Schutzmaßnahmen, die die Implementierung angemessener technischer und organisatorischer Maßnahmen zum Schutz der Geschäftsgeheimnisse vorsehen, sollten eingeführt werden. Weitere Maßnahmen sind Schulungen, die zur Sensibilisierung der Mitarbeitenden für den Umgang mit vertraulichen Informationen genutzt werden sollen. Es sollte eine regelmäßige Überprüfung und Aktualisierung der Schutzmaßnahmen durchgeführt werden. Besondere Aufmerksamkeit sollte auch dem Umgang mit fremden Geschäftsgeheimnissen gewidmet werden. Dazu gehören klare Richtlinien für Mitarbeitende zum Umgang mit vertraulichen Informationen von Geschäftspartnern oder Kunden. Zudem ist eine sorgfältige Prüfung bei der Einstellung neuer Mitarbeitenden unumgänglich, um unbeabsichtigte Verletzungen fremder Geschäftsgeheimnisse zu vermeiden sowie die Dokumentation der Herkunft von Informationen, um im Zweifelsfall die rechtmäßige Nutzung nachweisen zu können. Die systematische Identifizierung und der Schutz von Geschäftsgeheimnissen helfen Unternehmen, ihr geistiges Eigentum zu sichern, Innovationen zu schützen und rechtliche Risiken zu minimieren.

7.2.11 Offboarding-Prozess

ANMERKUNG Das Thema Offboarding-Prozess wird in Frage 5 des Selbst-Checks in Bezug genommen.

Der Offboarding-Prozess beschreibt den geregelten Ausstieg von Mitarbeitenden aus der Unternehmensstruktur aufgrund von (Eigen-)Kündigung oder anderweitiger Beendigung des Arbeitsverhältnisses. Das Ziel des Offboardings ist es, einen strukturierten Ablauf des Ausstiegsprozesses sicherzustellen und eine positive Atmosphäre zwischen dem Mitarbeitenden und dem Unternehmen zu erreichen. Mit einem gut strukturierten Offboarding-Prozess nimmt das Unternehmen seine soziale Verantwortung wahr und verringert die Gefahr von Image- oder Geheimnisschäden sowie anschließenden Rechtsstreitigkeiten. Der gesamte Prozess sollte ordentlich dokumentiert werden. Unterschieden wird zwischen dem *technischen* und dem *sozio-emotionalen* Offboarding.

Der *technische Offboarding-Prozess* beschreibt den inhaltlich-strukturellen Austritt. Besonders wichtig ist hier der Geschäftsgeheimnisschutz. Das Unternehmen muss dafür sorgen, dass Firmenhardware durch den Mitarbeitenden zurückgegeben und Zutrittsberechtigungen/Kennwörter zu firmeneigenen Systemen deaktiviert werden. Zudem ist ein geregelter Übergabeprozess von Vollmachten oder anderen sensiblen Dokumenten notwendig. Aber auch auf Unternehmensebene wird durch abschließende Entfernung der personenbezogenen Daten des (ehemaligen) Mitarbeitenden aus den unternehmenseigenen Systemen eine technisch reibungslose Trennung vollzogen.

Das *sozio-emotionale Offboarding* beschreibt die Trennung des Mitarbeitenden aus der Sozialstruktur des Unternehmens. Der Mitarbeitende soll sich trotz des Offboardings noch seiner Arbeit verpflichtet fühlen und sein Wissen weitergeben und somit eine hinreichende Arbeitsübergabe ermöglichen. Hierfür empfiehlt es sich, mit dem Mitarbeitenden ein konstruktives Offboarding-Gespräch zu führen.

7.2.12 IT-Vorkehrungen

ANMERKUNG Das Thema IT-Vorkehrungen wird in Frage 6 und 25 des Selbst-Checks in Bezug genommen.

Geeignete IT-Vorkehrungen schützen die Systeme des Unternehmens vor unbefugten internen sowie externen Zugriffen. Zur Sicherstellung eines hinreichenden Schutzes wird dem Unternehmen empfohlen, ein umfassendes IT-Sicherheitskonzept zu erarbeiten. Dieses sollte zum einen klare Vorgaben zur Nutzung der unternehmenseigenen EDV für die Mitarbeitende enthalten und zum anderen eine deutliche und einfach zu verstehende Vorgabe zum Umgang mit Passwörtern und anderen sensiblen (personenbezogenen) Daten machen. Zur Umsetzung eines solchen Sicherheitskonzepts bieten sich für mittelständische Unternehmen zunächst klare Rollen- und Berechtigungszuteilungen in einem entsprechenden System an. Hierbei werden die einzelnen Berechtigungen entsprechend der Geschäftsprozesse den einzelnen Mitarbeitenden zugeordnet. In diesem System empfehlen sich klare und sichere Passwortvorgaben für den Mitarbeitenden. Nutzen Mitarbeitende mobile Firmenhardware, sollten klare Regelungen über die Privatnutzung dieser Geräte getroffen werden. Ist den Mitarbeitenden Home-Office gestattet, sollten Vorgaben beispielsweise zum Umgang mit sensiblen Daten im privaten Raum festgelegt werden.

7.2.13 Vermeidung von Bargeld

ANMERKUNG Das Thema Vermeidung von Bargeld oder Bargeldobergrenze wird in Frage 8 des Selbst-Checks in Bezug genommen.

Bargeldzahlungen sind nicht per se verboten, allerdings potenziell risikobehaftet (Vermögensdelikte, Korruption, Geldwäsche), denn sie hinterlassen keine „Papierspur“. Sofern es das Geschäftsmodell des Unternehmens zulässt, sollte Bargeld vermieden werden oder eine Bargeldobergrenze eingeführt werden. Durch die Einführung eines solchen Verbots kann nicht nur das Risiko des Unternehmens für Vermögens- und Eigentumsdelikte minimiert werden, sondern das Unternehmen kann dadurch auch seine gesetzlichen Pflichten reduzieren.

BEISPIEL Entfall eines Geldwäscherisikomanagements bei Einführung eines Bargeldverbotes.

Die Bargeldobergrenze sollte an das Unternehmen angepasst werden. Dafür sollte das Volumen der Transaktionen geprüft und eine nicht zu niedrige Grenze festgelegt werden, damit der Geschäftsbetrieb nicht gestört wird. Eine zu hoch angesetzte Obergrenze ist hingegen wirkungslos.

7.2.14 Technische und organisatorische Maßnahmen (TOMs)

ANMERKUNG Das Thema Technische und organisatorische Maßnahmen (TOMs) wird in den Fragen 13, 23, 26, 28 und 30 des Selbst-Checks in Bezug genommen.

Die Implementierung von technischen und organisatorischen Maßnahmen (TOMs) ist von entscheidender Bedeutung. Bevor konkrete Maßnahmen ergriffen werden, ist eine gründliche Risikoanalyse unerlässlich. Sie ermöglicht es dem Unternehmen, potenzielle Schwachstellen zu identifizieren und geeignete Maßnahmen zu ergreifen, um Risiken zu minimieren. Dabei besteht ein wesentlicher Schritt darin, den Stand der Technik zu überprüfen, um sicherzustellen, dass die eingesetzten Technologien und Verfahren den aktuellen Anforderungen entsprechen. Dieser Stand sollte bei der Implementierung der TOMs berücksichtigt werden.

Soft- und Hardwaremaßnahmen spielen eine zentrale Rolle.

BEISPIEL Dazu gehören die Installation einer Firewall, die Verschlüsselung von Datenträgern und -transfers sowie eine automatisierte Protokollierung aller Datenbankzugriffe.

Darüber hinaus sollte die Datenerfassung auf ein Minimum beschränkt werden und Methoden wie die Pseudonymisierung genutzt werden, um die Privatsphäre der Betroffenen zu schützen. Ergänzend können auch physische Sicherheitsvorkehrungen erforderlich sein. Neben den technischen Aspekten sind auch organisatorische Maßnahmen von großer Bedeutung. Auch tragen das Registrieren aller Besuchenden, die das Unternehmen betreten, sowie regelmäßige Schulungen der Mitarbeitenden zur Sensibilisierung für Datenschutz- und Sicherheitsfragen zur Stärkung der Informationssicherheit bei. Zuletzt sollte auch die sorgsame Entsorgung von Dokumenten mit sensiblen Daten ein wichtiger Bestandteil organisatorischer Maßnahmen sein. Dabei

geht es mit der Implementierung dieser Maßnahmen nicht nur um den Schutz von persönlichen Daten, sondern auch um die Informationssicherheit des Unternehmens – in dem Fall das Sichern der eigenen Assets. Die Maßnahmen sollten in einem laufenden Prozess stetig aktualisiert werden und an die sich ständig ändernde Risikolage des Unternehmens angepasst werden.

7.2.15 Arbeitszeiterfassung

ANMERKUNG Das Thema Arbeitszeiterfassung wird in Frage 24 des Selbst-Checks in Bezug genommen.

Damit die gesetzlichen Arbeitszeitregelungen eingehalten werden und die Gesundheit der Mitarbeitenden vor möglicherweise unbezahlter Mehrarbeit geschützt wird, wurde in Deutschland im Arbeitsschutzgesetz (ArbSchG) verankert, dass Arbeitgeber ein verlässliches System zur Erfassung der täglichen Arbeitszeit ihrer Mitarbeitenden einführen. Physische und psychische Belastungen lassen sich so reduzieren. Außerdem ermöglicht eine effektive Arbeitszeiterfassung den Mitarbeitenden, ihre sozialen und kulturellen Bedürfnisse besser zu erfüllen. Flexible Arbeitszeiten und die Möglichkeit, Arbeit und Privatleben in Einklang zu bringen, steigern die Zufriedenheit und Motivation der Mitarbeitenden, was für Unternehmen eine höhere Produktivität und geringere Fehlzeiten bedeuten kann. Gerade für KMU, die oft auf das Engagement und die Loyalität ihrer Mitarbeitenden angewiesen sind, kann die Verbesserung der Vereinbarkeit von Beruf, Freizeit und Familie von großem Vorteil sein. Zusammenfassend ist die Arbeitszeiterfassung nicht nur eine gesetzliche Pflicht, sondern auch ein wichtiges Instrument zur Förderung der Gesundheit und Zufriedenheit der Mitarbeitenden. Moderne, digitale Zeiterfassungssysteme können die Erfassung und Auswertung der Arbeitszeiten erheblich erleichtern, wobei das System zu Unternehmensgröße, Digitalisierungsgrad, Digitalisierungsstrategie, Branche und Arbeitszeitmodellen passen sollte. Denkbar sind weiterhin stationäre Systeme, wie die Stempeluhr, per Niederschrift, Excel-Tabelle oder per Smartphone. Diese Systeme können dabei nicht nur eine präzise und zuverlässige Dokumentation bieten, sondern auch flexible und ortsunabhängige Zeiterfassung ermöglichen, was insbesondere in Zeiten von Homeoffice und Remote-Arbeit von Vorteil ist.

7.3 Detektion

7.3.1 Kommunikation

7.3.1.1 Allgemeines

Die Kommunikation zum Aufdecken von Compliance Verstößen kann in Kommunikation nach innen und nach außen unterteilt werden.

7.3.1.2 Kommunikation nach innen

Die Compliance-Detektion bedeutet, dass in Unternehmen verschiedene Formen von Kontrollen und Überwachungen stattfinden. Sie lösen oftmals ein unangenehmes Gefühl bei den kontrollierten Personen aus. Die Maßnahmen können eine Atmosphäre des Misstrauens und der Denunziation im Unternehmen auslösen, dem nur mit gezielter Kommunikation vorgebeugt werden kann. Es wird deshalb empfohlen, jede Maßnahme der Detektion – sofern sie nicht geheim ist oder überraschend stattfinden soll – rechtzeitig anzukündigen. Besonders wichtig ist es, immer wieder die Gründe für die Maßnahmen zu erklären, sie nachvollziehbar zu machen und bestenfalls zu verdeutlichen, dass sie zugunsten des Unternehmens, aber auch zugunsten der Mitarbeitenden erfolgen. Compliance ist immer dazu da das Unternehmen, die Arbeitsplätze, aber auch die Mitarbeitenden, die sich nichts zuschulden kommen lassen, zu schützen.

Bei längeren Maßnahmen ist es hilfreich, die Mitarbeitenden über deren Verlauf zu informieren und Zwischenergebnisse mitzuteilen. Werden bleibende Maßnahmen installiert, sollte immer wieder an die Maßnahmen erinnert werden, um die Nutzung zu unterstützen und so Compliance-Verstöße frühzeitig einzudämmen.

7.3.1.3 Kommunikation nach außen

Von Fall zu Fall kann es sinnvoll sein, auch das Umfeld des Unternehmens über Detektionsmaßnahmen zu informieren.

BEISPIEL Es kann sinnvoll sein, Lieferanten und Kunden über das Bestehen eines Hinweisgebersystems zu informieren, damit auch diese mögliche Verdachtsmomente melden können.

Gerät ein erster Verdacht eines Verstoßes an die Öffentlichkeit, wird empfohlen zu prüfen, ob bereits während der Detektion Maßnahmen der Krisenkommunikation (siehe auch Kommunikation als Teil der Reaktion [siehe 7.4.1]) vorbereitet oder eingeleitet werden sollten.

7.3.2 Regelmäßige Kontrollen

ANMERKUNG Das Thema Regelmäßige Kontrollen wird in den Fragen 1, 2, 14, 15, 20, 21, 22, 23, 25, 26, 27, 28, 29 und 30 des Selbst-Checks in Bezug genommen.

Kontroll- und Überwachungsmechanismen sind Teil der Aufdeckung. Sie sollen sicherstellen, dass Unternehmensrichtlinien eingehalten werden, Risiken für potenzielle Verstöße frühzeitig erkannt werden und die Transparenz insgesamt erhöht wird. Diese Mechanismen können je nach Unternehmensprozess variieren. Die Ergebnisse der Kontroll- und Überwachungsmaßnahmen sollten sorgfältig dokumentiert werden.

BEISPIEL Das Vier-Augen-Prinzip (siehe 7.3.8), Audits (siehe 7.4.2), Hinweisgebersystem (siehe 7.3.9).

7.3.3 Regelmäßige Prozesskontrollen

ANMERKUNG Das Thema Regelmäßige Prozesskontrollen wird in Fragen 2 und 4 des Selbst-Checks in Bezug genommen.

Operative Prozesskontrollen sind spezifische Maßnahmen, die zur Überwachung der Durchführung von Geschäftsprozessen implementiert werden, um hier die Einhaltung von Vorschriften und Richtlinien in Echtzeit sicherzustellen. Sie unterscheiden sich von Kontrollen, die nach Abschluss eines Prozesses erfolgen. Sie ermöglichen sofortige Korrekturen und verhindern potenzielle Verstöße. Durch operative Prozesskontrollen wird sichergestellt, dass potenzielle Probleme sofort identifiziert und behoben werden. Sie fördern die Prävention von Fehlern und Verstößen, erhöhen die Effizienz und tragen zur kontinuierlichen Verbesserung der Geschäftsprozesse bei.

BEISPIEL Operative Prozesskontrollen:

- Vier-Augen-Prinzip: Kritische Entscheidungen werden von mindestens zwei Personen überprüft;
- automatisierte IT-Kontrollen: Softwaresysteme überwachen Transaktionen und überprüfen Aktivitäten auf Anomalien;
- Checklisten: Verfahrensschritte werden anhand von Checklisten abgearbeitet und dokumentiert;
- Qualitätskontrollen: Regelmäßige Stichproben und Inspektionen zur Sicherstellung der Produktqualität;
- Befragung von Mitarbeitenden: Kontinuierliches Feedback der Mitarbeitenden zur Einhaltung von Prozessen und Vorschriften.

7.3.4 Regelmäßige (interne) Kontrollen

ANMERKUNG Das Thema Regelmäßige (interne) Kontrollen wird in den Fragen 2, 7, 17, 18 und 19 des Selbst-Checks in Bezug genommen.

Im Gegensatz zu operativen Prozesskontrollen, die während der Durchführung von Geschäftsprozessen stattfinden, umfassen andere interne Kontrollen Maßnahmen, die regelmäßig oder nach Abschluss bestimmter Prozesse durchgeführt werden. Diese Kontrollen bieten die Möglichkeit einer retrospektiven Bewertung und einer umfassenderen Analyse der Richtlinien- und Vorschrifteneinhaltung.

BEISPIEL Andere interne Kontrollen:

- interne Audits: Regelmäßige Überprüfungen von Prozessen und Systemen durch interne Revisionsteams;
- Finanzkontrollen: Überprüfung von Finanzberichten und Buchhaltungsprozessen zur Sicherstellung der Genauigkeit und Compliance;
- Compliance-Audits: Spezifische Überprüfungen zur Einhaltung gesetzlicher und interner Vorschriften;
- Risikoanalysen: Regelmäßige Bewertung und Überwachung potenzieller Risiken im Unternehmen;
- Befragung von Mitarbeitenden: Erhebung von Feedback zur Einhaltung und Wirksamkeit der Richtlinien und Prozesse;
- Management-Reviews: Regelmäßige Überprüfung des Managements der Unternehmensleistung und Compliance.

7.3.5 Funktionstrennung

ANMERKUNG Das Thema Funktionstrennung wird in den Fragen 14, 15, 16, 18 und 19 des Selbst-Checks in Bezug genommen.

Bestimmte Berechtigungen sollten nicht in einer Person vereint werden. Daher ist es sinnvoll, innerhalb des Unternehmens z. B. die Rechnungserfassung und die Zahlungsfreigabe voneinander getrennt durchzuführen. Dies minimiert das Fehlerrisiko und reduziert die Missbrauchsgefahr. Das Unternehmen sollte zunächst die notwendigen Informationen und die dazugehörigen Trennungsanforderungen identifizieren. Sodann lassen sich klare und nachvollziehbare Richtlinien schaffen, die einfach zugänglich sein sollten.

7.3.6 Aufsicht und Überprüfung

ANMERKUNG Das Thema Aufsicht und Überprüfung wird in Frage 12 des Selbst-Checks in Bezug genommen.

Eine Beauftragung oder auch Delegation ist nur wirksam, wenn der Fortschritt der Erfüllung der delegierten Aufgabe regelmäßig überprüft wird. Diese Überprüfung sollte stichprobenartig und i. d. R. über eine regelmäßige – nicht zwingend schriftliche – Berichterstattung über die Aufgabenerfüllung erfolgen. Wichtige Punkte sollten dokumentiert werden. Regelmäßiges Feedback hilft dem Mitarbeitenden, sich seiner Pflichten bewusst zu sein. Gerade in kleineren Unternehmen sollte der Grad der Formalisierung an dieser Stelle nicht zu hoch sein. Falls Abweichungen oder Mängel festgestellt worden sind, werden Korrekturmaßnahmen ergriffen. Diese können Anpassungen der Aufgabenstellung, zusätzliche Schulungen oder in extremen Fällen die Neuverteilung der Aufgaben bedeuten. Alle Schritte der Aufsicht und Überprüfung, einschließlich der Berichte, Bewertungen und Korrekturmaßnahmen sollten umfassend dokumentiert werden. Dies dient der Transparenz und Nachvollziehbarkeit und stellt sicher, dass alle Maßnahmen im Bedarfsfall nachvollzogen werden können.

7.3.7 Festlegung von Budgets und Budgetkontrollen

ANMERKUNG Das Thema Festlegung von Budgets und Budgetkontrollen wird in den Fragen 7, 28 und 30 des Selbst-Checks in Bezug genommen.

Budgetkontrollen werden eingeführt, um nicht nur finanzielle Stabilität, sondern auch um die Einhaltung von Compliance-Vorgaben sicherzustellen. Budgetkontrollen helfen dabei, sicherzustellen, dass alle Ausgaben den gesetzlichen Bestimmungen, internen Richtlinien und ethischen Standards entsprechen. Dies minimiert das Risiko von Verstößen, die zu rechtlichen Konsequenzen oder finanziellen Verlusten führen könnten.

Für die Einführung von Budgetkontrollen sollte das Unternehmen einen detaillierten Budgetplan erstellen, der auch Compliance-relevante Kostenarten und -vorgaben integriert. Für diese Budgetverantwortlichen muss ein Verantwortlicher im Unternehmen definiert werden. Regelmäßige Audits und die Erstellung von Berichten dienen dazu, Abweichungen zu identifizieren und sicherzustellen, dass alle Ausgaben sowohl budget- als auch regelkonform sind. Der Einsatz von automatisierten Tools ermöglicht eine lückenlose Nachverfolgung und Dokumentation, wodurch die Transparenz und die persönliche Verantwortlichkeit für Transaktionen erhöht werden.

7.3.8 Vier-Augen-Prinzip

ANMERKUNG Das Thema Vier-Augen-Prinzip wird in den Fragen 14, 15, 18 und 19 des Selbst-Checks in Bezug genommen.

Das Vier-Augen-Prinzip dient der präventiven Kontrolle von Arbeitsabläufen innerhalb des Unternehmens. Durch die Beteiligung von mindestens zwei Personen an bestimmten Vorgängen wird das Risiko von Fehlentscheidungen und Manipulationen verringert. Es erhöht die Objektivität von Entscheidungen und stärkt das Vertrauen in diese. Das Vier-Augen-Prinzip kann bei verschiedenen Unternehmensprozessen eine Rolle spielen. Bei der Etablierung ist zu beachten, dass die Entscheidungsträger unabhängig voneinander die Sachlage beurteilen und darüber entscheiden können. Zudem sollte der Entscheidungsträger über die nötige Fachkompetenz verfügen.

7.3.9 Hinweisgebersystem

ANMERKUNG Das Thema Hinweisgebersystem wird in den Fragen 1, 10, 11, 14, 15, 18, 19, 20, 21, 22, 23, 24, 25, 26 und 27 des Selbst-Checks in Bezug genommen.

Zur Aufdeckung von Compliance-Verstößen tragen vielfach Hinweise durch Mitarbeitende maßgeblich bei. Sie nehmen das Fehlverhalten oft als erste wahr und können so frühzeitig einschreiten. Durch ein effektives Hinweisgebersystem werden gegebene Hinweise kanalisiert und einem geordneten Verfahren zugeführt. Die (internen) Meldestellen sollen es ermöglichen, frühzeitig auf Vorgänge reagieren zu können. Außerdem kann ein solches System den Hinweisgebenden die Angst vor unerwünschten Konsequenzen nehmen. Nicht zuletzt haben Hinweisgebersysteme einen abschreckenden Charakter und verringern den Anreiz, sich regelwidrig zu verhalten.

Im Hinweisgeberschutzgesetz (HinschG) ist geregelt, dass Unternehmen ab 50 Mitarbeitenden ein solches Hinweisgeberschutzsystem mit Mindestanforderungen einführen müssen. Das Hinweisgeberschutzsystem sollte zumindest:

- Hinweisgeber über ihre Rechte und Möglichkeiten aufklären;
- den Hinweisgebern die Meldungsabgabe schriftlich oder mündlich und persönlich ermöglichen;
- die Identität des Hinweisgebers stets vertraulich behandeln;
- über das Eingehen der Meldungen den Hinweisgeber innerhalb von sieben Tagen informieren, und
- spätestens nach drei Monaten eine Rückmeldung über das Ergebnis mitteilen.

Ein solches (internes) Meldesystem kann auch durch einen externen Ombudsmann im Auftrag des Unternehmens umgesetzt werden, sofern die jeweils einschlägige Rechtsordnung dies rechtlich zulässt. Es werden Meldungen zu Sachverhalten, die mit einer beruflichen, unternehmerischen oder dienstlichen Tätigkeit in Zusammenhang stehen, erfasst.

Ein Hinweisgebersystem sollte möglichst niedrigschwellig gestaltet werden und zudem Anreize für die Abgabe von Meldungen setzen. Einen solchen Anreiz setzt vor allen Dingen ein vertrauenswürdiger Umgang mit den Informationen voraus. Hinweisgebende sollten ihre Meldungen in guten Händen wissen. Ein funktionierendes System wahrt die Anonymität und lässt sogar Rückfragen von anonymen Hinweisgebenden zu. Sowohl die Bearbeitung eingehender Hinweise als auch die Auswahl angemessener Folgemaßnahmen erfordern hinreichende Fachkunde und Erfahrung. Bei der Implementierung des Systems ist darauf zu achten, dass jeder Hinweis zu Beginn des Prozesses dem passenden Ansprechpartner zugeordnet wird. Nicht jeder Verstoß erfordert eine Weitergabe an den Ombudsmann, manche Hinweise können durch einen internen Verantwortlichen besser gelöst werden. Innerhalb des Unternehmens ist ein einheitliches System empfehlenswert, welches vor allem eine hinreichende Dokumentation und Rückmeldung ermöglicht. Nicht zuletzt ist das Hinweisgeberschutzsystem dafür da, den Hinweisgebenden Anonymität und Schutz zu bieten.

7.3.10 Dokumentation (Verarbeitungsverzeichnis) — Einführung zentrales Dokumentationsmanagement

ANMERKUNG Das Thema Dokumentation (Verarbeitungsverzeichnis) wird in Frage 23 und das Thema Einführung zentrales Dokumentationsmanagement in Frage 17 des Selbst-Checks in Bezug genommen.

Das Verarbeitungsverzeichnis ermöglicht, die Anforderungen der DSGVO zu erfüllen und den Datenschutz effektiv sicherzustellen. Für KMU ist es oft eine Herausforderung, alle Aspekte der Datenverarbeitung im Blick zu behalten und sicherzustellen, dass sie den rechtlichen Anforderungen entsprechen. Das Verarbeitungsverzeichnis bietet eine strukturierte Methode, um alle relevanten Informationen zu sammeln und zu dokumentieren. Durch die klare Benennung aller Verantwortlichen für die Datenverarbeitung, die Angabe der Kontaktdaten und die genaue Beschreibung der Verarbeitungszwecke können KMU sicherstellen, dass ihre Datenverarbeitungstätigkeiten transparent und nachvollziehbar sind. Zudem unterstützt das Verarbeitungsverzeichnis dabei, die Datenschutzbestimmungen einzuhalten und mögliche Risiken zu identifizieren. Indem die Kategorien der betroffenen Personen und der personenbezogenen Daten sowie die Empfängerkategorien genau definiert werden, können potenzielle Schwachstellen erkannt und entsprechende Maßnahmen ergriffen werden, um die Sicherheit der Daten sicherzustellen. In Anbetracht der begrenzten Ressourcen ist es besonders wichtig, effiziente und kostengünstige Lösungen für die Dokumentation der Datenverarbeitung zu finden. Die Möglichkeit, das Verarbeitungsverzeichnis sowohl in schriftlicher als auch in digitaler Form zu führen, erleichtert den Prozess erheblich und ermöglicht es flexibel auf Veränderungen und Aktualisierungen zu reagieren.

7.3.11 Vorfalldokumentation

ANMERKUNG Das Thema Vorfalldokumentation wird in Frage 20 des Selbst-Checks in Bezug genommen.

Die Vorfalldokumentation als Teil der Compliance-Maßnahmen dient dazu, sämtliche Vorfälle, die möglicherweise gegen interne Richtlinien, gesetzliche Vorschriften oder Branchenstandards verstoßen, systematisch zu erfassen, zu analysieren und entsprechende Maßnahmen zur Korrektur oder Vorbeugung zu ergreifen. Diese Dokumentationen sind wichtige Hilfen während interner Untersuchungen.

BEISPIEL Beim Verdacht auf strafbares Verhalten von Mitarbeitenden oder Geschäftspartnern wird eine breite Palette von Ereignissen geprüft, darunter Datenschutzverletzungen, Betrug, Korruption, Verstöße gegen Umweltvorschriften oder arbeitsrechtliche Probleme.

Ein strukturiertes Dokumentationssystem ermöglicht es, potenzielle Risiken frühzeitig zu erkennen und angemessen zu reagieren, bevor größere Probleme entstehen. Dies schließt auch die Einhaltung der rechtlichen Anforderungen zur Dokumentation während des Untersuchungsprozesses ein. Ein effektives Vorfalldokumentationssystem umfasst klar definierte Prozesse und Verantwortlichkeiten. Es ist wichtig, dass Mitarbeitende wissen, wie sie Vorfälle melden können, und dass diese Meldungen vertraulich behandelt werden. Darüber hinaus bieten die Dokumentationen detaillierte Informationen über den Vorfall, seine Ursachen, Auswirkungen und die durchgeführten Maßnahmen. Dies unterstützt die Erfüllung der gesetzlichen Anforderungen zur transparenten Berichterstattung während einer Untersuchung. Die regelmäßige Überprüfung und Aktualisierung der Vorfalldokumentation stellt sicher, dass sie den sich ändernden Compliance-Anforderungen gerecht wird. Trends und Muster in den Unternehmensabläufen, die auf systemische Probleme hinweisen könnten, lassen sich identifizieren und frühzeitig durchbrechen. In diesem Sinne dienen die Dokumentationen nicht nur der Reaktion auf Vorfälle, sondern auch der aktiven Risikominderung und der langfristigen Sicherstellung der Compliance.

7.4 Reaktion

7.4.1 Kommunikation

Ist es im Unternehmen zu einem Compliance-Verstoß gekommen, sollte dies immer auch kommunikativ begleitet werden. Es wird empfohlen, stetig zu prüfen, in welcher Situation, welche Ereignisse und welche Reaktionsmaßnahmen nach innen und außen kommuniziert werden müssen. Szenarien sind zu entwickeln und zu durchdenken, um Konsequenzen frühzeitig zu erkennen und darauf angemessen reagieren zu können. Auch ist

zu berücksichtigen, dass Informationen, die im Unternehmen kommuniziert wurden, auch nach außen dringen können.

Intern sollte mindestens gleichzeitig, wenn nicht sogar vorab bekannt sein, was anschließend auch außerhalb des Unternehmens bekannt wird.

Im Fall eines Compliance-Verstoßes, der möglicherweise von der Presse aufgenommen und in der Öffentlichkeit diskutiert wird, sind frühzeitig Maßnahmen der Krisenkommunikation zu ergreifen. Der Werkzeugkasten hierfür ist so umfangreich, dass an dieser Stelle nur auf entsprechende Fachliteratur und die Beratung durch Experten verwiesen werden kann.

7.4.2 Durchführung von Audits

ANMERKUNG Das Thema Durchführung von Audits wird in Fragen 3, 4 und 10 des Selbst-Checks in Bezug genommen.

Audits sind systematische und unabhängige Überprüfungen der Geschäftsprozesse und -aktivitäten eines Unternehmens. Sie dienen dazu, die Einhaltung von Gesetzen, internen Richtlinien und Best Practices zu überprüfen und mögliche Schwachstellen oder Risiken aufzudecken. Für mittelständische Unternehmen sind Audits ein wichtiges Instrument zur Sicherstellung der Compliance und zur kontinuierlichen Verbesserung der Unternehmensabläufe.

Wesentliche Aspekte bei der Durchführung von Audits:

- **Regelmäßigkeit:** Audits sollten in festgelegten Intervallen durchgeführt werden, um eine kontinuierliche Überwachung sicherzustellen.
- **Unabhängigkeit:** Die Auditoren sollten unabhängig von den zu prüfenden Bereichen sein, um Objektivität sicherzustellen.
- **Fokussierung:** Basierend auf der Risikoanalyse sollten Audits auf besonders relevante oder risikobehaftete Bereiche konzentriert werden.
- **Dokumentation:** Alle Audit-Ergebnisse müssen sorgfältig dokumentiert werden, um Fortschritte nachverfolgen und bei Bedarf Nachweise vorlegen zu können.
- **Maßnahmenableitung:** Aus den Audit-Ergebnissen sollten konkrete Verbesserungsmaßnahmen abgeleitet und umgesetzt werden.

Die Durchführung von Audits kann intern durch geschulte Mitarbeitende oder extern durch spezialisierte Dienstleister erfolgen. Externe Audits bieten oft zusätzliche Expertise und erhöhen die Glaubwürdigkeit der Ergebnisse, während interne Audits kosteneffizienter sein können und ein tieferes Verständnis der Unternehmensabläufe bieten. Ein effektives Audit-Programm hilft Unternehmen, Compliance-Risiken frühzeitig zu erkennen, Prozesse zu optimieren und das Vertrauen von Stakeholdern zu stärken.

BEISPIEL Typische Audit-Bereiche für mittelständische Unternehmen können sein:

- Finanzprozesse und Buchhaltung;
- Datenschutz und IT-Sicherheit;
- Arbeitssicherheit und Gesundheitsschutz;
- Umweltmanagement;
- Lieferkettenmanagement;
- Produktqualität und -sicherheit.

7.4.3 Durchsetzbarkeit und Sanktionen

ANMERKUNG Das Thema Durchsetzbarkeit und Sanktionen wird in Frage 2 des Selbst-Checks in Bezug genommen.

Ein effektives Compliance-Management-System erfordert nicht nur die Festlegung von Regeln und Richtlinien, sondern auch Mechanismen zur Durchsetzung angemessener Sanktionen bei Verstößen. Dies stellt sicher, dass die Compliance-Maßnahmen von allen Mitarbeitenden ernst genommen werden und im Unternehmensalltag wirksam sind.

Ein wichtiger Aspekt der Durchsetzbarkeit von Sanktionen ist eine klare Kommunikation. Es ist notwendig, alle Mitarbeitenden über die geltenden Regeln und die Konsequenzen bei Verstößen zu informieren. Sanktionen sollten fair und einheitlich angewendet werden, unabhängig von der Position des Mitarbeitenden im Unternehmen. Die Schwere der Sanktion sollte dem Grad des Verstoßes angemessen sein. Ein abgestuftes System von Sanktionen sollte vorhanden sein, das von Verwarnungen bis hin zur Kündigung reichen kann. Eine sorgfältige Dokumentation aller Verstöße und der ergriffenen Maßnahmen zur Nachvollziehbarkeit und rechtlichen Absicherung sollte sichergestellt sein. Alle Sanktionen müssen im Einklang mit dem geltenden Arbeitsrecht und anderen relevanten Gesetzen stehen. Neben Sanktionen sollten auch Möglichkeiten zur Korrektur und Wiedergutmachung von Fehlverhalten vorgesehen sein. Zum Schutz von Hinweisgebern sollte die Implementierung eines Whistleblowing-Systems erfolgen, das Mitarbeitende ermutigt, Verstöße zu melden, ohne Repressalien befürchten zu müssen. Für eine effektive Durchsetzung ist es wichtig, dass die Unternehmensführung die Compliance-Maßnahmen vorlebt und unterstützt. Regelmäßige Überprüfungen und Audits helfen, die Wirksamkeit der Durchsetzungs- und Sanktionsmechanismen zu evaluieren und bei Bedarf anzupassen.

Anhang A (informativ)

Compliance-Selbst-Check

Dem Anwender des Compliance-Selbst-Checks ist unbeschadet der Rechte von DIN an der Gesamtheit des Dokumentes die Vervielfältigung der Formblätter in Anhang A gestattet.

Tabelle A.1 — Compliance-Selbst-Check — Einführung

Datum:	
Wiedervorlage:	
Unternehmen:	
Sachbearbeiter:	
Funktion:	
E-Mail-Adresse:	
<p>Gefragt wird in einem ersten Schritt nach den unternehmensinternen Organisationsstrukturen und Risikoszenarien, die prozessübergreifend ein potenzielles Compliance-Risiko für Ihr Unternehmen darstellen können. Neben zentralen Fragen zu der Aufbau- und Ablauforganisation Ihres Unternehmens sind insbesondere Anreizstrukturen in den Blick zu nehmen. Leitfragen sind hier:</p> <p>(1) Bestehen Strukturen und Prozesse in Ihrem Unternehmen, die Compliance-Verstöße wahrscheinlicher machen oder implizieren?</p> <p>(2) Besteht Gelegenheit für Compliance-Verstöße?</p> <p>(3) Gibt es eine Kultur der Rechtfertigung (kleinerer) Regelverstöße?</p>	
<p>Die Bearbeitung des Compliance-Fragebogens soll Ihnen dabei helfen, einen ersten Überblick darüber zu erhalten, welche Strukturen in Ihrem Unternehmen potenziell Gefahren in sich bergen und wenn ja, warum. Der Fragenkatalog hat keinen Anspruch auf Vollständigkeit, sondern sollte um die unternehmensspezifischen Gegebenheiten ergänzt werden. Ggf. werden Ihnen weitere Fragen einfallen, die Sie ergänzen können.</p> <p>Wichtig ist: Bei der Beantwortung der einzelnen Fragen kommt es auf Ihre ehrliche Einschätzung an. Auch werden Ihnen sicherlich nicht alle Informationen vorliegen oder Sie die ein oder andere Information erst einholen müssen, um die einzelnen Fragen beantworten zu können. Machen Sie sich daher im Vorfeld Gedanken dazu, welche Fachbereiche und Mitarbeitenden Sie einbinden müssen.</p> <p>Je stärker diese Faktoren ausgeprägt sind, desto stärker ist das strukturelle Risiko eines Regelverstößes.</p>	<p>Wenn Sie Ihre Risiken kennen, wissen Sie, woran Sie arbeiten müssen. Ausgehend von Ihren Risiken sollten konkrete Maßnahmen entwickelt werden, die das Risiko angemessen adressieren. Sie werden im Rahmen Ihrer Analyse sicherlich mehrere Compliance-Risiken identifizieren. Nicht alle müssen aber sogleich angegangen werden. Sie können und sollten priorisieren.</p>
<p>Je höher der Score Ihrer Ergebnisse, desto größere Risiken konnten identifiziert werden.</p>	

Tabelle A.2 — Compliance-Selbst-Check — Allgemeine Fragen

Allgemeine Fragestellungen	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
<p>0 In wie weit sind die Prozesse bei Ihnen im Unternehmen bereits dokumentiert? Existieren möglicherweise bereits Zertifizierungen? Falls ja, welche?</p>	<p>Hinweis: Bauen Sie auf vorhandenen Strukturen (gelebten Abläufen) auf. Hilfreich ist, wenn Sie zunächst einen Blick auf die Prozesse und die Struktur Ihres Unternehmens werfen. Dabei sollten Sie (sofern vorhanden) folgende Unterlagen zu Rate ziehen:</p> <ul style="list-style-type: none"> — Gesellschaftsstruktur/Organigramm; — Prozesshandbuch und/oder -dokumentation; — Zertifizierungen. 	<p>1 = sehr gut; 10 = gar nicht</p>	<ul style="list-style-type: none"> — Erstellung/Aktualisierung Gesellschaftsstruktur/Organigramm — Prozessaufnahme und -dokumentation
<p>1 Wie ist Ihre Selbsteinschätzung zum Thema Compliance: Sehen Sie Ihr Unternehmen bislang gut aufgestellt?</p>	<p>Hinweis: Bei der Beantwortung dieser Frage sollten Sie auf Protokolle zu Gesellschafterversammlungen, Betriebsversammlungen, Führungskräfte Sitzungen, regelmäßige Meetings oder Jour-Fixe einschließlich Ihrer Jahresabschlussbilanz zurückgreifen. Sie können sich außerdem an folgenden Punkten orientieren:</p> <ul style="list-style-type: none"> — Hat sich die Unternehmensleitung zum Thema Compliance gegenüber den Mitarbeitenden öffentlich erklärt (en: Tone from the top)? — Sind Zuständigkeiten eindeutig und überschneidungsfrei festgelegt und bestehen klare Berichtswege? Ist dies dokumentiert? — Hat das Unternehmen Verhaltensanforderungen an seine Mitarbeitenden in dokumentierter Form und adressatengerechter Sprache kommuniziert (Verhaltenskodex, Compliance-Richtlinien/-handbuch)? — Sind die Mitarbeitenden aus Ihrer Sicht zum Thema Compliance hinreichend sensibilisiert/geschult? — Existieren Kontrollmechanismen zur Sicherstellung der Compliance im operativen Geschäft? — Ist ein Hinweisgebersystem eingerichtet worden, über das Mitarbeitende (ggf. auch außenstehende Dritte) Hinweise auf mögliche Compliance-Verstöße vertraulich melden können? — Wird in regelmäßigen Abständen eine Compliance-Risikoanalyse durchgeführt? Falls ja, schauen Sie sich die Ergebnisse an. Wurden im Nachgang an die Risikoanalyse die internen Compliance-Maßnahmen angepasst? 	<p>1 = sehr gut; 10 = sehr stark ausbaufähig</p>	<ul style="list-style-type: none"> — Tone from the Top der Geschäftsleitung (siehe 7.2.2) — Delegation (siehe 7.2.7) — Erarbeitung Verhaltenskodex (siehe 7.2.3) — Regelmäßige Compliance-Schulungen (siehe 7.2.8) — Einrichtung Kontroll- und Überwachungsmechanismen (siehe 7.3.2) — Einrichtung Hinweisgebersystem (siehe 7.3.9)

Tabelle A.2 (fortgesetzt)

Allgemeine Fragestellungen	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
<p>2 Wie schätzen Sie die Verständlichkeit und Zugänglichkeit der Compliance-Regeln in Ihrem Unternehmen ein?</p>	<p>Hinweis: Hier geht es darum einzuschätzen, ob es Ihnen gelingt, dass sich die Mitarbeitenden an die Regeln halten, sie erkennen, verstehen und befolgen. Wo Regeln zu schwer erreichbar oder wenig verständlich formuliert sind, werden sie wirkungslos. Nicht selten fristen Compliance-Regelwerke ein Schattendasein im Unternehmen, weil sie schwer zugänglich sind oder Mitarbeitende nicht wissen, dass Richtlinien überhaupt existieren.</p>	<p>1 = leicht verständlich; 10 = schwer verständlich/ schwer zugänglich</p>	<p>Überprüfung der Regelwerke (siehe 7.2.9) auf:</p> <ul style="list-style-type: none"> — Relevanz und Aktualität — Einklang mit Unternehmenswerten und -kultur — Klarheit und Verständlichkeit — Einfachheit und Praktikabilität <p>Sicherstellung der Umsetzung durch:</p> <ul style="list-style-type: none"> — Kommunikation (siehe 7.2.1) — Tone from the Top (siehe 7.2.2) — Erarbeitung Verhaltenskodex (siehe 7.2.3) — Stärkung Mitarbeiterbindung (siehe 7.2.4) — Lieferantenkodex (siehe 7.2.5) — Festlegung von Zuständigkeiten und Kompetenzen (siehe 7.2.6) — Delegation (siehe 7.2.7) — Regelmäßige Compliance-Schulung (siehe 7.2.8) <p>Überwachung und Überprüfung durch:</p> <ul style="list-style-type: none"> — Regelmäßige Kontrollen (siehe 7.3.2) — Regelmäßige Prozesskontrollen (siehe 7.3.3) — Regelmäßige (interne) Kontrollen (siehe 7.3.4) — Durchsetzbarkeit und Sanktionen (siehe 7.4.3)
<p>3 Für wie wirkungsvoll halten Sie die Kontrollmechanismen in Ihrem Unternehmen?</p>	<p>Hinweis: Es gibt verschiedene Arten von Compliance-Kontrollmechanismen, die je nach Art und Größe des Unternehmens, der Branche und den spezifischen Risiken variieren können. Präventive Kontrollen zielen darauf ab, Verstöße gegen Compliance-Vorschriften zu verhindern. Erkennende Kontrollen sind hingegen darauf ausgerichtet, potenzielle Verstöße oder Unregelmäßigkeiten aufzudecken (interne Prüfungen, Audits, Überwachungssysteme oder Compliance-Hotlines).</p>	<p>1 = sehr streng; 10 = leicht zu umgehen</p>	<p>Überprüfung der Wirksamkeit von Compliance-Kontrollmechanismen, z. B. durch:</p> <ul style="list-style-type: none"> — (interne/externe) Audits (siehe 7.4.2) — Compliance-Tests — Mitarbeitendenbefragungen

Tabelle A.2 (fortgesetzt)

Allgemeine Fragestellungen	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
<p>4 Wie hoch schätzen Sie das Risiko ein, dass Prozesse, die im Unternehmen geregelt sind, nicht eingehalten werden?</p>	<p>Hinweis: Stellen Sie sich als Hilfestellung hier am besten die Frage, wie Sie eine solche Tat begehen könnten, wenn Sie es wirklich darauf anlegen würden. Daneben ergeben sich Fehlerpotentiale auch aus besonders komplexen Prozessen oder fehlendem Wissen der Prozessbeteiligten.</p>	<p>1 = sehr niedrig; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Erarbeitung Richtlinien und Verfahrensvorgaben (siehe 7.2.9) — Regelmäßige Compliance-Schulungen (siehe 7.2.8) — Compliance-Incentives — Regelmäßige Prozesskontrollen (siehe 7.3.3) — Anlassbezogene Prozess-Audits (siehe 7.4.2)
<p>5 Wie stark ist die Mitarbeitendenfluktuation in zentralen/wichtigen Positionen?</p>	<p>Hinweis: Mitarbeitende, die das Unternehmen im Unfrieden verlassen, nehmen nicht selten Informationen zu Unternehmensstrukturen mit oder erweisen sich als unloyal gegenüber dem alten Arbeitgeber. Unterstellen Sie nicht jedem scheidenden Mitarbeitenden Böses, seien Sie sich aber des Problems bewusst. Außerdem: Ständig wechselnde Mitarbeitende müssen hinsichtlich der sie betreffenden Compliance-Regeln geschult werden. Dafür ist bei hoher Fluktuation oft nur wenig Zeit. Das ist bei der Risikobeurteilung in den Blick zu nehmen.</p>	<p>1 = sehr gering; 10 = sehr stark</p>	<ul style="list-style-type: none"> — Stärkung der Mitarbeitendenbindung/-identifikation und Unternehmenskultur (siehe 7.2.4) — Delegation (siehe 7.2.7) — Offboarding-Prozess (siehe 7.2.11)
<p>6 Gibt es/gab es in der Vergangenheit Ermittlungsverfahren gegen Ihr Unternehmen, dessen Mitarbeitende, die Geschäftsleitung, Gesellschafter, Wettbewerber oder sonstige Unternehmen Ihrer Branche?</p>	<p>Hinweis: In jedem Unternehmen kann es irgendwann zu Compliance-Verstößen kommen. Wichtig ist, dass Sie aus solchen Vorfällen die richtigen Schlüsse für die Zukunft Ihres Unternehmens ziehen („Lesson Learned“). Ermittlungsverfahren verlaufen oft in Wellen. Unternehmen derselben Branche haben oft ähnliche Prozesse und in ihnen schlummern ähnliche Compliance-Verstöße.</p> <p>Außerdem: Ermittlungsverfahren werden durch unterschiedliche Behörden durchgeführt. Neben der Staatsanwaltschaft, der Polizei und den Kartellbehörden führen auch der Zoll und die Datenschutzbehörde Ermittlungen durch.</p>	<p>1 = noch nie; 10 = sehr häufig</p>	<ul style="list-style-type: none"> — Erarbeitung Durchsuchungsleitfaden (siehe 7.2.9) — Regelmäßige Durchsuchungsschulungen (siehe 7.2.8) — IT-Vorkehrungen (siehe 7.2.12)

Tabelle A.2 (fortgesetzt)

Allgemeine Fragestellungen	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
7 In wie weit können einzelne Mitarbeitende über hohe Vermögenswerte im Unternehmen verfügen?	Hinweis: Je größer die Entscheidungsbandbreite eines Mitarbeitenden, desto größer die Gefahrneigung. Das macht Mitarbeitende anfälliger dafür, sich selbst Vorteile zu verschaffen, oder von anderen dazu verleitet zu werden, diese Macht nicht im Sinne des Unternehmens auszuüben. Legt der Gesellschafter- und/oder der Geschäftsführervertrag mitbestimmungspflichtige Vermögensentscheidungen fest?	1 = gar nicht; 10 = sehr einfach	<ul style="list-style-type: none"> — Regelmäßige (interne) Kontrollen (siehe 7.3.4) — Erarbeitung Antikorruptions-Richtlinie (siehe 7.2.9) — Festlegung von Zuständigkeiten/Kompetenzen (siehe 7.2.6) — Festlegung von Budgets und Budgetkontrollen (siehe 7.3.7) — Regelmäßige Antikorruptions-Schulungen (siehe 7.2.8)
8 Wie gut haben Sie sich mit dem Thema Bargeldzahlungen beschäftigt?	Hinweis: Bargeldzahlungen sind nicht per se verboten, allerdings potenziell risikobehaftet (Vermögensdelikte, Korruption, Geldwäsche). Denn sie hinterlassen keine „Papierspur“. Sofern es das Geschäftsmodell zulässt, sollten Bargeldzahlungen nach Möglichkeit untersagt werden, um Compliance-Verstößen vorzubeugen. Sollte dies nicht möglich sein, sind verbindliche Regelungen für den Umgang mit Bargeld zu treffen (insb. Bargeldobergrenze).	1 = sehr gut; 10 = gar nicht	<ul style="list-style-type: none"> — Vermeidung von Bargeld (sofern möglich) oder Bargeldobergrenze (siehe 7.2.13) — Erarbeitung Antikorruptions-Richtlinie (siehe 7.2.9) — Erarbeitung Antigeldwäsche-Richtlinie (siehe 7.2.9)
9 Blicken Sie auf Ihre Branche: Für wie risikogeneigt halten Sie die Branche, in der Sie aktiv sind?	Hinweis: Je nachdem, welches Compliance-Risiko Sie betrachten, sollten Sie auch auf Ihre Branchen und deren Umfeld achten. Es gibt Branchen, die sich in der Vergangenheit als korruptionsanfällig (z. B. Pharma, Maschinen-/Anlagenbau, Baubranche, Gas- und Ölindustrie) oder kartellgeneigt (z. B. Zement- oder Lebensmittelindustrie) erwiesen haben. In anderen Betätigungsfeldern erstreckt sich der Fokus vom Umwelt- bis zum Arbeitsschutz.	1 = gar nicht risikogeneigt; 10 = sehr risikogeneigt	Berücksichtigung Branchenrisiko bei: <ul style="list-style-type: none"> — Risikoanalyse und Umsetzung von Compliance-Maßnahmen — Regelmäßige Compliance-Schulungen (siehe 7.2.8)

Tabelle A.3 — Compliance-Selbst-Check — Managementprozess

Managementprozess	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
<p>Jeder Unternehmensprozess weist für sich genommen besondere Compliance-Risiken auf. Das gilt auch für den Managementprozess. Die Geschäftsleitung gibt die Ziele des Unternehmens aus und formuliert eine Strategie für das Unternehmen. Ihre Aufgabe besteht darin, zu identifizieren, ob und inwiefern Compliance dabei eine Rolle spielt (Stichwort: Tone from the top). Auch müssen Sie das Risiko mitbedenken, dass die Geschäftsleitung selbst Compliance-Verstöße begeht (etwa Straftaten zum Nachteil Ihres Unternehmens, Kartellverstöße oder Datenschutzverstöße, z. B. aufgrund exzessiver Überwachung von Mitarbeitenden).</p>			
<p>10 Wie schätzen Sie das Risiko ein, dass Mitglieder der Geschäftsleitung sich an Straftaten zum Nachteil Ihres Unternehmens beteiligen (z. B. Betrug, Untreue, Diebstahl, Unterschlagung)?</p>	<p>Hinweis: Für die sachgerechte Beantwortung der Frage ist eine Vielzahl an Faktoren relevant. Diese lassen sich häufig auf eine handlungsleitende Motivation, eine innere Rechtfertigung des Täters und die Gelegenheit zur Begehung einer Straftat herunterbrechen. Von Bedeutung sind daher sowohl die unternehmensinternen Strukturen und Prozesse, insbesondere deren Transparenz, aber auch die (nicht) vorhandenen Kontrollen (z. B. der Spesenabrechnung). Daneben spielt auch die Unternehmens-/Compliance-Kultur eine zentrale Rolle. Gibt es eine Kultur der Rechtfertigung (kleinerer) Regelverstöße? Je stärker diese Faktoren ausgeprägt sind, desto stärker ist das strukturelle Risiko eines Regelverstößes.</p>	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Tone from the top (siehe 7.2.2) — Implementierung Hinweisgebersystem (siehe 7.3.9) — Erarbeitung Antikorruptions-Richtlinie (siehe 7.2.9) — Erarbeitung Geldwäsche-Richtlinie (siehe 7.2.9) — Delegation (siehe 7.2.7) — Durchführung von Audits (siehe 7.4.2)
<p>11 Wie schätzen Sie das Risiko ein, dass Mitglieder der Geschäftsleitung sich an illegalen Absprachen mit Wettbewerbern beteiligen?</p>	<p>Hinweis: Verboten sind sowohl wettbewerbsbeschränkende Vereinbarungen und aufeinander abgestimmte Verhaltensweisen als auch der Missbrauch von Marktmacht. Je größer die Marktmacht, desto enger die wettbewerblichen Grenzen im operativen Geschäft. Typischerweise handelt es sich um Preisabsprachen, illegaler Informationsaustausch zwischen Wettbewerbern, Vereinbarungen zur Marktaufteilung, Ausschließlichkeitsvereinbarungen sowie Preis- und Konditionenbindungen. Unzulässiger Austausch von sensiblen Informationen (z. B. zu Preisen) kann genügen. Bei der Risikobetrachtung ist eine Vielzahl an Faktoren zu berücksichtigen. Relevant sind etwa:</p> <ul style="list-style-type: none"> — strategische Kooperationen mit Wettbewerbern oder sonstige personelle Verflechtungen mit Konkurrenzunternehmen; — regelmäßiger Kontakt/Austausch mit Wettbewerbern (z. B. anlässlich von Verbandsveranstaltungen, Messen, Tagungen, Normsetzungsgremien); — Besonderheiten des Marktes, z. B. Vertrieb homogener Massengüter, geringe Marktgröße, oligopolistische Marktstruktur. 	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Tone from the top (siehe 7.2.2) — Erarbeitung/Aktualisierung Verhaltenskodex (siehe 7.2.3) — Erarbeitung Kartellrechts-Richtlinie (siehe 7.2.9) — Implementierung Hinweisgebersystem (siehe 7.3.9)

Tabelle A.3 (fortgesetzt)

Managementprozess	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
12 Wurden gesetzlich vorgeschriebene Zuständigkeiten (z. B. Datenschutz-, Geldwäsche-, Umweltschutz-, Immissionsschutz-, Abfall-, Gefahrgut-, Menschenrechtsbeauftragte, Fachkraft für Arbeitssicherheit, Betriebsarzt usw.) im Unternehmen festgelegt?	Hinweis: Je nach Größe und Gegenstand des Unternehmens besteht mitunter eine gesetzliche Verpflichtung, bestimmte Betriebsbeauftragte zu bestellen, die für die Einhaltung bereichsspezifischer Pflichten im Unternehmen die Verantwortung tragen. Achtung: Fehlende Zuständigkeiten sind häufig bußgeldbewehrt.	1 = alle; 10 = keine	<ul style="list-style-type: none"> — Delegation (siehe 7.2.7) — Aufsicht und Überprüfung (siehe 7.3.6)
13 Inwieweit hat die Geschäftsleitung dafür Sorge getragen, dass Geschäftsgeheimnisse des Unternehmens, aber auch Dritter (Geschäftspartner/Lieferanten) vor unbefugter Nutzung/Offenlegung angemessen geschützt werden?	Hinweis: Schauen Sie auf die vorhandenen physischen, technischen und rechtlichen Maßnahmen zum Schutz von Geschäftsgeheimnissen (z. B. Zugangskontrollen, IT-Zugriffsbefugnisse, Vertraulichkeitsvereinbarungen mit Mitarbeitenden und Geschäftspartnern). <ul style="list-style-type: none"> — Wo bestehen ggf. Lücken? — Existieren interne Vorgaben zum Umgang mit Geschäftsgeheimnissen Ihres Unternehmens? — Ist der Kreis der Personen, die mit Geschäftsgeheimnissen in Berührung kommen, möglichst klein gehalten? — Existieren schriftliche Vertraulichkeitsvereinbarungen? Falls ja: für welchen Personenkreis? Wer trägt Sorge für deren Einhaltung? 	1 = sehr gut; 10 = gar nicht	<ul style="list-style-type: none"> — Identifizierung unternehmenseigener/fremder Geschäftsgeheimnisse (siehe 7.2.10) — Implementierung/Aktualisierung angemessener technischer, organisatorischer und rechtlicher Geheimhaltungsmaßnahmen (siehe 7.2.14)

Tabelle A.4 — Compliance-Selbst-Check — Einkaufsprozess

Einkaufsprozess	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
<p>Bei der Betrachtung der Risikoexposition Ihres Einkaufs-/Beschaffungsprozess sollten Sie mitbedenken, dass Risiken hier aus zwei „Richtungen“ drohen: zum einen aus dem Umgang mit Dritten (Lieferanten/Dienstleistern). Der Einkauf nimmt insofern eine wichtige Filter-/Verteidigungsfunktion ein. Es ist dafür Sorge zu tragen, dass „unsaubere“ Geschäftspartner konsequent aussortiert werden (Lieferantenauswahl/-bewertung/Geschäftspartnerprüfung). Außerdem hat der Einkauf dafür Sorge zu tragen, dass bei dem Bezug von Waren aus dem Ausland die zollrechtlichen Vorschriften eingehalten werden. Zum anderen verfügen die Mitarbeitenden des Einkaufs über eine „Machtposition“, die sie zum eigenen, aber auch zum Vorteil Dritter ausnutzen können (Stichwort: Korruption, Untreue).</p>			
<p>14 Wie schätzen Sie das Risiko ein, dass Mitarbeitende des Einkaufs sich mit Wettbewerbern über sensible Informationen (z. B. Preise oder Konditionen) austauschen?</p>	<p>Hinweis: Es geht hier nur um solche Informationen, die Einfluss auf das Wettbewerbsverhalten haben können. Beispiele sind nicht öffentliche Unternehmenszahlen, Margen, interne Preislisten, aber auch Vertragsklauseln usw. Dabei ist es schon ausreichend für eine Missachtung, wenn Informationen von einem Wettbewerber an Ihre Mitarbeitenden herangetragen werden und diese nicht unverzüglich zurückgewiesen werden. Schätzen Sie das Risiko ein.</p>	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Regelmäßige Schulungen zum Kartellrecht (siehe 7.2.8) — Erarbeitung einer Kartellrechts-Richtlinie (siehe 7.2.9) — Funktionstrennung (siehe 7.3.5) — Vier-Augen-Prinzip (siehe 7.3.8) — Regelmäßige Kontrollen (siehe 7.3.2) — Einrichtung Hinweisgebersystem (siehe 7.3.9)
<p>15 Wie schätzen Sie das Risiko ein, dass Mitarbeitende des Einkaufs persönliche Gegenleistungen (auch für Dritte) von Lieferanten/ Dienstleistern fordern?</p>	<p>Hinweis: Es kommt nicht auf die Höhe einer Zuwendung an. Es ist egal, ob eine Zuwendung gefordert oder geleistet wird. Es kommt nicht darauf an, ob Geld oder eine andere Zuwendung fließen sollen. Allein: Sehen Sie in Ihrem Unternehmen das Risiko, dass Mitarbeitende Zuwendungen von Lieferanten/Dienstleistern fordern? Achten Sie auch darauf, ob es Mitarbeitende (an relevanten Positionen) gibt, die gleichzeitig noch an anderen Unternehmen beteiligt sind oder bei denen sonstige Loyalitätskonflikte möglich erscheinen. Solche Loyalitäts-/ Interessenkonflikte können auf vielerlei Weise entstehen, wie bspw. durch die Beteiligung bei Wettbewerbern oder in einem wettbewerblichen (Neben-)Job. Auch familiäre Bindungen zu Wettbewerbern können hier Anreize bieten. Es ist wichtig, sich des strukturellen Problems bewusst zu sein und gegenzusteuern (z. B. durch Offenbarungsverpflichtungen und Regelungen zu potenziellen Interessenskollisionen).</p>	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Regelmäßige Antikorruptions-Schulungen (siehe 7.2.8) — Erarbeitung einer Antikorruptions-Richtlinie (siehe 7.2.9) — Funktionstrennung (siehe 7.3.5) — Vier-Augen-Prinzip (siehe 7.3.8) — Regelmäßige Kontrollen (siehe 7.3.2) — Einrichtung Hinweisgebersystem (siehe 7.3.9)

Tabelle A.4 (fortgesetzt)

Einkaufsprozess	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
16 Wie transparent ist aus Ihrer Sicht der Beschaffungsprozess organisiert?	Hinweis: Blicken Sie auf Ihr Lieferantenmanagement. Ist dieses nach Beschaffungsphasen (Präqualifikation, Lieferantenmanagement, Lieferantenbewertung) klar strukturiert? Sind Verantwortlichkeiten definiert? Wird die Bearbeitung von Reklamationen dokumentiert?	1 = sehr transparent; 10 = intransparent	<ul style="list-style-type: none"> — Festlegung von Zuständigkeiten/ Kompetenzen (siehe 7.2.6) — Funktionstrennung (siehe 7.3.5) — Erarbeitung einer Beschaffungs-/Einkaufsrichtlinie (siehe 7.2.9) — Erarbeitung eines Lieferantenkodex (siehe 7.2.5)
17 Wie bewerten Sie das Vertrags- und Dokumentenmanagement?	Hinweis: Intransparente, dezentrale Ablagesysteme erhöhen das Fehlerrisiko und begünstigen Compliance-Verstöße. Bei der Bewertung des Dokumenten-/ Vertragsmanagements sind auch die vorhandenen Kontrollmechanismen in den Blick zu nehmen (Budgetgrenzen und -kontrolle, Vier-Augen-Prinzip usw.). In Ihre Antwort sollten Sie sämtliche Faktoren (Übersichtlichkeit, Struktur, zentrale/dezentrale Dokumentation usw.) einbeziehen. Es kommt auf eine Gesamtabwägung sämtlicher Faktoren an.	1 = zentral, übersichtlich, strukturiert; 10 = dezentral, intransparent	<ul style="list-style-type: none"> — Einführung zentrales Dokumentationsmanagement (siehe 7.3.10) — Kommunikation (siehe 7.2.1/7.3.1) — Regelmäßige (interne) Kontrollen (siehe 7.3.4)

Tabelle A.5 — Compliance-Selbst-Check — Vertriebsprozess

Vertriebsprozess	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
<p>Der Vertrieb befindet sich in einem stetigen Zielkonflikt zwischen Umsatzsteigerung/-erhaltung und Beachtung der geltenden gesetzlichen Vorgaben. Der Vertrieb steht im direkten Kontakt zu Kunden, hat naturgemäß ein wirtschaftliches Interesse an langfristigen, lukrativen Geschäftsbeziehungen und möglichst reibungslosen Geschäftsabläufen. Aus diesen Rahmenbedingungen resultiert ein besonderes Risikopotenzial. Bei der Betrachtung der Compliance-Risiken im Vertriebsprozess sollten Sie daher den Fokus auf Anreizstrukturen legen, die die Begehung von Korruption und Kartellverstößen begünstigen. Der Direktvertrieb birgt zudem insbesondere im B2C-Geschäft (Privatkunden) Compliance-Risiken (z. B. unzulässige Verbraucherinformationen, Telefonwerbung, Cold Calling). Bei international ausgerichteten Unternehmen ist auch das Risiko von Verstößen gegen transnationale Sanktionen/Embargos in den Blick zu nehmen. Je nachdem, ob Ihr Unternehmen international ausgerichtet ist oder nicht, sind zudem außenwirtschafts- und exportrechtliche Vorgaben zu beachten.</p>			
<p>18 Wie schätzen Sie das Risiko ein, dass Vertriebsmitarbeitende sich an illegalen Absprachen mit Wettbewerbern beteiligen?</p>	<p>Hinweis: Innerhalb der Lieferketten bestehen oft zwischen den Marktbegleitern sowohl wettbewerbliche Beziehungen als auch Abhängigkeitsverhältnisse, die den Preis von der Qualität bis zu den individuellen Konditionen beeinflussen. Hier ist es wichtig die Beziehungen zu dokumentieren und den Vertrieb entsprechend zu steuern. Dies gilt ebenfalls im Handwerk, wo z. B. der Architekt und Kundenberater als Absatzmittler für die eingesetzten Produkte agiert.</p> <p>Neben dem Einkauf ist insbesondere der Vertrieb im Hinblick auf Kartellverstöße besonders gefährdet. Bei der Beantwortung der Frage sollten Sie folgende Punkte berücksichtigen:</p> <ul style="list-style-type: none"> — Nimmt Ihr Unternehmen an einem regelmäßigen/institutionalisierten Austausch mit Wettbewerbern teil (z. B. im Rahmen von Messe-, Verbandsveranstaltungen, Interessenvertretungen, gesellschaftlichen Clubs, gemeinsamen Projekten/Kooperationen)? — Kennen Sie laufende illegale (Preis-, Gebiets- oder Kunden-)Absprachen in der Branche? — Existieren Geschäftsbeziehungen mit Geschäftspartnern aus Hochrisikostaaten? — Werfen Sie auch einen Blick auf Ihr Marktumfeld. Gibt es Besonderheiten in Ihrem Marktumfeld die auf ein erhöhtes Kartellrisiko hindeuten (z. B. Oligopolistische Märkte, Wettbewerbsdruck usw.)? 	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Regelmäßige Schulungen zum Kartellrecht (siehe 7.2.8) — Erarbeitung einer Kartellrechts-Richtlinie (siehe 7.2.9) — Funktionstrennung (siehe 7.3.5) — Vier-Augen-Prinzip (siehe 7.3.8) — Regelmäßige (interne) Kontrollen (siehe 7.3.4) — Einrichtung Hinweisgebersystem (siehe 7.3.9)

Tabelle A.5 (fortgesetzt)

Vertriebsprozess	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
<p>19 Wie schätzen Sie das Risiko ein, dass Vertriebsmitarbeitende Beschäftigten der Kunden (dort insbesondere aus dem Bereich Einkauf) persönliche Gegenleistungen anbieten oder gewähren?</p>	<p>Hinweis: Folgende Faktoren beeinflussen das Korruptionsrisiko und sollten von Ihnen bei der Beantwortung der Frage mitbedacht werden:</p> <ul style="list-style-type: none"> — Gibt es besondere Anreizstrukturen im Unternehmen, die die Begehung korrupter Taten fördern (z. B. stark umsatzabhängiges Vergütungsmodell)? — Einsatz von Vertriebsmittlern, externen Beratern/Agenten. — Kontakt der Mitarbeitenden zu Amtsträgern. Besonders kritisch sind persönliche Leistungen an Richter, Beamte, Politiker. — Achten Sie auch darauf, ob es Mitarbeitende (an relevanten Positionen) gibt, die gleichzeitig noch an anderen Unternehmen beteiligt sind oder bei denen sonstige Loyalitätskonflikte möglich erscheinen. — Bestehen geschäftliche Kontakte zu Kunden in Hochrisikostaaten? 	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Regelmäßige Antikorruptions-Schulungen (siehe 7.2.8) — Erarbeitung einer Antikorruptions-Richtlinie (siehe 7.2.9) — Funktionstrennung (siehe 7.3.5) — Vier-Augen-Prinzip (siehe 7.3.8) — Regelmäßige (interne) Kontrollen (siehe 7.3.4) — Einrichtung Hinweisgebersystem (siehe 7.3.9)

Tabelle A.6 — Compliance-Selbst-Check — Wertschöpfungsprozess

Wertschöpfungsprozess (Produktion/Dienstleistung)	Erläuterungen	Antwort- möglichkeiten	Handlungsempfehlungen
<p>Wenn Sie Ihre Wertschöpfungsprozesse betrachten, sind Risiken aus dem Bereich Arbeitsstrafrecht (Arbeitsschutz, Arbeitssicherheit und Arbeitnehmerrechte) in den Fokus zu nehmen. Geeignete gesetzliche Schutzvorkehrungen zum Gesundheitsschutz der Arbeitnehmer sind zu beachten. Im produzierenden Gewerbe, dem Handwerk und dem Handel resultieren weitere Risiken aus dem Inverkehrbringen von Produkten. Denn Produktfehler können zu Gefahren für Mensch, Tier und Umwelt führen. Schließlich spielen Themen wie der Umweltschutz bis zur Überprüfung der Lieferketten eine herausgehobene Rolle bei der Beleuchtung des Wertschöpfungsprozesses. Umweltrechtliche Risiken ergeben sich etwa aus der behördlichen Genehmigungslage. Daneben birgt der Betrieb von (Produktions-)Anlagen für sich genommen Risiken für die Umwelt. Hinzu treten Risiken, die aus gefahrgeneigten Produktionsprozessen, dem Umgang mit und der Lagerung von Gefahrenstoffen sowie der Entsorgung von (gefährlichen) Abfällen resultieren. Neben dem Bereich Produktion dürfen Sie Dienstleistungen nicht aus dem Blick verlieren. Typische Risiken lauern hier etwa bei Beraterverträgen.</p>			
<p>20 Wie bewerten Sie das Risiko, dass Kunden oder die Umwelt durch Produkte Ihres Unternehmens in Mitleidenschaft gezogen werden?</p>	<p>Hinweis: Das produktstrafrechtliche Risiko betrifft typischerweise Unternehmen des produzierenden Gewerbes/Handwerk. Sie sollten sich (sofern relevant) einen Überblick darüber verschaffen, ob und wie häufig die von Ihrem Unternehmen vertriebenen Produkte durch Kunden reklamiert wurden. Relevant ist auch, ob es in der Vergangenheit ggf. bereits Rückrufaktionen Ihres Unternehmens gab. Risikoerhöhend wirkt es sich zudem aus, wenn besondere Kennzeichnungs- und Hinweispflichten für die hergestellten Waren gelten. Auch die Produktfolgehaftung kann bei mangelnden Hinweisen und Gebrauchsanweisungen erhebliche finanzielle und rechtliche Folgen haben.</p>	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Einrichtung Qualitätsmanagement (Aufbau-/Ablauforganisation) — Regelmäßige Kontrollen (siehe 7.3.2) — Vorfalldokumentation (siehe 7.3.11) — Einrichtung Hinweisgebersystem (siehe 7.3.9)

Tabelle A.6 (fortgesetzt)

Wertschöpfungsprozess (Produktion/Dienstleistung)	Erläuterungen	Antwort- möglichkeiten	Handlungsempfehlungen
<p>21 Wie gut sehen Sie Ihr Unternehmen aufgestellt, was die Einhaltung von Arbeitsschutzvorschriften (insbesondere im Produktionsprozess) angeht?</p>	<p>Hinweis: Von Bedeutung ist insofern zunächst der Geschäftsgegenstand Ihres Unternehmens. Unternehmen des produzierenden Gewerbes und des Handwerks weisen per se ein erhöhtes Risiko für Arbeitsschutzverstöße auf. Schauen Sie auf die vorhandenen Prozesse und Arbeitsschutzmaßnahmen (Zuständigkeiten, interne Betriebs- und Verfahrensanweisungen usw.).</p> <ul style="list-style-type: none"> — Sehen Sie Lücken oder Verbesserungsbedarf? — Wie häufig kommt es in Ihrem Unternehmen zu (meldepflichtigen) Betriebsunfällen? Was sind die Ursachen? (z. B. Prozessschwächen, mangelhafte Kommunikation oder menschliches Versagen) 	<p>1 = sehr gut; 10 = sehr schlecht</p>	<ul style="list-style-type: none"> — Regelmäßige Arbeitsschutz-/ Arbeitssicherheitsschulungen (siehe 7.2.8) — Erarbeitung Richtlinie Arbeitsschutz-/ Arbeitssicherheit (siehe 7.2.9) — Festlegung von Zuständigkeiten/ Kompetenzen (siehe 7.2.6) — Regelmäßige Kontrollen (siehe 7.3.2) — Einrichtung Hinweisgebersystem (siehe 7.3.9)
<p>22 Wie bewerten Sie das Risiko, dass Ihr Unternehmen gegen Umweltvorschriften/-standards oder behördliche Auflagen verstößt?</p>	<p>Hinweis: Umweltrechtliche Risiken ergeben sich auch aus der behördlichen Genehmigungslage, die den Rahmen der zulässigen Betriebstätigkeit absteckt. Daneben birgt der Betrieb von (Produktions-)Anlagen für sich genommen Risiken für die Umwelt (z. B. Boden-, Luft- oder Gewässerverunreinigungen). Hinzu treten Risiken, die aus gefahrgeneigten Produktionsprozessen, dem Umgang mit und der Lagerung von Gefahrenstoffen sowie der Entsorgung von (gefährlichen) Abfällen resultieren.</p>	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Regelmäßige Umweltschutz-Schulungen (siehe 7.2.8) — Erarbeitung Richtlinie Umweltschutz (siehe 7.2.9) — Festlegung von Zuständigkeiten/ Kompetenzen (siehe 7.2.6) — Regelmäßige Kontrollen (siehe 7.3.2) — Einrichtung Hinweisgebersystem (siehe 7.3.9)

Tabelle A.7 — Compliance-Selbst-Check — Personalprozess

Personalprozess	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
<p>In Personalprozessen können verschiedene Compliance-Risiken auftreten, die Unternehmen potenziell schädigen und rechtlichen Konsequenzen aussetzen können. Von der Einstellung bis zur Trennung von einem Mitarbeitenden sind Compliance-Risiken in jedem Schritt des Personalzyklus präsent. Dazu gehören Aspekte wie Diskriminierung, Datenschutz, Arbeitsrecht sowie Ethik und Integrität.</p>			
<p>23 Wie bewerten Sie das Risiko, dass es in Ihrem Unternehmen zu Datenschutzverstößen kommt?</p>	<p>Hinweis: Verhaltensweisen wie der Umgang mit E-Mails oder Videoüberwachung im Unternehmen sollten Sie betrachten. Problematisch kann etwa „Bring your own device“ sein. Problematische Prozesse können sich auch aus einer unzureichenden IT-Sicherheit oder einem unvollständigen Berechtigungssystem für den Zugriff auf personenbezogene Daten ergeben. Personenbezogene Daten können Mitarbeitendendaten sein. Also Personalakten, Geburtstage, Adressen (auch: E-Mail-Adressen) usw.</p>	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Regelmäßige Datenschutz-Schulungen (siehe 7.2.8) — Erarbeitung Datenschutz-Richtlinie (siehe 7.2.9) — Implementierung TOMs (siehe 7.2.14) — Regelmäßige Kontrollen (siehe 7.3.2) — Dokumentation (Verarbeitungsverzeichnis) (siehe 7.3.10) — Einrichtung Hinweisgebersystem (siehe 7.3.9)
<p>24 Wie schätzen Sie das Risiko ein, dass Ihr Unternehmen gegen Arbeitnehmerrechte verstößt?</p>	<p>Hinweis: Risiken lauern bei der Beschäftigung von Fremd-, Leih- oder ausländischen Arbeitnehmern:</p> <ul style="list-style-type: none"> — Liegen sämtliche erforderlichen Erlaubnisse und Genehmigungen vor? — Blicken Sie auch auf die Arbeitsorganisation: Ist sichergestellt, dass die höchstzulässige werktägliche Arbeitszeit eingehalten wird? — Wie erfolgt die Erfassung der Arbeitszeiten? <p>Daneben spielen auch Fragen der Diskriminierung am Arbeitsplatz und das Verhältnis des Arbeitgebers zu Gewerkschaften und Arbeitnehmervertretungen eine Rolle. Diesbezüglich ist v. a. die Zusammenarbeit mit dem Betriebsrat von Relevanz, hier insbesondere Auskunfts-, Informations- und Beteiligungspflichten. Schließlich sind alle Normen zu sozialversicherungsrechtlichen Pflichten (Beitrags- und Verwaltungspflichten aus Arbeitslosen-, Kranken-, Pflege-, Renten- und Unfallversicherungen) zu beachten.</p> <ul style="list-style-type: none"> — Sind auch alle Rahmenbedingungen für den Mindestlohn bekannt? — Werden alle Richtlinien für Mitarbeitende mit Schwerbehinderung eingehalten? 	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Regelmäßige Compliance-Schulungen (siehe 7.2.8) — Erarbeitung Handreichungen/Regelwerke (siehe 7.2.9) — Arbeitszeiterfassung (siehe 7.2.15) — Einbindung Betriebsrat — Festlegung von Zuständigkeiten/Kompetenzen (siehe 7.2.6) — Einrichtung Hinweisgebersystem (siehe 7.3.9)

Tabelle A.8 — Compliance-Selbst-Check — IT-Prozess

IT-Prozess	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
<p>IT-Prozesse durchziehen bereichsübergreifend das gesamte Unternehmen. Sie sind aus dem beruflichen Alltag nicht mehr hinwegzudenken. Mit der Nutzung von IT gehen zugleich zahlreiche Compliance-Risiken einher. Sowohl Externe als auch Mitarbeitende selbst können die IT-Landschaft des Unternehmens zur Begehung von Straftaten ausnutzen. Darüber hinaus birgt die Nutzung von IT selbst teilweise Risiken. Die Themen Datenschutz und IT-Sicherheit sind insofern zwei Seiten der gleichen Medaille. Nur wenn die IT-Geräte, auf denen personenbezogene Daten gespeichert sind, entsprechend geschützt werden, ist auch der Datenschutz hinreichend sichergestellt. Besonders relevant in international aufgestellten Unternehmen ist dabei der Transfer von Daten in andere Länder.</p>			
<p>25 Wie ist Ihre Selbsteinschätzung zum Thema IT-Sicherheit: Sehen Sie Ihr Unternehmen bislang gut aufgestellt?</p>	<p>Hinweis: Fragen Sie sich, wie Ihre IT gegen unbefugte Zugriffe sowohl von innen als auch außen geschützt ist. Existieren klare Vorgaben zur Nutzung der unternehmenseigenen EDV? Auch der Umgang mit Passwörtern, Berechtigungssysteme, d. h. die Regelung des Zugangs zu sensiblen/personenbezogenen Daten (z. B. Personalakten, Kunden- und Lieferantendaten) ist zu hinterfragen.</p>	<p>1 = sehr gut aufgestellt; 10 = sehr schlecht aufgestellt</p>	<ul style="list-style-type: none"> — Erarbeitung IT-Sicherheitskonzept (siehe 7.2.12) — Regelmäßige IT-Sicherheits-Schulungen (siehe 7.2.8) — Erarbeitung IT-Sicherheitsrichtlinie (siehe 7.2.9) — Regelmäßige Kontrollen (siehe 7.3.2) — Einrichtung Hinweisgebersystem (siehe 7.3.9)
<p>26 Wie bewerten Sie das Risiko, dass Geschäftsgeheimnisse Ihres Unternehmens und/oder von Geschäftspartnern unbefugt verwendet oder Dritten gegenüber offengelegt werden?</p>	<p>Hinweis: In einem ersten Schritt ist zu überlegen, wo im Unternehmen Geschäftsgeheimnisse „gelagert“ werden und welche Abteilung Berührungspunkte hierzu hat (z. B. Vertrieb, Einkauf, Forschung & Entwicklung). In einem zweiten Schritt sollten Sie hinterfragen, ob die vorhandenen Maßnahmen zum Schutz der Geschäftsgeheimnisse angemessen sind. Bedenken Sie in diesem Zuge auch die Nutzung von KI.</p>	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Implementierung/Aktualisierung angemessener technischer, organisatorischer und rechtlicher Geheimhaltungsmaßnahmen (siehe 7.2.14) — Regelmäßige Kontrollen (siehe 7.3.2) — Einrichtung Hinweisgebersystem (siehe 7.3.9)

Tabelle A.9 — Compliance-Selbst-Check — Logistikprozess

Logistikprozess	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlung
Bei der Betrachtung der Logistikprozesse sollte zum einen das Risiko möglicher Vermögensdelikte in den Blick genommen werden. Relevanz kommt daneben insbesondere dem Risikobereich Arbeitsschutz/-sicherheit zu. Weitere Risiken bestehen im produzierenden Gewerbe bei der Entsorgung von (Produktions-)Abfällen. Je nachdem, ob Ihr Unternehmen international ausgerichtet ist oder nicht, sind zudem außenwirtschafts- und exportrechtliche Vorgaben zu beachten.			
27 Wie bewerten Sie das Risiko, dass es im Logistikprozess zu Verstößen gegen den Arbeitsschutz/die Arbeitssicherheit kommt?	Hinweis: Zu betrachten sind sowohl die innerbetrieblichen Logistikprozesse als auch der Bereich der externen Logistik. Ist sichergestellt, dass eingesetzte Flurförderfahrzeuge, Fahrzeuge und Transportanlagen nur von solchen Personen bedient werden, die über die entsprechende Berechtigung verfügen? Daneben sollte kritisch hinterfragt werden, ob Verstöße gegen die höchstzulässigen Lenkzeiten im Unternehmen bekannt sind. Dasselbe gilt für mögliche Verstöße gegen Transport-/Ladungssicherungsvorschriften.	1 = vernachlässigbar; 10 = sehr hoch	<ul style="list-style-type: none"> — Regelmäßige Arbeitsschutz-/Arbeitssicherheitsschulungen (siehe 7.2.8) — Erarbeitung Richtlinie Arbeitsschutz-/Arbeitssicherheit (siehe 7.2.9) — Festlegung von Zuständigkeiten/Kompetenzen (siehe 7.2.6) — Regelmäßige Kontrollen (siehe 7.3.2) — Einrichtung Hinweisgebersystem (siehe 7.3.9)
28 Wie bewerten Sie das Risiko von Vermögensstraftaten zum Nachteil Ihres eigenen Unternehmens?	Hinweis: Ein sorgsam geführtes Wareneingangs- und -ausgangssystem verringert das Risiko von Vermögensdelikten zum Nachteil des eigenen Unternehmens. Blicken Sie auf Ihre Organisation: <ul style="list-style-type: none"> — Werden Warenbestände regelmäßig überprüft? Wenn ja, in welchem Ausmaß und mit welcher Intensität findet eine Prüfung der Lagerhaltung statt? — Gibt es unerklärliche Verringerungen des Lagerbestandes oder häufige Abschreibungen aufgrund von Diebstahl, Verlust, Beschädigung? 	1 = vernachlässigbar; 10 = sehr hoch	<ul style="list-style-type: none"> — Implementierung von technischen, organisatorischen und rechtlichen Schutzmaßnahmen (siehe 7.2.14) — Regelmäßige Kontrollen (siehe 7.3.2) — Erarbeitung Antikorruptions-Richtlinie (siehe 7.2.9) — Festlegung von Zuständigkeiten/Kompetenzen (siehe 7.2.6) — Festlegung von Budgets und Budgetkontrollen (siehe 7.3.7) — Regelmäßige Antikorruptions-Schulungen (siehe 7.2.8)

Tabelle A.10 — Compliance-Selbst-Check — Finanzprozess

Finanzabteilung (Entgeltabrechnung, Debitoren-/Kreditorenbuchhaltung)	Erläuterungen	Antwortmöglichkeiten	Handlungsempfehlungen
<p>Die unterschiedlichen Prozesse der Finanzabteilung (Entgeltabrechnung, Debitoren-/Kreditorenbuchhaltung) wurden für die hiesige Betrachtung zusammengefasst. Typische Compliance-Risiken der Finanzprozesse sind Vermögensdelikte zum Nachteil des eigenen Unternehmens (siehe dazu bereits vorstehend). Daneben sind steuer-, geldwäsche- und bilanzrechtliche Risiken in den Blick zu nehmen. Risiken im steuerlichen Bereich können neben der Missachtung regulatorischer Standards und der Nichteinhaltung der umfangreichen Anforderungen einzelner Steuerarten z. B. die fehlende steuerliche Berücksichtigung von Umstrukturierungen oder die Missachtung von Fristen sein.</p>			
<p>29 Wie schätzen Sie das Risiko ein, dass Steuerstraftaten zum Vorteil des Unternehmens begangen werden?</p>	<p>Hinweis: Die meisten Geschäftsvorfälle im Unternehmensalltag können auf irgendeine Art steuerlich relevant werden. Daher sind die mit steuerlichen Aufgaben im Unternehmen befassten Personen in Bezug auf strafrechtliche Risiken besonders exponiert. Betroffene Abteilungen sind zunächst die Geschäftsführung, die die meisten steuerlichen Pflichten aber regelmäßig an die Finanzbuchhaltung delegiert hat.</p> <p>Bei der Bewertung der steuerstrafrechtlichen Risikoexposition Ihres Unternehmens können Sie u. a. folgende Risikoszenarien berücksichtigen:</p> <ul style="list-style-type: none"> — Gab es in der Vergangenheit steuerstrafrechtliche Ermittlungen gegen das Unternehmen/dessen Geschäftsleitung? — Kommt es regelmäßig zu Lohnsteuernachforderungen? — Haben Betriebsprüfungen in der Vergangenheit zu nennenswerten Steuernachzahlungen geführt? 	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Regelmäßige Kontrollen (siehe 7.3.2) — Erarbeitung Richtlinie, Regelwerke und Handreichungen (siehe 7.2.9) — Festlegung von Zuständigkeiten/Kompetenzen (siehe 7.2.6) — Regelmäßige Tax-Compliance-Schulungen (siehe 7.2.8)
<p>30 Wie bewerten Sie das Risiko von Eigentums- und Vermögensdelikten (z. B. Unterschlagung, Betrug, Diebstahl) zum Nachteil Ihres eigenen Unternehmens?</p>	<p>Hinweis: Compliance-Risiken können aus einer fehlenden Funktionstrennung resultieren. Dies gilt insbesondere für eine fehlende Trennung der Zuständigkeit für das Anlegen von Kreditoren und die anschließende Prüfung, Freigabe und Zahlung der Rechnung. Auch eine unvollständige, intransparente Dokumentation und Aufbewahrung von Rechnungen erhöht das Missbrauchsrisiko. Auch sollten Sie die vorhandenen Kontrollmechanismen des Buchungssystems kritisch hinterfragen. Stellen Sie sich als Hilfestellung hier am besten die Frage, wie Sie eine solche Tat begehen könnten, wenn Sie es wirklich darauf anlegen würden.</p>	<p>1 = vernachlässigbar; 10 = sehr hoch</p>	<ul style="list-style-type: none"> — Implementierung von technischen, organisatorischen und rechtlichen Schutzmaßnahmen (siehe 7.2.14) — Regelmäßige Kontrollen (siehe 7.3.2) — Erarbeitung Antikorruptions-Richtlinie (siehe 7.2.9) — Festlegung von Zuständigkeiten/Kompetenzen (siehe 7.2.6) — Festlegung von Budgets und Budgetkontrollen (siehe 7.3.7) — Regelmäßige Antikorruptions-Schulungen (siehe 7.2.8)

Literaturhinweise

DIN ISO 30414:2019-06, *Personalmanagement — Leitlinien für das interne und externe Human Capital Reporting (ISO 30414:2018)*

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

DIN ISO 37002, *Hinweismanagementsysteme — Leitlinien*

DIN SPEC 27076:2023-05, *IT-Sicherheitsberatung für Klein- und Kleinstunternehmen*

DIN SPEC 91443:2021-08, *Systematisches Wissensmanagement für KMU — Instrumente und Verfahren*

ISO 20671-1:2021, *Brand evaluation — Part 1: Principles and fundamentals*

ISO 31073:2022, *Risk management — Vocabulary*

ISO/IEC/IEEE 24765:2017, *Systems and software engineering — Vocabulary*

ISO/IEC Guide 17:2016, *Guide for writing standards taking into account the needs of micro, small and medium-sized enterprises*

AEntG, *Gesetz über zwingende Arbeitsbedingungen für grenzüberschreitend entsandte und für regelmäßig im Inland beschäftigte Arbeitnehmer und Arbeitnehmerinnen (Arbeitnehmerentsendegesetz — AEntG); Arbeitnehmer-Entsendegesetz vom 20. April 2009 (BGBl. I S. 799), das zuletzt durch Artikel 1 des Gesetzes vom 28. Juni 2023 (BGBl. 2023 I Nr. 172) geändert worden ist.*

AWG, *Außenwirtschaftsgesetz; Außenwirtschaftsgesetz vom 6. Juni 2013 (BGBl. I S. 1482), das zuletzt durch Artikel 2 des Gesetzes vom 27. Februar 2024 (BGBl. 2024 I Nr. 71) geändert worden ist.*

AO, *Abgabenordnung; Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), die zuletzt durch Artikel 19 des Gesetzes vom 2. Dezember 2024 (BGBl. 2024 I Nr. 387) geändert worden ist.*

ArbSchG, *Gesetz zur Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit (Arbeitsschutzgesetz — ArbSchG); Arbeitsschutzgesetz vom 7. August 1996 (BGBl. I S. 1246), das zuletzt durch Artikel 32 des Gesetzes vom 15. Juli 2024 (BGBl. 2024 I Nr. 236) geändert worden ist.*

ArbZG, *Arbeitszeitgesetz; Arbeitszeitgesetz vom 6. Juni 1994 (BGBl. I S. 1170, 1171), das zuletzt durch Artikel 52 des Gesetzes vom 23. Oktober 2024 (BGBl. 2024 I Nr. 323) geändert worden ist.*

AWV, *Außenwirtschaftsverordnung; Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865), die zuletzt durch Artikel 2 der Verordnung vom 11. Dezember 2024 (BGBl. 2024 I Nr. 411) geändert worden ist.*

BDSG, *Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU — DSAnpUG-EU) (Artikel 1 Bundesdatenschutzgesetz (BDSG)); Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 7 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist.*

BetrSichV, *Verordnung über Sicherheit und Gesundheitsschutz bei der Verwendung von Arbeitsmitteln (Betriebssicherheitsverordnung — BetrSichV); Betriebssicherheitsverordnung vom 3. Februar 2015 (BGBl. I S. 49), die zuletzt durch Artikel 7 des Gesetzes vom 27. Juli 2021 (BGBl. I S. 3146) geändert worden ist.*

BlmSchG, Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz — BlmSchG); Bundes-Immissionsschutzgesetz in der Fassung der Bekanntmachung vom 17. Mai 2013 (BGBl. I S. 1274; 2021 I S. 123), das zuletzt durch Artikel 1 des Gesetzes vom 3. Juli 2024 (BGBl. 2024 I Nr. 225, Nr. 340) geändert worden ist.

BSIG, Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (Artikel 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz — BSIG)); Gesetz über das Bundesamt fuer Sicherheit in der Informationstechnik vom 14. August 2009 (BGBl. I S. 2821), 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist.

DSGVO, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

GeschGehG, Gesetz zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (Artikel 1 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)); Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (BGBl. I S. 466)

GWB, Gesetz gegen Wettbewerbsbeschränkungen (GWB); Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S. 1750, 3245), das zuletzt durch Artikel 6 des Gesetzes vom 5. Dezember 2024 (BGBl. 2024 I Nr. 400) geändert worden ist.

GWG, Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz — GwG); Geldwäschegesetz vom 23. Juni 2017 (BGBl. I S. 1822), das zuletzt durch Artikel 8 des Gesetzes vom 27. Dezember 2024 (BGBl. 2024 I Nr. 438) geändert worden ist.

HinSchG, Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz — HinSchG); Hinweisgeberschutzgesetz vom 31. Mai 2023 (BGBl. 2023 I Nr. 140), das durch Artikel 16 des Gesetzes vom 27. Dezember 2024 (BGBl. 2024 I Nr. 438) geändert worden ist.

IT-SiG, Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0); Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021, veröffentlicht im Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 25, ausgegeben zu Bonn am 27. Mai 2021

LkSG, Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten (Artikel 1 Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten (Lieferkettensorgfaltspflichtengesetz — LkSG)); Lieferkettensorgfaltspflichtengesetz vom 16. Juli 2021 (BGBl. I S. 2959)

MiLoG, Gesetz zur Regelung eines allgemeinen Mindestlohns (Mindestlohngesetz — MiLoG); Mindestlohngesetz vom 11. August 2014 (BGBl. I S. 1348), das zuletzt durch Artikel 2 des Gesetzes vom 28. Juni 2023 (BGBl. 2023 I Nr. 172) geändert worden ist.

OWiG, Gesetz über Ordnungswidrigkeiten; Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), das zuletzt durch Artikel 10 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234) geändert worden ist.

REACH, Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Agentur für chemische Stoffe, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EWG und 2000/21/EG der Kommission

StGB, Strafgesetzbuch; Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 7. November 2024 (BGBl. 2024 I Nr. 351) geändert worden ist.

UWG, Gesetz gegen den unlauteren Wettbewerb (UWG); Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3. März 2010 (BGBl. I S. 254), das zuletzt durch Artikel 21 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist.