Compliance Checklisten

Godzierz

6. Auflage 2025
ISBN 978-3-406-81779-3
C.H.BECK

insbes. deren Dokumentation, Nachverfolgung und Überwachung ihrer Umsetzung voraus.

4. Compliance Programm/Maßnahmen

Es gibt verschiedene Modelle und Rahmenwerke, die Organisationen bei der Entwicklung und Umsetzung eines Compliance-Programms unterstützen können. Einige der bekanntesten sind das Plan-Do-Check-Act (PDCA) Modell der ISO-Standards,[40] das 5-stufige COSO-Modell[41], die 7 Elemente des IDW PS 980[42] oder das im Folgenden genutzte „Prevent-Detect-Respond" Modell. Entsprechend dem gewählten Modell erfolgt dann der Aufbau der einzelnen Elemente des CMS und deren Operationalisierung, wobei bei der Ausgestaltung stets die individuelle Risikolage des Unternehmens zu berücksichtigen ist. **27**

a) Prevent

Unter den Punkt „Prevent" fallen die Compliance Elemente, welche vorwiegend der Vorbeugung von Compliance Verstößen dienen. **28**

aa) Gibt es einen allgemeinverbindlichen Verhaltenskodex sowie darauf aufbauende Compliance Richtlinien?

Ein grundlegendes Element einer Compliance Kultur ist ein Verhaltenskodex, in dem unter anderem das uneingeschränkte Bekenntnis der Organisation zu den einschlägigen Compliance-Verpflichtungen festgelegt ist.[43] Dieser sollte auf den Unternehmenswerten basieren und die Werte in konkrete Handlungsanweisungen für die Beschäftigten übersetzen. Ein Verhaltenskodex sollte für das ganze Unternehmen, also alle Mitarbeiter, gelten und allen relevanten internen und externen Parteien zugänglich sein. Auf der Grundlage des Verhaltenskodex sollten Compliance Maßnahmen (wie zB Trainings für Mitarbeiter, Prozesse und Richtlinien) in das Tagesgeschäft der Organisation integriert werden, um die Compliance Kultur zu fördern.[44] Unter dem Kodex sollten sich weiterführende Compliance Richtlinien einordnen, in denen die Ergebnisse der Compliance Risikoanalyse themenspezifisch berücksichtigt werden. Hierfür bietet sich unter anderem auch die Einführung eines Richtlinienmanagements an, für welches gerade bei größeren Organisationen auch eine Toollösung herangezogen werden). **29**

bb) Gibt es ein Beratungsangebot bei Compliance relevanten Fragestellungen?

Beschäftigte sollten über geeignete Kanäle die Möglichkeit haben, zu Fragestellungen mit Compliance Bezug beraten zu werden. Dies können dabei Ansprechpartner wie der Compliance Officer sein, oder auch passende Angebote im Unternehmensnetzwerk (FAQs, Guidelines, etc). Die Angebote sollten dabei leicht zugänglich und allgemein bekannt sein. Aufgrund der zunehmenden Integration von Technologie in Unternehmensprozesse können auch Chat-Bots eine effiziente Möglichkeit bieten, Mitarbeiter bei Compliance-Fragen zu unterstützen. Dabei ist jedoch darauf zu achten, dass die Qualität und Praktikabilität dieser Angebote gewährleistet ist, insbesondere aufgrund der sensiblen Themen im Bereich Compliance.[45] Gerade in größeren Unternehmen kann die Qualität der Beratung durch **30**

[40] Vgl. ISO 37301:2021 Compliance Management Systems – Requirements with guidance for use.
[41] COSO Framework: Committee of Sponsoring Organizations of the Treadway Commission (COSO).
[42] Rn. 27 IDW PS 980 n. F. (09.2022).
[43] Ziff. 2.4 UKBA; Ziff. I. B. ECCP; Bay/Hastenrath CMS/Daum § 5 Rn. 51 ff.
[44] A.8.1 ISO 37301.
[45] Moosmayer/Lösler Corporate Compliance/Klahold/Lochen § 13 Rn. 60 f.

Leitlinien und interne Standards sichergestellt werden. Nach erfolgter Beratung ist auf eine zeitnahe und vollständige Dokumentation dieser zu achten.

cc) Gibt es ein Compliance-Kommunikationskonzept, das Aspekte wie Zielgruppen, Botschaften, Kommunikationskanäle, Zeitplan und Frequenz berücksichtigt?

31 Der Kommunikation kommt im Rahmen von Compliance eine große Bedeutung zu. Mit einer effektiven und auf Zielgruppen angepassten Compliance Kommunikation werden Mitarbeiter und Geschäftspartner über die unternehmensinternen Regeln, Pflichten, Verantwortlichkeiten, Rollen und Berichtswege der Compliance Organisation so informiert, dass sie diese verstehen und einhalten können. Für das Kommunikationskonzept sollte ein Ansatz gewählt werden, der sowohl interne und externe Kommunikation berücksichtigt.

32 Die interne Kommunikation beeinflusst stark das Verhalten der Beschäftigten, was zur Förderung oder Schwächung der Compliance Kultur führen kann. Das Kommunikationskonzept sollte daher von der Compliance Funktion und der Geschäftsführung gemeinsam entwickelt und umgesetzt werden.[46] Die Compliance Kommunikation kann hier mittels einer Vielzahl von Instrumenten erfolgen, sinnvoll ist dabei, vorab zu ermitteln, wo und wie sich die Mitarbeiter informieren, um so eine Einbindung der Materialien in den Arbeitsalltag zu ermöglichen.[47] Führungskräfte können als Multiplikatoren im Compliance-Kommunikationskonzept eingesetzt werden, um die Botschaften zu verstärken, das Engagement der Mitarbeiter zu fördern und die Bedeutung von Compliance innerhalb des Unternehmens zu betonen. Hilfreich ist auch die Implementierung eines Feedback-Mechanismus, um die Wirksamkeit der Kommunikationsmaßnahmen zu bewerten und sicherzustellen, dass die Compliance-Botschaften verstanden und akzeptiert werden. Dies kann etwa durch Umfragen, Mitarbeiterbefragungen oder Schulungsevaluationen erfolgen.

33 Für die externe Kommunikation mit Dritten sollte ein praktikabler, an die Unternehmenspolitik angepasster Ansatz gewählt werden.[48] Relevante Drittparteien können dabei Kunden, Zulieferer, weitere Geschäftspartner, Investoren oder auch Behörden sein. Die Kommunikation sollte dabei die Prinzipien von Transparenz, Angemessenheit, Glaubwürdigkeit und Zugänglichkeit berücksichtigen.[49]

dd) Werden regelmäßige Schulungen zu relevanten Compliance Risikogebieten durchgeführt?

34 Compliance Schulungen dienen in erster Linie der Sensibilisierung von Mitarbeitern und zeigen auf, in welchen konkreten Situationen im Arbeitsalltag ein Compliance Risiko vorliegen kann. Sie unterstützen die Beschäftigten im Umgang mit Risikosituationen und fördern dadurch eine nachhaltige Compliance Kultur.[50] Die Inhalte sollten sich an den identifizierten Risikobereichen orientieren und zielgruppenspezifisch sein. Häufige Themen von Schulungen sind dabei der Verhaltenskodex oder individuelle Themenbereiche wie Antikorruption oder Geldwäsche. Trainingsmethoden können von Internen oder Externen durchgeführte Präsenzschulungen oder selbst erstellte oder erworbene E-Lear-

[46] Barbist/Ahammer/Fabian/Löffler, Compliance in der Unternehmenspraxis, 2. Aufl. 2015, S. 32 ff.
[47] Beispiele sind Kampagnen-Poster und Minibroschüren, Flyer und Karten, Newsletter und Mitarbeiterbriefe, Compliance Fallbeispiele (Best- und Worst-Cases), Einbindung in Online-Formate (Intranet), Compliance Schulungen.
[48] Beispiele sind Jahresberichte, Compliance Statements, Broschüren, Flyer und Karten, Newsletter, Veröffentlichungen auf der Homepage, Compliance Schulungen für Geschäftspartner.
[49] A.7.4ISO 37301.
[50] Ziff. 7.2.3 ISO 37301; Principle 5 UKBA; Ziff. I. C. ECCP; Schmahl in Makowicz Praxishandbuch Compliance Management Kap. 2–70, Nr. 2.1 ff.; Moosmayer/Lösler Corporate Compliance/Klahold/Lochen § 13 Rn. 62 ff.

nings sein. Präsenzschulungen kommen auch digital in Frage und sind dabei interaktiv, kostengünstig (da weder Trainer noch Mitarbeiter vor Ort sein müssen) und gut zu dokumentieren sowie auszuwerten.

ee) Wird die notwendige persönliche und fachliche Eignung von verantwortlichen Mitarbeitern und Führungskräften sichergestellt?

Der fachlichen Kompetenz und der persönlichen Eignung kommt eine Schlüsselfunktion im Hinblick auf das Compliance Management zu. Fehlt diese, kann dies schnell zu Verstößen gegen interne Richtlinien oder gesetzliche Vorschriften führen. Besonderer Bedeutung kommt daher der Schnittstelle zwischen Personal- und Compliance-Abteilung zu. Insbes. bei der Auswahl von Führungskräften und Mitarbeitern in risikoexponierten Positionen sollten Compliance Erwägungen einfließen und sorgfältig nach persönlicher und fachlicher Eignung ausgewählt werden.[51] Die Kompetenzen sollten daher regelmäßig überprüft werden, wobei bei Bedarf Schulungen und Trainings entsprechender Beschäftigter durchzuführen sind. Insbes. bei Neueinstellung und Beförderungen in kritische Positionen sollte ein Prozess existieren, welcher gebotene und rechtlich zulässige Maßnahmen enthält (Einsicht ins Führungszeugnis, Selbstauskunft, Backgroundcheck, etc).[52] **35**

ff) Wurden bei Betrachtung des Geschäftsmodells und der Compliance Risikoanalyse Themengebiete identifiziert, die die Etablierung spezifischer CMS-Elemente erfordern?

Soweit aufgrund des Geschäftsmodells spezielle oder besondere Risiken bestehen, kann die Etablierung weitergehender und geschäftsspezifischer CMS-Elemente erforderlich sein. Auch in diesem Fall sind die Prinzipien von Angemessenheit und Flexibilität bei der Entwicklung von Maßnahmen zu berücksichtigen. Zu den geschäftsspezifischen CMS-Elementen zählen solche, die aufgrund weitergehender, komplexer oder besonderer Geschäftsmodelle erforderlich sind. Dies können CMS-Elemente wie Geschäftspartnerprüfungen, Sanktionslistenchecks, Prozesse für den Umgang mit Geschenken und Einladungen, Spenden und Sponsoring oder Prozesse zur Minimierung weiterer spezifischer Risiken sein. Wichtig ist hierbei für jedes spezifische CMS-Element Zuständigkeiten und Verantwortlichkeiten klar zu dokumentieren. **36**

b) Detect

Unter der „Detect" Komponente finden sich die Compliance Elemente, welche zur Aufdeckung von Schwachstellen im CMS sowie von Compliance Verstößen gedacht sind. Neben Kontrollen zur kontinuierlichen Überwachung von kritischen Unternehmensprozessen ist hier insbeso. die Einrichtung eines Hinweisgebersystems zu nennen. Seit Juli 2023 gilt das deutsche HinSchG[53] verbindlich für alle Unternehmen und öffentlichen Einrichtungen mit mind. 50 Mitarbeitenden. Diese Organisationen sind dazu verpflichtet, einen internen Meldekanal wie beispielsweise ein Hinweisgebersystem einzurichten. Das Gesetz zielt darauf ab, Whistleblower vor Repressalien zu schützen, wenn sie innerhalb ihres beruflichen Umfelds Kenntnisse über Verstöße erlangen und diese an die Meldestellen weitergeben. Im Folgenden wird nun kurz auf wesentliche Elemente dieses Gesetzes eingegangen; die Einrichtung eines solchen Systems ist unabhängig davon, ob das Gesetz **37**

[51] LG München I CB 2014, 167 – Neubürger-Urteil.
[52] Ziff. 2.2.4 DICO Standard CMS.
[53] Gesetz zum Schutz von Hinweisgeberinnen und Hinweisgebern vor Benachteiligung (Hinweisgeberschutzgesetz – HinSchG).

Anwendung findet, zu empfehlen. Alle Beschäftigten sowie Dritte sollten in der Lage sein, auf mögliche Compliance Verstöße, Verdachtsfälle und Unregelmäßigkeiten im Geschäftsbetrieb hinzuweisen, und so dazu beitragen, Compliance Verstöße zu verhindern, aufzudecken oder Schwachstellen im CMS zu identifizieren.

aa) Gibt es ein Hinweisgebersystem, auf das alle Mitarbeiter Zugriff haben?

38 Interne Meldekanäle sollten mind. den eigenen Mitarbeitern sowie Leiharbeitnehmern, die dem Unternehmen überlassen sind, zugänglich sein. Unternehmen, die zur Einrichtung dieser Kanäle verpflichtet sind, haben die Möglichkeit zu entscheiden, ob das Meldeverfahren auch für externe Personen offen sein soll, die in Kontakt mit dem Unternehmen stehen.[54]

bb) Ermöglichen die internen Meldekanäle vertrauliche Meldungen sowohl mündlich als auch schriftlich und auf Wunsch persönlich?

39 Meldekanäle für Hinweise können vielfältig sein, von IT-gestützten Systemen wie Webplattformen oder speziellen E-Mail-Adressen bis hin zu mündlichen Möglichkeiten wie Hotlines oder Anrufbeantwortern. Es sollte auch die Option geben, Hinweise persönlich zu besprechen, entweder in einem physischen Treffen oder per Videokonferenz, wenn der Hinweisgeber zustimmt. Es gibt dabei keine klare Verpflichtung, interne Meldekanäle anonym zu gestalten, obwohl alle Hinweise, auch anonyme, behandelt werden sollen.[55] Das Vertraulichkeitsgebot ist entscheidend: Interne Meldekanäle sollten so gestaltet sein, dass die Identität der Hinweisgeber, der Betroffenen und anderer erwähnter Personen geschützt wird und nur befugte Personen Zugang zu diesen Informationen haben.[56]

cc) Ist die Zuständigkeit für das Hinweisgebersystem innerhalb des Unternehmens klar definiert?

40 Im Unternehmen sollten Personen oder Abteilungen als „Meldestellen-Beauftragte“ benannt werden. Ihre Aufgaben umfassen die Annahme von Meldungen, die Bestätigung des Eingangs innerhalb von sieben Tagen, die Prüfung der Meldung, die Einleitung entsprechender Maßnahmen und die Benachrichtigung des Hinweisgebers über getroffene Maßnahmen innerhalb von drei Monaten. Die genaue Zuständigkeit hängt dabei von der Unternehmensstruktur, -größe und -tätigkeit ab; mögliche Beauftragte können in der Compliance Funktion, Rechtsabteilung oder in der Innrevision sitzen, vorausgesetzt, dass diese Personen unabhängig agieren können und keine Interessenkonflikte haben. Sie sollten über das erforderliche Fachwissen verfügen und ggf. geschult werden.[57] Generelle Schulungen zum Hinweisgebersystem sollten darüber hinaus allen Mitarbeitern angeboten werden. Alternativ zur internen Entgegennahme können auch externe Dienstleister als Meldestellen-Beauftragte fungieren; hier haben sich eine Vielzahl von Anbietern im Markt etabliert. Unternehmen mit 50 bis 249 Mitarbeitern können Ressourcen teilen und eine gemeinsame Meldestelle einrichten, bleiben aber für die Maßnahmen zur Behebung des Verstoßes und die Rückmeldung an den Hinweisgeber selbst verantwortlich.

[54] § 16 Abs. 1 HinSchG.
[55] § 16 Abs. 3 HinSchG.
[56] § 8 HinSchG.
[57] § 15 Abs. 2 HinSchG.

dd) Ist die Möglichkeit externer Meldeverfahren klar kommuniziert?

Unternehmen müssen zudem Informationen über alternative externe Meldeverfahren an die zuständigen Behörden bereitstellen.[58] Diese Informationen müssen leicht zugänglich sein, etwa über die Unternehmens-Website oder das Intranet. Es liegt dabei im Eigeninteresse jedes Unternehmens, mögliche Verstöße intern aufzudecken und zu verhindern, dass Hinweisgeber sich an externe Stellen oder die Öffentlichkeit wenden. Daher sollten Unternehmen den internen Meldekanal benutzerfreundlich gestalten und soweit möglich die Mitarbeiter entsprechend zur Nutzung ermutigen. **41**

ee) Existiert ein Prozess für interne Untersuchungen und das Fallmanagement?

Unternehmen sind angehalten sämtlichen Verdachtsfällen auf Compliance Verstöße im Rahmen des CMS nachzugehen.[59] Die Unternehmensleitung muss eingreifen, sobald Anhaltspunkte für ein Fehlverhalten erkennbar sind. Eine solche Pflichtverletzung liegt bereits dann vor, wenn durch mangelhafte Organisation, unzureichende Anleitung oder ungenügende Kontrolle Straftaten oder Fehlhandlungen der Mitarbeiter ermöglicht oder erleichtert werden. Verdachtsmomenten in diesem Zusammenhang muss die Unternehmensleitung unverzüglich nachgehen.[60] Das Unternehmen sollte daher einen Prozess zur Durchführung von internen Untersuchungen vorhalten, um Hinweise über vermutete oder tatsächliche Verstöße unabhängig und ohne Interessenskonflikte zu evaluieren, zu bewerten, zu untersuchen und abzuschließen.[61] Dabei kann im Rahmen vorab festgelegter Prozesse (zB Fallmanagement/Untersuchungshandbuch) mit eigenen Teams oder externen Dienstleistern zusammengearbeitet werden, um den Sachverhalt unabhängig und systematisch aufzuklären. Die einzelnen Schritte und Ergebnisse der Untersuchung sollten dabei nachvollziehbar dokumentiert und archiviert werden. Der Unternehmensleitung sollte regelmäßig über die Anzahl und die Ergebnisse der Untersuchungen berichtet werden. Ergebnisse der internen Untersuchungen sollten im Anschluss für die Verbesserung des CMS genutzt werden.[62] **42**

ff) Gibt es Kontrollen zur kontinuierlichen Überwachung von kritischen Unternehmensprozessen?

Um eine fortlaufende Überwachung der Einhaltung von Vorschriften in den Compliance-Themengebieten sicherzustellen, sollte das CMS insbesondere in den Bereichen, die mit Fehlverhalten in Zusammenhang stehen entsprechende Kontrollelemente enthalten.[63] Zur Überwachungspflicht gehören hinreichende Kontrollen, die präventiv erfolgen müssen und die nicht erst dann einsetzen dürfen, wenn Missstände entdeckt worden sind.[64] Eine präventive strukturelle Kontrolle, wie bspw.das Vier-Augen-Prinzip, sollte für alle kritischen internen Unternehmensprozesse implementiert werden. Kritische Prozesse sind solche, bei deren nicht ordnungsgemäßer Durchführung Personenschäden oder erhebliche finanzielle Auswirkungen möglich sind.[65] Kontrollen, sollten so ausgestaltet sein, dass Unregelmäßig- **43**

[58] § 13 Abs. 2 HinSchG.
[59] LG München I CB 2014, 167 – Neubürger-Urteil.
[60] OLG Nürnberg NZG 2022, 1058 Rn. 79.
[61] Ziff. 8.4ISO 37301; I. D. ECCP.
[62] Ziff. 8.4 ISO 37301.
[63] Ziff. 2.3.1 DICO CMS Standard; Moosmayer/Lösler Corporate Compliance/Klahold/Lochen § 13 Rn. 85; Ziff. III. A. ECCP.
[64] OLG Nürnberg NZG 2022, 1058 Rn. 80.
[65] OLG Nürnberg NZG 2022, 1058 Rn. 104 ff.

keiten auch ohne ständige Überwachung vermieden werden. Je nach Unternehmensgröße und Komplexität können bereits kleinere, regelmäßige Kontrollen, wie die Prüfung von Stichproben, ausreichend sein. Solche stichprobenartigen und überraschenden Prüfungen genügen in der Regel, um Abschreckungseffekte zu erzielen. Falls diese nicht ausreichen, sind weitere Aufsichtsmaßnahmen, wie umfassendere und unerwartete Prüfungen, erforderlich.[66] Alle Maßnahmen müssen dabei objektiv zumutbar sein, die Eigenverantwortlichkeit der Mitarbeiter und den Vertrauensgrundsatz beachten sowie das Betriebsklima nicht unnötig belasten.[67] Compliance-Kontrollen sollten regelmäßig überprüft und bei Bedarf aktualisiert oder angepasst werden, um sicherzustellen, dass sie den sich ändernden rechtlichen Anforderungen und Geschäftsumgebungen entsprechen. Sie sind oft in das Risikomanagement des IKS integriert, um hier sicherzustellen, dass Risiken proaktiv identifiziert und adressiert werden. Diese Kontrollen sollten regelmäßig auf ihre Wirksamkeit getestet werden, wobei Abstimmungen mit Verantwortlichen den IKS und der Internen Revision unterstützen können.[68]

gg) Gibt es einen Prozess zur Prüfung der Integrität von Geschäftspartnern?

44 Soweit mit Dritten zusammengearbeitet wird oder Funktionen vollständig oder teilweise outgesourced werden, sollte eine effektive Geschäftspartnerprüfung im Hinblick auf Compliance Standards durchgeführt werden. Auf diese Weise kann sichergestellt werden, dass eigene Standards und Verpflichtungen zu Compliance nicht unterlaufen werden. Eine risikobasierte Geschäftspartnerprüfung (einschließlich von Vertretern, Vermittlern, Beratern, Händlern, Distributoren, Joint-Venture-Partnern etc) sollte regelmäßig aktualisiert und kann bspw. durch Schulungen, Audits und jährliche Compliance-Zertifizierungen der Partner ergänzt werden. Für Dienstleister sollten in Service-Level-Agreements verbindliche Compliance Maßnahmen festgelegt werden.[69]

c) Respond

45 Angemessene und konsequente Reaktionen auf Compliance Verstöße zeichnen ein wirksames CMS aus. Zusätzlich sollten identifizierte Lücken und Schwächen in Prozessen oder Kontrollen unverzüglich geschlossen werden. Neben diesem „Consequence-Management" wird im Folgenden auch das Krisenmanagement sowie das Berichtswesen der dritten Komponente „Respond" zugeordnet.[70]

aa) Besteht ein einheitlicher und dokumentierter Prozess für Sanktionierungen?

46 Sanktionierung wird relevant, wenn im Rahmen einer internen Untersuchung das Fehlverhalten eines Mitarbeiters bestätigt wird; sie sollte dann in Abstimmung mit der Personal- und Rechtsabteilung beraten werden. Auch hier empfiehlt sich ein festgelegter Prozess (zB die Möglichkeit zur Einberufung eines Disziplinarkomitees), damit Personalmaßnahmen objektiv, zeitnah und konsistent implementiert werden.[71] Ein einheitliches Sanktionierungskonzept dient dabei der internen Sanktionierung von Compliance Verstößen.[72] Organisatorisch sollte es in Zusammenarbeit mit der Rechts-, Compliance-, und Personalabteilung erstellt und umgesetzt werden. Die Kriterien, die für Disziplinarmaßnahmen heran-

[66] OLG Nürnberg NZG 2022, 1058 Rn. 80.
[67] OLG Nürnberg NZG 2022, 1058 Rn. 80.
[68] Ziff. 8.2, 9 ISO 37301.
[69] A.8.1 ISO 37301.
[70] Vgl. Ziff. 2.4 DICO CMS Standard.
[71] Clodius/Warda CB 2021, 137 (142) mwN.
[72] Ziff. 2.4.1. DICO Standard CMS; Ziff. 1.7 UKBA.

gezogen werden, sollten klar definiert sein. Im Einzelfall sind die Sanktionen adäquat, dabei jedoch konsequent und ohne Diskriminierung einzusetzen. Getroffene Maßnahmen sowie deren Umsetzung sollten dokumentiert werden.

bb) Gibt es einen internen Prozess zur Ursachenanalyse nach Compliance Vorfällen?

Durch aufdeckende Maßnahmen können neben dem Fehlverhalten einzelner Mitarbeiter auch Schwächen interner Strukturen, in Richtlinien und Prozessvorgaben sowie bei deren Einhaltung aufzeigt werden. In diesem Fall sollte eine Ursachenanalyse durchgeführt werden, um die prozessualen Schwachstellen schnellstmöglich vollumfänglich zu identifizieren und abzustellen.[73] Diese Analyse sollte dazu dienen, zu verstehen, welche Faktoren zum Fehlverhalten beigetragen haben und welcher Grad an Maßnahmen zur Beseitigung erforderlich ist, um ähnliche Ereignisse in Zukunft zu verhindern.[74] Es ist daher zu empfehlen, einen Prozess vorzuhalten, der sicherstellt, dass entsprechende Kenntnisse von Prozessschwächen und „Lessons Learned" zu Anpassungen im CMS oder in der Compliance Risikoanalyse, führen. Auch kann ein regelmäßiger Austausch mit der Internen Revision gewährleisten, dass anlassbezogene Audits zeitnah durchgeführt werden und bekannte Prozessschwächen in die jährliche Revisionsplanung aufgenommen werden können. **47**

cc) Gibt es ein Konzept für ein Compliance Krisenmanagement?

Im Rahmen eines unternehmensweiten Krisenmanagementsystems oder innerhalb des CMS sollte es ein Konzept für Compliance Krisen geben. So ein Konzept sollte insbes. dokumentieren, was eine Compliance-Krisensituation ist, und welche internen und externen Maßnahmen ergriffen werden müssen (zB Kommunikation mit Behörden).[75] Die Verantwortlichen für das Krisenmanagement sollten klar benannt und angemessen geschult werden.[76] **48**

dd) Erfolgt eine regelmäßige Berichterstattung an die Unternehmensleitung durch die Compliance Funktion?

Durch eine zeitnahe und regelmäßige Compliance Berichterstattung an die Unternehmensleitung wird diese über die Inhalte und die Funktion des CMS informiert. Dabei sollten sowohl regelmäßige Standardberichte als auch anlassbezogene Ad-hoc Berichte vorgesehen sein. Dies gewährleistet die Erfüllung der Aufsichtspflicht der Geschäftsleitung über die Compliance Funktion und trägt zur Effektivität des an diese delegierten CMS bei.[77] Auch sollten im Bericht die relevanten quantitativen und qualitativen Kennzahlen zu den Tätigkeiten der Compliance Funktion sowie ein kurzer Überblick über relevante Themengebiete (zB Compliance Risiken, Hinweise und Compliance Vorfälle) gegeben werden. Informiert werden sollte die Geschäftsleitung des Weiteren über die fortlaufende Überwachung, regelmäßige System-Evaluierungen und Maßnahmen zur Weiterentwicklung und Verbesserung des CMS.[78] **49**

[73] Clodius/Warda CB 2021, 137 (143).
[74] Ziff. III ECCP.
[75] Ziff. 2.4.4 DICO Standard CMS.
[76] Weitere Ausführungen hierzu finden sich in → § 14 Rn. 19–42.
[77] Bay/Hastenrath CMS/Daum § 5 Rn. 35 f.
[78] A.9.1.4 ISO 37301.

5. Evaluierung und Verbesserung des CMS

a) Wird die Wirksamkeit des CMS regelmäßig überprüft?

50 Das CMS sollte, sobald es umgesetzt ist, regelmäßig auf seine Angemessenheit und Wirksamkeit als Managementsystem überprüft werden.[79] Die praktische Wirksamkeit des CMS ist gegeben, wenn Compliance Verstöße, soweit möglich, tatsächlich verhindert werden können. Wenn Verstöße sich im Einzelfall nicht verhindern lassen, sollte Verdachtsmeldungen angemessen nachgegangen werden und diese adressiert sowie aufgeklärt werden.[80] Die Wirksamkeit des CMS oder einzelner Elemente davon kann von internen Stellen wie der internen Revision oder auch von unabhängigen Dritten wie (zB Rechtsanwaltskanzleien oder Wirtschaftsprüfungsgesellschaften) im Rahmen von Compliance Audit oder Compliance Assessments überprüft werden. Es wird empfohlen, die Zuständigkeiten für die Compliance Evaluierung klar festzulegen und einen detaillierten Plan zu entwickeln. Zudem sollten ausreichend erfahrene Ressourcen zur Durchführung der Evaluierungsmaßnahmen bereitgestellt werden. Die Berichtswege für die Ergebnisse sollten festgelegt werden, und es sollten regelmäßige Berichte erstellt werden, die von der zuständigen Stelle sorgfältig ausgewertet werden.[81] Spezifische Maßnahmen iRd Evaluierung sind zB Fragebögen, Auditierung von Prozessen, Richtlinien und Trainings, Datenanalysen sowie Prozesskontrollen. Auch Interviews mit relevanten Stakeholdern sind möglich. Wichtig ist, dass die Prozessunabhängigkeit beachtet wird. Auch eine Zertifizierung nach einem der oben genannten Standards ist möglich.

b) Wird das CMS fortlaufend optimiert?

51 Hat die Systemevaluierung ergeben, dass im Hinblick auf das CMS oder auf einzelne Elemente Handlungsbedarf besteht, sollten erkannte Prozessschwächen umgehend mitigiert werden.[82] Bei Hinweisen auf solche Schwachstellen sollten Maßnahmen zur Verbesserung der CMS-Wirksamkeit ergriffen werden, wie bspw. intensivere Kommunikation des Compliance-Programms oder zusätzliche Kontrollen. Werden Regelverstöße von Mitarbeitern oder Dritten entdeckt, sollten Maßnahmen zur Prävention zukünftiger Vorfälle folgen, etwa durch zusätzliche Schulungen oder die Berücksichtigung dieser Erkenntnisse bei Mitarbeiterbeurteilungen und Beförderungen.[83] Identifizierte Prozessschwächen werden nach Planung und Umsetzung der Verbesserungsmaßnahmen erneut geprüft. Nur so kann die fortlaufende Optimierung und Aktualität des CMS sichergestellt werden.

6. Herausforderungen eines globalen CMS

52 Compliance Verstöße haben oftmals einen internationalen Bezug und die Verantwortung für Compliance endet nicht an den Grenzen der einzelnen Gesellschaft. Innerhalb einer globalen Organisation sollten daher die Verantwortlichkeiten, Ressourcen und entsprechenden Berichtslinien im Bereich Compliance der Größe, Struktur und dem Risikoprofil des Unternehmens angemessen sein.

[79] Ziff. 9 ISO 37301; Principle 6 UKBA.
[80] Makowicz in Makowicz, Praxishandbuch Compliance Management, 2017, Kap. 1–10 Nr. 3.6.
[81] Rn. A 29 IDW PS 980 n. F. (09.2022).
[82] Ziff. 9 ISO 37301; Ziff. 2.5 DICO Standard CMS.
[83] Rn. A 29 IDW PS 980 n. F. (09.2022).