IDR Leitfaden 500 "Einrichtung und Prüfung eines kommunalen Compliance-Management-Systems (CMS)"

unter Berücksichtigung der Anforderungen des Hinweisgeberschutzgesetzes (HinSchG)

Stand 14.09.2023

ISBN 978-3-00-078377-7

Editorial

Als Vorsitzender des Instituts der Rechnungsprüfer (IDR) e.V. freue ich mich, dass die Projektgruppe Compliance die Leitlinie 500 „Einrichtung und Prüfung eines kommunalen Compliance-Management-Systems (CMS)" erarbeitet hat. Die Leitlinie stellt umfassend die Voraussetzungen für die Einrichtung eines CMS und dessen Prüfung dar.

Das IDR als Berufsverband der öffentlichen Finanzkontrolle hat sich in seinem Leitbild das Ziel gesetzt, dass Prüfungen der öffentlichen Revision Mehrwert schaffen sollen, indem sie dazu beitragen, Prozesse zu optimieren und Risiken aufzuzeigen. Hierbei ist die Prüfung eines vorhandenen Compliance Management Systems (CMS) ein wichtiger Baustein, um sicherzustellen, dass eine Kommune über angemessene und wirksame Verfahren und Maßnahmen verfügt, um die Einhaltung von Gesetzen, Vorschriften und internen Richtlinien zu gewährleisten. Die Prüfung ermöglicht es, die Stärken und Schwächen des Systems zu identifizieren, Lücken aufzudecken und Verbesserungspotenziale zu erkennen. Sie stellt sicher, dass das CMS effektiv funktioniert und den Anforderungen entspricht, die sich aus den rechtlichen und regulatorischen Rahmenbedingungen ergeben. Außerdem spielt sie eine nicht zu unterschätzende Rolle bei der Förderung einer Kultur der Compliance und des ethischen Verhaltens in einer Organisation.

Der vorliegende Leitfaden "Einrichtung und Prüfung eines kommunalen CMS" wurde von einer Projektgruppe des IDR erstellt. Er richtet sich dabei am bekannten Prüfungsstandard des IDW PS 980 aus, ergänzt um Aspekte des ISO 37301 und des ISO 37002, berücksichtigt jedoch Spezifika der öffentlichen, insbesondere kommunalen Verwaltung sowie Pflichten aus dem Hinweisgeberschutzgesetz. Vergleichbar mit dem IDW PS 980, beschreibt der Leitfaden als Grundlage einer Prüfung zudem, wie ein CMS in einer kommunalen (bzw. öffentlichen) Verwaltung eingerichtet werden sollte.

An dieser Stelle möchte ich meinen Dank an die Mitglieder der Projektgruppe sowie der Evaluierenden zum Ausdruck bringen, die ihr Fachwissen und ihre Zeit in den Leitfaden investiert haben.

Das Thema Compliance wird uns weiter begleiten, deshalb ist es folgerichtig, dass der Verwaltungsrat einen ständigen Arbeitskreis Compliance eingerichtet hat. Der Arbeitskreis wird die weitere Entwicklung begleiten, die Leitlinie 500 entsprechend anpassen und für dieses wichtige Thema sensibilisieren. Nichts ist gefährlicher für eine Demokratie, wenn der Eindruck entstehen sollte, dass sich Staat und Verwaltung nicht mehr an Regeln halten.

Hans-Dieter Wieden
Vorsitzender des IDR

Vorwort

Dass sich Städte mit dem Thema Compliance befassen, ist nicht mehr wegzudenken und wird wichtiger. Vereinfacht gesprochen bedeutet Compliance, dass sich eine Kommune an die geltenden Regeln hält. Dazu gehören gesetzliche, aber auch verwaltungsinterne Regelungen.
Die Einrichtung und Prüfung von Compliance-Management-Systemen hat daher in den vergangenen Jahren für die kommunale Verwaltung an Bedeutung gewonnen. Sie sollen gewährleisten, dass Fehlverhalten oder Compliance-Verstöße schon frühzeitig entdeckt, aufgeklärt oder verhindert werden können. Dementsprechend komplex sind die Anforderungen an ein wirksames Compliance-Management-System.
Mit dem vorliegenden Leitfaden soll den Kommunen ein weiterer Orientierungsrahmen für die Einrichtung, den Betrieb und die Prüfung eines kommunalen Compliance-Management-Systems an die Hand gegeben werden.

Markus Lewe
Präsident des Deutschen Städtetags,
Oberbürgermeister der Stadt Münster

Inhaltsverzeichnis

Abbildungsverzeichnis

Redaktioneller Hinweis:
Wir bitten um Verständnis, dass aus Gründen der Lesbarkeit auf eine durchgängige Nennung der weiblichen und männlichen Bezeichnungen verzichtet wird. Selbstverständlich beziehen sich die Texte in gleicher Weise auf Frauen, Männer und Diverse.

Teil 1 – Die zentralen Punkte eines kommunalen CMS

Die Einführung eines Compliance Management Systems (CMS) als Pflichtaufgabe für Landkreise, Städte und Gemeinden – Ein Überblick (nicht nur) für Landräte, (Ober-)Bürgermeister, Dezernenten und weitere Organmitglieder

Was ist Compliance?

Compliance bedeutet – mit einem Wort ausgedrückt – Regeltreue. Etwas ausführlicher beschrieben und auf die kommunale Ebene bezogen kann Compliance wie folgt definiert werden: Die Verwaltungsorgane einer Kommune haben im Rahmen ihrer Zuständigkeit dafür Sorge zu tragen, dass alle formellen und materiellen Gesetze sowie alle verwaltungsinternen Regelungen eingehalten werden. Sie wirken auf deren wirksame Beachtung in der Kommune hin.

Was ist ein Compliance Management System (CMS)?

Unter einem CMS werden (in Anlehnung an den Prüfungsstandard des Instituts der Wirtschaftsprüfer in Deutschland (IDW) PS 980) die Gesamtheit aller Regelungen (hinsichtlich Strukturen, Prozesse und Maßnahmen) der Kommune verstanden, die darauf abzielen bzw. sicherstellen sollen, dass die Akteure der Kommune (ihre gesetzlichen Vertreter, ihre Mitarbeitenden, die Mitglieder der kommunalen Volksvertretung, beauftragte Dritte, ihre Zuwendungsempfänger) regelkonform handeln und damit wesentliche Regelverstöße verhindert werden (= Verwaltungssystem zur Regeleinhaltung).

Warum braucht eine Kommune ein CMS?

Es gibt (bislang) keine Rechtsnorm, die die öffentliche Verwaltung zur Einrichtung eines CMS ausdrücklich verpflichtet. Jedoch kann eine solche Pflicht (das „Ob" von Compliance) implizit aus verfassungsrechtlichen Vorgaben (u.a. Bindung an Grundrechte, Rechtsstaatsprinzip, EU-Grundrechtecharta) sowie aus einzelnen Rechtsgebieten bzw. einzelgesetzlichen Bestimmungen (u.a. strafrechtliche Risiken von Amtsträgern, Organisationspflichten, Dienstrecht, steuerliche Vorschriften, Hinweisgeberschutzgesetz) abgeleitet werden. Ein CMS ist daher Teil einer guten Verwaltungsführung (good governance). Ein funktionieren-

des CMS trägt wesentlich dazu bei, ggf. bestehende persönliche Haftungsrisiken von Organen bzw. Organmitgliedern zu reduzieren und ist daher im Eigeninteresse von Organverantwortlichen.

Die Kommunen haben hierbei im Rahmen ihres Selbstverwaltungsrechts eigenverantwortlich für gesetzmäßiges Handeln zu sorgen (sachliche Compliance-Verantwortung). Der gesetzliche Vertreter der Kommune ist als Leiter der Verwaltung aufgrund seiner Pflicht, für die Einhaltung der bestehenden Regeln zu sorgen (Legalitätskontrollpflicht), nach pflichtgemäßem Ermessen für die angemessene Einrichtung und Ausgestaltung einer Compliance-Organisation verantwortlich (persönliche Compliance-Verantwortung). Dieses Ermessen ist grundsätzlich anhand der Größe der jeweiligen Kommune, ihrer Organisationsstruktur sowie der Heterogenität und Risikogeneigtheit der tatsächlich wahrgenommenen Aufgaben (übertragener Wirkungskreis) auszuüben.

Was umfasst ein angemessenes kommunales CMS?

In Anlehnung an den Prüfungsstandard des IDW PS 980 umfasst ein angemessenes CMS die folgenden miteinander in Wechselwirkung stehenden sieben Grundelemente, die in die Struktur und Abläufe der Organisation einzubinden sowie vollständig zu dokumentieren sind:

1. ***Förderung einer günstigen Compliance-Kultur:***

   Gegenstand der Compliance-Kultur ist die Bedeutung, die der Beachtung von Normen, Regelungen und Werten in der Organisation entgegengebracht wird. Herrscht eine „gute" Compliance-Kultur, sind die Mitarbeitenden in hohem Maße intrinsisch motiviert, sich integer zu verhalten bzw. gegenüber Regelverstößen nicht tolerant zu sein. Für eine günstige Compliance-Kultur bedarf es eines klaren Bekenntnisses der Leitung zu Compliance sowie ihrer Integrität und Vorbildfunktion („tone from the top"). Interessenkonflikte und mögliche Beeinflussungen sind zu vermeiden. Gleiches gilt für die oberen und mittleren Führungskräfte. Für vorsätzliche Regelverstöße muss es angemessene Sanktionen geben (Nulltoleranz).

   Wichtige Maßnahmen sind hier u.a.:

   - ✓ die Erstellung eines **Verhaltenskodex** (für Führungskräfte und Mitarbeitende),
   - ✓ eines **Ehrenkodex** (für kommunale Vertretungen),
   - ✓ eines **Geschäftspartnerkodex** für Lieferanten und Geschäftspartner sowie
   - ✓ die stetige **Sensibilisierung und Beratung** der Führungskräfte und Mitarbeitenden der Kommune.

2. ***Festlegung der Compliance-Ziele:***

   Mit einem CMS sollen in der Regel folgende Ziele erreicht werden:

- ✓ Recht- und Ordnungsmäßigkeit des Verwaltungshandelns (Art. 20 Abs. 3 GG),
- ✓ Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz),
- ✓ Vermeidung materieller Schäden für die Kommune (Vermögensbetreuungspflicht),
- ✓ Abwendung von Aufsichtspflichtverletzungen und Organisationsverschulden,
- ✓ Verringerung von Haftungsrisiken für die Kommune, ihre Organe und Mitarbeitenden,
- ✓ Wahrung des Vertrauens der Bürger*innen in die Rechtsstaatlichkeit, Objektivität und Neutralität der öffentlichen Verwaltung,
- ✓ Effiziente und wirksame Steuerung der Compliance-Risiken,
- ✓ Unterstützung bei der Erfüllung von Nachhaltigkeitszielen und sonstigen strategischen Zielen der Kommune.

Des Weiteren ist bei der Einrichtung eines CMS festzulegen, welche Teilbereiche (Antikorruption, Datenschutz und Datensicherheit, Abgabenrecht usw.) der Kommune vom CMS abgedeckt werden sollen. Sinnvoll ist es, wenn die Teilbereiche mindestens die nach dem Hinweisgeberschutzgesetz geschützten Rechtsgebiete umfassen.

3. Analyse der Compliance-Risiken:

Compliance-Risiken stellen die bewertete Gefahr bzw. Möglichkeit dar, gegen einzuhaltende Regeln zu verstoßen und damit festgelegte Compliance-Ziele zu verfehlen. Compliance-Risiken sind zu identifizieren und – sofern Maßnahmen nicht bereits aufgrund obligatorisch Anforderungen zu ergreifen sind – hinsichtlich ihrer Eintrittswahrscheinlichkeit und möglichen Folgen zu bewerten, um darauf abstellend geeignete Maßnahmen (☞ Compliance-Programm) festzulegen. Wichtige Instrumente hierbei sind die Erstellung:

- ✓ einer **Anforderungs-Maßnahmen-Matrix** und
- ✓ einer **Risiko-Kontroll-Matrix**.

Immaterielle Schäden dürfen bei der Bewertung nicht unberücksichtigt bleiben.

4. Erstellung eines Compliance-Programms:

Auf der Grundlage der identifizierten und bewerteten Compliance-Risiken sind Maßnahmen einzuführen, die auf die Begrenzung der Compliance-Risiken und damit auf die Vermeidung von Regelverstößen ausgerichtet sind. Die Gesamtheit aller dieser Maßnahmen stellt das Compliance-Programm dar, dass auf den drei Funktionen (Säulen) eines CMS aufbaut:

- ✓ die Verhinderung von Regelverstößen (Prävention): ☞ v.a. **Maßnahmen zur Compliance-Kultur**, Einrichtung eines **Internen Kontrollsystems**
- ✓ das rechtzeitige Erkennen von Regelverstößen (Aufdeckung): ☞ v.a. Einrichtung eines Internen Kontrollsystems und eines **Hinweisgebersystems**

- ✓ die Reaktion bei Regelverstößen: ☞ v.a. **Verfahren zum Vorgehen bei Verdachtshinweisen auf Regelverstöße**.

Das konkrete Compliance-Programm muss in Bezug auf die vorgenannten drei Funktionen angemessen sein und auch tatsächlich umgesetzt werden, d.h. wirksam sein.

5. Aufbau der Compliance-Organisation:

Die Compliance-Organisation umfasst die verbindliche Festlegung:

- ✓ der **Aufbau- und Ablauforganisation** des CMS sowie
- ✓ der **Aufgaben, Rollen und Verantwortlichkeiten** des CMS.

In der Regel gehört dazu die Bestellung eines Compliance-Beauftragten, der für die wirksame Ausübung seiner Funktion die notwendige Unabhängigkeit, Kompetenz und organisatorische Stellung haben muss sowie über die erforderlichen Ressourcen verfügen muss.

Die Entscheidung über die Ausgestaltung und Ressourcen der Compliance-Organisation liegt im pflichtgemäßen Ermessen der Kommune, sofern nicht spezialgesetzliche Regelungen (wie z.B. das Hinweisgeberschutzgesetz) greifen.

6. Entwicklung einer Compliance-Kommunikation:

Die Compliance-Kommunikation dient der adressatenorientierten Information aller Akteure eines CMS und umfasst Maßnahmen:

- ✓ zur **Information, Belehrung, Sensibilisierung, Beratung** sowie **Aus- und Weiterbildung** sowie
- ✓ die Festlegung der **Berichterstattung bei Verdachtsfällen** auf Regelverstößen.

7. Entwicklung eines Verfahrens zur Überwachung und Verbesserung des CMS:

Es sind Verfahren bzw. Maßnahmen einzuführen, die Angemessenheit und Wirksamkeit des CMS systematisch überwachen und verbessern. Den entsprechenden Rollen für die Überwachung und Verbesserung liegt das Drei-Linien-Modell des Institute of Internal Auditors (IIA) zugrunde. Danach obliegt:

- ✓ der *ersten Linie* (v.a. Fach- und Querschnittsämter), Compliance-Maßnahmen (einschließlich prozessintegrierter Kontrollen) umzusetzen;
- ✓ der *zweiten Linie* (Beauftragte für bestimmte Bereiche), wozu auch der Compliance-Beauftragte gehört, die erste Linie durch Festlegung von Anforderungen, Beratung und Überwachung der Funktionsfähigkeit der Compliance-Maßnahmen zu unterstützen;
- ✓ der *dritten Linie* (u.a. Interne Revision) die prozessunabhängige Überwachung.

Wozu verpflichtet das Hinweisgeberschutzgesetz?

Das Hinweisgeberschutzgesetz des Bundes verpflichtet **Unternehmen ab 50 Beschäftigten** zur Einrichtung einer internen Meldestelle. Für Kommunen ist das jeweilige Landesrecht maßgeblich, das jedoch nicht hinter der einschlägigen EU-Richtlinie zurückbleiben darf, die **Kommunen ab 10.000 Einwohner** in die Pflicht nimmt. Die wesentlichen Anforderungen an eine Interne Meldestelle sind unmittelbar dem Hinweisgeberschutzgesetz zu entnehmen. Hierbei gilt es u.a. folgende wesentliche Anforderungen zu beachten:

- ✓ Die internen Meldestellen müssen mindestens den Beschäftigten (einschließlich Beamtinnen und Beamten) der Kommune sowie überlassenen Leiharbeitern für die Meldung von Hinweisen auf Regelverstöße offenstehen (**Zugang zur internen Meldestelle**). Allerdings sollte der Kreis der Personen, für die die interne Meldestelle offensteht, aufgrund der allgemeinen Pflicht zur Compliance weitergefasst werden (am besten auch für Externe und Bürger offenstehen).
- ✓ Die internen Meldestellen haben sicherzustellen, dass die **Vertraulichkeit der Identität** der hinweisgebenden Person und der Personen, die Gegenstand einer Meldung sind, gewahrt wird.
- ✓ Die Tätigkeit der internen Meldestelle ist **unabhängig** und mit der erforderlichen **Fachkunde** wahrzunehmen.
- ✓ Zur Einrichtung einer internen Meldestelle gehört auch die **Festlegung des Verfahrens** zur wirksamen Prüfung von Hinweisen und zum Ergreifen weiterer Folgemaßnahmen.

Einzelne Aufgaben der internen Meldestelle können an externe Beauftragte (z.B. Ombudsperson) vergeben werden. Die Verantwortung für die Umsetzung der Vorgaben des Hinweisgeberschutzgesetzes und die Pflicht, geeignete Maßnahmen zu ergreifen, um etwaige Verstöße abzustellen, verbleibt jedoch bei der Leitung der Kommune. In keinem Fall darf die beauftragte Person völlig losgelöst agieren.

Zusammenfassung

Der vorliegende Leitfaden für ein kommunales CMS möchte in Anlehnung an den im geschäftlichen Bereich anerkannten Prüfungsstandard IDW PS 980 einen entsprechenden Standard für die öffentliche Verwaltung etablieren. Der hier vorangestellte Überblick über die zentralen Inhalte des CMS soll den kommunalen Organverantwortlichen eine Entscheidungshilfe für die Einrichtung eines kommunalen CMS sein. Eingeordnet in den größeren Zusammenhang der Agenda 2030 der Vereinten Nationen, in der 17 globale Ziele für nachhaltige Entwicklung festgelegt sind, gewährleistet ein CMS die uneingeschränkte demokra-

tische Rechenschaftslegung der Kommunalverwaltungen durch eine transparente und unbestechliche öffentliche Verwaltung. So heißt es im Entwurf des Hinweisgeberschutzgesetztes der Bundesregierung (Bundestag-Drucksache 20/3442 vom 19.09.2022): Mit Verweis auf die Deutsche Nachhaltigkeitsstrategie der Bundesregierung 2021 leistet der Entwurf *„damit insbesondere einen Beitrag zur Verwirklichung von Nachhaltigkeitsziel 16 ‚Friedliche und inklusive Gesellschaften für eine nachhaltige Entwicklung fördern, allen Menschen Zugang zur Justiz ermöglichen und leistungsfähige, rechenschaftspflichtige und inklusive Institutionen auf allen Ebenen aufbauen'. Insbesondere trägt er zur Förderung von Rechtsstaatlichkeit auf nationaler und internationaler Ebene (Unterziel 16.3) und zum Aufbau leistungsfähiger, rechenschaftspflichtiger und transparenter Institutionen (Unterziel 16.6) bei.*"

Das Gelingen einer guten Verwaltungsführung auf kommunaler Ebene, zu der vor allem auch ein effektives CMS zählt, hängt wesentlich von den Organverantwortlichen ab. Mit dem folgenden Teil 2 geben wir den Landkreisen, Städten und Gemeinden Module für die Einrichtung eines Compliance Management Systems an die Hand, das leicht an die konkreten örtlichen Anforderungen angepasst werden kann.

Teil 2 – Detaillierte Darstellung

1. Einleitung

1.1 Ausgangssituation

(1) Die Einrichtung und Prüfung von Compliance Management Systemen (CMS) hat in den letzten Jahren auch für die kommunale Verwaltung an Bedeutung gewonnen. Dazu haben Gesetzgebung und Rechtsprechung und nicht zuletzt die behördliche Praxis beigetragen.

1.2 Zielsetzung und Geltungsbereich

(2) Der vorliegende Leitfaden gibt den Verantwortlichen in den Kommunen (und öffentlichen Unternehmen) einen Orientierungsrahmen für die Einrichtung (und den Betrieb) sowie die Prüfung eines kommunalen CMS an die Hand, der sich am gesetzlichen Pflichtenrahmen ausrichtet und dabei auch das obligatorische Hinweisgebersystem berücksichtigt. Der Leitfaden ist unter Berücksichtigung der länder- und kommunalspezifischen Regelungen in den einzelnen Bundesländern anzuwenden. Darüber hinaus kann es für einzelne Teilbereiche (Rechtsgebiete) des CMS weitergehende gesetzliche Pflichten geben, die ebenfalls zu berücksichtigen sind.

1.3 Aufbau / Vorgehensweise

(3) Der Aufbau des kommunalen CMS richtet sich im Rahmen der rechtlichen Vorgaben an den Grundelementen des Prüfungsstandards des IDW PS 980 bzw. des IDW EPS 980 (Entwurf)[1] aus, ergänzt um Aspekte des ISO 37301[2]. Für das Hinweisgebersystem – als Teil des kommunalen CMS – kann subsidiär zu den gesetzlichen Vorgaben die ISO 37002[3] herangezogen werden.

(4) Für die Prüfung des CMS sind über diesen Leitfaden hinaus die Standards für die berufliche Praxis heranzuziehen.[4]

---

1 IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980), Stand 11.03.2011 sowie Entwurf einer Neufassung als IDW EPS 980, Stand 28.10.2021.

2 ISO 37301:2021 Compliance management systems – Requirements with guidance for use (Nachfolger der ISO 196000).

3 ISO 37002:2021, Whistleblowing Management Systems – Guidelines (First Edition 2021-07-27).

4 Vgl. u.a. Deutsches Institut für Interne Revision e. V. (DIIR), Institut für Interne Revision Österreich (IIA Austria), Schweizerischer Verband für Interne Revision (IIA Switzerland) als Herausgeber der deutschen Auflage der International Professional Practices Framework (IPPF): Internationale Standards für die berufliche Praxis der Internen Revision 2017, Version 6.1 vom 10. Januar 2018, Frankfurt am Main.

1.4 Verfasser

(5) Der Leitfaden wurde durch die Projektgruppe Antikorruption-Compliance des Instituts der Rechnungsprüfer e.V. (Deutschland) erstellt. An der Erstellung haben mitgewirkt:

- *Adam Breuninger*, Compliance Officer (Univ.), stellvertretender Leiter der Zentralen Antikorruptionsstelle und Sachgebietsleiter im Amt für Revision der Landeshauptstadt Stuttgart, vormals Rechtsanwalt bei einer Kanzlei
- *Dr. Peter Glinder*, stellvertretender Leiter des Amts für Revision und Leiter der Zentralen Antikorruptionsstelle der Landeshauptstadt Stuttgart, Lehrbeauftragter an der Hochschule für Verwaltung und Finanzen Ludwigsburg
- *Prof. Dr. Dr. Jürgen Louis*, Bürgermeister der Gemeinde Rheinhausen/Breisgau, Rechtsanwalt (Rechte aus der Zulassung ruhen kraft Gesetzes wegen Amtsausübung als Bürgermeister), Honorarprofessor an der Hochschule für öffentliche Verwaltung Kehl, Leiter der Regionalgruppe Baden-Württemberg von Transparency International Deutschland e.V.
- *Otto Reiners*, Internvertreter der Landesrätin des Dezernats Jugend und Schule, Referatsleiter für Schulen, Jugendheime, Controlling im Landschaftsverbands Westfalen-Lippe (LWL), vormals stellvertretender Leiter des Rechnungsprüfungsamts des LWL
- *Kathrin Rönsch*, Mitarbeiterin der Zentralen Antikorruptionsstelle der Landeshauptstadt Stuttgart
- *Dr. Christel Schrage,* Stellvertretende Leiterin des Rechnungsprüfungsamtes des Landschaftsverbands Westfalen-Lippe (LWL) und Referatsleiterin für Querschnittsprüfungen.
- *Anna Schwarzer*, Compliance Officer (Univ.), Mitarbeiterin der Zentralen Antikorruptionsstelle der Landeshauptstadt Stuttgart, vormals Rechtsanwältin bei einer größeren Kanzlei

Der Leitfaden wurde evaluiert von:

- *Prof. Dr. Ludwig M. Bauer*, Professor für Internes und Externes Rechnungswesen, Duale Hochschule Baden-Württemberg (DHBW), Villingen-Schwenningen, Fakultät für Wirtschaft; Dipl.-Betriebswirt, Dipl.-Handelslehrer, Wirtschaftsprüfer/Steuerberater.
- *Peter Huber*, Leiter des Revisionsamts der Landeshauptstadt Mainz.
- *Mara Manzel,* Beauftragte für Compliance, Stadt Dortmund
- *Gerhard Richter,* Partner bei Rödl & Partner, Wirtschaftsprüfer / Steuerberater.

- *Kathrin Scholz,* Antikorruptionskoordinatorin der Stadt Chemnitz, Dezernat Recht, Sicherheit und Umweltschutz
- *Oliver Schulz*, Vertriebs-/Marketingleiter WTT CampusONE als Partner für das Thema digitale Mitarbeiterschulungen/Unterweisungen.

September 2023

2. Quick Guide (Kurzanleitung)

(6) Der Quick Guide ist eine kompakte Kurzform des vorliegenden Leitfadens zur Einrichtung und Prüfung eines kommunalen CMS und stellt übersichtlich die wichtigsten Anforderungen für einen schnellen Einstieg in die Materie dar. Es werden die einzelnen Schritte zur Einrichtung und Prüfung eines kommunalen CMS aufgeführt. Jeder Schritt beginnt mit einer Übersichtsdarstellung in Tabellenform. Dort sind die jeweiligen Aktivitäten bzw. Aufgaben („was ist zu tun?") aufgeführt, die einzelnen CMS-Grundelementen zugeordnet sind. Außerdem wird angezeigt, ob mit der Aufgabe eine Finanzrelevanz oder ein hoher Zeitaufwand einhergehen (dabei handelt es sich um Einschätzungen, die je Kommune unterschiedlich sein können). An die Übersichtstabelle schließen sich – soweit erforderlich – kurze Erläuterungen und Verweise auf die Langfassung (die in den Abschnitten 3 ff. dargestellt ist) an. Für die Auslegung dieses Leitfadens ist die Langfassung maßgeblich.

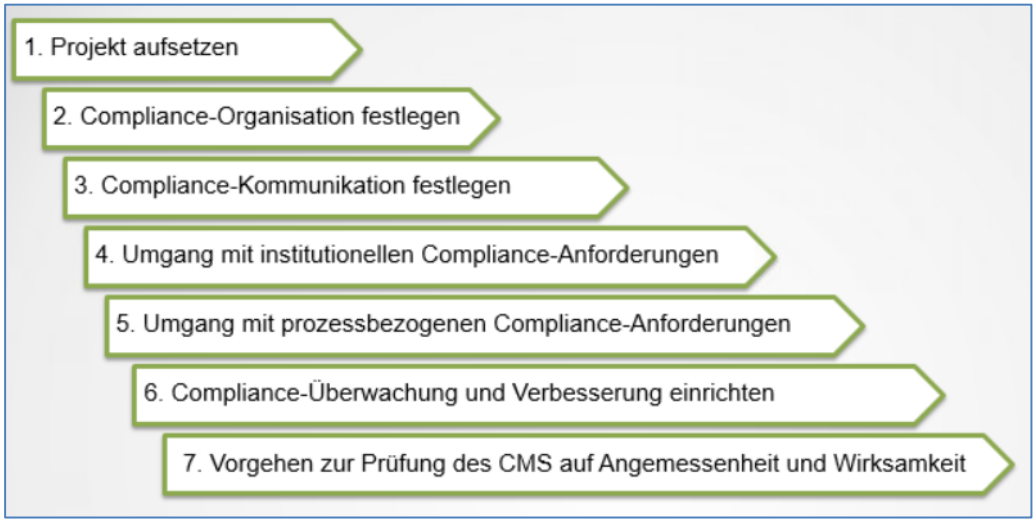
(7) Begrifflichkeiten:

- *Compliance*: Die Verwaltungsorgane einer Kommune haben im Rahmen ihrer Zuständigkeit dafür Sorge zu tragen, dass alle formellen und materiellen Gesetze[5] sowie alle verwaltungsinternen Regelungen[6] eingehalten werden.
- *Compliance Management System – CMS* (☞ Tz. 31): Die Gesamtheit aller Regelungen (hinsichtlich Strukturen, Prozesse und Maßnahmen) der Kommune, die sicherstellen sollen, dass die Akteure der Kommune regelkonform handeln und damit wesentliche Regelverstöße verhindert werden.
- *Akteure der Kommune (*☞ Tz. 32*)*: Behördenleitung wie (Ober-)Bürgermeister, Landrat etc., Mitarbeitende, Mitglieder der Volksvertretung, beauftragte Dritte, Zuwendungsempfänger.
- *CMS-Funktionen - drei Säulen* (☞ Tz. 34): Prävention, Aufdeckung, Reaktion.
- *CMS*-Grundelemente: Jedes angemessene CMS umfasst die sieben miteinander in Wechselwirkung stehenden Grundelemente: Compliance-Kultur, Compliance-Ziele, Compliance-Risiken, Compliance-Programm, Compliance-Organisation, Compliance-Kommunikation, Compliance-Überwachung und Verbesserung. Sie sind in die Struktur und Abläufe der Organisation einzubinden.
- *CMS-Teilbereiche (*☞ Tz. 33): Nach Rechtsgebieten abgrenzbare Teilbereiche eines CMS.

[5] V.a. Bundes- oder Landesrecht sowie Rechtsverordnungen, Satzungen oder Verwaltungsvorschriften.
[6] V.a. Dienstanweisungen, Richtlinien, Rundschreiben oder Anweisungen.

- *CMS-Richtlinie* (☞ Abschnitt 4.6.5): Dienstanweisung, in der alle Festlegungen zu Aufbau, Verfahren, Zuständigkeiten, Rollen und Befugnissen des CMS der Kommune aufgenommen werden.
- *CMS-Dokumentation* (☞ Tz. 53): CMS-Richtlinie, weitere relevante CMS-Regelungen der Kommune, Zuständigkeitsregelungen, Prozessbeschreibungen und -visualisierungen sowie im Rahmen der Umsetzung des CMS erstellte Berichte, Protokolle, Anforderungs- und Risikoinventars, Checklisten etc.

Abbildung 1: Quick Guide - Einrichtung und Prüfung eines kommunalen CMS



2.1 Schritt 1: Projekt aufsetzen

(8)

Aufgaben / Aktivitäten	Wesentlich tangierte CMS-Grundelemente	**F**inanzrelevant, rel. hoher **Z**eitaufwand
a. Projektauftrag durch Behördenleitung		
b. Commitment Behördenleitung (tone at the top)	C.-Kultur	
c. Festlegung Compliance-Ziele (strategische Ziele, Teilbereiche)	C.-Ziele	Z
d. Festlegung Projektteam		
e. Festlegung Projektorganisation (Aufbau, Ablauf, Steuerung)		
f. Angemessene Ressourcenausstattung		F
g. Beteiligung Personalrat, Gemeinderat		

(9) Erläuterungen:

- Die Festlegung der Compliance-Ziele determiniert den Umfang bzw. die Komplexität des einzurichtenden CMS. Der Umfang der einzubeziehenden Teilbereiche hängt maßgeblich von der Größenklasse (Kategorie) einer Kommune ab ☞ Abschnitt 3.5.

(10) Verweise:

- Für Projekt insgesamt ☞ Abschnitt 3.6.
- Für b. ☞ Tz. 58.
- Für c. ☞ Abschnitt 4.2.

2.2 Schritt 2: Compliance-Organisation festlegen

(11)

Aufgaben / Aktivitäten	Wesentlich tangierte CMS-Grundelemente	**F**inanzrelevant, rel. hoher **Z**eitaufwand
a. Zentrale Zuordnung der Compliance-Funktion zu einer Organisationseinheit der Kommune ☞ i.d.R. direkt unter der Behördenleitung oder eine ihr naheliegende Stellung.	C.-Organisation	
b. Bestellung eines Compliance-Beauftragten (Wahrnehmung der Compliance-Funktion), Festlegung von dessen Aufgaben und Befugnissen (u.a. dessen Unabhängigkeit).	C.-Organisation	
c. Bereitstellung erforderlicher Ressourcen (Stellen, Sachmittel, IT)	C.-Organisation	F
d. Bei größeren Kommunen ggf. zusätzlich dezentrale Ansprechpersonen für Compliance-Teilbereiche festlegen.	C-Organisation	
e. Ggf. ergänzende Beauftragung Externer (festlegen, in welchen Fällen dies erfolgen kann).	C-Organisation	F
f. Erstellen einer CMS-Richtlinie (Dienstanweisung), in der Aufbau, Verfahren, Rollen und Zuständigkeiten im CMS der Kommune festgelegt werden.	C-Organisation	Z

(12) Erläuterungen:

- Die Festlegung der Compliance-Organisation liegt im pflichtgemäßen Ermessen der Kommune (insbesondere der Behördenleitung, ggf. Gemeinderat).
- Die Festlegungen zur Aufbauorganisation umfassen die Zuordnung der Compliance-Funktion an eine zentrale Organisationseinheit in der Kommune sowie die Bestellung eines Compliance-Beauftragten, der für eine wirksame

Aufgabenwahrnehmung mindestens folgende Befugnisse erhalten sollte: direktes Vortragsrecht beim Behördenleiter, Initiativrecht beim Aufgreifen Compliance-relevanter Themen, Unabhängigkeit und Weisungsungebundenheit beim Nachgehen von Verstößen. Der Compliance-Beauftragte sollte über die notwendigen fachlichen und sozialen Kompetenzen verfügen, damit er seinen Aufgaben wirksam nachgehen kann.

- Für eine wirksame Wahrnehmung der Compliance-Funktion durch den Compliance-Beauftragten bedarf es einer angemessenen Ressourcenausstattung (Stellen, Sachmittel, IT).

(13) Verweise:

- Für a. ☞ Abschnitt 4.6.1.
- Für b. ☞ Abschnitt 4.6.2.
- Für c. ☞ Abschnitt 4.6.4.
- Für d. ☞ Abschnitt 4.5.3.
- Für e. ☞ Abschnitt 4.6.1.
- Für f. ☞ Abschnitt 4.6.5.

2.3 Schritt 3: Compliance-Kommunikation festlegen

(14)

Aufgaben / Aktivitäten	Wesentlich tangierte CMS-Grundelemente	**F**inanzrelevant, rel. hoher **Z**eitaufwand
a. Festlegungen zum Compliance-Berichtswesen innerhalb der Kommune.	C.-Kommunikation	
b. Festlegungen zur Compliance-Kommunikation mit externen Stellen (v.a. Strafverfolgungsbehörden, externe Stellen der öffentlichen Verwaltung, beauftragte Rechtsanwälte).	C-Kommunikation	
c. *Kommunikation der Compliance-Kultur (siehe Schritt 4: institutionelle Anforderung).*	C-Kommunikation, C.-Risiken	

(15) Erläuterungen:

- Das Compliance-Berichtswesen umfasst folgende Berichtspflichten an die Behördenleitung und die verantwortlichen Führungsebenen der Kommune: Berichte zu identifizierten Compliance-Anforderungen bzw. Compliance-Risiken und den ergriffenen Maßnahmen; Berichte zu den eingegangenen und überprüften Verdachtshinweisen auf Regelverstöße; Berichte zur Reaktion

auf festgestellte Regelverstöße; Berichte zu den Ergebnissen der Überwachung und Verbesserung des CMS.

- Die Compliance-Kommunikation mit externen Stellen findet i.d.R. im Zusammenhang mit Verdachtshinweisen auf Regelverstöße und deren Aufarbeitung statt.
- Die Festlegungen zur Compliance-Kommunikation sind in der CMS-Richtlinie aufzunehmen.

(16) Verweise:

- Für a. bis c. ☞ Abschnitt 4.7.

2.4 Schritt 4: Umgang mit institutionellen Compliance-Anforderungen

(17)

Aufgaben / Aktivitäten	Wesentlich tangierte CMS-Grundelemente	**F**inanzrelevant, rel. hoher **Z**eitaufwand
a. Analyse der institutionellen Compliance-Anforderungen als systematischen Prozess ausgestalten und in CMS-Richtlinie (Dienstanweisung) festlegen.	C-Risiken, C.-Organisation	Z
b. Institutionelle Compliance-Anforderungen aus den CMS-Grundelementen und rechtlichen Anforderungen identifizieren und Anforderungsinventar erstellen.	C.-Risiken	Z
c. Für die identifizierten institutionellen Compliance-Anforderungen angemessene Maßnahmen und die dafür Verantwortlichen festlegen (Compliance-Programm) und Anforderungs-Maßnahmen-Matrix erstellen.	C-Risiken, C-Programm	

(18) Erläuterungen:

- Der systematische Prozess zur Anforderungsanalyse ist in der CMS-Richtlinie festzulegen.
- Institutionelle Compliance-Anforderungen bestehen für die gesamte betrachtete Kommune über alle CMS-Teilbereiche hinweg. Sie ergeben sich aus den Anforderungen der einzelnen CMS-Grundelemente sowie rechtlichen Anforderungen.
- Angemessene Maßnahmen umfassen in der Regel mindestens: Verhaltenskodex für Mitarbeitende, Regelungen zur Vermeidung von Interessenkonflikten (aus Befangenheit, Nebentätigkeit, Vorteilsannahme, Spenden, Sponsoring), Ehrenkodex für die kommunalen Mandatsträger, Geschäftspartnerko-

dex, Sensibilisierung (einschließlich Information, Belehrung, Beratung, Fortbildung), Veröffentlichung wesentlicher Regelungen, Einrichtung eines Hinweisgebersystems (Hinweise entgegennehmen und ihnen nachgehen) und Verfahren für Folgemaßnahmen (Sanktionen für nicht regelkonformes Verhalten, Verbesserung des CMS) festlegen.

(19) Verweise:

- Für a. ☞ Abschnitte 4.4.3, 4.6.5.
- Für b. und c. ☞ Abschnitte 4.4.1, 4.5

2.5 Schritt 5: Umgang mit prozessbezogenen Compliance-Risiken

(20)

Aufgaben / Aktivitäten	Wesentlich tangierte CMS-Grundelemente	**F**inanzrelevant, rel. hoher **Z**eitaufwand
a. Analyse der prozessbezogenen Compliance-Risiken als systematischen Prozess ausgestalten und in CMS-Richtlinie (Dienstanweisung) festlegen.	C-Risiken, C.-Organisation	Z
b. Prozessbezogene Compliance-Risiken in den einzelnen Verwaltungsprozessen der CMS-Teilbereiche identifizieren und Risikoinventar erstellen.	C.-Risiken	Z
c. Die identifizierten prozessbezogenen Compliance-Risiken sind zu bewerten (Eintrittswahrscheinlichkeit, mögliche Folgen) und in einer Risikomatrix darzustellen.	C-Risiken	Z
d. Für die bewerteten prozessbezogenen Compliance-Risiken sind angemessene Maßnahmen (insbesondere Kontrollen, IKS) und die dafür Verantwortlichen festzulegen (Compliance-Programm) und in eine Risiko-Kontroll-Matrix aufzunehmen.	C-Risiken, C-Programm	

(21) Erläuterungen:

- Der systematische Prozess der Risikoanalyse ist in der CMS-Richtlinie festzulegen.
- Prozessbezogene Risiken treten in den einzelnen Verwaltungs- und Geschäftsprozessen der CMS-Teilbereiche auf. Zur Identifizierung und Bewertung der dort enthaltenen Risiken bedarf es der detaillierten Betrachtung dieser Prozesse.

- Auf der Grundlage der Bewertung der identifizierten Risiken sind angemessene Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit und/oder der möglichen Folgen festzulegen. In Betracht kommen hier v.a. Kontrollmaßnahmen im Rahmen eines Internen Kontrollsystems (IKS).
- Da der Aufwand für die Risikoidentifizierung erfahrungsgemäß hoch ist, kann aus Aufwands- und/oder Akzeptanzgründen zunächst mit den Teilbereichen und Geschäftsprozessen begonnen werden, denen wesentliche bzw. bedeutsame Compliance-Risiken inhärent sind (sukzessives Vorgehen).

(22) Verweise:

- Für a. ☞ Abschnitte 4.4.3, 4.6.5.
- Für b., c. und d. ☞ Abschnitte 4.4.2, 4.5.

2.6 Schritt 6: Compliance-Überwachung und Verbesserung einrichten

(23)

Aufgaben / Aktivitäten	Wesentlich tangierte CMS-Grundelemente	**F**inanzrelevant, rel. hoher **Z**eitaufwand
a. Festlegung der Überwachung des CMS auf *Angemessenheit* und *Wirksamkeit* durch die zweite Linie (Compliance-Beauftragter, Beauftragte für einzelne Teilbereiche) und dritte Linie (prozessunabhängige Rechnungsprüfung, Interne Revision, externe Prüfer), insbesondere Erstellung eines mehrjährigen Überwachungsplans (Prüfungsmaßnahmen, Verantwortliche, Termine). Festlegung, dass bei (gravierenden) Regelverstößen Sanktionsmaßnahmen zu prüfen sind.	C.-Überwachung	F (bei Externen) Z
b. Festlegungen zur Ursachenanalyse und zum Konsequenzen-Management bei festgestellten Schwachstellen im CMS der Kommune.	C.-Verbesserung	

(24) Erläuterungen:

- Der Überwachung und Verbesserung des CMS liegt das Drei-Linien-Modell des Institute of Internal Auditors (IIA) zugrunde.

(25) Verweise:

- Für a. ☞ Abschnitt 4.8.1; für die Begriffe Angemessenheit und Wirksamkeit ☞ Abschnitt 7.1.
- Für b. ☞ Abschnitte 4.8.2.

2.7 Schritt 7: Vorgehen zur Prüfung des CMS auf Angemessenheit und Wirksamkeit

(26)

Aufgaben / Aktivitäten	Wesentlich tangierte CMS-Grundelemente	**F**inanzrelevant, rel. hoher **Z**eitaufwand
1. Festlegung, ob die Prüfung als *Angemessenheits- oder Wirksamkeitsprüfung* angelegt wird. 2. Planung und Vorbereitung der Prüfung: a. Ressourcen bereitstellen. b. Prüfung ankündigen, CMS-Dokumentation anfordern und sichten. c. Prüfungskonzept und *Prüfungscheckliste* mit Bewertungsskala (sie bildet den Grundsatz der Wesentlichkeit ab) erstellen. 3. Prüfung durchführen anhand Befragungen, Analyse der vorhandenen CMS-Dokumentation, Beobachtungen, IT-gestützter Prüfungshandlungen zum IKS, vorhandener Prüfungsberichte. 4. Prüfungsbericht mit Prüfungsfeststellungen und Empfehlungen sowie einem Prüfungsurteil (ergibt sich nach der Beantwortung der Prüfungscheckliste) an die Behördenleitung fertigen. 5. Maßnahmenverfolgung durchführen.	C.-Überwachung	Z

(27) Erläuterungen:

- Die Prüfung des eingerichteten CMS der Kommune muss nicht notwendigerweise mit Abschluss der vorherigen Schritte im Rahmen des Projektes erfolgen. Für die Wirksamkeitsprüfung ist ohnehin erforderlich, dass das CMS bereits seit einem gewissen Zeitraum implementiert ist. Darüber hinaus ist die Prüfung des CMS eine Daueraufgabe, die im Rahmen der Mehrjahresprüfungsplanung zu berücksichtigen ist.
- Die Prüfung des CMS der Kommune ist eine Systemprüfung und nicht darauf gerichtet, einzelne Regelverstöße aufzudecken. Sie umfasst aufgrund ihres Charakters als Systemprüfung stets alle Grundelemente eines CMS. Eine isolierte Prüfung einzelner CMS-Grundelemente liegt nicht im Anwendungsbereich dieses Leitfadens. Hingegen ist es möglich, dass nur einzelne Teilbereiche des CMS geprüft werden (hierfür jedoch alle CMS-Grundelemente).

- Es ist empfehlenswert, eine Prüfungscheckliste zu erstellen. Hierzu kann auf die in Anlage 9 (☞ Abschnitt 8.9) beigefügte Muster-Prüfungscheckliste zurückgegriffen werden, die für die jeweilige Prüfung anzupassen ist. Der Grundsatz der Wesentlichkeit für die Beurteilung des Prüfungsergebnisses spiegelt sich in der Muster-Prüfungscheckliste in der Bewertungsskala wider.

(28) Verweise:

- Für 1. bis 5. ☞ Abschnitt 7.

3. Rahmen und Begrifflichkeiten eines kommunalen CMS

3.1 Definition von Compliance

(29) Für diesen Leitfaden wird Compliance wie folgt definiert: Die Verwaltungsorgane einer Kommune haben im Rahmen ihrer Zuständigkeit dafür Sorge zu tragen, dass alle formellen und materiellen Gesetze[7] sowie alle verwaltungsinternen Regelungen[8] eingehalten werden. Sie wirken auf deren wirksame Beachtung in der Kommune hin.

(30) Bislang gibt es in Deutschland keine einheitliche Definition für den Begriff „Compliance" bzw. für ein Compliance Management System. Die in Tz. 29 verwendete Definition ist aus folgenden bedeutenden Quellen hergeleitet:

- Der Bundesgerichtshof (BGH) führte in seinem Urteil vom 09.05.2017, 1 StR 265/16, Rdnr. 118, aus, dass Unternehmen die Pflicht haben, *„Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden"* und dass ein Compliance Management *„auf die Vermeidung von Rechtsverstößen ausgelegt"* ist.
- Im Deutschen Corporate Governance Kodex (DCGK)[9], der Grundsätze, Empfehlungen und Anregungen zur Leitung und Überwachung deutscher börsennotierter Gesellschaften enthält, wird mit dem Grundsatz 5 im Abschnitt A. I. Compliance wie folgt definiert: *„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance)."*
- Im Deutschen Public Corporate Governance Musterkodex (D-PCGM)[10], welcher Standards für die gute Unternehmensführung öffentlicher Unternehmen

---

7 V.a. Bundes- oder Landesrecht sowie Rechtsverordnungen, Satzungen oder Verwaltungsvorschriften.

8 V.a. Dienstanweisungen, Richtlinien, Rundschreiben oder Anweisungen.

9 Vgl. DCGK (2022): Deutscher Corporate Governance Kodex (DCGK) vom 28.04.2022; jeweils aktuelle Fassung: https://www.dcgk.de/de/kodex.html.

10 Vgl. D-PCGM (2022): Expertenkommission D-PCGM (2022): Deutscher Public Corporate Governance-Musterkodex (D-PCGM), Hrsg. Ulf Papenfuß/Klaus-Michael Ahrend/Kristin Wagner-Krechlok, in der Fassung vom 14.03.2022, https://doi.org/10.13140/RG.2.2.14710.47688.

festlegt, steht in Ziffer 7.2, Tz. 136 D-PCGM folgende Definition: *„Das Geschäftsführungsorgan hat für die Einhaltung der gesetzlichen Bestimmungen, der öffentlich-rechtlichen Vorschriften insbesondere im Zusammenhang mit den übertragenen Aufgaben und deren Finanzierung, der unternehmensinternen Richtlinien und Regelungen, die aus identifizierten Risiken und daraus abgeleiteten Maßnahmen resultieren, zu sorgen (Legalitätskontrollprinzip) und auch auf deren wirksame Beachtung durch die Konzernunternehmen hinzuwirken (Compliance).*"

- Nach dem IDW PS 980[11], Nr. 2, Tz. 5 ist unter Compliance schlicht *„die Einhaltung von Regeln zu verstehen (gesetzliche Bestimmungen und unternehmensinterne Richtlinien)*."

3.2 Definition und Funktionen eines CMS

(31) Unter einem CMS werden – in Anlehnung an IDW PS 980[12] – für diesen Leitfaden die Gesamtheit aller Regelungen (hinsichtlich Strukturen, Prozesse und Maßnahmen) der Kommune verstanden, die darauf abzielen bzw. sicherstellen sollen, dass die Akteure der Kommune regelkonform handeln und damit wesentliche Regelverstöße verhindert werden (Verwaltungssystem zur Regeleinhaltung).

(32) ***Akteure*** der Kommune (in diesem Sinne) sind:

- ihre gesetzliche Vertretung, also (Ober-)Bürgermeister, Landrat etc. (bei öffentlichen Unternehmen ihre Geschäftsführungen),
- ihre Mitarbeitenden,
- die Mitglieder der kommunalen Volksvertretung (Gemeinderat, Kreistag etc.),
- Dritte, bei deren Beauftragung von der Kommune Sorgfaltspflichten zu erfüllen sind (u.a. Verwaltungshelfer, Lieferanten) sowie
- Dritte, die von der Kommune als Zuwendungsgeberin freiwillige zweckgebundene Leistungen erhalten[13].

(33) Ein CMS umfasst in der Regel mehrere nach Rechtsgebieten (und ggf. darunter nach einzelnen Organisationseinheiten) abgrenzbare ***Teilbereiche***, für die eine Analyse der jeweiligen Compliance-Risiken durchzuführen ist. In einer Kommune sind u.a. folgende Teilbereiche betroffen (keine vollständige Aufzählung):

---

[11] IDW PS 980, Stand 11.03.2011.

[12] Vgl. IDW PS 980, Stand 11.03.2011, Nr. 2, Tz. 6; vgl. Entwurf IDW EPS 980, Stand 28.10.2021, Nr. 1.2, Tz. 13b).

[13] Zur Abgrenzung des Begriffs Zuwendungen vgl. VV-BHO zu § 23 Nr. 1. Danach gehören nicht zu den Zuwendungen insbesondere: Sachleistungen, Leistungen, auf die ein unmittelbar begründeter Rechtsanspruch besteht, Aufwandsersatz, vertragliche Entgelte, Mitgliedsbeiträge, Pflichtumlagen.

- Kommunalrecht (u.a. Gemeindeordnung, Landkreisordnung, Gemeindehaushaltsverordnung)
- Antikorruptionsrecht (Bestechungs- und Begleitdelikte)
- Abgabenrecht (Steuern, Gebühren, Beiträge)
- Vergaberecht, auch Verpflichtungsgesetz (förmliche Verpflichtung nichtbeamteter Personen, wenn diese Aufgaben der öffentlichen Verwaltung wahrnehmen)
- Subventions-, Zuwendungs- und EU-Beilhilferecht
- Datenschutz- und Datensicherheitsrecht sowie rechtliche Anforderungen an die IT
- Umweltrecht
- Gesundheitsschutz
- öffentliches Planungsrecht
- Sozial- und Jugendrecht, u.a. auch Sorgfaltspflichten
- Recht der öffentlichen Sicherheit
- Garanten-, Aufsichts- und Betreiberpflichten
- Spenden und Sponsoring
- Dienst- und Arbeitsrecht (u.a. auch Arbeitszeitrecht, Reisekostenrecht, Überstundenvergütung, Zulagen, Gleichstellungsrecht, Verbot der Annahme von Vorteilen und Nebentätigkeitsrecht)
- Recht zur Arbeitssicherheit und Unfallverhütung
- kommunalrechtliche und verwaltungsverfahrensrechtliche Hinderungsgründe und Befangenheitsregeln
- Haushalts- und Kassenrecht (u.a. Regelungen zu Funktionstrennungen und zum Mehr-Augenprinzip)
- Rechtliche Vorgaben zum Schutz von Dienst-, Geschäfts- und Betriebsgeheimnissen
- Einhaltung von Anzeige- und Veröffentlichungspflichten
- *vornehmlich bei öffentlichen Unternehmen*: Kartellrecht, Recht des unlauteren Wettbewerbs, Konzessionsrecht
- Public Corporate Governance Kodizes *für öffentliche Unternehmen* (sie haben zwar an sich freiwilligen Charakter, können aber durch Aufnahme in Satzungen und Gesellschaftsverträge verbindlich werden).

(34) Ein wirksames CMS erfüllt folgende drei Funktionen (***drei Säulen eines CMS***):

- ***Präventionsfunktion*:** Mögliche Gesetzes- und Regelverstöße sollen vermieden werden. Hierzu sind Richtlinien und Abläufe innerhalb einer Organisation zu schaffen, die die Handelnden vor einem Fehlverhalten bewahren. Diese Präventionsfunktion umfasst u.a.:
  - *Beratung und Information*: Das Wissen von bestehenden Regeln und das Bewusstsein für Risiken von Regelverstößen und deren Konsequenzen müssen bei den Akteuren (☞ Tz. 32) geschärft werden.[14]
  - *Formalisierung und Standardisierung* bzgl. der Festsetzung von (angemessenen) Verhaltensstandards.[15]
  - *Qualitätssicherung und Integrität*: Sicherstellung der Ausführungsqualität der zu erbringenden kommunalen Leistungen, u.a. durch Einrichtung eines Internen Kontrollsystems, sowie kontinuierliche Weiterentwicklung bestehender organisatorischer und personalwirtschaftlicher Maßnahmen. Dabei ist insbesondere auch das integre Verhalten aller Akteure (☞ Tz. 32) zu fördern.
  - *Transparenz*: Verwaltungshandeln muss nachvollziehbar und kontrollierbar sein.[16] Dies bedingt auch die Herstellung von Öffentlichkeit, soweit dies gesetzlich möglich ist.
  - *Öffentlichkeitsarbeit*: Vertrauensbildung in die Integrität der öffentlichen Verwaltung[17] durch angemessene Öffentlichkeitsarbeit.
- ***Aufdeckungsfunktion:*** Die Höhe der Entdeckungswahrscheinlichkeit von Regelverstößen hat mit Einfluss darauf, ob bzw. wie häufig Regelverstöße auftreten. Für eine angemessene Entdeckungswahrscheinlichkeit sind wirksame Maßnahmen bzw. Mechanismen zu installieren, wozu insbesondere ein Internes Kontrollsystem und ein Hinweisgebersystem gehören. Solche Maßnahmen haben zugleich präventiven Charakter. Hinweisen auf Regelverstößen ist nachzugehen.
- ***Reaktionsfunktion:*** Die Reaktion auf aufgedeckte Regelverstöße besteht aus der Sanktionierung des Verhaltens, das zu Regelverstößen geführt hat,

---

[14] Vgl. Lösler, Thomas: Das moderne Verständnis von Compliance im Finanzmarktbereich, in: NZG 2005, 104 (105).

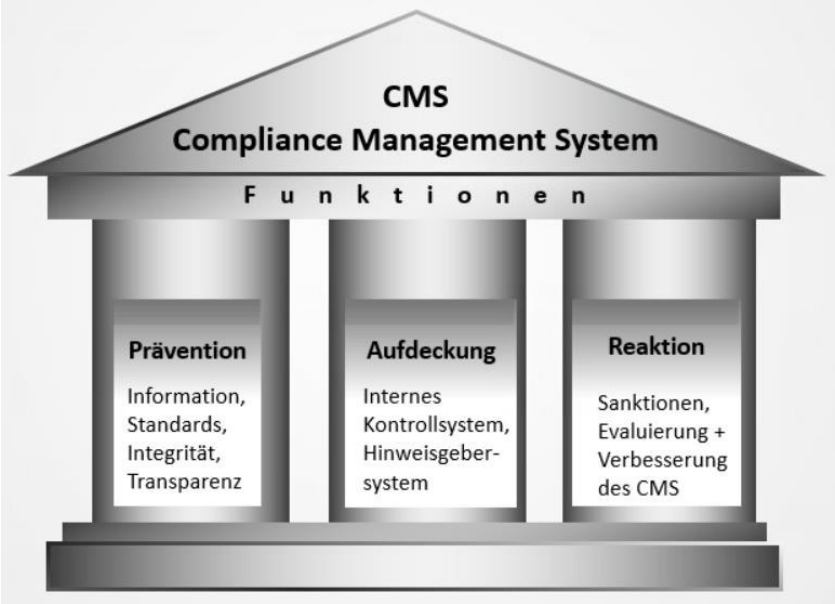
[15] Vgl. Schulz/Galster, in: Bürkle/Hauschka et al.: Der Compliance Officer, 1. Auflage 2015, § 3 Rn. 16.

[16] Vgl. Stober, Rolf, in: Stober/Ohrtmann: Compliance, Handbuch für die öffentliche Verwaltung, 2. Auflage 2022, § 1 Rn. 28; vgl. auch den Transparenzgrundsatz im Vergaberecht gemäß § 97 Abs. 1 GWB.

[17] Vgl. Schulz/Galster, in: Bürkle/Hauschka et al.: Der Compliance Officer, 1. Auflage 2015, § 3 Rn. 17; vgl. Lösler, a.a.O.

sowie aus der Evaluierung und Verbesserung der Abläufe, die die Regelverstöße ermöglicht haben.

Abbildung 2: Die drei Säulen eines CMS



3.3 Rechtlicher Rahmen für Compliance in der öffentlichen Verwaltung

(35) Es gibt keine ausdrückliche Pflicht für die öffentliche Verwaltung ein CMS einzurichten. Jedoch kann eine solche Pflicht der öffentlichen Verwaltung (das „Ob" von Compliance) aus den folgenden *verfassungsrechtlichen Vorgaben* abgeleitet werden[18]:

- *Bindung an Grundrechte (Art. 1 Abs. 3 GG):* Staatliche Eingriffe in die Rechte eines Einzelnen müssen die grundrechtlichen Grenzen beachten.
- *Rechtsstaatsprinzip (Art. 20 Abs. 3 GG):* Nach Art. 20 Abs. 3 GG ist die vollziehende Gewalt an Gesetz und Recht gebunden (Prinzip des Vorrangs des Gesetzes). Dieses Prinzip des Vorrangs des Gesetzes gilt ohne Ausnahme für jedes exekutive Handeln und soll u.a. die Gleichbehandlung der Bürger sicherstellen[19]. Das Rechtsstaatsprinzip begründet sowohl Compliance-Pflichten im Außenverhältnis (Bürger, Geschäftspartner, Allgemeinheit) als auch im Innenverhältnis (Bedienstete)[20]. Zugleich folgt aus Art. 20 Abs. 3 GG

[18] Vgl. Knauf und Stober, in: Stober/Ohrtmann, Compliance, Handbuch für die öffentliche Verwaltung, 2. Auflage 2022, § 2 Rn. 59 ff, § 5 Rn. 178 ff.
[19] Rozek, in: Schoch/Schneider, Verwaltungsverfahrensgesetz, 1. Ergänzungslieferung August 2021, § 54 Rn. 5-7.
[20] Knauff, in: Stober/Ohrtmann, Compliance, Handbuch für die öffentliche Verwaltung, 2. Auflage 2022, § 2 Rn. 51.

mittelbar auch das Prinzip des Vorbehalts des Gesetzes, welches besagt, dass die Verwaltung durch ein Gesetz zu dem konkreten Handeln ermächtigt sein muss. Diskutiert wird jedoch, ob das Prinzip des Vorbehalts des Gesetzes nur für die Eingriffsverwaltung oder auch für die Leistungsverwaltung gilt[21]. Das Rechtsstaatsprinzip haben die Länder auch in ihren jeweiligen Landesverfassungen verankert. Die *Gesetzmäßigkeit der Verwaltung* der einzelnen Kommunen wird durch die Länder überwacht[22].

- Führt eine Kommune bei ihrer Verwaltungstätigkeit EU-Recht aus, bindet Art. 51 Abs. 1 der *EU-Grundrechtecharta* diese ebenfalls an die Achtung der Rechte und Einhaltung der Grundsätze. Ebenso ist in Art. 41 der EU-Grundrechtecharta das „*Recht auf eine gute Verwaltung*" verankert. Nach dem ersten Absatz hat „jede Person ein Recht darauf, dass ihre Angelegenheiten von den Organen, Einrichtungen und sonstigen Stellen der Union unparteiisch, gerecht und innerhalb einer angemessenen Frist behandelt werden".
- Für *Angehörige des öffentlichen Dienstes* ergibt sich aus der in Art. 33 Abs. 4 GG verankerten gegenseitigen Dienst- und Treuepflicht die *Pflicht zur Staats- und Verfassungstreue*[23]. Dies erfordert nicht nur ein Bekenntnis zur freiheitlich demokratischen Grundordnung im Sinne des Grundgesetzes, sondern auch die Pflicht, diese zu erhalten und die eigene Verwaltungstätigkeit daran auszurichten.

(36) Darüber hinaus ergibt sich aus *einzelnen Rechtsgebieten* bzw. *einzelgesetzlichen Bestimmungen* die Notwendigkeit, zumindest einzelne Bausteine bzw. Elemente eines CMS in der öffentlichen Verwaltung einzurichten. Insbesondere folgende bundes-, landes- und verwaltungsrechtliche Vorschriften sind bei der konkreten Ausgestaltung eines kommunalen CMS zu berücksichtigen:

- *Regelungen im Strafgesetzbuch (StGB)*[24]: Für Amtsträger bestehen strafrechtliche Haftungsrisiken, die sich v.a. aus Beihilfe durch Unterlassen bei Garanten- bzw. Verkehrssicherungspflichten oder aus Nichteinschreiten bei

[21] Huster/Rux, in: BeckOK Grundgesetz, 47. Edition Stand: 15.11.2021, Art. 20 Rn. 172 ff.
[22] Vgl. beispielsweise Art. 75 Abs. 1 Verfassung des Landes BW, Art. 78 Abs. 4 Verfassung des Landes NRW.
[23] Battis, in: Sachs, Grundgesetz, 9. Auflage 2021, Art. 33 Rn. 51 ff.
[24] Vgl. Amtsdelikte wie z.B. Vorteilsannahme § 331 StGB und Bestechlichkeit § 332 StGB oder Straftatbestände, bei denen der Strafrahmen sich bei Begehung durch einen Amtsträger erhöht (z. B. Betrug, Untreue §§ 263 Abs. 1 und 3, 266 Abs. 1 und 2 StGB).

Aufsichts- und Kontrollpflichten ergeben[25]. Neben Verkehrssicherungspflichten aus Garantenstellungen sollte auch die Verhinderung der sogenannten Korruptionsdelikte des StGB bei der Ausgestaltung eines CMS einen hohen Stellenwert einnehmen. Derzeit fehlt es in Deutschland auf Bundes- und Landesebene an einem zentralen Korruptionsbekämpfungs- oder Antikorruptionsgesetz mit klaren verfahrensrechtlichen Regelungen zur Vermeidung von Korruptionsstraftaten. Das Korruptionsbekämpfungsgesetz des Landes NRW stellt insoweit eine Ausnahme dar[26]. Allerdings gibt es Verwaltungsvorschriften von Bund, Ländern und Selbstverwaltungsträgern, die Richtlinien für die Korruptionsprävention vorgeben[27]. Für die Kommunen gelten diese Verwaltungsvorschriften nicht unmittelbar. Dennoch wird diesen empfohlen, sich an den landesrechtlichen Vorschriften zu orientieren.

- *Recht der Ordnungswidrigkeiten (OWiG)*: Nach § 130 Abs. 1 OWiG hat ein Unternehmens- oder Betriebsinhaber die Pflicht, ein Unternehmen mit der gebotenen Aufsicht zu führen. Eine Ordnungswidrigkeit begeht der Inhaber, der Maßnahmen unterlässt, die erforderlich und zumutbar sind, um eine Zuwiderhandlung gegen betriebs- und unternehmensbezogene Pflichten zu verhindern. Durch die Maßnahmen sollen Gesetzesverstöße zumindest wesentlich erschwert werden (Hinwirken auf das Einhalten gesetzlicher Bestimmungen). Dazu gehören u.a. die Bestellung sorgfältig ausgewählter Aufsichtspersonen und deren Überwachung (§ 130 Abs. 1 S. 2 OWiG) sowie die Schulung und Kontrolle des Personals hinsichtlich der unternehmens- oder branchenspezifischen Risiken. Diese dargestellten Anforderungen an Unternehmens- und Betriebsleitungen gelten gem. § 130 Abs. 2 OWiG ausdrücklich auch für öffentliche Unternehmen bzw. andere Organisationsformen, mit denen sich die öffentliche Verwaltung am Wirtschaftsleben beteiligt (u.a. Ei-

[25] § 13 StGB – Begehen durch Unterlassen. Vgl. z.B. Süßmann, Joshua: Die strafrechtliche Haftung kommunaler Amtsträgerinnen und Amtsträger in Baden-Württemberg für Sicherungs- und Überwachungspflichten aus einer Garantenstellung, Bachelorarbeit zur Erlangung des Grades eines Bachelor of Arts (B.A.) im Studiengang gehobener Verwaltungsdienst – Public Management der Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg, September 2021.

[26] Korruptionsbekämpfungsgesetz NRW vom 16.12.2004 in der Fassung der letzten Änderung vom 22.09.2021; abrufbar unter: https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=2820131014143952768.

[27] VwV Korruptionsverhütung und -bekämpfung BW vom 15.01.2013 (GABl. 2013, S. 55) in der Fassung der letzten Änderung vom 30.11.2021 (GABl. 2021, S. 491); abrufbar unter: https://www.landesrecht-bw.de/jportal/?quelle=jlink&query=VVBW-LReg-20130115-SF&psml=bsbawueprod.psml&max=true.

genbetriebe, öffentlich-rechtliche Anstalten, Gesellschaften des Privatrechts)[28]. Allerdings gilt § 130 OWiG nicht für Stellen/Behörden, die öffentliche Verwaltungsaufgaben wahrnehmen.

- *Steuerrechtliche Vorschriften*: Ein CMS sollte auch Schutz vor steuerstrafrechtlichen Risiken bieten. Hierbei muss sichergestellt werden, dass steuerrelevante Sachverhalte vollständig und richtig erfasst und bestehende Erklärungspflichten gegenüber den Finanzbehörden fristgerecht erfüllt werden. Die zunehmende Komplexität des Steuerrechts erhöht auch für den öffentlichen Sektor das Risiko von potentiellen Verstößen. Im Falle von Steuerhinterziehung oder leichtfertiger Steuerverkürzung können der Verwaltungsspitze und ggf. weiteren Personen Bußgelder und Haftungsrisiken drohen. Nach dem BMF-Anwendungserlass zu § 153 AO vom 23.05.2016 kann ein innerbetriebliches Kontrollsystem zur Erfüllung der steuerlichen Pflichten ein Indiz gegen das Vorliegen von Vorsatz oder Leichtfertigkeit bei der Prüfung einer möglichen Steuerstraftat sein[29].
- *Befangenheitsregelungen und Beamtenrecht*: Befangenheitsregelungen im Verwaltungs- und Kommunalrecht sollen ein faires Verwaltungsverfahren sicherstellen. Die Befangenheitsvorschriften werden durch beamtenrechtliche Regelungen ergänzt (z. B. Pflicht der Beamten zur Unparteilichkeit, Vorschriften über die Uneigennützigkeit der Amtsführung, grundsätzliches Verbot der Annahme von Vorteilen).
- *Verwaltungsinterne Vorschriften der Kommunen*: Im Rahmen ihrer eingeräumten Verwaltungsautonomie sind Kommunen befugt, eigene Vorschriften zur Einhaltung der bestehenden Compliance-Pflichten zu erlassen (Satzungen, Richtlinien, Rundschreiben, Anweisungen). In der Regel lassen sich bei Kommunen einzelne Compliance-Regelungen zu bestimmten Themenbereichen (Umgang mit Geschenken, Spenden und Sponsoring u. s. w.) finden.
- *Gesellschaftsrecht:* Im Gesellschaftsrecht sind Sorgfaltspflichten für Vorstände bzw. Geschäftsführer und Aufsichtsräte normiert (§§ 93, 116 AktG, 43 GmbHG), die auch für privatrechtliche öffentliche Unternehmen gelten und für solche des öffentlichen Rechts analog anwendbar sind[30].

---

[28] Bei Verletzung der Pflicht kann dem Inhaber des Betriebes eine Geldbuße bis zu 1 Mio. EUR drohen (§ 130 Abs. 3 OWiG). Über den Verweis in § 130 Abs. 3 S. 2 auf § 30 Abs. 2 S. 3 OWiG erhöht sich der Höchstbetrag der Verbandsgeldbuße sogar auf 10 Mio. EUR.

[29] BMF-Schreiben vom 26.01.2016, IV A 3 – S 0324/15/10001.

[30] Für Anstalt des öffentlichen Rechts und Eigenbetriebs vgl. PWC (Hrsg.): Öffentlich-rechtliche Unternehmen der Gemeinden – Länderübergreifende Darstellung, 6. überarbeitete Auflage, Stuttgart, 2015, Rn. 121, 583.

- *Lieferkettensorgfaltspflichtengesetz (LkSG)*[31]*:* Das LkSG gibt Mindestanforderungen für Sorgfaltspflichten größerer Unternehmen in den Lieferketten vor, wozu auch die Einführung von Elementen eines CMS gehören. Kommunen fallen nicht unter den Anwendungsbereich des Gesetzes, aber es verpflichtet größere kommunale Unternehmen in privater oder öffentlicher Rechtsform, sofern sie nicht lediglich Verwaltungsaufgaben einer Gebietskörperschaft wahrnehmen.
- *Hinweisgeberschutzgesetz als nationale Umsetzung der Richtlinie der Europäischen Union betreffend den Hinweisgeberschutz:* Im Oktober 2019 hat die Europäische Union die Hinweisgeberschutz-Richtlinie[32] verabschiedet, die mit dem mit dem Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Hinweisgeberschutzgesetz[33]) in deutsches Recht umgesetzt worden ist. Ziel beider Regelungen ist es, den zuvor unzureichenden Schutz von hinweisgebenden Personen zu verbessern. Demnach sind auch Gemeinden und Gemeindeverbände ab einer festgelegten Größenordnung verpflichtet, eine interne Meldestelle einzurichten und zu betreiben. Die hinweisgebenden Personen sind vor Repressalien zu schützen. Siehe Näheres in Abschnitt 6.

(37) Darüber hinaus sind in der 20. Legislaturperiode des Deutschen Bundestags gemäß dem Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP) noch folgendes Gesetzesvorhaben geplant, das für die Ausgestaltung eines CMS von Bedeutung ist:

- *Verbandssanktionengesetz (VerSanG – Gesetz zur Stärkung der Integrität in der Wirtschaft)*: Das Gesetz soll die Verhängung von Sanktionen gegen einen Verband ermöglichen. Voraussetzung hierfür ist eine Straftat, die aus einem Verband (juristische Personen und Personenvereinigungen) heraus begangen wurde (umfasst auch Gebietskörperschaften und sonstige öffentlich-rechtliche Personen, sofern sie wirtschaftlich (nicht hoheitlich) tätig

[31] Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten vom 16.07.2021, BGBl I 2021, S. 2959 (auch Lieferkettengesetz oder Sorgfaltspflichtengesetz genannt).

[32] Richtlinie (EU) 2019/1937 v. 23.10.2019, ABl. L 305 vom 26.11.2019.

[33] Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (HinSchG) – BGBL 2023 I Nr. 140 vom 02.06.2023. Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019. Für weitere Informationen zum Hinweisgeberschutz siehe Kapitel 6.

sind). Bisher kann nach geltendem Recht der Verband lediglich mit einer Geldbuße nach dem OWiG geahndet werden. Nach dem ursprünglichen, inzwischen nicht weiter verfolgten Gesetzesentwurf[34] war eine Sanktionierung u.a. vorgesehen, wenn eine Leitungsperson im Rahmen der Wahrnehmung der Angelegenheiten des Verbands eine Straftat begangen hat, durch die verbandsbezogene Pflichten verletzt worden sind oder durch die der Verband bereichert wurde oder werden sollte.

(38) Nach der *Rechtsprechung* kommt es – zusammenfassend – für eine angemessene Ausgestaltung von Compliance-Strukturen in einer Organisation auf die Größe und Komplexität der jeweiligen Organisation an. Den Vertretungsorganen bzw. Führungskräften soll diesbezüglich im Rahmen der Risikoanalyse ein Ermessensspielraum zustehen. Dies sowie die haftungsrechtlichen Auswirkungen der Einrichtung eines angemessenen CMS können insbesondere den folgenden Gerichtsentscheidungen entnommen werden[35] (☞ Anlage 1, Abschnitt 8.1):

- LG München I, Urteil vom 10.12.2013 – 5 HK O 1387/10 – BeckRS 2014, 1998 (Siemens/Neuburger-Urteil);
- BGH, Urteil vom 9.5.2017 – 1 StR 265/16 – BeckRS 2017, 114578;
- BGH, Urteil vom 17.7.2009 – 5 StR 394/08 – BeckRS 2009, 18039 („BSR-Entscheidung");
- BGH, Urteil vom 20.10.2011 – 4 StR 71/11 – BeckRS 2011, 27599 („Mobbing-Entscheidung").

3.4 Verantwortung für Compliance

(39) Für die Einrichtung und die konkrete Ausgestaltung eines kommunalen CMS gelten folgende Verantwortlichkeiten:

(40) *Sachliche Compliance-Verantwortung:* Kommunen haben im Rahmen ihres Selbstverwaltungsrechts eigenverantwortlich für gesetzmäßiges Handeln zu sorgen. Eine Ausnahme gilt für vom Land übertragene Aufgaben, sofern das Land von seinem Weisungsrecht Gebrauch macht. In diesem Fall übernimmt das Land die Verantwortung für die Gesetzmäßigkeit des Handelns. Bei den Kommunen ist dann „nur" zu überprüfen, ob die Ausführung der Weisung erkennbar den Gesetzen zuwiderläuft (Evidenzkontrolle). Öffentliche Unternehmen haben unabhängig von ihrer Rechtsform die sachliche Compliance-Verantwortung.

---

[34] Vgl. RegE: Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft, Stand 16.06.2020 (abrufbar unter: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Staerkung_Integritaet_Wirtschaft.html).

[35] Eine kurze Übersicht über die Inhalte der jeweiligen Gerichtsentscheidungen findet sich in Abschnitt 6 Anlagen, Anlage 1.

(41) *Persönliche Compliance-Verantwortung*:[36]

- Aus den Zuständigkeitsregelungen[37] folgt, dass der gesetzliche Vertreter der Kommune (Bürgermeister, Landrat etc.) als Leiter der Verwaltung aufgrund seiner Gesamtverantwortung für die Einhaltung der Legalitätspflicht (Legalitätskontrollpflicht) in der Kommunalverwaltung für die Einrichtung und Ausgestaltung einer Compliance-Organisation verantwortlich ist[38]. Ebenso hat er als Dienstvorgesetzter die erforderlichen Schritte einzuleiten, wenn ihm eine Verfehlung oder Unregelmäßigkeit zur Kenntnis gelangt. Die Verwaltungsleitung kann Compliance-Aufgaben auf Bedienstete (Compliance-Beauftragter, ☞ Abschnitt 4.6.2) übertragen, wozu eine ordnungsgemäße Delegation erforderlich ist. In einem solchen Fall besteht bei einer Pflichtverletzung für diese Bediensteten unter Berücksichtigung der Grundsätze der Arbeitnehmer- oder Beamtenhaftung das Risiko einer Regresspflicht[39].
- Hinsichtlich der Compliance-Verantwortung von Ratsmitgliedern liegt es nahe, eine Parallele zu sog. dualistischen Unternehmensstrukturen (z. B. Vorstand und Aufsichtsrat bei einer Aktiengesellschaft) zu ziehen. Dem Gemeinderat obliegt die Kontrolle des Bürgermeisters und der Gemeindeverwaltung[40]. Jedoch können die Mitglieder des Gemeinderats den Bürgermeister hinsichtlich der Aufgaben der Gemeindeverwaltung lediglich auf Missstände hinweisen und mit der Beseitigung beauftragen. Ein Weisungsrecht gegenüber dem Bürgermeister hat der Gemeinderat nicht[41], zumindest kann

---

36 Vgl. u.a. Glinder, in: Louis/Glinder/Waßmer (Hrsg.), Korruptionsprävention in der öffentlichen Verwaltung, Stuttgart 2020, Abschnitt 2.2, S. 133 ff.

37 Innerhalb der Kommunalverwaltung entscheiden die Ratsmitglieder als Gremium über alle Angelegenheiten der Gemeinde, soweit nicht durch Gesetz etwas Anderes bestimmt ist (vgl. z. B. § 24 Abs. 1 GemO BW, § 41 GO NRW; § 28 SächsGO). Dem Bürgermeister obliegt die Leitung und Beaufsichtigung des Geschäftsgangs der Verwaltung (vgl. § 42 Abs. 1 und § 44 Abs. 1 GemO BW; § 70 GO NRW; § 53 SächsGO).

38 Vgl. VG Regensburg, Urteil vom 10.11.2004 – RN 1 K 04.1573 – BeckRS 2004, 32604. Hinsichtlich der strafrechtlichen Verantwortlichkeit von Führungskräften vgl. auch die sog. „Lederspray-Entscheidung“ (BGH, Urteil vom 6.7.1990 – 2 StR 549/89 – BeckRS 1990, 1008). In dieser Entscheidung wird hervorgehoben, dass die Führungsebene eine Generalverantwortlichkeit und Allzuständigkeit für sämtliche Belange eines Unternehmens innehat. Unternehmens- oder Betriebsleitungen verantworten nicht nur eigenes (Fehl-)Verhalten, sondern unter bestimmten Voraussetzungen auch das Verhalten ihrer Mitarbeiter. Der BGH geht nach der sog. „Mauerschützen-Entscheidung“ (BGH, Urteil vom 26.7.1994 – 5 StR 98/94 – BeckRS 9998, 166424) davon aus, dass die Entscheidungsträger auf der Leitungsebene dann als mittelbare Täter anzusehen sind, wenn sie die „regelhaften Abläufe“ des Geschehens kontrollieren. Es liegt sodann eine sogenannte „mittelbare Täterschaft kraft Organisationsherrschaft“ vor. Zur Legalitätspflicht bzw. Legalitätskontrollpflicht von Behördenleitern vgl. Glinder/Schröfel, in: Louis/Glinder/Wassmer (Hrsg.), Korruptionsprävention in der öffentlichen Verwaltung, Stuttgart 2020, S.133 ff.

39 Vgl. § 3 Abs. 6 TVöD und Art. 34 S. 1 GG i. V. m § 839 Abs. 1 BGB.

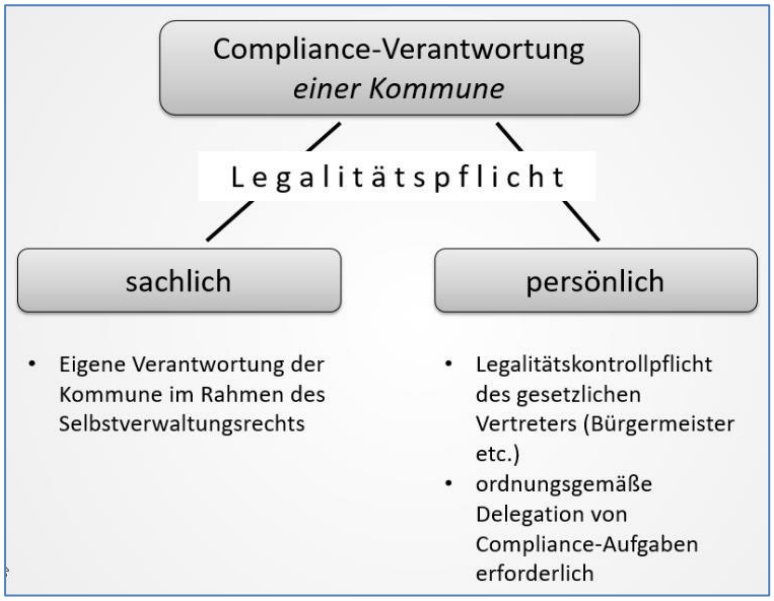
40 Vgl. § 24 Abs. 1 3 GemO BW.

41 Vgl. Brenndörfer, in: BeckOK Kommunalrecht BW, 16. Edition Stand: 01.01.2022, § 24 Rn. 7.

der Gemeinderat Maßnahmen nicht unmittelbar selbst vollziehen[42]. Vielmehr hat sich der Gemeinderat in entsprechenden Fällen an die Rechtsaufsichtsbehörde zur Beseitigung des Missstands zu wenden.

- Bei öffentlichen Unternehmen trifft die Compliance-Verantwortung in erster Linie die Betriebs- und Geschäftsleitungen, abgeleitet aus den allgemeinen Sorgfaltspflichten (§ 93 AktG, § 43 GmbHG). Auch Personen der Führungsebene können für Verstöße verantwortlich gemacht werden, sofern diesen entsprechende Compliance-Aufgaben übertragen wurden (z. B. Compliance Officer). Der Aufsichtsrat hingegen übernimmt lediglich die Überwachung der Geschäftsleitung[43].

Abbildung 3: Compliance-Verantwortung



3.5 Ausgestaltung des CMS für Kommunen

(42) Kommunen ab 10.000 Einwohnern oder ab 50 Mitarbeitern sowie öffentliche Unternehmen ab 50 Mitarbeitern müssen die Bausteine bzw. Elemente eines CMS einführen, die nach der *EU-Whistleblower-Richtlinie*, dem *Hinweisgeberschutzgesetz* sowie entsprechenden Verordnungen verpflichtend vorgegeben sind. Durch gesetzliche

[42] Vgl. Armbruster, in: Kunze/Bronner/Katz, Gemeindeordnung für Baden-Württemberg – Kommentar, Loseblattsammlung, Stand: 30. Lieferung April 2020, § 24 Rn. 11.

[43] Hierzu gehört zwar nach Nr. 4.1.3 D-PCGK (Deutscher Public Corporate Governance Musterkodex) auch die Überwachung der Wahrnehmung der Compliance-Aufgaben durch den Vorstand, ein entsprechendes Weisungsrecht gegenüber dem Vorstand besteht aber nicht. Die Intensität der geschuldeten Überwachung richtet sich nach der konkreten Risikosituation (vgl. hierzu VG Regensburg, Urteil vom 10.11.2004 – RN 1 K 04.1573 – BeckRS 2004, 32604).

Vorgaben kann eine geringere Einwohnerzahl oder Mitarbeiterzahl als Grenzwert für Kommunen oder öffentliche Unternehmen festgelegt werden.[44] Ebenso können auch durch spezialgesetzliche Bestimmung öffentliche Unternehmen mit weniger als 50 Mitarbeitern verpflichtet sein, bestimmte Elemente eines CMS einzuführen[45]. Siehe Näheres zur Pflicht und zu den Anforderungen eines Hinweisgebersystems nach der EU-Whistleblower-Richtlinie und dem Hinweisgeberschutzgesetz in Abschnitt 6.

(43) Sofern Teile des CMS nicht konkret gesetzlich vorgegeben sind, liegt die *angemessene Ausgestaltung* eines kommunalen CMS im Ermessen der verantwortlichen gesetzlichen Vertreter der Kommune. Dieses ist grundsätzlich anhand der Größe der jeweiligen Kommune, ihrer Organisationsstruktur sowie der Heterogenität und Risikogeneigtheit der tatsächlich wahrgenommenen Aufgaben auszuüben (☞ Abschnitt 4.4.1). Für eine Kategorisierung der Städte und Gemeinden ist der ihnen jeweils übertragene Wirkungskreis (Aufgaben) von Bedeutung, da sich danach die Anzahl der im CMS zu berücksichtigenden Teilbereiche (☞ Tz. 33) richtet. Die Abbildung 4 gibt dazu eine grobe Übersicht.

(44) Leitungen öffentlicher Unternehmen haben auch jenseits gesetzlicher Vorschriften aufgrund ihrer allgemeinen Sorgfaltspflichten für ein nach Art und Umfang angemessenes CMS zu sorgen.

(45) Für die Ausgestaltung eines CMS in Unternehmen wurden mehrere Rahmenkonzepte entwickelt. In der Compliance-Praxis begegnet man mittlerweile am häufigsten dem vom Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) verabschiedeten IDW Prüfungsstandard (PS) 980 (sowie der Überarbeitungsentwurf IDW EPS 980)[46] und der von der International Organization for Standardization (ISO) erstellten Norm ISO 37301[47] (der IDW PS 980 basiert auf sieben Grundelementen eines CMS, während die ISO 37301 auf vier Elementen aufbaut). Des Weiteren gibt es den DICO-Standard Compliance-Management-Systeme vom März 2021[48]. Der vorliegende Leitfaden zieht den IDW PS 980 als Orientierungshilfe für einen kommunalen Standard heran, da er

---

44 Art. 8 Abs. 1 i.V.m. Abs. 9 der Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23.Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (EU-Whistleblower-Richtlinie).

45 U.a. Kredit- und Finanzleistungsinstitute (§ 25a Abs. 1 KWG), Versicherungsunternehmen (§ 29 Abs. 1 VAG), Geldwäscherichtlinien.

46 IDW Prüfungsstandard 980: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980), Stand 11.03.2011 sowie Entwurf einer Neufassung als IDW EPS 980, Stand 28.10.2021 (siehe https://www.idw.de/idw/verlautbarungen).

47 ISO 37301:2021 Compliance management systems – Requirements with guidance for use (Nachfolger der ISO 196000).

48 DICO (Deutsches Institut für Compliance): Compliance-Management-Systeme – Übergreifender Standard der DICO-Standard-Reihe, März 2021.

auch auf die Prüfung eines CMS eingeht. Dem steht eine ergänzende Heranziehung des ISO 37301 nicht entgegen. Darüber hinaus ist die ISO 37002[49] - subsidiär und ergänzend zu den gesetzlichen Vorgaben – eine brauchbare Richtschnur für Hinweisgebersysteme.

Abbildung 4: Kategorisierung der Kommunen nach ihrem Wirkungskreis

Größe der Kommune*	Umfang des CMS
Kleine Kommunen ☛ (einfache) kreisangehörige Gemeinden < 10.000 Einwohner ☛ Gemeindehoheiten**, eigener Wirkungskreis, freiwillige Aufgaben, Pflichtaufgaben ohne Weisung	• Keine Pflicht zur internen Meldestelle • Wenige CMS-Teilbereiche • Institutionelle Anforderungen gering (Verhaltenskodex, DA Antikorruption)
Mittlere Kommunen ☛ (einfache) kreisangehörige Gemeinden ab 10.000 Einwohner bis Einwohnerzahl für größere Kommunen ☛ Gemeindehoheiten**, eigener Wirkungskreis, freiwillige Aufgaben, Pflichtaufgaben ohne Weisung	• Pflicht zur internen Meldestelle • Wenige CMS-Teilbereiche • Institutionelle Anforderungen mittel (Verhaltenskodex, DA Antikorruption, Pflichten nach dem HinSchG)
Größere Kommunen ☛ große Kreisstadt, selbständige Gemeinden und Städte, mittlere/große kreisangehörige Städte ☛ Gemeindehoheiten**, eigener Wirkungskreis, freiwillige Aufgaben, Pflichtaufgaben ohne Weisung, viele Weisungsaufgaben (untere Verwaltungsbehörde), übertragener Wirkungskreis	• Pflicht zur internen Meldestelle • Mehr CMS-Teilbereiche • Mehr institutionelle Anforderungen (Verhaltenskodex, DA Antikorruption, Pflichten nach dem HinSchG, Anforderungen aus Teilbereichen)
Große Kommunen ☛ Kreisfreie Stadt / Stadtkreis ☛ Gemeindehoheiten**, eigener Wirkungskreis, freiwillige Aufgaben, Pflichtaufgaben ohne Weisung, alle Weisungsaufgaben (untere Verwaltungsbehörde), übertragener Wirkungskreis, Kreisaufgaben	• Pflicht zur internen Meldestelle • Umfangreiche CMS-Teilbereiche • Umfangreiche institutionelle Anforderungen

* *Bei der Größeneinteilung handelt es sich um eine vereinfachende Darstellung auf der Grundlage des jeweiligen Wirkungskreises von Gemeinden, die je nach Bundesland Unterschiede aufweisen.*
** *Gemeindehoheiten: Organisations-, Personal-, Finanz-, Planungshoheit*

[49] ISO 37002:2021, Whistleblowing Management Systems – Guidelines (First Edition 2021-07-27).

3.6 Projekt zur Einrichtung eines CMS

(46) Zur Einführung eines CMS sollte von der Leitung der Kommune ein *Projekt* aufgesetzt werden. Der Projektauftrag ist von der Behördenleitung zu geben. Im Projektauftrag sind aufzunehmen:

- Ein eindeutiges, unmissverständliches Commitment der Behördenleitung zu Compliance ☞ *tone at the top* (Compliance-Kultur, ☞ Tz. 58).
- Festlegung der *Compliance-Ziele der Kommune* ☞ strategische Compliance-Ziele, Teilbereiche (Compliance-Ziele, ☞ Tz. 69 ff.).
- Festlegung eines geeigneten *Projektteams*: Ein wirksames CMS lässt sich in einer Kommune nicht durch eine Einzelperson oder eine einzelne Organisationseinheit einrichten. Vielmehr bedarf es eines Projektkernteams, dass aus dem Compliance- bzw. Antikorruptions-Beauftragten (soweit schon vorhanden bzw. bekannt) sowie aus Vertretern der Bereiche Recht, Organisation, Personal und Rechnungsprüfung (interne Revision) bestehen sollte. Letztere dürfen zur Wahrung der Unabhängigkeit ihrer Prüfungsaufgabe nur beratend oder prüfungsbegleitend tätig werden (☞ Tz. 172). Für die einzelnen Compliance-Teilbereiche (☞ Tz. 33) sollten Ansprechpersonen hinzugezogen werden; sofern es für Teilbereiche bereits bestellte Beauftragte[50] gibt, sollten diese – zumindest teilbereichsspezifisch – hinzugezogen werden. Je nach Bedarf (insbesondere fehlendes Knowhow) kann es sinnvoll sein, externe Berater (ggf. auch nur für Teilbereiche) hinzuziehen.
- Festlegung einer geeigneten *Projektorganisation*. Der Projektaufbau sollte aus einer Projektlenkung, einer Projektleitung und – v.a. abhängig vom Umfang der einbezogenen Teilbereiche – aus Projektgruppen, die einzelne Teilaspekte bearbeiten, bestehen. In der Projektlenkung sollte für ein überzeugendes Commitment (tone at the top) die Behördenleitung oder zumindest deren dauerhafte Stellvertretung vertreten sein. Für den Projektablauf bedarf es der Aufgaben- und Zeitplanung einschließlich der Festlegung von Meilensteinen. Zudem ist für die Projektsteuerung ein projektspezifisches Dokumentations- und Berichtswesen einzurichten.
- Bereitstellung einer angemessenen *sachlichen Ressourcenausstattung* (u.a. Budget, IT).

[50] U.a. Beauftragte für Datenschutz, Brandschutz, Umweltschutz, Arbeitssicherheit, Gleichstellung, Hygiene.

(47) Für ein angemessenes und wirksames kommunales CMS ist darauf zu achten, dass das Projekt zur Einrichtung dieses CMS mit angemessenen Ressourcen ausgestattet ist.

(48) Es empfiehlt sich eine frühzeitige Beteiligung des Personalrats. Auch der Gemeinderat sollte informiert werden; zusätzliche Stellen und Budgetmittel hat er im Regelfall zu beschließen.

(49) Bei der Einrichtung und den Betrieb des CMS sollte dessen Unterstützung durch spezielle *Software* bzw. IT-Verfahren geprüft werden. Diese kommen u.a. für folgende Anwendungsbereiche infrage:

- Wahrnehmung der Aufgaben des Hinweisgebersystems einschließlich der Hinweisbearbeitung (Fallmanagement),
- Durchführung der Compliance-Risikoanalyse,
- E-Learning für Belehrungen und Sensibilisierungen interner Akteure (☞ Tz. 32).

4. Grundelemente eines kommunalen CMS

4.1 Allgemeine Anforderungen, Dokumentationspflicht

(50) In Anlehnung an Ziffer 23 des IDW PS 980 (Ziffer 27 des IDW EPS 980 - Entwurf) umfasst jedes angemessene CMS die folgenden sieben miteinander *in Wechselwirkung* stehenden Grundelemente, die in die Struktur und Abläufe der Organisation einzubinden sind:

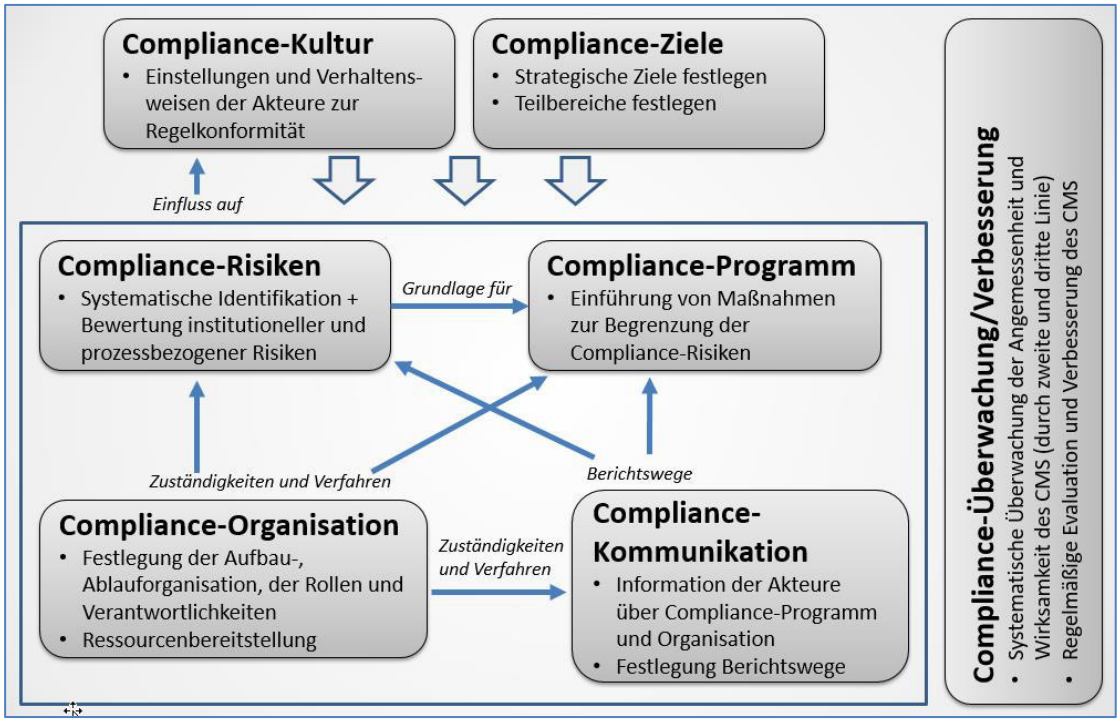
1. Förderung einer günstigen *Compliance-Kultur*,
2. Festlegung der *Compliance-Ziele*,
3. Prozess der Feststellung und Analyse der *Compliance-Risiken* der Kommune (bzw. des öffentlichen Unternehmens),
4. Erstellung eines *Compliance-Programms*,
5. Aufbau der *Compliance-Organisation*,
6. Entwicklung eines Kommunikationsprozesses (*Compliance-Kommunikation*) sowie
7. Entwicklung eines Verfahrens zur Überwachung und Verbesserung des CMS (*Compliance-Überwachung und Verbesserung*)[51].

(51) Das CMS ist auf die spezifische Anforderungs- und Risikosituation der Kommune auszurichten (☞ Abschnitte 3.5, 4.3.1, 4.3.2).

[51] Vgl. IDW Verlautbarungen; verabschiedet vom Hauptfachausschuss (HFA) am 11.03.2011, Werkstand: IDW Life 6 / 2021 Rn. 23.

(52) Soweit keine rechtlichen Vorgaben bestehen, liegt die Ausgestaltung im pflichtgemäßen Ermessen der Kommune. Ein wirksames CMS setzt jedoch dessen Angemessenheit (☞ Tz.164 f.) als notwenige Bedingung voraus.

Abbildung 5: Die sieben Grundelemente eines CMS



(53) *Pflicht zur vollständigen Dokumentation des CMS*: Die Einrichtung und der Betrieb eines CMS mit seinen Grundelementen ist vollständig, für einen objektiven sachverständigen Dritten nachvollziehbar und revisionssicher zu dokumentieren und über einen ausreichend langen Zeitraum zu archivieren. Dies sichert auch eine personenunabhängige Funktion des CMS. Die Dokumentation hat die Regelungen der Strukturen (Aufbauorganisation), Prozesse und Maßnahmen, die konkreten Umsetzungshandlungen sowie die jeweils verantwortlichen Personen zu enthalten. Zur CMS-Dokumentation gehören v.a.:

1. eine CMS-Beschreibung der Leitung der Kommune als zusammenfassende Darstellung der wesentlichen Aspekte des eingerichteten CMS; diese Beschreibung kann auch Bestandteil der CMS-Richtlinie sein (☞ Abschnitt 4.6.5);
2. die CMS-relevanten Regelungen der Kommune (u.a. Dienstanweisungen, Zuständigkeitsregelungen, Regelungen zur Aufbauorganisation);
3. Beschreibungen bzw. Visualisierungen der CMS-Prozesse;

4. Dokumente zur organisatorischen und prozessualen Ausgestaltung von Compliance-Maßnahmen und deren Umsetzung (u.a. Berichte, Protokolle, Anforderungs-Maßnahmen-Matrix, Risiko-Kontroll-Matrix, Checklisten, Konzepte).

In der öffentlichen Verwaltung gilt das Schriftlichkeits- bzw. Dokumentationsprinzip; es ist Teil des Rechtsstaatlichkeitsprinzips und Voraussetzung für die Verwirklichung von gesetzlich garantierten Akteneinsichts- und Informationsrechten. Das Schriftlichkeits- und Dokumentationsprinzip ist auch Voraussetzung für die Wirksamkeit eines CMS. Eine fehlende oder unvollständige Dokumentation des CMS kann zu Zweifeln an der dauerhaften Funktionsfähigkeit der eingerichteten Regeln und Maßnahmen führen.[52]

4.2 Compliance-Kultur

(54) Gegenstand der Compliance-Kultur - als Teil der bestehenden Organisations- bzw. Unternehmenskultur – ist die Bedeutung, die der Beachtung von Normen, Regelungen und Werten in der Organisation entgegengebracht wird. Herrscht eine „gute" Compliance-Kultur, sind die Mitarbeitenden in hohem Maße intrinsisch motiviert, sich integer zu verhalten bzw. gegenüber Regelverstößen nicht tolerant zu sein[53].

(55) Folgende *Merkmale* prägen die Compliance-Kultur und damit die Einstellungen und das Verhalten der Mitarbeitenden:[54]

- die Integrität der gesetzlichen Vertreter, v.a. durch ihre Vorbildfunktion bei Grundeinstellung und Verhaltensweise;
- das Bekenntnis des Managements zur Bedeutung eines verantwortungsvollen Verhaltens im Einklang mit den zu beachtenden Regeln, u.a. tone at the top, Hinweisgeberschutz, Nulltoleranz bzw. Sanktionen bei Regelverstößen (*Hinweis*: Sofern nicht Beihilfe durch Unterlassen vorliegt, liegt es zwar grundsätzlich im Ermessen der Behördenleitung, ob sie die Staatsanwaltschaft bei begründeten Hinweisen auf strafbare Handlungen informiert, doch steht in solchen Fällen ein Unterlassen der Information in der Regel nicht in Übereinstimmung mit einer Nulltoleranz-Politik);

---

52 Vgl. IDW PS 980, Tz A 10.

53 Vgl. u.a. Wilmers, Burkhard Wolf / Fahr, Réne: Behavioral Compliance in der Unternehmenspraxis, in: ComplianceBusiness, Ausgabe 4, November 2017, S. 6 – 9.

54 Vgl. IDW 980 (2011) (in IDW-EPS 980 n.F. (10.2021) Tz. A23 leicht abweichend formuliert): Grundsätze ordnungsgemäßer Prüfung von Compliance Managementsystemen, Tz. A14. Vgl. auch ISO 37301 (2021), Nrn. 5.1.1, 5.1.2.

- die von den gesetzlichen Vertretern aufgestellten und kommunizierten Verhaltensgrundsätze (u.a. Regelkonformität, ethisches Verhalten, Ehrlichkeit, Redlichkeit, Vermeidung von Interessenkonflikten);
- die Anreizsysteme, mit denen regelkonformes Verhalten gefördert wird, einschließlich der Berücksichtigung von Compliance bei Personalbeurteilungen und Beförderungen (*Hinweis*: Anreize finanzieller Art sollten hierbei nicht im Vordergrund stehen und sind im öffentlichen Dienst über den gesetzlichen oder tariflichen Rahmen hinaus ohnehin nicht zulässig);
- der Führungsstil und die Personalpolitik der Organisation (z. B. Bedeutung der Kompetenz, Erfahrung und Integrität der Mitarbeitenden, Transparenz) sowie
- die Stellung und die Art der Wahrnehmung durch das Aufsichtsorgan im Zusammenhang mit Risikomanagement und Compliance.

(56) Eine *Zielgruppe* von Maßnahmen der Compliance-Kultur sind alle Mitarbeitenden der Kommune. Bei ihnen ist zwischen Führungskräften mit Aufsichts- und Kontrollfunktion sowie Sachbearbeitern zu unterscheiden. Eine weitere Zielgruppe sind die mit der Kommune „verbundenen Akteure", wozu u.a. gehören: Geschäftspartner (z. B. Lieferanten, Auftragnehmer), Zuwendungsempfänger oder die Mitglieder der kommunalen Volksvertretung. Schließlich stellen die Bürger (als Antragsteller bzw. Leistungsempfänger) eine Zielgruppe für Öffentlichkeitsarbeit dar, auch wenn sie nicht direkt für das kommunale CMS verpflichtet werden können.

(57) Für die Förderung und Entwicklung einer starken Compliance-Kultur stehen der öffentlichen Verwaltung verschiedene *Maßnahmen* bzw. Instrumente zur Verfügung. Die folgende Aufzählung möglicher Maßnahmen ist nicht abschließend und stellt keine Hierarchie in Bezug auf die Wichtigkeit der einzelnen Maßnahmen oder eine zeitliche Reihenfolge in Bezug auf die Implementierung dar:

(58) *„Tone at the top" („tone from the top"), „tone from the middle"*: Die Compliance-Kultur wird maßgeblich geprägt durch die Grundeinstellungen und Verhaltensweisen der Leitung und oberen Führungskräfte („tone at the top") sowie der mittleren Führungsebene („tone from the middle").[55] Hierbei geht es um ein eindeutiges Bekenntnis der Leitung zur Compliance in Wort und im Handeln, dass allen Führungskräften und Mitarbeitenden stetig zu vermitteln ist. Für die Vermittlung des Bekenntnisses sind Maßnahmen der Compliance-Kommunikation (☞ Abschnitt 4.7) anzuwenden.

[55] Vgl. IDW PS 980, Tz 23.

Alle Führungskräfte müssen ihre Vorbildfunktion für rechtskonformes und integres Verhalten verinnerlicht haben.

(59) *Verhaltenskodex (Compliance-Kodex), Ehrenkodex, Geschäftspartnerkodex:* Ziel eines Verhaltenskodex ist es, verbindliche Verhaltensstandards festzulegen, um Verstöße gegen Normen (rechtliche Rahmenbedingungen wie formelle und materielle Gesetze, Regelungen, Richtlinien u. s. w.) und Werte der Organisation vorzubeugen. Solche Verhaltenskodexe sollten zielgruppenorientiert aufgesetzt werden:

- *Verhaltenskodex für alle Mitarbeitenden der Kommune*:[56] In der öffentlichen Verwaltung sind in unterschiedlichen Gesetzen und kommunalinternen Anweisungen bereits zahlreiche Verhaltensnormen festgelegt (u.a. Arbeits-, Beamtenrecht, Vergaberecht, Haushalts- und Kassenrecht), sodass im Verhaltenskodex auf sie zu verweisen ist. Weitere Verhaltensnormen können aufgenommen werden. Insbesondere sollte auch die Pflicht aller Mitarbeitenden aufgenommen werden, konkrete Verdachtsmomente zu melden. Entsprechend sollten auch Meldewege (Meldekanäle) von Regelverstößen bzw. von Verdachtsfällen angegeben werden. Der Verhaltenskodex sollte sprachlich einfach bzw. auch für Nichtjuristen verständlich formuliert werden. Die Mitarbeitenden sind auf den Verhaltenskodex und seine Verbindlichkeit bei Einstellung und danach regelmäßig zu belehren. Die Belehrung ist zu dokumentieren.
- Sogenannter *Ehrenkodex (Ehrenordnung) für kommunale Vertretungen* (v. a. Gemeinderäte und vergleichbare Vertretungsorgane):[57] Mit dem Ehrenkodex bekennen sich die Mandatsträger zu ihrer Verantwortung, das Mandat uneigennützig und zum Wohle der Kommune auszuüben. Nach derzeitiger Rechtslage können solche Ehrenkodexe nur als freiwillige Verpflichtung der Mitglieder des Vertretungsorgans von diesem beschlossen werden; Sanktionierungen bei Verstößen sind nicht möglich.

---

[56] Vgl. Konstanz Institut für Corporate Governance (KICG) der Hochschule Konstanz Technik, Wirtschaft und Gestaltung: Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen – KICG CMS-Leitlinie 2 2014 für Unternehmen mit 250 bis 3.000 Mitarbeitern, Stand 04/2014, Seiten 48 ff.; vgl. Glinder/Schröfel, in: Louis/Glinder/Wassmer (Hrsg.), Korruptionsprävention in der öffentlichen Verwaltung, Stuttgart 2020, S. 154 f.

[57] Vgl. zur Rechtsqualität und zu Regelungsinhalten eines Ehrenkodex Louis, Glinder, Wassmer (Hrsg.): Korruptionsprävention in der öffentlichen Verwaltung, Stuttgart 2020, S.191 ff. Transpareny International Deutschland e.V. hat November 2022 ein Muster eines Verhaltenskodexes für kommunale Mandatsträger*innen veröffentlich: https://148262.seu2.cleverreach.com/c/78456107/6c387b7e60c7-rmsggl

- *Verhaltenskodex für Lieferanten bzw. Geschäftspartner (Geschäftspartnerkodex) und vertragliche Antikorruptionsklauseln*:[58] Ein solcher Kodex legt verbindliche Verhaltensgrundsätze für die Geschäftspartner und ihre Mitarbeitenden fest[59]. Die Befolgung des Verhaltenskodex sollte schriftlich vom Geschäftspartner erklärt bzw. vertraglich vereinbart werden, ebenso wie zusätzliche Antikorruptionsklauseln, die bei Verletzung Vertragsstrafen bzw. Vertragskündigungen vorsehen. Sofern die Voraussetzungen des Verpflichtungsgesetzes vorliegen, sollten Personen, die nicht Amtsträger sind und öffentliche Aufgaben wahrnehmen, nach dem *Verpflichtungsgesetz* förmlich verpflichtet werden, wonach diese Personen bei Verwirklichung von Amtsträger-Korruptionsstraftatbeständen strafrechtlich Amtsträgern gleichgestellt werden.

Die Verhaltenskodexe sind regelmäßig auf Aktualität zu überprüfen und ggf. anzupassen.

(60) *Integritätsaspekt bei Personalauswahl und -entwicklung:* Bei der Personalauswahl sollte auf die Integrität der Bewerber geachtet werden. Um über die persönliche Einstellung eines Bewerbers ein belastbares Bild zu erhalten, kann eine Organisation auf das Instrument eines professionellen Integritäts-Tests zurückgreifen. Alternativ können den Bewerbern im Personalauswahlgespräch Fragen mit Compliance-Bezug gestellt werden. Auch eine Beteiligung des Compliance- bzw. Antikorruptions-Beauftragten an dem Personalauswahlverfahren bei Besetzungen von Schlüsselstellen bzw. besonders korruptionsgefährdeten Stellen ist denkbar. Des Weiteren sollten bei der Personalauswahl bekannt gewordene Auffälligkeiten berücksichtigt werden, wie z.B.[60]:

- straf- oder disziplinarrechtliche Ermittlungen;
- interne Ermittlungen wegen Korruptionsverdacht;
- Verschuldung, nicht geordnete Verhältnisse;
- soziale Probleme (wie Alkohol-, Drogen- oder Spielsucht);
- auffällige Verhaltensweisen, die die Zuverlässigkeit in Frage stellen.

---

[58] Vgl. u.a. Konstanz Institut für Corporate Governance (KICG) der Hochschule Konstanz Technik, Wirtschaft und Gestaltung: Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen – KICG CMS-Leitlinie 2 2014 für Unternehmen mit 250 bis 3.000 Mitarbeitern, Stand 04/2014, Seite 61. Vgl. zur förmlichen Verpflichtung nach dem Verpflichtungsgesetz Louis, Glinder, Wassmer (Hrsg.): Korruptionsprävention in der öffentlichen Verwaltung, Stuttgart 2020, S.190.

[59] Für öffentliche Unternehmen ist ein solcher Geschäftspartnerkodex auch im Hinblick auf Anforderungen des Lieferkettensorgfaltspflichtengesetztes (LkSG) sinnvoll.

[60] Empfehlungen zur Korruptionsprävention in der Bundesverwaltung vom 09.02.2012 zu Nr. 4 der Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung vom 30.07.2004, abrufbar unter: https://www.verwaltungsvorschriften-im-internet.de/BMI-O4-0001-NF-673-KF-001-A003.htm.

(61) *Compliance-Verhalten als Kriterium in Mitarbeiterbeurteilungen*: Hier sollten die in Tz. 60 angesprochenen Auffälligkeiten berücksichtigt werden.

(62) *Vermeidung von Interessenkonflikten bzw. Beeinflussungen*: Ein Interessenkonflikt ist nach der OECD „ein Konflikt zwischen den Amtspflichten und den Privatinteressen eines öffentlichen Bediensteten, bei dem die Interessen, die ein öffentlicher Bediensteter in seiner Eigenschaft als Privatperson hat, die Wahrnehmung seiner amtlichen Pflichten und Verantwortlichkeiten auf unbillige Weise beeinflussen können"[61]. Zur Vermeidung von Interessenkonflikten sind die gesetzlichen Regelungen zu Befangenheit und Hinderungsgründen (v.a. Verwaltungsverfahrensrecht, Kommunalrecht), zu Nebentätigkeiten (Arbeits- und Dienstrecht) und zum Verbot der Annahme von Vorteilen (Straf-, Arbeits- und Dienstrecht) zu beachten. Spenden, Sponsoring und sonstige Zuwendungen sind im Hinblick auf mögliche Interessenkonflikte zu prüfen und transparent zu machen. Die Vorgesetzten haben diesbezüglich ihrer Kontrollpflicht nachzukommen.[62]

(63) *Information, Belehrung, Sensibilisierung, Beratung sowie Aus- und Weiterbildung:* ☞ Tz. 123.

(64) *Transparenz bzw. Veröffentlichung wesentlicher Regeln und Informationen zu Compliance bzw. CMS der Kommune*: ☞ Tz. 124.

(65) *Rotation:*[63] Durch jahrelang unveränderte dienstliche Verwendungen auf einem Dienstposten können Verbindungen entstehen, die Regelverstöße begünstigen. Der Wechsel von Mitarbeitenden auf andere Dienstposten (Personalrotation) sowie die Umressortierung besonders korruptionsgefährdeter Aufgaben zu einem anderen Dienstposten (Aufgabenrotation) kann dem Entstehen solcher Verbindungen entgegenwirken.

(66) *Einrichtung und Betrieb eines Hinweisgebersystems*: ☞ Abschnitt 6.

(67) *Sanktionen für nicht regelkonformes Verhalten*: ☞ Tz. 135.

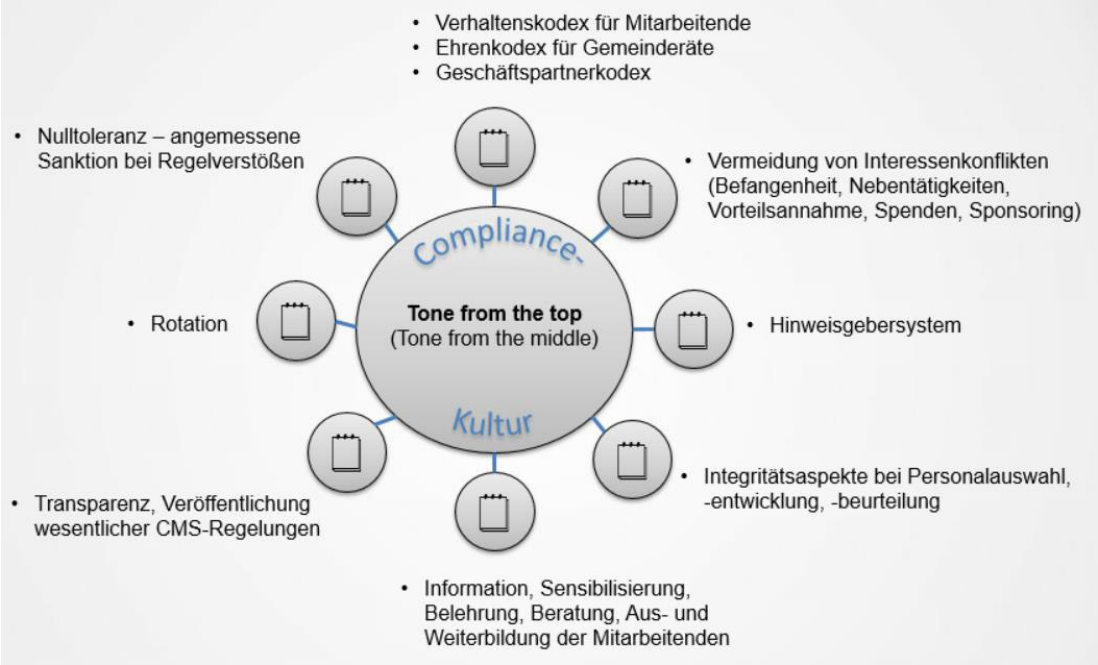
---

61 OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung): OECD-Leitlinien für die Behandlung von Interessenkonflikten im öffentlichen Dienst, 2006, S. 8.

62 Vgl. Glinder/Schröfel: Einführung von Antikorruptionsprozessen in die öffentliche Verwaltung; in: Louis/Glinder/Wassmer (Hrsg.): Korruptionsprävention in der öffentlichen Verwaltung – Handbuch für die kommunale Praxis, Stuttgart 2020, S. 160 - 174.

63 Vgl. Glinder/Schröfel, in: Louis/Glinder/Wassmer (Hrsg.): Korruptionsprävention in der öffentlichen Verwaltung, Stuttgart 2020, S. 183.

Abbildung 6: Compliance-Kultur



4.3 Compliance-Ziele

(68) Mit den Compliance-Zielen wird festgelegt, was mit dem CMS erreicht werden soll.[64] Die Compliance-Ziele ergeben sich aus den folgenden Fragestellungen:

(69) *1.) Welche strategischen Ziele verfolgt die Kommune?* Solche strategischen Ziele ergeben sich aus formellen und materiellen gesetzlichen Vorgaben, sonstigen Regelungen sowie strategischen Vorgaben der Organe der Kommune.

(70) Daraus ergeben sich in der öffentlichen Verwaltung mindestens folgende obligatorische Compliance-Ziele:

- Kommunen als Teil der öffentlichen Verwaltung sind an das Rechtsstaatsprinzip (Art. 20 Abs. 3 GG), d.h. an Recht und Gesetz gebunden. Daraus ergibt sich unmittelbar das Ziel, dass kommunales Handeln rechtskonform und ordnungsmäßig zu erfolgen hat.
- Schutz von hinweisgebenden Personen durch Einrichtung eines Hinweisgebersystems (EU-Wistleblower-Richtlinie, Hinweisgeberschutzgesetz).
- Vermeidung von materiellen Schäden für die Kommune bzw. pfleglicher Umgang mit deren Vermögen; Einhaltung bestehender Vermögensbetreuungspflichten seitens der kommunalen Organe und Mitarbeitenden; Abwendung

[64] Vgl. IDW PS 980, Tz. 23, A 15.

von Aufsichtspflichtverletzungen und Organisationsverschulden im kommunalen Pflichtenkreis.

- Verringerung der Haftungsrisiken für die Kommune, ihre Organe und Mitarbeitenden.

(71) Als weitere strategische Compliance-Ziele kommen u.a. in Betracht[65]:

- Wahrung des Vertrauens der Bürger*innen in die Rechtsstaatlichkeit, Objektivität und Neutralität der öffentlichen Verwaltung; Abwehr entsprechender Reputationsrisiken.
- Effiziente (wirtschaftliche) und effektive (wirksame) Steuerung der Compliance-Risiken (u.a. durch Transparenz von Risiken und Optimierung von Prozessen und Maßnahmen).
- Unterstützung bei der Erfüllung von Nachhaltigkeitszielen[66].

(72) *2.) Welche Teilbereiche* (☞ Tz. 33) *dieser Institution sollen vom CMS abgedeckt werden (Teilbereichsziele)?* Bei der Festlegung der Teilbereichsziele müssen die gesetzlichen Mindestanforderungen erfüllt werden, wobei die Größe und der Aufgabenkreis der Kommune eine entscheidende Rolle spielen (☞ Abschnitt 3.5). Die in den betreffenden Teilbereichen einzuhaltenden Regeln sind dem CMS zugrunde zu legen.

(73) Die *Festlegung* der Compliance-Ziele erfolgt durch die Leitung der Kommune, die für die Einhaltung der Compliance verantwortlich ist.

(74) Bei der Festlegung der Compliance-Ziele sollte u.a. geachtet werden auf[67]

- deren Konsistenz, Verständlichkeit und Praktikabilität sowie
- eine Abstimmung mit den verfügbaren (oder ggf. zusätzlich bereitzustellenden) Ressourcen (Umsetzbarkeit der Ziele).

(75) Die festgelegten Compliance-Ziele sind in die CMS-Dokumentation der Kommune aufzunehmen.

(76) Die festgelegten Compliance-Ziele sind allen Mitgliedern der Organe und den Mitarbeitenden bekanntzumachen. Ein dafür geeignetes Medium ist ein Verhaltenskodex (siehe dazu Abschnitt „Compliance-Programm").

(77) Compliance-Ziele sollten einer regelmäßigen Überprüfung (Monitoring) hinsichtlich ihrer Aktualität unterzogen werden.

---

65 Vgl. u.a. ISO 37301:2021, Introduction, S. VI.

66 Z.B. die globalen Sustainable Development Goals der UN-Agenda 2030 für nachhaltige Entwicklung (vgl. u.a. Deutsche Nachhaltigkeitsstrategie der Bundesregierung – Weiterentwicklung 2021, im Internet: https://www.bundesregierung.de/resource/blob/998006/1873516/9d73d857a3f7f0f8df5ac1b4c349fa07/2021-03-10-dns-2021-finale-langfassung-barrierefrei-data.pdf?download=1

67 Vgl. IDW PS 980, Tz. A 15.

4.4 Compliance-Risiken

(78) Compliance-Risiken stellen die bewertete Gefahr bzw. Möglichkeit dar, gegen einzuhaltende Regeln zu verstoßen und damit die festgelegten Compliance-Ziele zu verfehlen. Bezogen auf die einzelnen Compliance-Ziele (insbesondere die dem CMS unterliegenden Teilbereiche) sind anhand einer Compliance-Risikoanalyse die Compliance-Risiken zu identifizieren und zu bewerten. Die Risikobewertung dient als Grundlage für die Ausgestaltung und Festlegung des Compliance-Programms.

(79) Für die *Risikoidentifizierung* wird ein Verfahren zur systematischen Risikoerkennung und -berichterstattung eingeführt. Ihr schließt sich eine *Risikobewertung* an.[68]

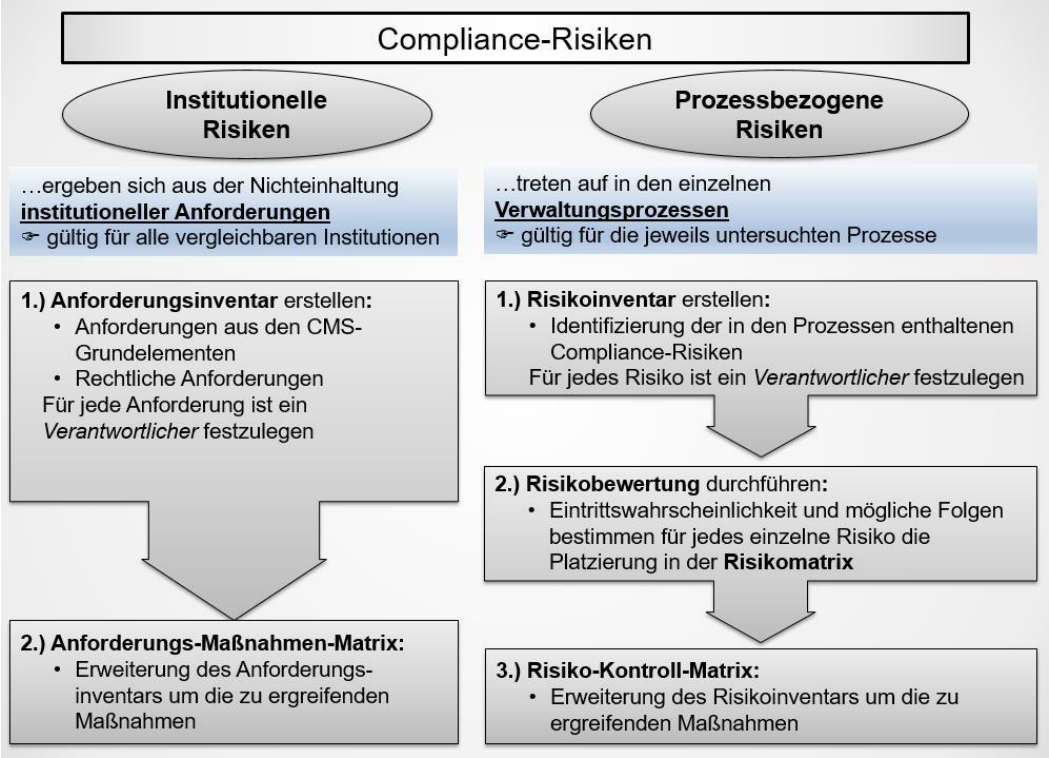
(80) Die Compliance-Risikoanalyse besteht[69]

- zum einen aus der Betrachtung der *institutionellen* Compliance-Risiken, auf deren Grundlage sich allgemeine institutionelle Anforderungen und Maßnahmen ableiten lassen, die für alle vergleichbaren Institutionen Gültigkeit haben;
- zum anderen aus der Betrachtung der konkreten *prozessbezogenen* (Produkte, Prozesse) Compliance-Risiken der jeweiligen Kommunalverwaltung bzw. des jeweiligen kommunalen Unternehmens.

[68] Vgl. IDW PS 980, Tz 23. Siehe zur praktischen Durchführung einer Risikoanalyse (Risikoidentifikation und -bewertung) einschlägige Literatur zum Risikomanagement; für eine kurze Übersicht vgl. Haag/Bindschädel: Das idealtypische Compliance Risk Assessment – Teil 2, in: Compliance-Berater 4/2021, S.112-117.

[69] Die Unterscheidung in institutionelle und spezielle Risiken erfolgt in Anlehnung an Moosmayer, Klaus: Compliance - Praxisleitfaden für Unternehmen, 4. Auflage 2021 Rn. 210 ff.

Abbildung 7: Compliance-Risiken



4.4.1 Analyse der institutionellen Compliance-Risiken

(81) *Risikoidentifizierung:* Institutionelle (prozessunabhängige) Compliance-Risiken bestehen entweder für die gesamte betrachtete Kommunalverwaltung bzw. das gesamte betrachtete kommunale Unternehmen, d.h. über alle CMS-Teilbereiche hinweg, oder für einzelne CMS-Teilbereiche. Solche institutionellen Compliance-Risiken ergeben sich v. a. aus der Nichteinhaltung von

- *Grundelementen eines CMS*: Aus den sieben Grundelementen eines CMS (☞ Tz. 50) ergeben sich Anforderungen, die – als notwendige Bedingung – zu erfüllen sind, damit das CMS überhaupt angemessen und wirksam sein kann.
- *rechtlichen Vorgaben*: Pflichten ergeben sich aus dem Hinweisgeberschutzgesetz bzw. der EU-Whistleblower-Richtlinie (☞ Abschnitt 6); auch das Verbandssanktionengesetz setzt Regeln für Compliance-Maßnahmen[70]. Notwendige Anforderungen an ein CMS für Kommunalverwaltungen finden sich zudem u.a. im Dienst-, Arbeits-, Straf-, Steuer- und Kommunalrecht. Für kommunale Unternehmen finden sich solche u.a. im Arbeits-, Straf-, Steuer- und Gesellschaftsrecht sowie in Public Corporate Governance Kodizes. Darüber

[70] Das Verbandssanktionengesetz liegt bisher nur als Entwurf vor.

hinaus kommen – abhängig vom Compliance-Ziel bzw. den jeweiligen umfassten Teilbereichen des CMS – möglicherweise weitere institutionsbezogene rechtliche Vorgaben infrage. Die rechtlichen Compliance-Vorgaben sind regelmäßig auf ihre Aktualität und ihre Auswirkung für das CMS hin zu überwachen.

- der *Compliance-Kultur* (☞ Abschnitt Nr. 4.2).

(82) Festgestellte Compliance-Verstöße sollten immer Anlass zur Überprüfung der Compliance-Risiken sein.

(83) Die identifizierten institutionellen Compliance-Risiken bzw. die korrespondierenden *institutionellen Compliance-Anforderungen* werden für die Kommune in Form eines *Anforderungsinventars* (☞ Anlage 2, Abschnitt 8.2) zusammengetragen. Sie lassen sich einzelnen oder mehreren Funktionen eines CMS (Prävention, Aufdeckung, Reaktion) zuordnen. Für jedes Risiko bzw. für jede Anforderung ist ein Verantwortlicher festzulegen. Dies alles ist zu dokumentieren.

(84) *Risikobewertung:* Da sich die identifizierten institutionellen Compliance-Risiken aus notwendig zu erfüllenden Anforderungen an ein CMS ergeben, bedarf es keiner Risikobewertung von Eintrittswahrscheinlichkeit und möglichen Folgen. Der Fokus liegt hier allein auf Art und Umfang der im Rahmen der Erstellung des Compliance-Programms bereits vorhandenen oder noch zu ergreifenden Maßnahmen. Dafür wird das bei der Risikoidentifikation erstellte Anforderungsinventar um die vorhandenen und im Rahmen des zu erstellenden Compliance-Programms noch zu ergreifenden Maßnahmen zu einer *Anforderungs-Maßnahmen-Matrix* (☞ Anlage 3, Abschnitt 8.3) erweitert. Dies ist zu dokumentieren (☞ Tz. 53).

4.4.2 Analyse der prozessbezogenen Compliance-Risiken

(85) *Risikoidentifizierung*: Prozessbezogene Compliance-Risiken treten in einzelnen Verwaltungs- bzw. Geschäftsprozessen (bei der Erstellung von Leistungen, Produkten) der CMS-Teilbereiche auf. Solche prozessbezogenen Compliance-Risiken ergeben sich v. a. aus

- der (bewussten oder unbewussten) Nichteinhaltung von rechtlichen Vorgaben für Abläufe in den vom CMS umfassten Teilbereichen (☞ Tz. 33). Compliance-Vorgaben sind regelmäßig auf ihre Aktualität und ihre Auswirkung für das CMS hin zu überwachen.

- der konkreten Ablauforganisation bzw. der Geschäftsprozesse. Risikobeeinflussende Faktoren in Geschäftsprozessen sind u.a. der Grad der Komplexität und Transparenz der Abläufe sowie die Eindeutigkeit der Zuständigkeiten.
- dem Grad der Angemessenheit und Wirksamkeit der bereits getroffenen Maßnahmen zur Vermeidung bzw. Verminderung der Compliance-Risiken, insbesondere des Internen Kontrollsystems.
- der Einführung neuer Technologien und Methoden.

Zur Risikoidentifizierung bieten sich folgende Quellen an:

- Dokumente wie u.a. Organisationsunterlagen, Prozessbeschreibungen, visualisierte Prozesse, Gemeinderatsunterlagen, Berichte der Organisationseinheiten, Prüfungsberichte, Rechtsprechungen, Mitteilungen der kommunalen Verbände, Pressemitteilungen;
- Interviews und Workshops mit Personen, die Kenntnisse zu einzelnen Compliance-Risiken haben können, wie Compliance-Beauftragter, Rechtsamt, Interne Revision, Beauftragte für einzelne Risiken, IT-Amt, Personalamt, Vergabeamt und solche aus den sonstigen Ämtern und Organisationseinheiten.

(86) Festgestellte Compliance-Verstöße sollten immer Anlass zur Überprüfung der Compliance-Risiken sein.

(87) Die identifizierten prozessbezogenen Compliance-Risiken sind in einem *Risikoinventar* (☞ Anlage 5, Teil 1, Abschnitt 8.5) zusammenzutragen. Für jedes Risiko ist ein Risiko-Verantwortlicher festzulegen. Beides ist zu dokumentieren.

(88) *Risikobewertung*: Die einzelnen identifizierten Compliance-Risiken sind jeweils im Hinblick auf Eintrittswahrscheinlichkeit und mögliche Folgen (potenzielle Schadenshöhe bzw. Auswirkung) zu bewerten. Die Bewertung erfolgt in einem ersten Schritt ohne – d.h. Bewertung als *Bruttorisiko* – und in einem zweiten Schritt mit Berücksichtigung – d.h. Bewertung als *Nettorisiko* mit Beurteilung der Wirksamkeit – eventuell vorhandener Maßnahmen des Compliance-Programms (☞ Abschnitt 4.5) zur Reduzierung der Eintrittswahrscheinlichkeit und der möglichen Folgen. Die Kombination aus beidem erlaubt in Form einer *Risikomatrix* (Risikolandkarte) die Einstufung der einzelnen Compliance-Risiken (brutto und netto) und damit deren Priorisierung. Dabei ist für die Eintrittswahrscheinlichkeit, für die möglichen Folgen und die Kombination aus beidem eine geeignete *Risikobewertungs-Systematik* zugrunde zu legen, die aus Kategorien mit quantitativen und qualitativen Bewertungskriterien besteht (☞

Anlage 4, Abschnitt 8.4).[71] Die Risikobewertungs-Systematik ist geeignet, wenn sie es erlaubt, die Notwendigkeit, Bedeutung und den Wirkungsgrad von Maßnahmen des Compliance-Programms einschätzen zu können.[72] Das bei der Risikoidentifikation erstellte Risikoinventar wird um die Ergebnisse der Risikobewertung sowie die vorhandenen und noch im Rahmen des zu erstellenden Compliance-Programms zu ergreifenden Maßnahmen zu einer *Risiko-Kontroll-Matrix* (☞ Anlage 5, Abschnitt 8.5) erweitert. Dies ist zu dokumentieren (☞ Tz. 53).

4.4.3 Risikoanalyse als systematischer Prozess

(89) Die Identifizierung und Bewertung der Compliance-Risiken erfolgt *systematisch*, indem

- dafür ein strukturiertes und dokumentiertes *Verfahren* mit klaren Zuständigkeiten festgelegt ist, das regelmäßig bzw. in angemessenen Zeitabständen durchlaufen wird;
- eine *vollständige* Betrachtung aller Compliance-Risiken (im Hinblick auf die Compliance-Ziele bzw. aller in das CMS aufgenommenen Teilbereiche) innerhalb der Kommunalverwaltung bzw. des kommunalen Unternehmens sowie aus dem – v. a. rechtlichen – Umfeld sichergestellt ist (z. B. durch Verwendung kommunaler oder auf Teilbereiche bezogener Risikokataloge);
- die rechtlichen Compliance-Vorgaben (im Rahmen der Risikoidentifizierung) regelmäßig auf relevante Änderungen hin überwacht werden;
- festgestellte Compliance-Verstöße bei der Risikoanalyse berücksichtigt werden;
- eine geeignete und nachvollziehbare *Bewertungssystematik* (Bewertungskriterien, Kategorien) verwendet wird;
- die Risikoanalyse unter Beteiligung der für die jeweiligen Bereiche und Compliance-Risiken *sachkundigen Personen* erfolgt (z. B. durch Interviews und Workshops);
- das festgelegte Verfahren und die Zuständigkeiten, die Bewertungssystematik, die Ergebnisse der Identifikation und der Bewertung der Compliance-Risiken bzw. der institutionellen Anforderungen sowie die Festlegung der jeweils Verantwortlichen angemessen und revisionsfähig *dokumentiert* werden;

---

[71] Vgl. Schmigale, Jenny: Compliance Management, Herangehensweise an das Compliance-Risikomanagement, in: https://www.compliance-manager.net/fachartikel/herangehensweisen-das-compliance-risikomanagement-1774965701

[72] In Anlehnung an IDW PS 981, Tz. A25.

- das Ergebnis der Risikoanalyse an die Leitung der Kommune und die jeweils zuständigen Leitungsebenen unverzüglich und nachvollziehbar kommuniziert wird, es dort zur Kenntnis genommen sowie ggf. Anforderungen an die Leitung dokumentiert und berücksichtigt werden.

(90) Die Identifikation und Bewertung der Compliance-Risiken ist Voraussetzung für das zu erstellende Compliance-Programm. Es kann daher grundsätzlich nicht auf eine solche Risikoanalyse verzichtet werden, unabhängig von der Größe der Kommunalverwaltung oder des kommunalen Unternehmens. Jedoch reduziert sich für kleinere und mittlere Kommunen bereits aus ihrem im Vergleich zu großen Kommunen kleineren Aufgabenkreis der Aufwand einer Risikoanalyse. Des Weiteren müssen institutionelle Compliance-Risiken bzw. Compliance-Anforderungen i. d. R. nicht gesondert erhoben werden, sondern können von anderen Kommunen – ggf. angepasst – übernommen werden.

(91) Compliance-Anforderungen ergeben sich für Kommunen – neben den allgemeinen Vorgaben – auch aus rechtlichen Vorgaben für *Teilbereiche* (☞ Tz. 33).

4.5 Compliance-Programm

(92) Auf der Grundlage der Ergebnisse der Compliance-Risikoanalyse sind Maßnahmen einzuführen, die auf die Begrenzung der Compliance-Risiken und damit auf die Vermeidung von Regelverstößen ausgerichtet sind. Des Weiteren sind die bei Compliance-Verstößen zu ergreifenden Maßnahmen festzulegen [vgl. IDW PS 980, Tz. 23][73]. Die Maßnahmen ergeben sich aus den Anforderungen aller CMS-Grundelemente bzw. entsprechend der Unterscheidung bei der Compliance-Risikoanalyse aus den für alle Kommunen gleichen *institutionellen* Anforderungen und den konkreten *prozessbezogenen* Compliance-Risiken[74]. Das Compliance-Programm stellt die Gesamtheit aller dieser Maßnahmen dar.

(93) Ein Compliance-Programm baut auf den drei Funktionen (Säulen) eines CMS auf (☞ Tz. 34):[75]

- die Verhinderung von Regelverstößen (Prävention);
- das rechtzeitige Erkennen von Compliance-Verstößen (Aufdeckung);
- die Reaktion bei Compliance-Verstößen.

[73] Der IDW PS 980 unterscheidet zwischen Grundsätzen und Maßnahmen, wobei unter Grundsätzen Regelungen verstanden werden, mit denen Mitarbeitende und ggf. Dritte zu regelkonformem Verhalten angehalten werden [vgl. IDW PS 980, Tz. A17]. Diese Unterscheidung ist jedoch kaum trennscharf durchführbar, weshalb hier auf die Unterscheidung verzichtet wird und Grundsätze unter Maßnahmen subsumiert werden.

[74] Die Unterscheidung in institutionelle und spezielle Risiken erfolgt in Anlehnung an Moosmayer, Klaus: Compliance - Praxisleitfaden für Unternehmen, 4. Auflage 2021, Rn. 210 ff.

[75] Vgl. Schmidt, Wirtschaftsprüfung und CMS-Prüfung, Rn. 35 f., in: Hauschka/Moosmayer/Lösler: Corporate Compliance, 3. Auflage 2016.

4.5.1 Anforderungen

(94) Folgende *Anforderungen* sind im Zuge der Erstellung eines Compliance-Programms zu erfüllen:

(95) *1.) Ableitung aus der Compliance-Risikoanalyse:* Die einzelnen Maßnahmen des Compliance-Programms stellen eine Reaktion auf die analysierten Compliance-Risiken dar, d.h. sie leiten sich aus der Compliance-Risikoanalyse, konkret dem Anforderungsinventar auf der Basis institutioneller Risiken und dem Risikoinventar mit den bewerteten prozessbezogenen Risiken, ab (☞ Abschnitt Nr. 4.4). Die Maßnahmen lassen sich mindestens einem der drei Funktionen bzw. Säulen (☞ Tz. 34) eines Compliance-Programms zuordnen: Prävention, Aufdeckung, Reaktion. Die Maßnahmen werden in der Anforderungs-Maßnahmen-Matrix bzw. Risiko-Kontroll-Matrix aufgeführt (☞ Abschnitte 4.4.2 und 4.4.3).

(96) *2.) Angemessenheit*: Ein Compliance-Programm ist angemessen, wenn die dort enthaltenen Maßnahmen im Einzelnen oder insgesamt als System geeignet sind, mit hinreichender Sicherheit wesentliche Regelverstöße zu verhindern (Prävention) als auch solche rechtzeitig zu erkennen (Aufdeckung) und darauf zu reagieren (Reaktion). Dies umfasst auch die unverzügliche Berichterstattung eingetretener Regelverstöße an die zuständige Stelle in der Kommunalverwaltung bzw. im kommunalen Unternehmen [vgl. IDW PS 980, Tz. 20]. Die zuständige Stelle ist in der Regel die Leitung der Behörde, der Dienstvorgesetze bzw. die Leitung des Unternehmens, die/der für die Folgemaßnahmen (Reaktion) verantwortlich ist. Die Geeignetheit und damit die konkrete Ausgestaltung des Compliance-Programms für eine Kommunalverwaltung bzw. ein kommunales Unternehmen hängt jeweils im Einzelfall insbesondere ab von [vgl. IDW PS 980, Tz. 23]:

- den festgelegten Compliance-Zielen bzw. den zu umfassenden Teilbereichen (☞ Abschnitt 4.3);
- der Größe der Verwaltung bzw. des öffentlichen Unternehmens;
- Art und Umfang der Verwaltungs- bzw. Geschäftstätigkeit sowie
- den rechtlichen Vorgaben (☞ Abschnitte 3.3 und 3.4).

Zur Angemessenheit eines Compliance-Programms gehört außerdem, dass dessen Maßnahmen auch tatsächlich implementiert bzw. in Kraft gesetzt worden sind.

(97) *3.) Wirksamkeit*: Die Wirksamkeit eines Compliance-Programms ist dann gegeben, wenn die jeweiligen dort enthaltenen Maßnahmen (☞ Abschnitt 4.5.2) angemessen sind und in den laufenden Verwaltungs- bzw. Geschäftsprozessen von den hiervon

Betroffenen nach Maßgabe ihrer Verantwortung zur Kenntnis genommen und beachtet werden (vgl. IDW PS 980, Tz. 21], d.h., dass die Maßnahmen wie konzipiert tatsächlich umgesetzt werden.

(98) *4.) Festlegung von Maßnahmen- und Umsetzungsverantwortlichen*: Für jede Compliance-Maßnahme ist ein Verantwortlicher festzulegen. Sind neue Compliance-Maßnahmen einzuführen oder vorhandene zu ändern, ist auch ein Umsetzungsverantwortlicher festzulegen. Die jeweiligen Verantwortlichen werden in der Anforderungs-Maßnahmen-Matrix bzw. Risiko-Kontroll-Matrix aufgeführt (☞ Abschnitte 4.4.1 und 4.4.2).

(99) *5.) Dokumentation und Schriftlichkeit*: ☞ Tz. 53.

4.5.2 Maßnahmen

(100) Compliance-Maßnahmen ergeben sich entsprechend der Unterscheidung bei der Compliance-Risikoanalyse aus den für Kommunen geltenden institutionellen Anforderungen (☞ Abschnitt Nr. 4.4.1) und den prozessbezogenen Compliance-Risiken (☞ Abschnitt Nr. 4.4.2).

(101) *Institutionelle Maßnahmen*: ☞ Anlage 2, Abschnitt 8.2.

(102) *Prozessbezogene Maßnahmen – Internes Kontrollsystem:* Prozessbezogene Maßnahmen sind vor allem Steuerungs- und Kontrollmaßnahmen eines Internen Kontrollsystems innerhalb von Prozessen. Sie sind in eine Risiko-Kontroll-Matrix (☞ Anlage 5, Abschnitt 8.5) aufzunehmen. Ein Internes Kontrollsystem besteht aus systematisch gestalteten organisatorischen (Sicherungs-) Maßnahmen und Kontrollen in der Kommune zur Einhaltung von Richtlinien und zur Abwehr von Schäden, die durch das eigene Personal oder böswillige Dritte verursacht werden können[76]. Die Maßnahmen beruhen auf technischen und organisatorischen Prinzipien. Ein Internes Kontrollsystem dient sowohl der Verhinderung als auch der Aufdeckung von Regelverstößen. Voraussetzung für ein wirksames Internes Kontrollsystem ist die Beschreibung bzw. Visualisierung der den Teilbereichen zugrundeliegenden Prozesse. Darüber hinaus sind ggf. spezifische Maßnahmen zur Begegnung von Risiken erforderlich, die sich aus komplexen Geschäftsprozessen mit vielen Schnittstellen und unterschiedlichen Zuständigkeiten oder aus der Einführung neuer Technologien und Methoden ergeben.

[76] IDR Prüfungsleitlinie L 111 „Die IKS-Prüfung in der Rechnungsprüfung“, Stand 29.11.2018, Tz 4.

4.6 Compliance-Organisation

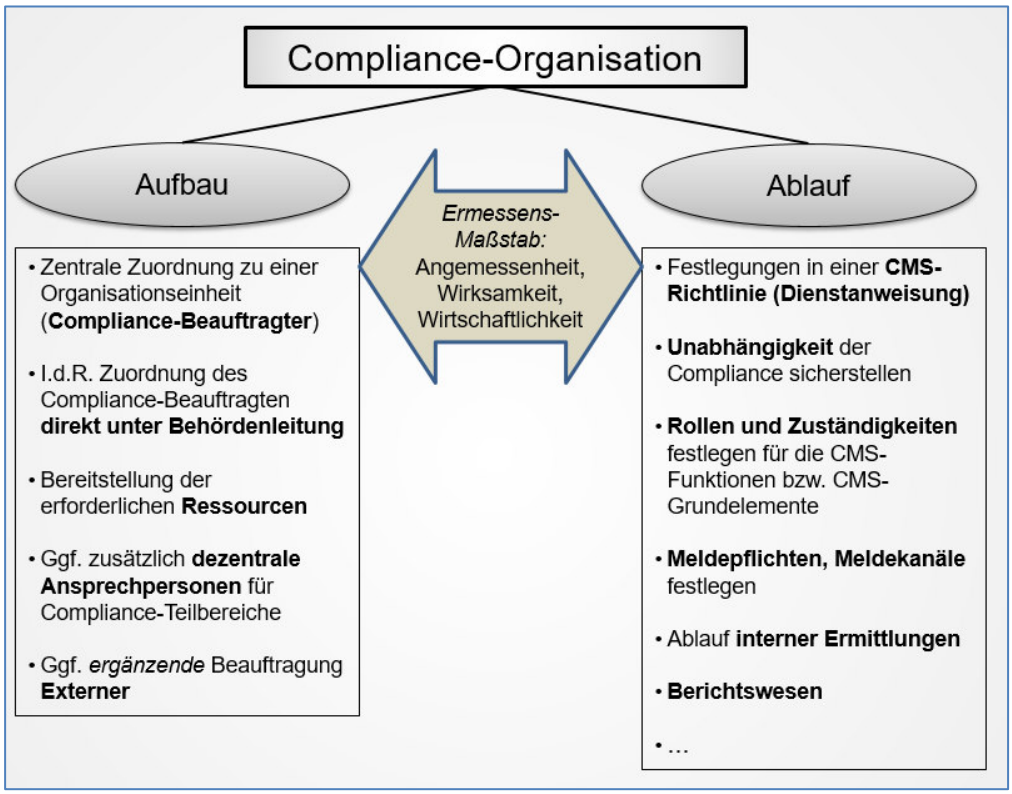
(103) Die Organisation des CMS umfasst:[77]

a. die verbindliche Festlegung der *Aufbau- und Ablauforganisation* des CMS als integraler Bestandteil der Behördenorganisation;
b. die verbindliche Festlegung der *Aufgaben, Rollen und Verantwortlichkeiten* im CMS; Bestellung des Compliance-Beauftragten und von Ansprechpersonen für Teilbereiche;
c. die der Compliance-Funktion zugeordneten Mitarbeitenden haben die notwendige *Unabhängigkeit, Kompetenz und organisatorische Stellung* für eine wirksame Wahrnehmung ihrer Rollen.
d. die Bereitstellung der erforderlichen personellen, technischen (v.a. Hard- und Software) und finanziellen *Ressourcen*.

(104) Die Entscheidung über die Ausgestaltung der Compliance-Organisation liegt im pflichtgemäßen Ermessen der Kommune, sofern nicht spezialgesetzliche Regelungen greifen.[78] Bei der praktischen Umsetzung sind Wirksamkeit, Angemessenheit und Wirtschaftlichkeit als Maßstab für die bestmögliche Erreichung der festgelegten Compliance-Ziele zu wählen. Dabei empfiehlt es sich an den bestehenden Compliance-Risiken auszurichten.

[77] Vgl. IDW PS 980, Tz 23 und Tz A18; vgl. IDW EPS 980 Entwurf, Tz 27 und Tz A27.
[78] Vgl. Stober/Ohrtmann, Compliance, Handbuch für die öffentliche Verwaltung, 2. Auflage 2022, Rn. 906.

Abbildung 8: Compliance-Organisation



4.6.1 Organisatorische Zuordnung der Compliance-Funktion

(105) Um eine einheitliche Ausübung der Compliance-Funktion sicherzustellen, ist sie in aller Regel zentral einer Organisationseinheit zuzuordnen. Aufgrund der Letztverantwortung des gesetzlichen Vertreters der Kommune für Compliance sollte ihm der Compliance-Beauftragte direkt zugeordnet sein oder eine ihm nahe Stellung einnehmen. Für eine Zuordnung kommen in der Regel folgende Organisationseinheiten in Betracht, mit den jeweils damit verbundenen Vor- und Nachteilen:

Zuordnung	Vorteile	Nachteile
Neue Organisationseinheit „Compliance"	• I.d.R. direktes Vortragsrecht • Einrichtung einer Stabstelle zeigt Bedeutung der Compliance für die Führungsebene	• Ggf. fehlendes Know-How für interne Ermittlungen (Prüfungen) • Neue Organisationseinheit muss sich erst etablieren

Interne Revision / Rechnungsprüfungsamt	• Unabhängigkeit und Weisungsgebundenheit sind für den Prüfungsauftrag gesetzlich verankert • Direkt dem (Ober)Bürgermeister unterstellt • Örtliche Prüfung / Interne Revision ist bereits selbst wesentlicher Teil der Selbstkontrolle der Kommune (Three-Lines-Modell) • Wissen über örtliche kommunale Strukturen ist bereits vorhanden • Prüfungs-Know-How vorhanden	• Nicht bei jeder Kommune vorhanden • Kann als Bestandteil des CMS nicht mehr selbst das ganze CMS prüfen (ggf. nur Teile des Systems)
Rechtsabteilung / Rechtsamt	• Breites juristisches Fachwissen vorhanden • (Teil-)Zuständigkeit für Folgemaßnahmen	• Fehlende Unabhängigkeit (vertritt Rechtsposition der Kommune) • Weisungsgebunden • Fehlendes Prüfungs-Know-How
Personalabteilung	• Breites arbeits- und dienstrechtliches Fachwissen vorhanden • Nimmt bereits beratende und unterstützende Funktion ein	• Fehlende Unabhängigkeit (vertritt Rechtsposition der Kommune) • Weisungsgebunden • Fehlendes Prüfungs-Know-How

(106) Neben der zentralen Organisationseinheit für die Compliance-Funktion sollten bei mittleren und größeren Kommunen Ansprechpersonen für Compliance-Teilbereiche eingebunden werden; sofern es für Teilbereiche bereits bestellte Beauftragte gibt, sollten diese eingebunden werden.

Teile des CMS können auch an externe Dienstleister vergeben werden (Outsourcing), z.B. Beauftragung einer Ombudsperson oder externer Compliance-Schulungen. Die Verantwortung für die Wirksamkeit des CMS verbleibt jedoch immer bei der Leitung der Kommune bzw. des Unternehmens. Vor der Entscheidung über Outsourcing sind daher dessen Risiken (z.B. dass der Beauftragte Compliance-Anforderungen selbst nicht einhält, ihm Kenntnisse interner Abläufe fehlen oder Akzeptanzprobleme bei den Mitarbeitenden der Kommunalverwaltung bestehen) zu bewerten.

4.6.2 Compliance-Beauftragter

(107) Der Compliance-Beauftragte ist eine Person, die in der Kommune mit der Compliance-Funktion bzw. dem Aufbau und dem Betrieb eines CMS zur Umsetzung der festgelegten Compliance-Ziele (☞ Abschnitt 4.3) betraut ist. Die konkreten Aufgaben des Compliance-Beauftragten und die zugehörigen Prozesse lassen sich den drei Funktionen bzw. Säulen eines CMS (☞ Tz. 34) zuordnen:

(108) Zu typischen Aufgaben bei der *Prävention* gehören:[79]

- Funktionsfähigkeit des CMS sicherstellen[80], wozu u.a. gehören: Konzeption des CMS erstellen, Leitlinien bzw. Richtlinien entwickeln, einen Prozess zur Identifikation und Bewertung von Compliance-Pflichten und -Risiken sowie deren Adressierung durch Maßnahmen einrichten, ein Berichtswesen aufbauen, auf eine angemessene Dokumentation des CMS achten, das bestehende CMS auf Anpassungs- und Verbesserungsbedarf evaluieren;
- aufklären (schulen, informieren, trainieren);
- Führungskräfte, Mitarbeitende, Organisationseinheiten beraten;
- Compliance-Fragen beantworten und Hinweise geben zu Compliance-relevanten Themen;
- Öffentlichkeitsarbeit;
- Erfahrungsaustausch mit anderen Kommunen, Verbänden, wissenschaftlichen Einrichtungen u. s. w.

(109) Zu typischen Aufgaben bei der *Aufdeckung* gehören[81]:

- Betrieb der internen Meldestelle, Entgegennahme von Hinweisen;
- Interne Ermittlungen / Sachverhaltsaufklärung / Ermittlungsberichte.[82]

(110) Zu typischen Aufgaben bei der *Reaktion* gehören[83]:

- Zusammenarbeit mit anderen internen und externen Bereichen (z.B. den Strafverfolgungsbehörden);

---

79 Vgl. Glinder/Schröfel: in: Louis/Glinder/Wassmer (Hrsg.), Korruptionsprävention in der öffentlichen Verwaltung, Stuttgart 2020, S. 146.

80 Vgl. ISO 37301 (2021), Nr. 5.3.2.

81 Vgl. Glinder/Schröfel, in: Louis/Glinder/Wassmer (Hrsg.), Korruptionsprävention in der öffentlichen Verwaltung. S. 194-210.

82 Laut der DICO-Studie „Interne Untersuchungen in Deutschland – 2022“ des Deutschen Instituts für Compliance (DICO), S.15, werden interne Untersuchungen/Ermittlungen von den befragten Unternehmen grundsätzlich durch eigene Mitarbeitende durchgeführt; nur bei komplexeren Untersuchungen wird externe Unterstützung hinzugezogen.

83 Vgl. Glinder/Schröfel, in: Louis/Glinder/Wassmer (Hrsg.), Korruptionsprävention in der öffentlichen Verwaltung. S. 211-214.

- Unterstützung der zuständigen Stellen bei der Geltendmachung von zivilrechtlichen Ansprüchen (z.B. Schadensersatzforderungen, Herausgabeansprüche);
- Unterstützung der zuständigen Stellen bei der Überprüfung der durch Regelverstöße zustande gekommenen Rechtsakte bzw. -geschäfte;
- Unterstützung der zuständigen Stellen bei der Einleitung arbeits- oder dienstrechtlicher Maßnahmen;
- Evaluierung und Verbesserung des CMS bzw. von Maßnahmen.

(111) Dem Compliance-Beauftragten sollten zur effektiven Erfüllung der Aufgaben bestimmte Rechte bzw. *Befugnisse* schriftlich zugestanden werden:

- direktes Vortragsrecht bei der Leitung der Kommune;
- Initiativrecht beim Aufgreifen von Themen;
- Unabhängigkeit bei der Wahrnehmung der Compliance-Aufgaben, insbesondere unabhängiges und weisungsungebundenes Nachgehen von Verstößen (weitgehende Prüfrechte).

Der Compliance-Beauftragte sollte daher auf einer entsprechenden Hierarchiestufe in der Kommune angesiedelt sein.[84]

(112) Hinsichtlich der notwendigen *Qualifikation* eines Compliance-Beauftragten bestehen im öffentlichen Bereich keine ausdrücklichen gesetzlichen Vorgaben. Gleichwohl bedarf es für die effektive Wahrnehmung der Pflichten des Compliance-Beauftragten – und i.d.R. auch seiner Mitarbeitenden – bestimmter sozialer und fachlicher Voraussetzungen:

(113) Fachliche Kompetenzen (Aufzählung nicht abschließend):

- Rechtskenntnisse in den relevanten Bereichen, insb. im Arbeits-, Dienst-, Straf- und Zivilrecht;
- vertiefte Kenntnisse im Bereich der Korruptionsprävention und -bekämpfung;
- betriebswirtschaftliche Kenntnisse, u.a. zur Buchhaltung, zum Rechnungswesen;
- Kenntnisse über Prozesse und Systeme;
- Kenntnisse im Projekt- und Risikomanagement;
- Bereitschaft zur kontinuierlichen Fort- und Weiterbildung;

[84] I.d.R. „mindestens auf der 3. Führungsebene“ (Konstanz Institut für Corporate Governance (KICG) der Hochschule Konstanz Technik, Wirtschaft und Gestaltung: Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen – KICG CMS-Leitlinie 2 2014 für Unternehmen mit 250 bis 3.000 Mitarbeitern, Stand 04/2014, Seite 40).

- Kenntnisse und Erfahrungen über die öffentliche Verwaltung bzw. bestehenden Verwaltungsstrukturen;
- Führungserfahrung.

(114) Soziale Kompetenzen (Aufzählung nicht abschließend):

- Integrität;
- Selbstständigkeit bzw. Eigenverantwortlichkeit und Zuverlässigkeit;
- Initiative;
- Verhandlungsgeschick und Durchsetzungsfähigkeit;
- Empathie;
- Belastbarkeit.

4.6.3 Dezentrale Ansprechpersonen für Compliance

(115) Bei größeren Kommunen kann es für eine wirksame Compliance-Organisation sinnvoll sein, Ansprechpersonen für Compliance in dezentralen Organisationseinheiten zu haben. Sie arbeiten dem Compliance-Beauftragten zu, unterstützen ihn und stimmen sich mit ihm ab. Zu den Aufgaben solcher dezentralen Ansprechpersonen für Compliance können gehören:

- Unterstützung bei der Organisation von Schulungen;
- Erste Anlauflaufstelle bei Fragen zur Compliance im jeweiligen Teilbereich bzw. in der jeweiligen Organisations-Einheit (z. B. beim Umgang mit angebotenen Vorteilen);
- Unterstützung des Compliance-Beauftragten bei internen Ermittlungen.

Die dezentralen Ansprechpersonen für Compliance sollten die für ihre Aufgaben erforderlichen Kenntnisse und Erfahrungen haben.

(116) Der Ansprechperson sollten bestimmte Rechte zugestanden werden. Hierzu zählen mindestens:

- direktes Vortragsrecht bei der Leitung der dezentralen Organisations-Einheit;
- Anhörungs- und Initiativrecht bei Regelungen zur Compliance;
- Zurverfügungstellung benötigter Ressourcen;
- regelmäßige Fortbildungen im Bereich Compliance.

4.6.4 Ausstattung des Compliance-Beauftragten mit Ressourcen

(117) Für ein wirksames CMS müssen dem Compliance-Beauftragten im angemessenen Umfang personelle Ressourcen, sowohl quantitativ als auch qualitativ, zur Verfügung stehen.

(118) Kriterien für die Angemessenheit der *quantitativen Personalausstattung* des Compliance-Beauftragten sind insbesondere:[85]

- Größe der kommunalen Verwaltung;
- Anzahl und Komplexität der entsprechend der Compliance-Ziele in das CMS aufzunehmenden Teilbereiche und der sich daraus ergebenden Compliance-Risiken;
- Art der Ausgestaltung der einzelnen Abläufe bzw. Prozesse des CMS (hierarchische Tiefe, Anteil von Outsourcing etc.) und der sich daraus ergebenden Compliance-Risiken;
- eventuelle Synergieeffekte durch Einbeziehung bestehender Funktionsstellen (u.a. Personalamt, Rechtsamt, Rechnungsprüfungsamt) in das CMS, wenn diese Stellen bereits Teilaspekte des CMS abdecken.

(119) Die *qualitative Personalausstattung* richtet sich auch für die weiteren Mitarbeitenden des Compliance-Beauftragten – abhängig vom konkreten Aufgabenzuschnitt – grundsätzlich nach den Anforderungen für den Compliance-Beauftragten (☞ Abschnitt Nr. 4.6.2).

(120) Daneben bedarf es eines angemessenen *Compliance-Budgets*, aus dem Sachmittel, IT-Ausstattung, Fortbildungen, Dienstleistungen und Maßnahmen für die Compliance-Funktion finanziert werden können, die von Lieferanten, externen Anbietern oder mit Unterstützung externer Dienstleister bereitgestellt werden.

4.6.5 CMS-Richtlinie (Dienstanweisung)

(121) Die gesetzlichen und internen Vorgaben sowie die CMS-Grundelemente bilden den Rahmen für die der Compliance-Organisation zuzuweisenden Aufgaben und einzurichtenden Abläufe bzw. Prozesse (rechtliche Stellung der Compliance-Organisation). Sie sind in eine CMS-Richtlinie (Dienstanweisung) aufzunehmen (☞ Abschnitt 4.6.5). Dies sind konkret insbesondere folgende Punkte:

- Unabhängigkeit: Eine effektive Erfüllung der übertragenen Aufgaben im Bereich der Compliance ist nur bei ausreichender Unabhängigkeit der Compliance-Verantwortlichen möglich. Dies gilt in hierarchischer, disziplinarischer

[85] Für die quantitative Personalausstattung der Compliance-Aufgaben findet sich in der Literatur ein Richtwert von „mindestens ein Vollzeitäquivalent (VZÄ) pro 2.000 Mitarbeiter“ (Konstanz Institut für Corporate Governance (KICG) der Hochschule Konstanz Technik, Wirtschaft und Gestaltung: Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen – KICG CMS-Leitlinie 2 2014 für Unternehmen mit 250 bis 3.000 Mitarbeitern, Stand 04/2014, Seite 41).

und organisatorischer Hinsicht. Zuweisung anderer Aufgaben, die zu einem Interessenskonflikt führen, müssen ausgeschlossen werden.[86]

- Begriffsbestimmung und festgelegte Ziele der Compliance;
- Grundlegende Darstellung der Aufgaben (Prävention und Repression);
- Festlegung wesentlicher Zuständigkeiten innerhalb der Kommune;
- Festlegung von Meldepflichten;
- Festlegung der Meldekanäle für das Hinweisgebersystem (☞ Abschnitt 6)
- Festlegungen zum Berichtswesen;
- Rechte und Pflichten der Compliance-Organisation bzw. der Rollen / Verantwortlichen;
- Ablauf interner Ermittlungen;
- Festlegung sonstiger zur Umsetzung der einzelnen CMS-Grundelemente erforderlichen Abläufe bzw. Prozesse (u.a. zu Compliance-Risiken, zum Compliance-Programm, zur Compliance-Kommunikation und Compliance-Überwachung);
- ggf. Regelungen zur Beteiligungsverwaltung.

4.7 Compliance-Kommunikation

(122) Die Compliance-Kommunikation dient der adressatenorientierten Information aller Akteure (☞ Tz. 32) eines CMS. Eine wirksame Compliance-Kommunikation besteht aus mindestens den folgenden fünf Elementen:

(123) 1.) *Information, Belehrung, Sensibilisierung, Beratung und Aus- und Weiterbildung* der Mitarbeitenden und ggf. von Dritten, bei deren Beauftragung von der Kommune Sorgfaltspflichten zu erfüllen sind (u.a. Verwaltungshelfer, Lieferanten), im Rahmen der Compliance-Kultur (☞ Abschnitt 4.2):

- *Information* zu den bestehenden Compliance-Regeln und dem eingerichteten CMS (Aufbau-, Ablauforganisation) der Kommune in Form von – möglichst an den Adressaten (v.a. Führungskräfte, Sachbearbeiter, Funktionsträger, Mitarbeitende in sensiblen Funktionen, neue Mitarbeitende) orientierten und praxisnahen – Schulungen (in Präsenz, online), Informationsmaterial, Intranetauftritt, Videos u.ä. Für die Schulungen sollte ein Konzept mit den adressatenbezogenen Inhalten und ggf. den Schulungsmethoden erstellt werden. Schulungen und Informationsmedien sollten regelmäßig evaluiert und ggf. aktualisiert werden.

[86] Vgl. Eckert/Deters, Praxiswissen Compliance, 2. Auflage 2018, S. 43. Auch das Hinweisgeberschutzgesetz (§ 15) fordert die Unabhängigkeit der Personen, die Hinweise bearbeiten.

- *Belehrung* ist die Bestätigung der Mitarbeitenden oder ggf. Dritter, dass sie von den Compliance-Regeln der Kommune (u.a. dem Verhaltenskodex) Kenntnis genommen haben. Die Bestätigung erfolgt u.a. durch Unterschrift, Teilnahmelisten bei Schulungen oder Dienstbesprechungen, Zertifikate an teilgenommenen Online-Schulungen. Belehrungen sollten regelmäßig (z.B. jährlich) wiederholt werden. Eine besondere Form ist die förmliche Verpflichtung von Personen, die nicht Amtsträger sind und öffentliche Aufgaben nach dem Verpflichtungsgesetz wahrnehmen, wonach diese Personen bei Verwirklichung von Amtsträger-Korruptionsstraftatbeständen strafrechtlich Amtsträgern gleichgestellt werden.
- *Sensibilisierung* der Mitarbeitenden oder ggf. von Dritten in Bezug auf Gefahren für Regelverstöße, die aus bestimmten Situationen entstehen können, durch Schulungen, Informationsmaterial oder auf Dienstbesprechungen, Workshops u.ä., mit dem Ziel, das Verhalten der Akteure (☞ Tz. 32) im Sinne eines regelkonformen Verhaltens zu beeinflussen.
- *Beratung* meint die Klärung konkreter Compliance-Fragestellungen, entweder in Bezug auf einen bestimmten Sachverhalt oder auf eine abstrakte Sachverhaltskonstellation (z.B. Unterstützung bei der Erstellung von Dienstanweisungen). Sofern es für Compliance-Teilbereiche und Rechtsberatung gesonderte Beauftragte bzw. Zuständige gibt, ist deren vorrangige Hinzuziehung zu berücksichtigen bzw. die Beratung mit ihnen abzustimmen.
- *Aus- und Weiterbildung* für die mit Compliance-Funktionen betrauten oder dort zuarbeitenden Mitarbeitenden, z.B. zur Compliance-Risikoanalyse, zu konkreten Maßnahmen des Compliance-Programms oder zum Hinweisgebersystem.

(124) 2.) *Information von (potenziellen) hinweisgebenden Personen* nach der EU-Whistleblower-Richtlinie bzw. dem Hinweisgeberschutzgesetz zum Verfahren der eingerichteten Meldestellen sowie Kommunikation mit hinweisgebenden Personen unter Wahrung der Vertraulichkeit (☞ Abschnitt 6).

(125) 3.) *Information der Bürger und der Presse* (öffentliche Kommunikation) zum eingerichteten CMS und ggf. zu Regelverstößen. Ziel dieser Öffentlichkeitsarbeit ist zum einen die Information der Bürger und Unternehmen zu für sie relevanten Compliance-Regelungen der Kommune (insbesondere zu den Regelungen zum Verbot der Annahme von Vorteilen für Mitarbeitende der Kommune sowie zu den Regelungen zum Sponsoring und zu Spenden zugunsten der Kommune). Zum anderen ist seitens der

Kommune dem Presseauskunftsrecht und eventuellen Transparenzpflichten (z.B. durch Veröffentlichung im Internet) nachzukommen.

(126) 4.) *Compliance-Berichterstattung* an die Leitung und die verantwortlichen Führungsebenen der Kommune sowie – wenn geeignet – in aufbereiteter, komprimierter Form an die Mitarbeitenden. Zu berichten sind (Berichtspflichten):

- die identifizierten Compliance-Risiken und ergriffenen Maßnahmen,
- eingegangene und überprüfte Verdachtshinweise (Aufdeckung),
- Reaktion auf festgestellte Regelverstöße und
- die Ergebnisse der Überwachung und Verbesserung des CMS.

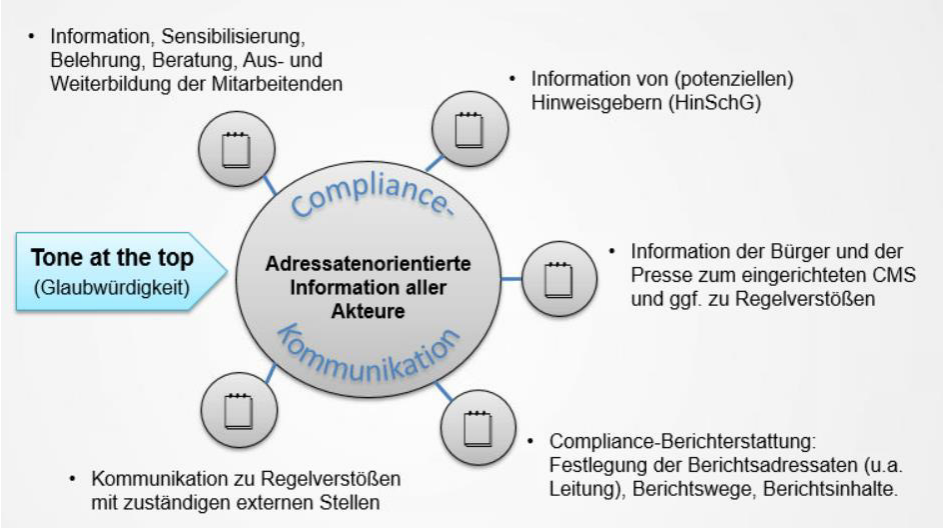
Zu den Berichtspflichten sind die jeweils verantwortlichen Ersteller und Adressaten und deren Pflichten (u.a. Fristen, Reaktionen) sowie die Berichtswege und ggf. die Aufbereitung bzw. der Detailgrad der Berichtsinhalte festzulegen (Systematik). Bei Berichten zu Verdachtshinweisen bzw. Regelverstößen ist besonders auf die Vertraulichkeit zu achten.

(127) 5.) *Kommunikation zu Regelverstößen bzw. entsprechenden Hinweisen mit zuständigen externen Stellen* (Kommunikation mit externen Stellen), wie Strafverfolgungsbehörden, externe Meldestellen nach dem Hinweisgeberschutzgesetz (u.a. Bundesamt für Justiz[87]), Landesdatenschutzbeauftragte, beauftragte Rechtsanwälte etc. Hier sind insbesondere die Zuständigkeiten festzulegen.

(128) Der Erfolg bzw. die Wirksamkeit der Compliance-Kommunikation ist maßgeblich abhängig vom „tone at the top", dem Verhalten der Leitung und Führungskräfte, sowie der Führungs- und Behördenkultur (☞ Tz. 58). Glaubwürdigkeit ist eine notwendige Bedingung guter Compliance-Kommunikation. Die Compliance-Kommunikation sollte auch die Möglichkeiten der aktuellen Technik (u.a. Internet, E-Learning bzw. webbasierte Trainings) nutzen. Je nach Adressatenkreis ist ggf. auch Mehrsprachigkeit verwendeter Medien von Nöten.

[87] Verordnung über die Organisation der nach dem Hinweisgeberschutzgesetz einzurichtenden externen Meldestelle des Bundes (Hinweisgeberschutzgesetz-Externe-Meldestelle-des-Bundes-Verordnung – HEMBV) vom 7. August 2023

Abbildung 9: Compliance-Kommunikation



4.8 Compliance-Überwachung und -Verbesserung

(129) Es sind Verfahren bzw. Maßnahmen einzuführen, die Angemessenheit und Wirksamkeit des CMS systematisch überwachen und verbessern. Den entsprechenden Rollen für die Überwachung und Verbesserung liegt das *Drei-Linien-Modell* des Institute of Internal Auditors (IIA) zugrunde.[88] Danach obliegt:

- der ersten Linie (v.a. Fach- und Querschnittsämter), Compliance-Maßnahmen (einschließlich prozessintegrierter Kontrollen) umzusetzen;
- der zweiten Linie (Beauftragte für bestimmte Bereiche), wozu auch der *Compliance-Beauftragte* gehört, die erste Linie durch Festlegung von Anforderungen, Beratung und Überwachung der Funktionsfähigkeit der Compliance-Maßnahmen zu unterstützen;
- der dritten Linie (u.a. die *Interne Revision*) die prozessunabhängige Überwachung.

(130) Die Compliance-Überwachung und -Verbesserung dient den CMS-Funktionen Aufdeckung und Reaktion. Eine wirksame Compliance-Überwachung und -Verbesserung wirkt auch präventiv.

4.8.1 Überwachung

(131) Überwachungsmaßnahmen bestehen aus

- einer durch die zweite Linie durchzuführenden *compliance-prozessintegrierten* Überwachung der Angemessenheit und Wirksamkeit

[88] Vgl. Institute of Internal Auditors (IIA), Das Drei Linien Modell des IIA, Juli 2020 (Deutsche Übersetzung durch den DIIR).

a. der Maßnahmen zur Umsetzung der institutionellen Compliance-Anforderungen und
b. des von der ersten Linie eingerichteten Internen Kontrollsystems (IKS) (☞ Tz. 102), das als solches Teil des Compliance-Programms für die prozessbezogenen Risiken ist, sowie

- der Überwachung durch *compliance-prozessunabhängige* Stellen der dritten Linie, wie z. B. Rechnungsprüfung, Interne Revision, beauftragte externe Auditoren. Vgl. zu Begriff, Funktion und Aufbau eines Internen Kontrollsystems die IDR-Prüfungsleitlinie L111 – „Die IKS-Prüfung in der Rechnungsprüfung".

Die getroffenen Überwachungsmaßnahmen sind mit den Zuständigkeiten zu dokumentieren, z.B. in Ergänzung der Anforderungs-Maßnahmen-Matrix bzw. der Risiko-Kontroll-Matrix (☞ Anlagen 3 und 5, Abschnitte 8.3 und 8.5).

(132) Durch die Überwachungsmaßnahmen festgestellte Schwachstellen im CMS und festgestellte Regelverstöße sind – als Teil der Compliance-Kommunikation – an die Leitung bzw. die für Ursachenanalyse und Konsequenzen-Management zuständige Stelle (Compliance-Beauftragter) in der Kommune zu berichten.[89]

(133) Voraussetzung für die Überwachung ist eine ausreichende Dokumentation des CMS[90] (Tz.26).

(134) Wesentliche Voraussetzungen für die Wirksamkeit der Überwachung sind u.a.:[91]

- Bereitstellung *ausreichender Ressourcen* für die Überwachung (Teil der Compliance-Organisation).
- Festlegung der *Zuständigkeiten* für die Überwachung (Teil der Compliance-Organisation).
- Aufstellung eines (mehrjährigen) allgemeinen *Überwachungsplans* (Prüfungsmaßnahmen, Verantwortliche, Termine) für die prozessintegrierte Überwachung (organisatorische, technische und manuelle Kontrollen, regelmäßige Überprüfung der eingesetzten IT, Untersuchungen zur Compliance-Kultur und zum Bekanntheitsgrad des Compliance-Programms u. s. w.) und prozessunabhängige Überwachung (Prüfungsplanung). *Hinweis:* In Abgrenzung zu den einzelnen prozessbezogenen Überwachungsmaßnahmen in der Risiko-Kontroll-Matrix geht es beim hiesigen Überwachungsplan hingegen

[89] Vgl. Eibelshäuser, Beate / Schmidt, Stefan: IDW PS 980: Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen (CMS), in: IDW (Hrsg.), Praxisleitfaden Governance, Risk und Compliance; Düsseldorf 2017, S. 104.
[90] IDW PS 980, Tz. 23.
[91] Vgl. IDW PS 980, Tz. A 20.

um Prüfungsaktivitäten, die sicherstellen sollen, dass das eingerichtete CMS hinsichtlich der Grundelemente und der institutionellen und prozessbezogenen Maßnahmen angemessen und wirksam ist.

- *Dokumentation* aller prozessintegrierten und prozessunabhängigen Überwachungsmaßnahmen, Erstellung von Berichten und Auswertungen zu den Feststellungen der Überwachungsmaßnahmen (Risiko-Kontroll-Matrix, Berichte, Besprechungsprotokolle u. s. w.).
- Festlegung der *Berichtswege* für die Ergebnisse der Überwachungsmaßnahmen (Teil der Compliance-Kommunikation).
- *Maßnahmen zur Aufdeckung* von Compliance-Verstößen, insbesondere ein wirksames Internes Kontrollsystem sowie die Einrichtung eines Hinweisgebersystems (☞ Abschnitt 6).

(135) *Maßnahmen zur Reaktion auf gravierende Regelverstöße, die bei der Überwachung festgestellt wurden:* Ausgangspunkt von Maßnahmen zur Reaktion auf festgestellte Regelverstöße sind die Ergebnisse der Überwachung bzw. Prüfung entsprechender Hinweise bzw. Verdachtsfälle. Bei gravierenden Regelverstöße bzw. gravierender Missachtung wesentlicher Regelungen sind von den dafür zuständigen Stellen insbesondere folgende Maßnahmen zu prüfen:

- Maßnahmen zur Verhinderung weiterer Regelverstöße, z. B. Entzug von Berechtigungen, Zugriffen, Befugnissen u. s. w.;
- konkrete arbeits- und dienstrechtliche Maßnahmen (Sanktion);
- die Geltendmachung von Rückforderungen, Herausgabe- und Schadensersatzansprüchen, Regress (Sanktion);
- die Einschaltung von Strafverfolgungsbehörden (Sanktion);
- gesetzlich erforderliche Meldungen an Behörden vornehmen;
- die Überprüfung der durch die festgestellten Regelverstöße zustande gekommenen Rechtsakte bzw. -geschäfte einschließlich ihrer steuerlichen Auswirkungen.

Das Sanktionieren von aufgedeckten gravierenden Regelverstößen ist Ausdruck einer guten Compliance-Kultur. Die Verwaltungsspitze bzw. die vorgesetzte Stelle müssen einschreiten, wenn Regelverstöße entdeckt werden. In den Regelwerken vorgesehene Sanktionen müssen bei nachweislichen Verstößen auch vollzogen werden. Angemessene Maßnahmen der Reaktion entfalten zugleich präventive Wirkung, wenn sie in geeigneter Weise kommuniziert werden (*Hinweis*: arbeits-, dienst-, strafrechtliche Maßnahmen können, wenn überhaupt, jedoch nur begrenzt kommuniziert werden). Inkonsequentes Verhalten beim Umgang mit erfolgten Verstößen wirken sich

negativ auf die Compliance-Kultur aus. Wesentlich ist die Kommunikation einer Nulltoleranz.

4.8.2 Verbesserung

(136) Gibt es als Ergebnis der Überwachungsmaßnahmen oder sonstiger Maßnahmen Hinweise auf Schwachstellen des CMS bzw. Regelverstöße, sind Maßnahmen zu ergreifen, die die Angemessenheit und Wirksamkeit des CMS verbessern bzw. die solche Vorfälle in der Zukunft vermeiden.[92]

(137) Für die Umsetzung der Verbesserungsmaßnahmen ist die Leitung bzw. die jeweils fachlich zuständige Stelle in der Kommune verantwortlich. Der Compliance-Beauftragte ist als die für Ursachenanalyse und Konsequenzen-Management zuständige Stelle an der Ausarbeitung der Verbesserungsmaßnahmen zu beteiligen.

(138) Soweit ein Aufsichtsorgan eine Überwachungsfunktion hinsichtlich Angemessenheit und Wirksamkeit des CMS wahrnimmt, sollte es über die Überwachungs- und Verbesserungsmaßnahmen informiert werden.[93]

5. Kommunales Tax-Compliance-Management-System (TCMS)

(139) Die verspätete, fehlerhafte oder unvollständige Einreichung einer Steuererklärung birgt für die steuerpflichtige Kommune erhebliche finanzielle und politische Risiken und kann darüber hinaus strafrechtliche Konsequenzen für die Verwaltungsleitung und die Mitarbeiter nach sich ziehen. Der Aufbau eines umfangreichen Management Systems (TCMS) ist daher zur Risikoreduzierung unabdingbar. Dies unterstreicht der Anwendungserlass zu § 153 AO. Die Finanzverwaltung stellt hier klar, dass ein konzeptionell überzeugendes TCMS bzw. IKS ein Indiz dafür ist, dass der Steuerpflichtige ohne Vorsatz und Leichtfertigkeit gehandelt hat. Dies kann sich im Falle steuerlicher Rechtsverstöße strafmindernd auswirken[94] (☞ Abschnitt 4.3, Tz. 36).

(140) Unter einem TCMS ist ein klar abgegrenzter Teilbereich eines CMS zu verstehen, dessen Zweck die vollständige und zeitgerechte Erfüllung steuerlicher Pflichten ist.[95]

(141) Im Allgemeinen sind zum Aufbau eines TCMS folgende Arbeitsschritte erforderlich:

- Grundlagen beschreiben
- Risiken analysieren
- Handlungsbedarf ermitteln
- Ausarbeitung eines Tax Compliance Management Systems

[92] Vgl. IDW PS 980, Tz. A 20.
[93] Vgl. IDW PS 980, Tz. A 20.
[94] Vgl. Deutscher Städtetag, S. 1 ff.
[95] Vgl. IDW Praxishinweis 1/2016, Tz. 8.

- Laufende Überwachung und Verbesserung

(142) Von wesentlicher Bedeutung ist hierbei die Sammlung und Sichtung bereits bestehender Dokumente. Soweit bereits vorhanden, sollten Organisationshandbücher, Richtlinien und weitere relevante Unterlagen auf Aktualität und Vollständigkeit überprüft werden. Handlungsbedarf besteht häufig nur in der Aktualisierung, teilweisen Ergänzung und Überführung in ein zusammenhängendes System.

(143) Ein angemessenes CMS i. S. d. IDW PS 980/IDW EPS 980 sollte grundsätzlich die dort genannten sieben Grundelemente aufweisen. Diese bilden auch die Grundlage eines TCMS als abgegrenzter Teilbereich eines CMS.[96] *Dieser Leitfaden ist daher auch auf die Einführung und Prüfung eines TCMS anwendbar; es gelten die Ausführungen in Abschnitten 4, 6 und 7*.

(144) Die geforderte **Tax Compliance-Kultur** einer Kommune lässt sich u.a. an einer regelmäßigen Kommunikation von Tax Compliance-Themen auf Ebene der Verwaltungsspitze (tone at the top) und durch die Verwaltungsleitung in die einzelnen Fachbereiche hinein (tone from the top) erkennen (☞ Tz. 58). Auch kommt die Tax Compliance-Kultur darin zum Ausdruck, dass die zuständigen Mitarbeitenden frühzeitig und umfassend in steuerrelevante Fragen eingebunden werden. Grundeinstellungen und erwartete Verhaltensweisen sollten offen kommuniziert und auch dokumentiert werden. So etwa in Form einer Steuerrichtlinie, einer Steuerstrategie, eines Leitbilds oder Verhaltenskodexes.

(145) Die **Tax Compliance-Ziele** bilden den Rahmen für die Aufgaben der zuständigen Mitarbeitenden und liegen in der Verantwortung der gesetzlichen Vertreter der Kommune. Übergeordnete Tax Compliance-Ziele können u.a. die Vermeidung von außerplanmäßigen Haushaltsbelastungen oder die Vermeidung von Reputations- und Imageschäden sein, welche z. B. in der o. g. Steuerrichtlinie, einem Leitbild oder in gesonderten Dokumenten hinreichend konkretisiert, kommuniziert und dokumentiert werden sollten.

(146) Unter Berücksichtigung der Tax Compliance-Ziele sind die **Tax Compliance-Risiken**, d.h. die Risiken für Verstöße gegen einzuhaltende Regeln, bspw. bezogen auf die jeweilige Steuerart und die damit verbundenen Prozesse festzustellen und schriftlich festzuhalten. Folgen von Regelverstößen können u.a. finanzieller und bilanzieller Art sein. Darüber hinaus können aus steuerlichen Pflichtverstößen Reputations- und

[96] Vgl. IDW Praxishinweis 1/2016. Tz. 22 ff.

Imageschäden sowie nicht zuletzt persönliche Haftungsrisiken für die verantwortlichen Führungskräfte und Mitarbeitenden in der Kommune resultieren. Diese Risiken gilt es zu minimieren.[97]

(147) Auf der Grundlage der Beurteilung der Tax Compliance-Risiken sollten Grundsätze und Maßnahmen eingeführt werden, die den Risiken entgegenwirken und damit auf die Vermeidung von Verstößen ausgerichtet sind, das sog. **Tax Compliance-Programm**. Dieses sollte auch die bei festgestellten Compliance-Verstößen zu ergreifenden Maßnahmen umfassen. Maßnahmen des Tax Compliance-Programms können grundsätzlich präventiven und detektiven Charakter haben. Präventive Maßnahmen eines solchen Programms können z. B. die Erstellung von Richtlinien und fachlichen Anweisungen, die Bereitstellung von Checklisten oder auch Zuständigkeitsregelungen und Berechtigungskonzepte sein. Prozessintegrierte Kontrollen wie das 4-Augen-Prinzip und systematische Auswertung von Daten in Bezug auf Besonderheiten stellen demgegenüber Beispiele für detektive Maßnahmen dar.

(148) Im Rahmen der **Tax Compliance-Organisation** sollten steuerliche Schnittstellen der Kommune, die in die Erfüllung ihrer steuerlichen Pflichten einbezogen und/oder Teil der steuerrelevanten Informationskette sind, klar und eindeutig definiert und Verantwortlichkeiten hierfür konkret zugewiesen werden. Die Tax Compliance-Organisation kann in der *Steuerrichtlinie* oder einem Organisationshandbuch dargestellt werden.

(149) Mit Hilfe einer angemessenen **Tax Compliance-Kommunikation** können die betroffenen Mitarbeiter und ggfs. Dritte über das Tax Compliance-Programm sowie die festgelegten Rollen und Verantwortlichkeiten informiert werden. Auch kann an dieser Stelle festgelegt werden, wie Tax Compliance-Risiken sowie (mögliche) Regelverstöße an die zuständigen Stellen in der Kommune berichtet werden.

(150) Das TCMS sollte letztlich in geeigneter Weise überwacht werden. Voraussetzung für die **Tax Compliance-Überwachung** ist eine geeignete Dokumentation des TCMS. Werden im Rahmen der Überwachung Mängel im TCMS bzw. Regelverstöße festgestellt, sollten diese an die zuständigen Stellen berichtet und Zuwiderhandlungen sanktioniert werden. Darüber hinaus sollten erkennbare Maßnahmen getroffen werden, um Mängel zu beseitigen bzw. künftige Regelverstöße möglichst zu vermeiden.

(151) Abschließend kann festgehalten werden, dass die Einrichtung eines TCMS gleichbedeutend mit einer umfassenden Erfassung, Beschreibung, Wirksamkeitsanalyse und Dokumentation der Steuererklärungsprozesse in der Kommune ist (d.h. sämtliche

[97] Vgl. Deutscher Städtetag, S. 13.

Prozesse der Kommune, die zu einer Steuerpflicht führen, sind zu berücksichtigen). Das bietet Chancen, bisherige Organisationsstrukturen und Arbeitsprozesse systematisch zu hinterfragen und gegebenenfalls effektiver zu gestalten.[98]

(152) Hat die Kommune ein TCMS eingerichtet, kann eine nach IDW PS 980/IDW EPS 980 durchgeführte **Prüfung** grundsätzlich als Angemessenheitsprüfung oder Wirksamkeitsprüfung erfolgen (☞ Abschnitt 7). Für Kommunen, die ein TCMS erstmals einrichten oder erweitern, kann es zweckmäßig sein, bereits während der Entwicklung, Einführung, Änderung oder Erweiterung des Systems projektbegleitend eine Angemessenheitsprüfung durchführen zu lassen.[99]

6. Hinweisgebersystem – interne Meldestelle

(153) Zweck eines Hinweisgebersystems ist es, Mitarbeitenden oder anderen potentiellen hinweisgebenden Personen einen vertraulichen Kommunikationskanal (Meldekanal) über Einrichtung von *Meldestellen* zu eröffnen, um Missstände oder Unregelmäßigkeiten melden zu können. Seit dem Erlass der sogenannten *„Whistleblower-Richtlinie*" (im Folgenden „WBRL") durch die Europäische Union[100] gibt es verbindliche Vorgaben für die Einrichtung eines solchen Hinweisgebersystems, welche durch die EU-Mitgliedstaaten umzusetzen sind. Die WBRL dient einem besseren Schutz von hinweisgebenden Personen, die in ihrem beruflichen Kontext Informationen über Verstöße gegen Unionsrecht melden. Eine Umsetzung in nationales Recht erfolgte nach langer Verzögerung am 12. Mai 2023 durch das Gesetz für einen besseren Schutz hinweisgebender Personen (sog. Hinweisgeberschutzgesetz[101]), welches Juli 2023 in Kraft getreten ist. Der Hinweisgeberschutz wird zudem durch Anpassungen gesetzlicher Regelungen[102], insbesondere auch im Bereich des Dienstrechts, sichergestellt.

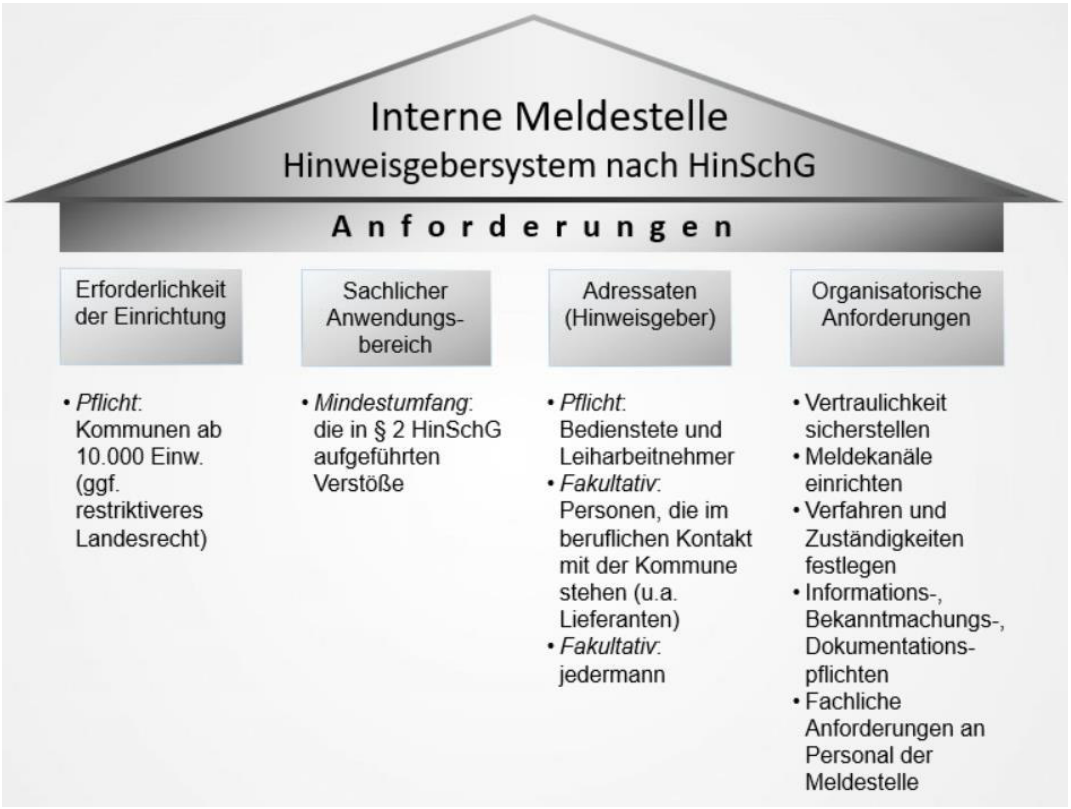
(154) Die WBRL bezieht sich aufgrund der eingeschränkten Kompetenzen der EU nur auf den Schutz von Meldungen bei Verstößen gegen das in der WBRL genannte Unionsrecht (vgl. Art. 2 WBRL). Das Hinweisgeberschutzgesetz erweitert jedoch den *sachlichen Anwendungsbereich* (vgl. § 2 HinSchG) und erfasst u.a. auch alle Meldungen von strafbewehrten Verstößen und Meldungen von bußgeldbewehrten Verstößen,

[98] Vgl. Deutscher Städtetag, S. 4.
[99] Vgl. IDW Praxishinweis 1/2016, Tz. 62 und Tz. 66.
[100] RICHTLINIE (EU) 2019/1937 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.
[101] Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (HinSchG) – BGBL 2023 I Nr. 140 vom 02.06.2023.
[102] Vgl. Art. 2 bis 8 des Hinweisgeberschutzgesetzes.

wenn die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient (vgl. § 2 Abs. 1 Nr. 2 HinSchG).

(155) Für das Hinweisgebersystem kann subsidiär zu den gesetzlichen Vorgaben die ISO 37002[103] herangezogen werden.

Abbildung 10: Anforderungen an interne Meldestellen nach HinSchG



6.1 Pflicht zur Einrichtung einer internen Meldestelle

(156) Nach Art. 8 Abs. 1 i. V. m. Abs. 9 Satz 1 und 2 WBRL sind alle juristischen Personen des öffentlichen Sektors, folglich auch Kommunen, verpflichtet, bei sich interne Meldestellen zur Mitteilung von Informationen über Regelverstöße (Hinweise) und Verfahren für Folgemaßnahmen einzurichten und zu betreiben. Die Mitgliedstaaten können jedoch Gemeinden mit weniger als 10.000 Einwohner oder weniger als 50 Arbeitsnehmer von der Verpflichtung ausnehmen. Nach § 12 Abs. 1 Satz 4 HinSchG gilt für Gemeinden und Gemeindeverbände und solche Beschäftigungsgeber, die im Eigentum oder unter der Kontrolle von Gemeinden und Gemeindeverbänden stehen,

[103] ISO 37002:2021, Whistleblowing Management Systems – Guidelines (First Edition 2021-07-27).

die Pflicht zur Einrichtung und zum Betrieb interner Meldestellen nach Maßgabe des jeweiligen Landesrechts.[104]

(157) Auch bei Kommunen und kommunalen Unternehmen, die nicht zur Einrichtung einer internen Meldestelle nach dem HinSchG verpflichtet sind, empfiehlt es sich, eine solche einzurichten (ggf. durch Outsourcing), um Regelverstöße frühzeitig aufzudecken und ggf. (weiteren) Schaden abwenden zu können.

(158) Ein Hinweisgebersystem sollte Bestandteil eines kommunalen CMS sein (siehe Anlage7)[105]. Es ist daher sicherzustellen, dass die internen Meldestellen Teil der Compliance-Organisation sind. Es bietet sich deshalb an, den Compliance-Beauftragten die Verantwortung bzw. Zuständigkeit für eingerichtete interne Meldestellen zu übertragen. Anderenfalls sind ihm Befugnisse zur Steuerung und Prüfung der Meldestellen sowie Informationsrechte zu übertragen, damit er seine Pflichten erfüllen kann. Nach § 15 Abs. 1 Satz 1 HinSchG ist zu beachten, dass die mit den Aufgaben einer internen Meldestelle beauftragten Personen bei der Ausübung ihrer Tätigkeit unabhängig sind. Die Vermeidung von Interessenskonflikte ist sicherzustellen (Satz 1).

6.2 Anforderungen an interne Meldestellen

(159) Bei der Einrichtung interner Meldestellen sind folgende Anforderungen des HinSchG zu beachten [in eckiger Klammer ist das jeweils zugehörige CMS-Grundelement angegeben]:

a. *Sachlicher Anwendungsbereich [Compliance-Ziele]*: Der gesetzliche Mindestumfang des sachlichen Anwendungsbereichs (☞ Tz 154) ist sicherzustellen. Er gibt gleichzeitig die sachliche Zuständigkeit einer internen Meldestelle wieder. Der Kommune bleibt es unbenommen, den Zuständigkeitsbereich für sich zu erweitern (z.B. auf Verstöße gegen interne Regelungen). Es sollte auch identifiziert werden, welche weiteren Prozesse in der Kommune bestehen (oder bestehen sollten), die mit gemeldeten Regelverstößen umgehen, die (nicht) in den sachlichen Anwendungsbereich des Hinweisgebersystems bzw. die sachliche Zuständigkeit der internen Meldestelle fallen[106].

b. *Adressat der internen Meldestelle [Compliance-Ziele]*: Das Hinweisgeberschutzgesetz gibt vor, dass für die Beschäftigten sowie überlassenen Leiharbeitnehmer interne Meldekanäle einzurichten sind, damit diese Informationen

[104] Dem Bund ist aufgrund des „Durchgriffsverbots“ nach Art. 84 Abs. 1 Satz 7 eine unmittelbare Aufgabenübertragung verwehrt.
[105] Vgl. IDW EPS 980 (2021), A23 – 17. Aufzählungspunkt. Vgl. auch ISO 37301, Nr. 5.3.2 und A.8.3.
[106] Vgl. ISO 37002, Nr. 4.3.

über Verstöße melden können (§ 16 Abs. 1 Satz 1 HinSchG). Neben den eigenen Beschäftigten können die Meldekanäle auch weiteren Personengruppen zugänglich gemacht werden. Nach § 16 Abs. 1 Satz 3 HinSchG kann der interne Meldekanal auch so gestaltet werden, dass er auch natürlichen Personen offensteht, die im Rahmen ihrer beruflichen Tätigkeit mit dem jeweiligen Beschäftigungsgeber oder der jeweiligen Organisationseinheit in Kontakt stehen. Überdies sollte nach hier vertretener Auffassung im kommunalen Bereich eine noch darüberhinausgehende Ausweitung in Betracht gezogen werden (z.B. auf Bürger*innen).[107]

c. *Wahrung der Vertraulichkeit [Compliance-Kommunikation]*: Die internen Meldestellen haben sicherzustellen, dass die Vertraulichkeit der Identität der hinweisgebenden Person, der Personen, die Gegenstand einer Meldung sind, und der sonstigen in der Meldung genannten Personen gewahrt wird (§ 8 Abs. 1 HinSchG). Dies gilt unabhängig davon, ob die Meldestelle für die eingehende Meldung zuständig ist (Abs. 1). Das Hinweisgeberschutzgesetz sieht keine Verpflichtung vor, dass der Meldekanal so ausgestaltet wird, dass die Abgabe anonymer Meldungen möglich ist. Die Bearbeitung entsprechender Meldungen wird aber empfohlen (§ 16 Abs. 1 HinSchG).

d. *Meldekanäle [Compliance-Organisation]*: Interne Meldungen müssen schriftlich (z.B. Brief, E-Mail, webbasierte Plattform) oder mündlich (telefonisch oder andere Art der Sprachübermittlung) möglich sein (§ 16 Abs. 3 Satz 1 HinSchG). Auf Ersuchen des Hinweisgebenden ist eine persönliche Zusammenkunft zu ermöglichen (Satz 2). Eine Übersicht von Kriterien für die Auswahl von Meldekanälen findet sich in Anlage 6.

e. *Festlegung des Verfahrens zur wirksamen Prüfung von Hinweisen und zum Ergreifen weiterer Folgemaßnahmen (§ 12 Abs. 4, §§ 13 ff. HinSchG) [Compliance-Organisation]*: Nach Eingang einer Meldung (eines Hinweises) hat die interne Meldestelle zu prüfen, ob der gemeldete Regelverstoß in den sachlichen Anwendungsbereich (siehe Tz 113) fällt und stichhaltig (plausibel) ist. Ist dies der Fall, sind angemessene *Folgemaßnahmen* zu ergreifen, wozu auch

[107] Unabhängig von den Meldekanälen zielt die WBRL „*nicht ausschließlich auf den Schutz von Mitarbeitern (Arbeitnehmer und Beamte) ab. Unter den Schutz der EU-Richtlinie fallen nach Art. 4 der Richtlinie auch Bewerber, bezahlte und unbezahlte Praktikanten, ehemalige Mitarbeiter, Unterstützer des Hinweisgebers sowie Journalisten, Anteilseigner und Personen, die dem Verwaltungs-, Leitungs- oder Aufsichtsorgan eines Unternehmens angehören. (…*des Weiteren*) Personen, die unter der Aufsicht und Leitung von Auftragnehmern, Unterauftragnehmern und Lieferanten arbeiten (…).“* (Ruhmannseder/Behr/Krakow: Hinweisgebersysteme, 2. Auflage, Heidelberg 2021, S.39f.).

interne Ermittlungen gehören (§ 17 Abs. 1, § 18 HinSchG).[108] Für interne Ermittlungen sollte ein Verfahren eingerichtet werden, dass Unparteilichkeit sicherstellt, von qualifiziertem Personal durchgeführt wird und weitere Standards eines fairen Verfahrens berücksichtigt[109] sowie weitere gesetzliche Regelungen und Standards einhält. Für das gesamte Verfahren vom Eingang eines Hinweises bis zum Abschluss der Folgemaßnahmen ist sicherzustellen, dass es ohne unangemessene zeitliche Verzögerungen abläuft[110], auch um den Erfolg von Folgemaßnahmen nicht zu gefährden, und die Informationspflichten gegenüber den hinweisgebenden Personen (siehe unten Buchstabe g.) eingehalten werden können.

f. *Anforderungen an die Befugnisse der internen Meldestelle [Compliance-Organisation]*: Die interne Meldestelle muss mit den notwendigen Befugnissen ausgestattet sein, um ihren Aufgaben (Entgegennahme von Meldungen/Hinweisen, Kommunikation mit der hinweisgebenden Person, Prüfung der Meldungen, Ergreifen von Folgemaßnahmen im Sinne der Richtlinie) nachkommen zu können § 12 Abs. 4 HinSchG).

g. *Informationspflichten* gegenüber hinweisgebenden Personen *[Compliance-Kommunikation]*: Die interne Meldestelle muss der hinweisgebenden Person innerhalb von sieben Tagen den Eingang der Meldung bestätigen. Des Weiteren muss die interne Meldestelle drei Monate nach Bestätigung des Eingangs oder, wenn der Eingang nicht bestätigt wurde, spätestens drei Monate und sieben Tage nach Eingang der Meldung den hinweisgebenden Personen eine Rückmeldung zu geplanten sowie bereits ergriffenen Folgemaßnahmen sowie die Gründe für diese geben (§ 17 Abs. 2 Satz 1 und Satz 2 HinSchG).

h. *Dokumentationspflicht zu eingegangenen Hinweisen [gilt für das gesamte CMS]:* Die interne Meldestelle bzw. das dafür zuständige Personal hat alle eingehenden Meldungen zu dokumentieren. Dabei sind die detaillierten Vorgaben in § 11 HinSchG zu beachten. Zum Nachweis der Einhaltung eines ordnungsmäßigen Verfahrens ist darüber hinaus auch der weitere Umgang mit

[108] Bei der Frage, ob interne Untersuchungen eingeleitet werden, hat die Leitung grundsätzlich kein Ermessen, „*sondern lediglich einen Beurteilungsspielraum, ob die Voraussetzungen vorliegen, vor allem dahingehend, ob ein hinreichender Verdacht auf Compliance-Verstöße besteht.*“ (Hülsberg/Fassbach: Die Versicherbarkeit von Compliance-Risiken im Lichte der strengen Organhaftung. Überlegungen aus Sicht der Beratungspraxis, in: Wirtschaftsprüfung (WPg) 08.2023, S.484).

[109] Vgl. ISO 37002, Nr. 8.4.1. vgl. § 17 RegE Gesetz zur Stärkung der Integrität in der Wirtschaft – Verbandssanktionengesetz.

[110] Vgl. ISO 37002, Nr. 8.1.

eingegangenen Hinweisen (v.a. Prüfung, Folgemaßnahmen) vollständig zu dokumentieren. Die Dokumentation der Meldung ist drei Jahre nach Abschluss des Verfahrens zu löschen (§ 11 Abs. 5 Satz 1). Die Dokumentation der Meldung kann länger aufbewahrt werden, um die Anforderungen nach diesem Gesetz oder nach anderen Rechtsvorschriften zu erfüllen, solange dies erforderlich und verhältnismäßig ist (Satz 2).

i. *Anforderungen an das Personal der Meldestelle [Compliance-Organisation]*: Die interne Meldestelle kann durch ausdrücklich bestimmtes eigenes Personal oder durch beauftragte Dritte (z. B. Vertrauensanwalt) betrieben werden (§ 14 Abs. 1 HinschG). Jedoch entlässt die Beauftragung eines Dritten den jeweiligen Beschäftigungsgeber nicht aus der Pflicht, geeignete Maßnahmen zu ergreifen, um einen etwaigen Verstoß abzustellen. In keinem Fall kann der Dritte völlig losgelöst von der betroffenen Kommune agieren (vgl. Gesetzesbegründung zu § 14 Abs. 1 HinSchG). Damit die Meldungen zügig bearbeitet und die Informationspflichten eingehalten werden können, sollte die Meldestelle mit ausreichend kompetenten Personal ausgestattet sein.[111] Wieviel Personal benötigt wird, hängt von der Anzahl eingehender Meldungen ab, was wiederum durch die Größe der Kommune, die ausgewählten Teilbereiche sowie der Zahl der zur Meldung berechtigten Personen bestimmt wird. An die Eigenschaften des Personals der internen Meldestelle werden folgende Anforderungen gestellt:

   - Das in der Meldestelle eingesetzte Personal muss unabhängig sein. Bei der Aufgabenwahrnehmung dürfen keine Interessenskonflikte entstehen (§ 15 Abs. 1 HinSchG))[112]. Sinnvoll ist es, die Meldestelle direkt beim Compliance-Beauftragen anzusiedeln.
   - An die Kompetenzen des in der Meldestelle eingesetzten Personals sollten zudem besondere Anforderungen gestellt werden (§ 15 Abs. 2 HinSchG). Sie entsprechen grundsätzlich den fachlichen und sozialen Kompetenzen des Compliance-Beauftragten[113] (vgl. Rn 84 ff.). Auch dies spricht für eine direkte Ansiedelung der Meldestelle beim Compliance-Beauftragten. Ebenso besteht entsprechender Schulungs- und Fortbildungsbedarf.

[111] Vgl. ISO 37002, Nr. 5.3.2.
[112] Hinweisgebersystem sollte die Einhaltung der Grundsätze Vertrauen, Unparteilichkeit und Schutz sicherstellen (vgl. ISO 37002, Nr. 4.4).
[113] Vgl. auch ISO 37002, Nr. 7.2.

j. *Bekanntmachung / Kommunikation des Melde- bzw. Hinweisgebersystems [Compliance-Kommunikation]*: Nach § 13 Abs. 2 HinSchG ist es von wesentlicher Bedeutung, dass Informationen über externe Meldestellen (u.a. Bundesamt für Justiz[114]) klar und leicht zugänglich gemacht werden. Gleichzeitig dürfte es unbestritten sein, dass auch Informationen über die interne Meldestelle den Beschäftigten gegenüber kommuniziert werden, um eine Bevorzugung der internen Meldekanäle zu erreichen. Die Ausweitung der Kommunikation auch auf Personen, die nicht Beschäftigte der Kommune sind, die aber aufgrund ihrer beruflichen Tätigkeit mit der Kommune in Kontakt treten, beispielsweise Dienstleistungsunternehmen, Vertriebsunternehmen, Lieferanten und andere Geschäftspartner, wird empfohlen. Darüber hinaus sollte auch eine Bekanntmachung gegenüber Bürgern in Betracht gezogen werden. Hierbei ist die Wichtigkeit der internen Meldekanäle und der Tätigkeit der internen Meldestelle durch die Leitung der Kommune hervorzuheben (v.a. „tone at the top" und „zero tolerance" als Teil der Compliance-Kultur[115]). Wichtige und notwendige Informationen zur internen Abgabe von Meldungen sollten zudem in einfach verständlicher Weise an barrierefrei zugänglichen Stellen regelmäßig kommuniziert werden (siehe Checkliste zur Bekanntmachung/Kommunikation des Melde- bzw. Hinweisgebersystems in Anlage 8).[116]

k. *Evaluation und Verbesserung [CMS-Überwachung und -Verbesserung]*: Auch das Hinweisgebersystem sollte hinsichtlich Verfahren, Befugnissen, Ressourcen und Einhaltung gesetzlicher Vorgaben regelmäßig prozessintern evaluiert werden. Änderungen in der Organisation der Kommune, Rechtsänderungen und Hinweise auf Fehlfunktionen des eingerichteten Hinweisgebersystems (z.B. aus CMS-Prüfungen) sollten unverzüglich auf Anpassungsbedarf des Hinweisgebersystems hin evaluiert werden.[117]

(160) Das eingerichtete Hinweisgebersystem ist zu dokumentieren (☞ Tz. 53). Es empfiehlt sich, die Zuständigkeiten und das Verfahren (einschließlich der Berichtswege) der

[114] Verordnung über die Organisation der nach dem Hinweisgeberschutzgesetz einzurichtenden externen Meldestelle des Bundes (Hinweisgeberschutzgesetz-Externe-Meldestelle-des-Bundes-Verordnung – HEMBV) vom 7. August 2023

[115] Die Leitung der Kommune sollte zum Ausdruck bringen, dass sie das bei ihr eingerichtete Hinweisgebersystem mit seinen Zielen und Grundsätzen als eigene Angelegenheit ansieht, indem sie die Existenz, die Wichtigkeit und das Verfahren des Hinweisgebersystems eindeutig kommuniziert (vgl. ISO 37002, Nr. 5.1.1).

[116] Die ISO 37002 sieht es als Teil einer guten „Whistleblower Policy" an, dass zusätzlich zum internen Meldekanal auch auf externe Meldekanäle hingewiesen wird (vgl. ISO 37002, Nr. 5.2 m).

[117] Vgl. ISO 37002, Nrn. 10.1 und 10.2.

internen Meldestelle sowie für die Folgemaßnahmen in einer verbindlichen Regelung bzw. Dienstanweisung festzulegen.

7. Prüfung des CMS auf Angemessenheit und Wirksamkeit

7.1 Gegenstand, Arten und Ziele der Prüfung

(161) Die Prüfung eines CMS ist eine Systemprüfung. Sie ist nicht darauf ausgerichtet, einzelne Regelverstöße zu erkennen und kann daher auch keine Prüfungssicherheit über die tatsächliche Einhaltung von Regeln geben.[118]

(162) Gegenstand bzw. Ausgangspunkt der Prüfung sind die Aussagen zum eingerichteten CMS in der CMS-Beschreibung (☞ Tz.53 Nr.1).[119] Ein eingerichtetes Hinweisgebersystem wird dabei als Teil des CMS angesehen.

(163) Es wird hinsichtlich der Prüfungsarten zwischen Angemessenheitsprüfung und Wirksamkeitsprüfung unterschieden. Eine Angemessenheitsprüfung kann bereits begleitend zur Einrichtung eines CMS durchgeführt werden[120]; eine Wirksamkeitsprüfung setzt hingegen voraus, dass das eingerichtete CMS bereits für einen bestimmten Zeitraum, der für ein sicheres Prüfungsurteil erforderlich ist, in der Kommune umgesetzt worden ist. Ziel der Prüfung ist es, die Angemessenheit bzw. Wirksamkeit mit hinreichender Sicherheit beurteilen bzw. eine Aussage dazu treffen zu können.

(164) Die *Angemessenheitsprüfung* erfolgt in folgenden drei Schritten:[121]

1. Beurteilung, ob die Aussagen der CMS-Beschreibung (☞ Tz.53 Nr.1) zu den Regelungen des CMS der Kommune in allen wesentlichen Belangen in Übereinstimmung mit den CMS-Grundsätzen (das sind die konkreten inhaltlichen Anforderungen an ein CMS, wie sie im Abschnitt 3 ausgeführt werden) angemessen dargestellt sind. Dies ist dann der Fall, wenn die Aussagen auf sämtliche sieben Grundelemente eines CMS (☞ Tz. 50) im Sinne der CMS-Grundsätze eingehen und keine wesentlich falschen (unvollständige, falsche oder irreführende) Darstellungen enthalten.[122]

---

[118] Vgl. IDW-EPS 980 (10.2021), Tz. 21. Ergänzend zum IDW PS 980 kann für die Prüfung des CMS zusätzlich der prinzipienbasierte, allgemein gehaltene ISAE 3000 (International Standard on Assurance Engagements other than Audits or Reviews of Historical or Financial Information) herangezogen werden.

[119] Vgl. IDW-EPS 980 (10.2021), Tz. 15.

[120] Vgl. IDW-EPS 980 (10.2021), Tz. 20.

[121] Vgl. IDW-EPS 980 (10/2021), Tz. 19; vgl. IDW (Hrsg.): Praxisleitfaden Governance, Risk und Compliance - Ausgewählte Fachbeiträge zur Einrichtung und Prüfung von Corporate-Governance-Systemen; Düsseldorf 2017, S.13.

[122] Vgl. IDW-EPS 980 (10/2021), Tz. 22, 13i.

2. Beurteilung, ob die Regelungen des CMS der Kommune in Übereinstimmung mit den CMS-Grundsätzen in allen wesentlichen Belangen geeignet sind, mit hinreichender Sicherheit
    - Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen (Aufdeckung),
    - solche Regelverstöße zu verhindern (Prävention),
    - eingetretene Regelverstöße unverzüglich an die zuständige Stelle in der Kommune zu berichten,
    - solche von der zuständigen Stelle zu sanktionieren und
    - erforderliche Verbesserungen des CMS vorzunehmen.[123]

   Hinreichende Sicherheit bedeutet nicht absolute Sicherheit, dass das CMS alle wesentlichen Regelverstöße verhindert bzw. aufdeckt. Auch geeignete Regelungen können durch bewusste oder ungewollte menschliche Fehlleistungen ein System an seine Grenzen führen.[124]
3. Beurteilung, ob die Regelungen des CMS der Kommune zu einem bestimmten Zeitpunkt in allen wesentlichen Belangen implementiert, d.h. in die Verwaltungs- bzw. Geschäftsprozesse der Kommune eingeführt waren (u.a. durch erlassene Aufbau-, Verfahrensregelungen, Musterformulare, Anweisungen, IT-Anwendungen für das CMS).

(165) Die *Wirksamkeitsprüfung* umfasst die drei Schritte der Angemessenheitsprüfung und wird durch einen weiteren Schritt ergänzt:[125]

4. Beurteilung, ob die Regelungen des CMS der Kommune in allen wesentlichen Belangen während des geprüften Zeitraums wirksam waren, d.h. ob die als angemessen beurteilten Regelungen in den laufenden Verwaltungs- bzw. Geschäftsprozessen von den hiervon betroffenen Personen nach Maßgabe ihrer Verantwortung in einem bestimmten Zeitraum wie vorgesehen kontinuierlich eingehalten und beachtet werden.[126]

(166) Eine CMS-Prüfung umfasst aufgrund ihres Charakters als Systemprüfung stets alle Grundelemente eines CMS (☞ Tz. 50). Eine isolierte Prüfung einzelner CMS-Grundelemente liegt nicht im Anwendungsbereich dieses Leitfadens.[127] Hingegen ist

[123] Vgl. IDW-EPS 980 (10.2021), Tz. 23.
[124] Vgl. IDW-EPS 980 (10.2021), Tz. A20.
[125] Vgl. IDW-EPS 980 (10/2021), Tz. 17; vgl. IDW (Hrsg.): Praxisleitfaden Governance, Risk und Compliance - Ausgewählte Fachbeiträge zur Einrichtung und Prüfung von Corporate-Governance-Systemen; Düsseldorf 2017, S.12.
[126] Vgl. IDW-EPS 980 (10/2021), Tz. 25, A51.
[127] Vgl. IDW-EPS 980 (10/2021), Tz. 7, A6.

es möglich, dass nur einzelne Teilbereiche des CMS (☞ Tz. 33) geprüft werden (hierfür jedoch alle CMS-Grundelemente).

(167) Die Bestimmung der *Wesentlichkeit*, d.h. in welchen Fällen eine falsche Darstellung in der CMS-Beschreibung (☞ Tz.53 Nr.1) der Kommune bzw. ein festgestellter Mangel des CMS der Kommune als wesentlich einzustufen ist, liegt im pflichtgemäßen Ermessen des CMS-Prüfers.[128]

(168) Eine *wesentliche falsche Darstellung in der CMS-Beschreibung* liegt z.B. dann vor, wenn

- sie einen vorhandenen wesentlichen Mangel des CMS nicht erkennen lassen,
- sie falsche Angaben enthalten oder Angaben fehlen, die – einzeln oder in der Summe – für die Adressaten der CMS-Beschreibung entscheidungsrelevant sein können, oder
- sie unangemessene Verallgemeinerungen oder unausgewogene und verzerrende Darstellungen enthalten, die eine Irreführung der Adressaten der CMS-Beschreibung zur Folge haben können.[129]

(169) Ein *wesentlicher Mangel des CMS* liegt dann vor, wenn das in der CMS-Beschreibung dargestellte CMS nicht mit hinreichender Sicherheit sowohl Risiken für wesentliche Verstöße gegen die Regeln, auf deren Einhaltung das CMS in den von der Kommune abgegrenzten Teilbereichen ausgerichtet ist, rechtzeitig erkennt als auch solche Regelverstöße verhindert. Ein wesentlicher Mangel des CMS kann auch bei einer Kumulation von nicht rechtzeitig erkannten Risiken und nicht vom System verhinderten Regelverstößen vorliegen, die einzeln betrachtet nicht wesentlich sind.[130]

(170) Bei der Bestimmung der Wesentlichkeit von (möglichen) *Regelverstößen* sind insb. folgende Fragestellungen von Bedeutung:[131]

- *Bedeutung der verletzten Regel*: Handelt es sich um einen Verstoß gegen Rechtsvorschriften oder gegen interne Richtlinien?
- *Folgen des Regelverstoßes*: Ist mit dem Regelverstoß ein hoher finanzieller oder sonstiger Schaden für die Kommune oder ggf. Dritte verbunden?
- *Motivation für den Regelverstoß*: Handelt es sich um einen beabsichtigten Regelverstoß? Ist mit dem Regelverstoß eine persönliche Bereicherung oder ein sonstiger Vorteil verbunden?

[128] Vgl. IDW-EPS 980 (10.2021), Tz. 47.
[129] Vgl. IDW-EPS 980 (10.2021), Tz. A41.
[130] Vgl. IDW-EPS 980 (10.2021), Tz. A42.
[131] Vgl. IDW-EPS 980 (10.2021), Tz. A43.

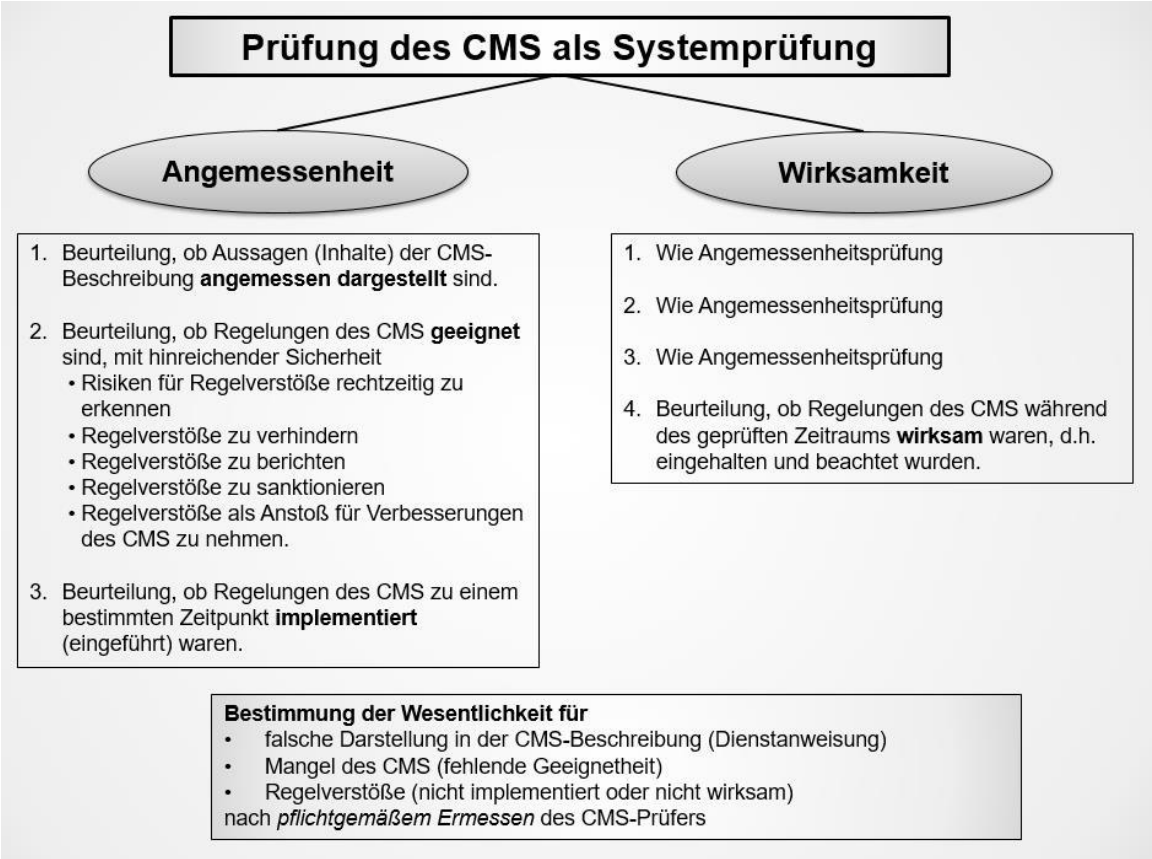
- *Tragweite des Regelverstoßes*: Ist der Regelverstoß auf eine systemimmanente Schwachstelle zurückzuführen oder handelt es sich um eine einmalige Durchbrechung des Systems? Wurden interne Kontrollen durch Mitglieder des Managements außer Kraft gesetzt?

(171) *Anhaltspunkte für wesentliche Mängel* des in der CMS-Beschreibung (☞ Tz.53 Nr.1) dargestellten CMS können sich u.a. aus den folgenden Umständen ergeben:[132]

- Es werden keine geeigneten CMS-Grundsätze verwendet.
- Die Konzeption des CMS weist Lücken auf, die dazu führen können, dass nicht alle Risiken für wesentliche Regelverstöße, die eine mehr als vertretbar niedrige Eintrittswahrscheinlichkeit haben, identifiziert werden, z.B. gibt es kein angemessenes Verfahren zur Meldung von Verdachtsfällen durch Mitarbeitende.
- Der Prozess zur systematischen Erfassung und Analyse von wesentlichen Compliance-Risiken weist Schwachstellen auf, z.B. werden im Rahmen der Prüfung wesentliche Compliance-Risiken erkannt, die vom CMS zuvor nicht erfasst und analysiert worden sind.
- Die Regelungen des CMS werden nicht regelmäßig auf Anpassungsbedarf wegen geänderter Rahmenbedingungen überprüft und ggf. geändert.
- Im CMS werden keine ausreichenden Ressourcen eingesetzt.
- Das CMS wird in der Kommune nicht ausreichend kommuniziert und überwacht.
- Das CMS wird nicht konsequent durchgesetzt, z.B. wenn bei aufgedeckten Regelverstößen die Nichtbeachtung des CMS durch die Mitarbeiter keine wirksamen Konsequenzen hat.

[132] Vgl. IDW-EPS 980 (10.2021), Tz. A 44.

Abbildung 11: Prüfung des CMS als Systemprüfung



7.2 Voraussetzungen für Übernahme der Prüfung

(172) Der CMS-Prüfer (und sein Prüfungsteam) darf die Prüfung des CMS insbesondere nur unter folgenden persönlichen und Kapazitäts-Voraussetzungen übernehmen, wovon er sich vor Übernahme der Prüfung zu vergewissern hat:[133]

- Der CMS-Prüfer muss den *Grundsatz der Unabhängigkeit* beachten. Er darf demnach nicht wesentlich an der Konzeption und Einführung des CMS beteiligt gewesen sein (dies schließt jedoch eine projektbegleitende Angemessenheitsprüfung nicht aus). Auch darf er nicht selbst eine Verantwortlichkeit im CMS der Kommune bzw. ihrer CMS-Grundelemente übernehmen (sollte der Compliance-Beauftragte bei der Internen Revision angesiedelt sein, so darf die Prüfung nicht vom ihm oder seiner Organisationseinheit durchgeführt werden; sie kann aber von einer anderen Organisationseinheit der Internen Revision übernommen werden).

[133] Vgl. IDW-EPS 980 n.F. (10.2021), Tz. 29 ff.; vgl. IDW (Hrsg.): Praxisleitfaden Governance, Risk und Compliance - Ausgewählte Fachbeiträge zur Einrichtung und Prüfung von Corporate-Governance-Systemen; Düsseldorf 2017, S. 16.

- Der CMS-Prüfer muss über die für die Prüfung erforderlichen Kompetenzen, Rechts- und sonstigen Fachkenntnisse verfügen oder erforderlichenfalls Sachverständige hinzuziehen. Außerdem sind die weiteren Grundsätze der beruflichen Praxis von Prüfern – Integrität, Objektivität und Vertraulichkeit – einzuhalten.[134]
- Die für eine ordnungsmäßige Durchführung der Prüfung erforderlichen personellen und zeitlichen Ressourcen müssen zur Verfügung stehen.

(173) Die Prüfungsleitung hat sicherzustellen, dass die vorgenannten Voraussetzungen eingehalten werden.[135]

7.3 Planung und Durchführung der Prüfung

(174) Die CMS-Prüfung ist in Abhängigkeit von der Prüfungsart (Angemessenheits- oder Wirksamkeitsprüfung)

- in sachlicher, personeller und zeitlicher Hinsicht,
- unter Beurteilung der Risiken, dass die CMS-Beschreibung (☞ Tz.53 Nr.1) falsche Darstellungen enthält, dass Mängel des CMS vorliegen und dass Regelverstöße nicht erkannt werden sowie
- unter Beachtung des Grundsatzes der Wesentlichkeit (☞ Tz. 167 - 171)

von Umfang und Zeit her so zu planen, dass sie eine ordnungsgemäße Prüfungsdurchführung ermöglicht. Dabei ist eine kritische Grundhaltung einzunehmen.[136]

(175) Für die Prüfungsplanung (insbesondere für die Beurteilung der Risiken) hat der CMS-Prüfer ein angemessenes Verständnis (Überblick) von den Abläufen und rechtlichen Hintergründen der Kommune sowie von dem in der CMS-Beschreibung dargestellten CMS der Kommune (Strukturen, Prozesse, Verantwortlichkeiten) zu gewinnen. Dazu nimmt er Einblick in erforderliche Dokumente und führt Befragungen geeigneter Personen durch.[137]

---

[134] Vgl. u.a. Deutsches Institut für Interne Revision e. V. (DIIR), Institut für Interne Revision Österreich (IIA Austria), Schweizerischer Verband für Interne Revision (IIA Switzerland) als Herausgeber der deutschen Auflage der International Professional Practices Framework (IPPF): Internationale Standards für die berufliche Praxis der Internen Revision 2017, Version 6.1 vom 10. Januar 2018, Frankfurt am Main, Ethikkodex (S.13 ff.).

[135] Vgl. IDW-EPS 980 (10.2021), Tz. 36. Die im IDW-EPS 980 in Tz. 29 ff. genannten weiteren Voraussetzungen, die seitens der Geprüften zu erfüllen sind, stellen in Abweichung zum IDW EPS 980, Tz. 36 für den kommunalen Bereich kein Prüfungshemmnis dar, sondern führen stattdessen ggf. zur Einschränkung des Prüfungsurteils. Begründung: Im Gegensatz zum externen Wirtschaftsprüfer, der beauftragt wird, prüft die kommunale/örtliche Rechnungsprüfung nach eigener Maßgabe (Prüfungsplanung, Erforderlichkeit). Es darf daher nicht sein, dass die Geprüften durch fehlende Prüfungsbereitschaft die Prüfung der kommunalen/örtlichen Prüfung selbst verhindern können.

[136] Vgl. IDW-EPS 980 (10.2021), Tz. 39-42.

[137] Vgl. IDW-EPS 980 (10.2021), Tz. 48-53, A45-48.

(176) Es empfiehlt sich, eine auf den konkreten Prüfungsfall angepasste Checkliste mit Prüfungsfragen zu erstellen (☞ Muster-Prüfungscheckliste in Anlage 9, Abschnitt 8.9).

(177) Das Ergebnis der Prüfungsplanung und die geplanten Prüfungshandlungen sind in einem Prüfungsprogramm (Prüfungskonzept) aufzunehmen.[138]

(178) Bei der *Prüfungsdurchführung* ist darauf zu achten, die Beurteilungen entsprechend den Schritten der Angemessenheits- (☞ Tz. 164) bzw. Wirksamkeitsprüfung (☞ Tz. 165) abgeben zu können. Dazu gehört auch die Beurteilung,

- ob die betreffenden Regelungen aktuell sind[139] und
- ob festgestellte Regelverstöße auf Mängel im CMS zurückzuführen und geeignete Maßnahmen zu deren Behebung veranlasst worden sind oder ob es sich um Einzelverstöße handelt, die die Angemessenheit bzw. Wirksamkeit des CMS nicht berühren[140].

(179) Für die einzelnen Beurteilungsschritte der Angemessenheits- und Wirksamkeitsprüfung kommen insbesondere folgende Prüfungshandlungen in Betracht:[141]

- Befragungen der Personen, die für das CMS verantwortlich sind, es konzipiert, implementiert oder weiterentwickelt haben oder Kenntnisse über mögliche Schwachstellen oder Nichteinhaltungen von Compliance-Regelungen oder Regelverstöße haben.
- Befragungen der anderen Mitarbeiter zu ihren Kenntnissen über und Erfahrungen mit dem eingerichteten CMS.
- Analyse der CMS-Dokumentation hinsichtlich CMS-Beschreibung und CMS-Regelungen zu Aufbauorganisation, Ressourcenausstattung des CMS, Verfahren, Rollen und Zuständigkeiten sowie Methoden und Maßnahmen zu den CMS-Grundelementen.
- Analyse der CMS-Dokumentation hinsichtlich der durch das CMS generierten Dokumente (u.a. Besprechungsprotokolle, Dokumente der Risikoidentifizierung und -bewertung, Dokumente zu Maßnahmen und Kontrollen, Checklisten, Berichte zur Risikoanalyse oder zu Regelverstößen, Unterlagen zur Maßnahmenverfolgung bei Regelverstößen).
- Beobachtungen von Abläufen im CMS der Kommune bzw. der Einhaltung von CMS-Grundsätzen (z.B. bei Besprechungen zur Risikoidentifikation und -bewertung anwesend sein).

---

[138] Vgl. IDW-EPS 980 (10.2021), Tz. 44.
[139] Vgl. IDW-EPS 980 (10.2021), Tz. 55.
[140] Vgl. IDW-EPS 980 (10.2021), Tz. 64, A61.
[141] Vgl. IDW-EPS 980 (10.2021), Tz A49-A59.

- IT-gestützte Prüfungshandlungen zum Internen Kontrollsystem der Kommune.
- Einsicht in vorhandene Prüfungsberichte zur Angemessenheit und Wirksamkeit des CMS sowie in Prüfungsberichte der Internen Revision / Rechnungsprüfung.

Befragungen allein sind für das Prüfungsurteil nicht hinreichend; es bedarf zusätzlich anderer Prüfungshandlungen.[142]

(180) Die CMS-Prüfung ist nicht auf die Aufdeckung einzelner Regelverstöße ausgerichtet. Stellt der CMS-Prüfer bei seinen Prüfungshandlungen dennoch selbst Regelverstöße oder Anhaltspunkte auf solche fest, unterrichtet er in angemessener Zeit die Leitung der Kommune, sofern sie darüber noch nicht informiert ist.

(181) Der CMS-Prüfer hat alle Prüfungshandlungen und Prüfungsnachweise, die der Stützung des Prüfungsurteils dienen, in der Prüfungsakte so zu dokumentieren, dass sich ein objektiver fachkundiger Dritter, der nicht mit der Prüfung befasst war, in angemessener Zeit ein Bild vom Ablauf, der Feststellungen und der Bildung des Prüfungsurteils machen kann.[143]

7.4 Prüfungsurteil, Prüfungsbericht und Maßnahmenverfolgung

(182) Der CMS-Prüfer hat einen schriftlichen *CMS-Prüfungsbericht* zu fertigen, der insbesondere folgende Inhalte enthalten muss:[144]

- Prüfungsauftrag
- Gegenstand, Art und Umfang der Prüfung
- Aussage, dass die Prüfung in Übereinstimmung mit diesem IDR-Leitfaden durchgeführt wurde
- Beschreibung des zu prüfenden CMS
- Prüfungsfeststellungen
- Vereinbarungen bzw. Empfehlungen für zu ergreifende Maßnahmen oder Aussage, dass die verantwortlichen Führungskräfte das Risiko auf sich genommen haben, keine Maßnahmen durchzuführen[145]
- Zusammenfassendes Prüfungsurteil.

---

142 Vgl. IDW-EPS 980 (10.2021), Tz. A53.
143 Vgl. IDW-EPS 980 (10.2021), Tz. 94 ff.
144 Vgl. IDW-EPS 980 (10.2021), Tz. 104.
145 Vgl. Deutsches Institut für Interne Revision e. V. (DIIR), Institut für Interne Revision Österreich (IIA Austria), Schweizerischer Verband für Interne Revision (IIA Switzerland) als Herausgeber der deutschen Auflage der International Professional Practices Framework (IPPF): Internationale Standards für die berufliche Praxis der Internen Revision 2017, Version 6.1 vom 10. Januar 2018, Frankfurt am Main, Nr. 2500.A1.

(183) Der CMS-Prüfer hat auf der Grundlage ausreichender geeigneter Prüfungsnachweise sein *Prüfungsurteil* zu bilden. Liegen diese ihm nicht vor und war er nicht in der Lage, sie zu erlangen, liegt ein Prüfungshemmnis vor. Bezieht sich das Prüfungshemmnis auf einen wesentlichen Aspekt des CMS (vgl. Tz. 167 ff.), aber ist noch eine Gesamtbeurteilung des CMS möglich, ist im Prüfungsbericht das Prüfungsurteil entsprechend einzuschränken. Ist das Prüfungshemmnis so wesentlich, das eine Gesamtbeurteilung des CMS nicht möglich, ist im Prüfungsbericht zu erklären, dass ein Prüfungsurteil nicht abgegeben werden kann.[146]

(184) Liegt kein Prüfungshemmnis vor und enthält die CMS-Beschreibung (☞ Tz. 53 Nr.1) keine wesentlich falschen Darstellungen und liegt kein wesentlicher Mangel des CMS vor (vgl. Tz. 167 ff.), ist vom CMS-Prüfer ein uneingeschränktes Prüfungsurteil abzugeben. Anderenfalls ist das Prüfungsurteil einzuschränken oder zu versagen.[147]

(185) Es ist Aufgabe der Internen Revision / Rechnungsprüfung, im Rahmen des von ihr eingerichteten Verfahrens zur *Maßnahmenverfolgung* (Follow-up) zu überwachen, dass die im CMS-Prüfungsbericht dargestellten vereinbarten bzw. empfohlenen Maßnahmen wirksam umgesetzt werden oder die verantwortlichen Führungskräfte das Risiko auf sich genommen haben, keine Maßnahmen durchzuführen.

[146] Vgl. IDW-EPS 980 (10.2021), Tz. 89.
[147] Vgl. IDW-EPS 980 (10.2021), Tz. 86 f.

8. Anlagen

8.1 Anlage 1: Übersicht über relevante Gerichtsentscheidungen zur Ausgestaltung eines CMS

Urteil	Wesentlicher Inhalt
LG München I, Urteil vom 10.12.2013 – 5 HK O 1387/10 – BeckRS 2014, 1998 (Siemens/Neuburger-Urteil)	Im Zusammenhang mit den Korruptionsfällen im Siemens-Konzern äußerte sich das LG München I ausführlich zu den Grundlagen einer Vorstandshaftung wegen unzureichender Beachtung der Compliance-Pflichten. Nach diesem Urteil hat jedes Vorstandsmitglied dafür Sorge zu tragen, dass im Unternehmen eine Compliance-Organisation eingerichtet und laufend überprüft wird, die geeignet ist, Gesetzesverstöße zu verhindern. Hinsichtlich des konkreten Pflichtenrahmens stellt das LG München I in dem Urteil fest, dass es für die Ausgestaltung der Compliance-Organisation auf Art, Größe und Organisation des Unternehmens, die zu beachtenden Vorschriften sowie die geografische Präsenz und mögliche bestehende Verdachtsfälle in der Vergangenheit ankomme. Aus dem Urteil lassen sich die folgenden Pflichten für Betriebs- und Unternehmensleitungen ableiten: ➢ Einrichtungs- und Ausgestaltungspflichten: Aufgrund einer Risikoanalyse sollten Compliance-Richtlinien ausgearbeitet und bekanntgemacht werden. Ein solches Regelwerk muss ein klares Bekenntnis der Unternehmensleitung zu den Compliance-Zielen enthalten und setzt funktionsfähige Organisationsstrukturen sowie klare Zuordnung der Verantwortlichkeiten und eine angemessene Ressourcenausstattung voraus. ➢ Unverzügliches Einschreiten bei Verdachtsmomenten und Verstößen: Ergeben sich Verdachtsmomente für Gesetzes- oder Regelverstöße, ist ein unverzügliches Einschreiten und eine unternehmensinterne Untersuchung zu veranlassen. ➢ Prüfungs- und Nachbesserungspflichten: Die Compliance-Pflichten fordern eine kontinuierliche Anpassung, Fortentwicklung, Überwachung und Kontrolle. Diesbezüglich verlangt die Rechtsprechung zu § 130 OWiG die wiederholte Durchführung unangekündigter Stichproben.
BGH, Urteil vom 9.5.2017 – 1 StR 265/16 – BeckRS 2017, 114578	Der BGH äußert sich in dem Urteil in Form eines obiter dictum zu den Auswirkungen eines CMS auf die Bußgeldbemessung nach § 30 OWiG: Demnach ist bei der Bemessung einer Geldbuße nach § 30 OWiG gegen ein Unternehmen die Implementierung eines CMS zu berücksichtigen. Gab es im Zeitpunkt, in welchem sich die Gesetzesverstöße realisierten, ein aus ex ante-Sicht angemessenes und effektives CMS, kann

Urteil	Wesentlicher Inhalt
	sich dies bußgeldmindernd auswirken. In die Bußgeldbemessung ist nach den Aussagen im Urteil auch einzubeziehen, ob zu Tage getretene Defizite des CMS durch die Einführung von Maßnahmen, welche vergleichbare Verstöße in Zukunft verhindern oder zumindest wesentlich erschweren, behoben werden.
BGH, Urteil vom 17.7.2009 – 5 StR 394/08 – BeckRS 2009, 18039 („BSR-Entscheidung")	Ebenfalls in einem obiter dictum begründete der BGH in einer Entscheidung zu einem Vorstandsmitglied der Berliner Stadtreinigung (BSR) eine strafrechtliche Verantwortung eines Compliance-Beauftragten für die Verhinderung von Straftaten innerhalb des Unternehmens, die durch dessen (untergeordnete) Mitarbeiter begangen wurden. Im zugrundeliegenden Fall war der Compliance-Beauftragte der Leiter der Innenrevision einer Anstalt des öffentlichen Rechts. Nach dem BGH folgt eine Garantenpflicht des Compliance-Beauftragten aus dem durch diesen gegenüber seinem Arbeitgeber tatsächlich übernommenen Pflichtenkreis. Dies begründe eine „Sonderverantwortlichkeit" für die Integrität des übernommenen Verantwortungsbereiches.
BGH, Urt. v. 20.10.2011 – 4 StR 71/11 – BeckRS 2011, 27599 („Mobbing-Entscheidung")	Der BGH bestätigt die Aussagen zur strafrechtlichen Garantenpflicht von Geschäftsherren aus der „BSR-Entscheidung" und stellt klar, dass für eine Haftung die Betriebsbezogenheit der zu verhindernden Tat erforderlich ist. Betriebsbezogen ist eine Tat dann, wenn sie einen inneren Zusammenhang mit der betrieblichen Tätigkeit des Begehungstäters oder mit der Art des Betriebs aufweist und eine spezifische Gefahr des Betriebs darstellt. Eine Handlungspflicht bei Straftaten von Mitarbeitern wird danach nicht begründet, wenn der Mitarbeiter die Straftat lediglich „bei Gelegenheit" der Berufsausübung begeht.
BGH, Urt. v. 09.05.2017 – 1 StR 265/16 – BeckRS 2017, 114578 („Panzerhaubitzen-Entscheidung")	Im Zusammenhang mit den Ausführungen zur Strafzumessung bei Vorliegen einer Steuerstraftat weist der BGH in dieser Entscheidung erstmals darauf hin, dass ein effizientes Compliance Management System, welches auf die Vermeidung von Rechtsverstößen ausgelegt sein muss, bußgeldmindernd berücksichtigt werden kann. Dabei kann ebenfalls eine Rolle spielen, ob das Unternehmen in der Folge der aktuellen vor dem Gericht anhängigen Straftat seine Regelungen optimiert hat und die betriebsinternen Abläufe nun so gestaltet, dass vergleichbare Normverletzungen zukünftig deutlich erschwert werden.

8.2 Anlage 2: Institutionelle Compliance-Anforderungen

Die folgende Liste der institutionellen Compliance-Anforderungen ist an die spezifischen Gegebenheiten der Kommune anzupassen.

Compliance-Maßnahmen P = Prävention A = Aufdeckung R = Reaktion	**Institutionelle Anforderungen**							
	Compliance-Kultur	Compliance-Ziele	Compliance-Risiken	Compliance-Programm	Compliance-Organisation	Compliance-Kommunikation	Compliance-Überwachung, Verbesserung	teilbereichsbezogene rechtliche Anforderungen
„Tone at the top" (P)	X			X				
Verhaltenskodex (P)	X			X				
Ehrenkodex Gemeinderäte (P)	X			X				
Geschäftspartnerkodex (P)	X			X				auch Verpflichtungsgesetz, Lieferkettensorgfaltspflichtengesetz (öffentliche Unternehmen)
Personalauswahl (P)	X			X				
Rotation (P)	X							
Schulungen, Sensibilisierungen (P)	X			X		X		
Compliance-belohnendes Anreizwesen (P)	X			X				
Festlegung der Teilbereiche, die das CMS beinhalten soll (P, A, R)		X		X	X			
Festlegung der Aufbau- und Ablauforganisation des CMS, CMS-Richtlinie (P, A, R)				X	X			EU-Whistleblower-Richtlinie, Hinweisgeberschutzgesetz
Angemessene Ressourcenausstattung (P, A, R)				X	X			
Berichtswesen (P, A, R)	X		X	X	X	X	X	EU-Whistleblower-Richtlinie, Hinweisgeberschutzgesetz

Transparenz – Publication, Reporting, Öffentlichkeitsarbeit (P)	X					X		EU-Whistleblower-Richtlinie, Hinweisgeberschutzgesetz
Schriftlichkeits-, Dokumentationsprinzip (P, A, R)	X	X	X	X	X	X	X	Verwaltungsverfahrensgesetz, Informationsfreiheitsgesetz, EU-Whistleblower-Richtlinie, Hinweisgeberschutzgesetz
Hinweisgebersystem – interne Meldestelle, Verfahren zur Hinweisbearbeitung, Folgemaßnahmen (A, R)	X						X	EU-Whistleblower-Richtlinie, Hinweisgeberschutzgesetz, Verbandssanktionengesetz
Identifikation und Bewertung von Compliance-Risiken (P)			X					
Internes Kontrollsystem – v.a. bei prozessbezogenen Risiken (P, A)							X	Zum Teil Haushalts-, Kassen-, Vergaberecht
Spezifische Maßnahmen in folgenden Teilbereichen (falls zutreffend, nicht vollzählig):								*Ermittlung der jeweiligen Rechtsgrundlagen erforderlich*
Antikorruption, Betrugsbekämpfung								:
Beschaffungen								:
Gesundheitsschutz								:
Umweltschutz								:
Öffentliches Planungsrecht								:
Sozial- und Jugendrecht								:
Öffentliche Sicherheit								:
Garanten-, Aufsichts-, Betreiberpflichten								:
Abgaben und Steuern								:
Spenden und Sponsoring								:
Zuwendungsrecht								:

Dienst-, Arbeitsrecht								:
Hinderungsgründe, Befangenheitsregeln								:
Haushalts-, Kassenrecht, Rechnungswesen								:
Daten-, IT-Sicherheit								:
Datenschutz								:
Arbeitssicherheit, Unfallverhütung								:
Schutz v. Dienst-, Geschäfts-, Betriebsgeheimnissen								:
Public Corporate Governance öffentlicher Unternehmen								:
:								:

8.3 Anlage 3: Anforderungs-Maßnahmen-Matrix institutioneller Compliance-Risiken

Teil 1 – Anforderungsinventar:

Nr.	Compliance-Anforderung (Bezeichnung)	Compliance-Anforderung (Beschreibung)	Betrifft Compliance-Ziel(e) (alle oder Teilbereich)	Verantwortliche*r für Anforderung

Fortsetzung mit Teil 2 – Umsetzungsbewertung:

Nr.	vorhandene Maßnahme(n)	Verantwortliche*r für Maßnahme(n)	Wirksamkeit der Maßnahme(n)*	Erläuterung zur Bewertung

* Hier kann z.B. eine Darstellung als Ampel erfolgen.

Fortsetzung mit Teil 3 – Beurteilung:

Nr.	Beurteilung der Umsetzungsbewertung – To-Do's: Sind Verbesserungen der vorhandenen Maßnahme(n) oder neue Maßnahmen erforderlich (Wirksamkeit der Maßnahmen)? Wenn ja, welche?	Umsetzungs-Verantwortliche*r	Zeitliche Vorgabe

Fortsetzung mit Teil 4 – Überwachungsplan:

Nr.	Überwachungsmaßnahme	Überwachungs-Verantwortliche*r	Zeitliche Vorgabe	Überwachungsergebnis

8.4 Anlage 4: Muster einer Risikobewertungs-Systematik und Risikomatrix

Die Mustervorlage sollte ggf. an die spezifischen Gegebenheiten der Kommune angepasst werden.

Kategorien zur Bewertung der Eintrittswahrscheinlichkeit von Compliance-Risiken:[148]

(5) Sehr wahrscheinlich	> 75 % oder < 1 Jahr (fast sicher)
(4) Wahrscheinlich	bis 75 % oder > 1 Jahr
(3) Möglich	bis 50 % oder > 2 Jahre (beides ist in etwa gleich wahrscheinlich)
(2) Selten	bis 25 % oder > 4 Jahre
(1) Unwahrscheinlich	bis 5 % oder > 20 Jahre

Kategorien zur Bewertung der potenziellen Schadenshöhe von Compliance-Risiken:

Bewertung	Potenzieller Schaden
(5) Sehr hoch	➢ Potenzieller finanzieller Schaden für Kommune > X Euro ➢ Potenzielle Haftung wegen Aufsichtspflichtverletzung, Organisationsverschulden oder Fehlentscheidung (Strafe, Ordnungswidrigkeit, Regress) für Leitung bzw. verantwortliche Mitarbeitende der Kommune > X Euro oder in Form einer Gefängnisstrafe ➢ Potenzielle wesentliche Verletzung von Grundrechten ➢ Sehr einschneidende potenzielle Maßnahmen der Rechtsaufsicht ➢ Sehr hoher potenzieller reputativer Schaden für Kommune und/oder Leitung bzw. sehr hoher potenzieller Schaden für Demokratie und Rechtsstaat durch Vertrauensverlust in Unparteilichkeit der Kommunalverwaltung als Teil der öffentlichen Verwaltung (Art. 20 GG), z.B. durch langanhaltende intensive negative Medienberichterstattung, öffentlichkeitswirksame langdauernde Gerichtsverfahren etc.
(4) Bedeutend	• Potenzieller finanzieller Schaden für Kommune > X Euro • Potenzielle Haftung wegen Aufsichtspflichtverletzung, Organisationsverschulden oder Fehlentscheidung (Strafe, Ordnungswidrigkeit, Regress) für Leitung bzw. verantwortliche Mitarbeitende der Kommune > X Euro • Potenzielle bedeutende Verletzung von Grundrechten • Bedeutende potenzielle Maßnahmen der Rechtsaufsicht

148 Einteilung der Skala der Eintrittswahrscheinlichkeit nach: Schwarting, Gunnar, Risikomanagement in Kommunen, Berlin 2015, S. 115.

Bewertung	Potenzieller Schaden
	• Bedeutender potenzieller reputativer Schaden für Kommune und/oder Leitung bzw. bedeutender potenzieller Schaden für Demokratie und Rechtsstaat durch Vertrauensverlust in Unparteilichkeit der Kommunalverwaltung als Teil der öffentlichen Verwaltung (Art. 20 GG), z.B. durch negative Medienberichterstattung, öffentlichkeitswirksame Gerichtsverfahren etc.
(3) Mittel	• Potenzieller finanzieller Schaden für Kommune > X Euro • Potenzielle Haftung wegen Aufsichtspflichtverletzung, Organisationsverschulden oder Fehlentscheidung (Strafe, Ordnungswidrigkeit, Regress) für Leitung bzw. verantwortliche Mitarbeitende der Kommune > X Euro • Potenzielle Verletzung von Grundrechten, die noch nicht bedeutend ist • Potenzielle Maßnahmen der Rechtsaufsicht • Mittlerer potenzieller reputativer Schaden für Kommune und/oder Leitung bzw. mittlerer potenzieller Schaden für Demokratie und Rechtsstaat durch Vertrauensverlust in Unparteilichkeit der Kommunalverwaltung als Teil der öffentlichen Verwaltung (Art. 20 GG), z.B. durch kurze, nicht nachhaltige negative Medienberichterstattung, kaum öffentlichkeitswirksame Gerichtsverfahren etc.
(2) Gering	• Potenzieller finanzieller Schaden für Kommune > X Euro • Potenzielle Haftung wegen Aufsichtspflichtverletzung, Organisationsverschulden oder Fehlentscheidung (Strafe, Ordnungswidrigkeit, Regress) für Leitung bzw. verantwortliche Mitarbeitende der Kommune > X Euro • Potenzielle Verletzung von Grundrechten, die lediglich gering ist • Keine oder unwesentliche potenzielle Maßnahmen der Rechtsaufsicht • Geringer reputativer Schaden für Kommune und/oder Leitung bzw. geringer potenzieller Schaden für Demokratie und Rechtsstaat durch Vertrauensverlust in Unparteilichkeit der Kommunalverwaltung als Teil der öffentlichen Verwaltung (Art. 20 GG), z.B. da keine oder kaum merkbare negative Medienberichterstattung, keine öffentlichkeitswirksamen Gerichtsverfahren etc.

Bewertung	Potenzieller Schaden
(1) Vernachlässigbar	• Potenzieller finanzieller Schaden für Kommune > X Euro • Potenzielle Haftung wegen Aufsichtspflichtverletzung, Organisationsverschulden oder Fehlentscheidung (Strafe, Ordnungswidrigkeit, Regress) für Leitung bzw. verantwortliche Mitarbeitende der Kommune > X Euro oder kaum denkbar • Keine potenzielle Verletzung von Grundrechten • Keine potenziellen Maßnahmen der Rechtsaufsicht • Kein potenzieller reputativer Schaden für Kommune und/oder Leitung bzw. kein potenzieller Schaden für Demokratie und Rechtsstaat durch Vertrauensverlust in Unparteilichkeit der Kommunalverwaltung als Teil der öffentlichen Verwaltung (Art. 20 GG), da Schadenseintritt nicht öffentlichkeitswirksam

Hinweis: Ein Compliance-Risiko ist in die jeweils höchste Schadens-Kategorie einzuordnen, für die mindestens ein Kriterium erfüllt ist.

Risikomatrix zur Bewertung (brutto und netto) der Compliance-Risiken[149]:

Hinweis: Es bietet sich an, die Risikobewertung in Ampelfarben darzustellen.

Potenzielle Schadenshöhe	(5) Sehr hoch	*Geringes Risiko*	*Mittleres Risiko*	*Hohes Risiko*	*Sehr hohes Risiko*	*Sehr hohes Risiko*
	(4) Bedeutend	*Geringes Risiko*	*Mittleres Risiko*	*Hohes Risiko*	*Sehr hohes Risiko*	*Sehr hohes Risiko*
	(3) Mittel	*Geringes Risiko*	*Mittleres Risiko*	*Hohes Risiko*	*Hohes Risiko*	*Hohes Risiko*
	(2) Gering	*Sehr geringes Risiko*	*Geringes Risiko*	*Mittleres Risiko*	*Mittleres Risiko*	*Mittleres Risiko*
	(1) Vernachlässigbar	*Sehr geringes Risiko*	*Sehr geringes Risiko*	*Geringes Risiko*	*Geringes Risiko*	*Geringes Risiko*
		(1) Unwahrscheinlich	(2) Selten	(3) Möglich	(4) Wahrscheinlich	(5) Sehr wahrscheinlich
		Eintrittswahrscheinlichkeit				

[149] Risikomatrix leicht modifiziert aus: Schmigale, Jenny: Compliance Management, Herangehensweise an das Compliance-Risikomanagement, in: https://www.compliance-manager.net/fachartikel/herangehensweisen-das-compliance-risikomanagement-1774965701

8.5 Anlage 5: Risiko-Kontroll-Matrix für prozessbezogene Compliance-Risiken

Teil 1 – Risikoinventar:

Nr.	Produkt / Funktion / Prozess / Organisationseinheit (ggf. weiter untergliedern)	Compliance-Ziel (Teilbereich)	Compliance-Risiko (Bezeichnung)	Compliance-Risiko (Beschreibung)	Risiko-Verantwortliche*r

Fortsetzung mit Teil 2 – Risikobewertung (brutto):

Nr.	Eintrittswahrscheinlichkeit	Potenzieller Schaden (Auswirkung)	Bruttorisiko	Erläuterung zur Bewertung

Fortsetzung mit Teil 3 – Risikobewertung (netto):

Nr.	Vorhandene Compliance-Maßnahmen (IKS)	Kontroll-Maßnahmen-Verantwortliche*r	Wirksamkeit der Maßnahmen?*	Eintrittswahrscheinlichkeit	Potenzieller Schaden (Auswirkung)	Netto-Risiko	Erläuterung zur Bewertung

* *Hier kann z.B. eine Darstellung als Ampel erfolgen.*

Fortsetzung mit Teil 4 – Beurteilung:

Nr.	Beurteilung des Nettorisikos – To-Do's: Sind Verbesserungen der vorhandenen Kontroll-Maßnahmen oder neue Kontroll-Maßnahmen erforderlich (sind interne Kontrollen wirksam)? Wenn ja, welche?	Umsetzungs-Verantwortliche*r	Zeitliche Vorgabe

Fortsetzung mit Teil 5 – Überwachungsplan:

Nr.	Überwachungsmaß-nahme	Überwachungs-Verantwortliche*r	Zeitliche Vor-gabe	Überwachungsergebnis

8.6 Anlage 6: Kriterien für die Auswahl von Meldekanälen

Vor einer Implementierung sollte gut überlegt werden, welche Anforderungen die Meldekanäle erfüllen müssen bzw. sollen. Dabei helfen die folgenden Fragen (nicht abschließend), die

a.) zwingend zu erfüllen sind:

- Wird technisch jederzeit die Vertraulichkeit gewahrt?
- Werden die erforderlichen Datenschutzvorgaben eingehalten?
- Soll der Server in Deutschland stehen?
- Ist der Zugang zum Meldekanal barrierefrei zugänglich?
- Kann der Meldekanal unbeobachtet genutzt werden?
- Ist der Meldekanal technisch leicht verständlich zu bedienen?

b.) die optional sind:

- Wo sollen die Meldungen eingehen? Nur „hausintern" oder z. B. bei einem beauftragten externen Vertrauensanwalt?
- Sollen auch anonyme Meldungen möglich sein (d.h. ohne, dass die hinweisgebende Person identifiziert werden kann)?
- Bei einem webbasierten Meldekanal: In welchen Sprachen soll der Meldekanal zur Verfügung stehen?
- Soll eine Kommunikation zwischen hinweisgebenden Personen und Meldestelle möglich sein (für Rückfragen seitens der Meldestelle)?
- Soll die Entgegennahme von Meldungen rund um die Uhr oder nur während der üblichen Bürozeiten möglich sein? Wer soll für die Entgegennahme der Hinweise zuständig sein? Stehen ausreichend personelle Ressourcen zur Verfügung?
- Soll der Zugang zum Meldekanal auch mobil per Handy möglich sein?
- Kann ein eigenes Inter- bzw. Intranet-basiertes IT-Tool mit vernünftigem Ressourceneinsatz (Personal, Zeit, Finanzen) für Beschaffung, Einführung und laufende Betreuung betrieben werden oder wäre ein externes IT-Tool kostengünstiger?
- …

8.7 Anlage 7: Hinweisgebersystem im Gefüge der CMS-Grundelemente

Die folgende Übersicht geht auf die wesentlichen Aspekte ein:

Ziele	• Vermeidung / Verringerung von materiellen Schäden für die Kommune • Image einer integren und ethisch handelnden Kommune (Reputation) • Stärkung des Vertrauens der Bürger in ihre öffentliche Verwaltung
Kultur	„tone at the top", d.h. ein klares Bekenntnis von der Spitze der Kommune / Verwaltung • zum Meldesystem und zum Schutz der hinweisgebenden Personen, • dass Meldungen keinen Verrat darstellen, sondern ein wichtiges Instrument sind, um Schäden für die Kommune (finanzielle Schäden, Reputationsschäden / Imageverlust) zu verhindern bzw. zu verringern, • dass sowohl Verstöße gegen die geltenden Regeln (entsprechend dem sachlichen Anwendungsbereich) als auch vorsätzlicher Missbrauch des Meldesystems sanktioniert werden
Risiken	• Missbrauch des Meldesystems, Falschmeldungen / irrelevante Meldungen • Verletzung der Schutzpflichten gegenüber hinweisgebenden Personen • Verletzung der Fürsorgepflicht gegenüber betroffenen Mitarbeitenden • Keine oder nicht wirksame Folgemaßnahmen nach Hinweiseingang
Programm	• Festlegung der passenden internen Meldekanäle • Festlegung, wer die Meldekanäle nutzen kann • Schulung des in der Meldestelle eingesetzten Personals • Folgemaßnahmen nach Hinweiseingang (v.a. Aufklärung, Sanktionierung, Verbesserung) • Einführung eines Sanktionssystems zur Verhinderung von Missbrauch des Meldesystems
Organisation	• Festlegung von Zuständigkeiten und Verantwortlichkeiten • Einrichtung eines Verfahrens für Folgemaßnahmen nach Hinweiseingang • Zurverfügungstellung der erforderlichen personellen und finanziellen Ressourcen
Kommunikation	• Bekanntmachung des Meldesystems gegenüber den festgelegten Nutzern bzw. potenziellen hinweisgebenden Personen • Veröffentlichung der Arbeitsergebnisse der Meldestelle (z.B. im Jahresbericht)

Kontrolle, Evaluation und Optimierung	Auswertung der eingegangenen Meldungen und Berichtserstattung an verantwortliche Leitung hinsichtlich • Relevanz (Thema Korruption bzw. andere Themen, Anzahl Falschmeldungen) • Aussagekraft (konnte die Meldestelle aufgrund des Hinweises weitere Ermittlungen durchführen oder war der Hinweis zu vage?) • Art der Quelle (intern / extern, anonym / hinweisgebende Person bekannt) • Plausibilität (Anzahl plausibler / nicht plausibler Hinweise) • Ergebnisse (Feststellung aufgedeckter / verhinderter Schäden, Einleitung von Strafverfahren, arbeits-/ dienstrechtliche Konsequenzen) Optimierung (Behebung mögl. Fehlerquellen, Vereinfachung des Zugangs, etc.)

8.8 Anlage 8: Checkliste Bekanntmachung / Kommunikation des Melde- bzw. Hinweisgebersystems

Alle wichtigen und notwendigen Informationen zur internen Abgabe von Meldungen sollten in einfach verständlicher Weise an barrierefrei zugänglichen Stellen regelmäßig (in der Regel jährlich) kommuniziert werden. Insbesondere sollten folgende Informationen bekannt gemacht werden:

1. Vorhandensein, Zugang und Bedienung der vorhandenen internen Meldekanäle sowie der ausdrückliche Wille zu deren Nutzung;
2. Darstellung der Themen, zu denen Hinweise gewünscht werden;
3. Ggf. der ausdrückliche Hinweis, dass auch anonyme Meldungen bearbeitet werden;
4. Zusicherung, dass die Wahrung der Vertraulichkeit der Identität der hinweisgebenden Person oberste Priorität hat (§ 8 HinSchG). Sofern ein externer Vertrauensanwalt mit der Entgegennahme von Meldungen beauftragt ist, sollte explizit darauf hingewiesen werden, dass der Vertrauensanwalt die Identität der hinweisgebenden Person gegenüber der Kommune grundsätzlich nicht offenlegt (Ausnahmen vom Vertraulichkeitsgebot werden in § 9 HinSchG geregelt).
5. Klare und leicht zugängliche Informationen über externe Meldeverfahren (§ 13 Abs. 2 HinSchG).
6. Information über die bestehenden Informationspflichten und Fristen (Eingangsbestätigung und Folgemeldung).
7. Klarstellung, dass hinweisgebende Personen nach § 36 Abs. 1 HinSchG keine Repressalien aufgrund ihrer Meldung oder Offenlegung zu befürchten haben. Zu den Nachteilen gehören u.a. Abmahnung, Kündigung, Disziplinarmaßnahmen, Verweigerung von Fortbildungen oder Aufstiegsmöglichkeiten, Diskriminierung, Mobbing.
8. Klarstellung, dass hinweisgebende Personen dabei unterstützt werden, drohende oder bereits eingetretene Repressalien abzuwehren.
9. Information, dass Repressalien gegen hinweisgebende Personen aufgrund einer Meldung oder Offenlegung verboten sind (§ 36 Abs. 1 HinSchG). Ein Verstoß gegen das Verbot von Repressalien kann zu einem Schadensersatzanspruch der hinweisgebenden Person führen (§ 37 Abs. 1HinSchG).

10. Information über die bestehende Beweislastumkehr in Bezug auf nachteilige Maßnahmen gegen hinweisgebende Personen nach erfolgter Meldung oder Offenlegung (§ 36 Abs. 2 HinSchG).
11. Klarstellung, dass Hinweisgeber nur geschützt sind, wenn sie nicht bewusst falsche Hinweise melden (vgl. § 3 Abs. 3 HinSchG sowie § 38 HinSchG), sondern im Zeitpunkt der Meldung hinreichenden Grund zur Annahme hatten, dass ihre gemeldeten Informationen der Wahrheit entsprechen und zu den Themen gehören, für die die internen Meldekanäle offenstehen. Wichtig ist zudem der Hinweis, dass der Schutz auch dann besteht, wenn sich die als wahr geglaubte Meldung nachträglich als falsch herausstellt.
12. Bereitstellung von Informationen über bestehende Schutzmaßnahmen und allgemein zugängliche Rechtsschutzmöglichkeiten, Informationen sowie Beratungs- und Unterstützungsangebote.
13. Klarstellung, dass auch die Rechte der von einer Meldung betroffenen Personen geschützt werden (vgl. § 8 HinSchG).

8.9 Anlage 9: Muster- Prüfungscheckliste zum kommunalen CMS[150]

Die abgebildete Muster-Prüfungscheckliste ist an die jeweilige Prüfungsart (Angemessenheitsprüfung, Wirksamkeitsprüfung) und ggf. an Bereichsspezifika, die sich aus besonderen Vorschriften (für das CMS, einzelne CMS-Grundelemente oder Maßnahmen) oder aus der Art oder dem Aufbau der Kommune ergeben können, anzupassen.

Bewertungsskala für die Prüfungsfragen:

Stufe (Punkte)	**Bedeutung**	**Erfüllungsgrad**
4 (dunkelgrün)	Anforderung voll erfüllt	mindestens 80%
3 (hellgrün)	leichter Verbesserungsbedarf	mindestens 70%
2 (gelb)	deutlicher Verbesserungsbedarf	mindestens 50%
1 (rot)	unzureichend	< 50%
0 (rot	Es liegen keine bewertbaren Dokumente/Aussagen vor	
n. a.	Frage ist nicht anwendbar (und geht somit nicht in die Bewertung ein)	

Das Prüfungsurteil sollte eingeschränkt werden, wenn

- mindestens eine als Grundanforderung gekennzeichnete Prüfungsfrage mit 0 oder 1 bewertet wurde;
- der Punkte-Durchschnitt eines CMS-Grundelements kleiner 2 ist.

Die nachfolgenden Fragen sind durch geeignete Prüfungshandlungen zu beantworten bzw. zu bewerten. Ergänzende Fragen für die Wirksamkeitsprüfung (die über die Angemessenheitsprüfung hinausgehen) sind mit der Bezeichnung „Wirksamkeit" gekennzeichnet.

150 Aufbau der Prüfungscheckliste und der Bewertungsskala in Anlehnung an: DIIR-Arbeitskreis „Interne Revision in gesetzlichen Kranken- und Pflegeversicherungen", hier: Checkliste zur Prüfung des Compliance Management Systems in der gesetzlichen Kranken- und Pflegeversicherung, Stand 01.10.2020, im Internet abrufbar: https://www.diir.de/arbeitskreise/interne-revision-in-gesetzlichen-kranken-und-pflegeversicherungen/aufgaben-und-ziele/

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
A. Compliance-Kultur:				
A.1	Ist das Thema Compliance-Kultur und dessen Zielsetzung eines integren Verhaltens in der CMS-Beschreibung (z.B. CMS-Richtlinie) angemessen dargestellt?	X		
A.2	Werden zur Umsetzung der gewünschten Compliance-Kultur geeignete Regelungen, Maßnahmen bzw. Instrumente eingesetzt?	X		
A.3	Gibt es ein eindeutiges Bekenntnis der Leitung zur Rechts- und Regeltreue (Compliance) und zur Nichttoleranz gegenüber Regelverstößen („tone at the top“)?	X		
A.4	*Wirksamkeit:* Entspricht das Verhalten der Leitung und oberen Führungskräfte („tone at the top“) dem Anspruch der Rechts- und Regeltreue bzw. spiegelt sich die Compliance-Kultur im Führungsstil wider?			
A.5	*Wirksamkeit:* Werden Entscheidungsmöglichkeiten als inakzeptabel angesehen, die der Kommune zwar Vorteile bringen oder politisch opportun erscheinen, jedoch nicht regelkonform sind?			
A.6	*Wirksamkeit:* Wird die Herbeiführung von Entscheidungen der Leitung und oberen Führungskräfte vollständig in ausreichendem Umfang schriftlich dokumentiert (so dass alle Beteiligten, wesentlichen Argumente und Verantwortlichkeiten bis zur jeweiligen Entscheidung erkennbar und nachvollziehbar sind)?			
A.7	*Wirksamkeit:* Haben Regelverstöße Konsequenzen (werden Regelverstöße angemessen sanktioniert und werden Gründe der Regelverstöße analysiert, um zukünftig vergleichbare Verstöße zu vermeiden)?			
A.8	Gibt es einen Verhaltenskodex für die Kommune bzw. kommunale Verwaltung? Wird dort auch das Verbot der Annahme von Vorteilen sowie die Vermeidung von Interessenkonflikten eingegangen (oder wird zumindest dort auf gesonderte Regelungen dazu verwiesen)?	X		

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
A.9	Ist der Verhaltenskodex Gegenstand der regelmäßigen Belehrung?			
A10	*Wirksamkeit:* Sind der Verhaltenskodex und seine Inhalte allen Führungskräften und Mitarbeitern bekannt?			
A.11	*Wirksamkeit:* Haben Regelverstöße (auch wenn sie auf oberer Führungsebene erfolgen) Konsequenzen (werden Regelverstöße angemessen sanktioniert und werden sie zum Anlass genommen, vorhandene Prozesse zu überprüfen und zu verbessern, um zukünftig vergleichbare Verstöße zu vermeiden)?			
A.12	Gibt es einen Ehrenkodex (Ehrenordnung) für den Gemeinderat?			
A.13	Wird der Ehrenkodex den Gemeinderäten zu Beginn einer Amtszeit bekannt gemacht?			
A.14	*Wirksamkeit:* Ist der Ehrenkodex mit seinen Inhalten den Gemeinderäten bekannt?			
A.15	*Wirksamkeit:* Werden Regelverstöße gegen den Ehrenkodex angemessen thematisiert und werden Gründe solcher Regelverstöße analysiert, um zukünftig vergleichbare Verstöße zu vermeiden?			
A.16	Gibt es einen geeigneten Geschäftspartnerkodex und soll dessen Befolgung vertraglich vereinbart werden?			
A.17	*Wirksamkeit:* Wird die Befolgung des Geschäftspartnerkodex mit den Geschäftspartnern tatsächlich vertraglich vereinbart?			
A.18	*Wirksamkeit:* Werden Regelverstöße gegen den Geschäftspartnerkodex sanktioniert?			
A.19	Ist vorgesehen, dass Personen, die nicht Amtsträger sind und öffentliche Aufgaben wahrnehmen, nach dem Verpflichtungsgesetz förmlich verpflichtet werden sollen?			
A.20	*Wirksamkeit:* Werden Personen, die nicht Amtsträger sind und öffentliche Aufgaben wahrnehmen, tatsächlich nach dem Verpflichtungsgesetz förmlich verpflichtet?			

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
A.21	Ist vorgesehen, dass Integritätsaspekte bei Personalauswahl, Personalentwicklung und Beurteilungen berücksichtigt werden?			
A.22	*Wirksamkeit:* Finden Integritätsaspekte tatsächlich angemessene Berücksichtigung bei Personalauswahl, Personalentwicklung und Beurteilungen?			
A.23	Ist vorgesehen, dass in angemessenem Umfang Rotation in dafür geeigneten Bereichen stattfinden soll?			
A.24	*Wirksamkeit:* Findet tatsächlich in angemessenem Umfang Rotation in dafür geeigneten Bereichen statt?			
A.25	Gibt es ein Hinweisgebersystem? ☞ siehe H.	X		
A.26	*Wirksamkeit:* Ist das eingerichtete Hinweisgebersystem wirksam? ☞ siehe H.			
A.27	Ist vorgesehen, dass zum Thema Compliance ausreichend sensibilisiert, geschult, beraten und veröffentlicht wird? ☞ siehe F.	X		
A.28	*Wirksamkeit:* Wird zum Thema Compliance ausreichend sensibilisiert, geschult, beraten und veröffentlicht? ☞ siehe F.			
B. Compliance-Ziele:				
B.1	Sind Compliance-Ziele festgelegt, die sich aus strategischen Zielen ergeben (die v.a. in formellen und materiellen gesetzlichen Vorgaben, sonstigen Regelungen sowie Vorgaben der Organe der Kommune niedergelegt sind)? Gehören zu den Zielen mindestens: Bindung an Recht und Gesetz, Vermeidung materieller Schäden, Abwendung von Aufsichtspflichtverletzungen und Organisationsverschulden, Verringerung von Haftungsrisiken, Erfüllung der gesetzlichen Pflicht zur Einrichtung eines Hinweisgebersystems, Abwehr von Reputationsschäden.	X		
B.2	Umfasst die Festlegung der Compliance-Ziele auch die Festlegung, welche Teilbereiche (Rechtsgebiete, darunter ggf. Orga.-Einheiten) der Kommune vom CMS abgedeckt	X		

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
	werden sollen? Sind die wesentlichen risikoreichen Teilbereiche umfasst?			
B.3	Sind die Compliance-Ziele in der CMS-Beschreibung (z.B. CMS-Richtlinie) angemessen dargestellt?	X		
B.4	Sind die festgelegten Compliance-Ziele konsistent, verständlich und praktikabel (sind u.a. Teilbereiche sinnvoll abgegrenzt)?			
B.5	*Wirksamkeit:* Sind die Compliance-Ziele in der Verwaltung / Einrichtung kommuniziert worden bzw. den Führungskräften und Mitarbeitern bekannt?			
B.6	*Wirksamkeit:* Sind die Compliance-Ziele Ausgangspunkt / Grundlage bei der Festlegung der Maßnahmen im CMS?			
B.7	Sind die festgelegten Compliance-Ziele mit den verfügbaren Ressourcen umsetzbar? ☞ siehe E.			
C. Compliance-Risiken:				
C.1	Ist ein strukturiertes und dokumentiertes Verfahren zur Identifizierung und Bewertung der (institutionellen und prozessbezogenen) Compliance-Risiken mit klaren Zuständigkeiten festgelegt, das regelmäßig bzw. in angemessenen Zeitabständen durchlaufen wird? Ist für die Dokumentation der Risikoanalyse die Verwendung einer einheitlichen Anforderungs-Maßnahmen-Matrix / Risiko-Kontroll-Matrix verbindlich vorgeschrieben?	X		
C.2	*Wirksamkeit*: Wird das festgelegte Verfahren zur Identifizierung und Bewertung der (institutionellen und prozessbezogenen) Compliance-Risiken eingehalten? Ist das Verfahren den Verantwortlichen bekannt?			

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
C.3	Ist eine vollständige Betrachtung aller Compliance-Risiken (im Hinblick auf die festgelegten Compliance-Ziele) innerhalb der Kommunalverwaltung bzw. des kommunalen Unternehmens sowie aus dem – v.a. rechtlichen – Umfeld festgelegt (z.B. durch Verwendung kommunaler, bereichs- oder funktionsbezogener Risikokataloge)?	X		
C.4	*Wirksamkeit*: Erfolgt tatsächlich die vollständige Betrachtung aller Compliance-Risiken (im Hinblick auf die festgelegten Compliance-Ziele), d.h. sind diesbezüglich alle wesentlichen Compliance-Risiken identifiziert worden?			
C.5	Ist festgelegt, dass die rechtlichen Compliance-Vorgaben (im Rahmen der Risikoidentifizierung) regelmäßig auf relevante Änderungen hin überwacht werden?			
C.6	*Wirksamkeit*: Werden die rechtlichen Compliance-Vorgaben (im Rahmen der Risikoidentifizierung) tatsächlich regelmäßig auf relevante Änderungen hin überwacht?			
C.7	Ist festgelegt, dass festgestellte Compliance-Verstöße bei der Risikoanalyse berücksichtigt werden?			
C.8	*Wirksamkeit*: Werden festgestellte Compliance-Verstöße tatsächlich bei der Risikoanalyse berücksichtigt			
C.9	Ist festgelegt, dass für die Risikobewertung eine geeignete und nachvollziehbare Bewertungssystematik (Bewertungskriterien, Kategorien) verwendet wird?			
C.10	*Wirksamkeit*: Wird für die Risikobewertung tatsächlich eine geeignete und nachvollziehbare Bewertungssystematik (Bewertungskriterien, Kategorien) verwendet? Ist sie den Verantwortlichen bekannt?			
C.11	*Wirksamkeit*: Sind die wesentlichen Compliance-Risiken hinsichtlich ihrer Wahrscheinlichkeit und quantitativen Auswirkung (potenzieller Schaden) plausibel und nachvollziehbar bewertet?			

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
C.12	Ist festgelegt, dass die Risikoanalyse unter Beteiligung der für die jeweiligen Bereiche und Compliance-Risiken sachkundigen Personen (z.B. durch Interviews und Workshops) durchgeführt wird?			
C.13	*Wirksamkeit*: Wird die Risikoanalyse tatsächlich unter Beteiligung der für die jeweiligen Bereiche und Compliance-Risiken sachkundigen Personen (z.B. durch Interviews und Workshops) durchgeführt?			
C.14	Ist festgelegt, dass das vorgesehene Verfahren und die Zuständigkeiten, die Bewertungssystematik, die Ergebnisse der Identifikation und der Bewertung der Compliance-Risiken bzw. der institutionellen Anforderungen sowie die Festlegung der jeweils Verantwortlichen angemessen und revisionsfähig dokumentiert wird?			
C.15	*Wirksamkeit*: Werden das vorgesehene Verfahren und die Zuständigkeiten, die Bewertungssystematik, die Ergebnisse der Identifikation und der Bewertung der Compliance-Risiken bzw. der institutionellen Anforderungen sowie die Festlegung der jeweils Verantwortlichen angemessen und revisionsfähig dokumentiert?			
C.16	Ist vorgesehen, dass das Ergebnis der Risikoanalyse an die Leitung und die jeweils zuständigen Leitungsebenen unverzüglich und nachvollziehbar kommuniziert und dort zur Kenntnis genommen wird sowie daraus resultierende Vorgaben und Entscheidungen der Leitung angemessen dokumentiert und an die umsetzungsverantwortlichen Stellen kommuniziert werden?			
C.17	*Wirksamkeit:* Werden das Ergebnis der Risikoanalyse an die Leitung und die jeweils zuständigen Leitungsebenen unverzüglich und nachvollziehbar kommuniziert und dort zur Kenntnis genommen sowie daraus resultierende Vorgaben und Entscheidungen der Leitung angemessen dokumentiert und an die umsetzungsverantwortlichen Stellen kommuniziert?			

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
C.18	Sind Ereignisse, Schwellenwerte etc. definiert, wann eine Aktualisierung der Risikoanalyse außerplanmäßig durchgeführt wird?			
C.19	*Wirksamkeit*: Erfolgt tatsächlich eine außerplanmäßige Aktualisierung der Risikoanalyse, wenn definierte Ereignisse eintreten oder Schwellenwerte erreicht werden?			
D. Compliance – Programm:				
D.1	Ist festgelegt, dass für die benannten Compliance-Risiken angemessene Maßnahmen zur Risikoreduzierung bzw. -minimierung festzulegen sind?	X		
D.2	*Wirksamkeit*: Sind für die benannten Compliance-Risiken angemessene Maßnahmen zur Risikoreduzierung bzw. -minimierung benannt worden? Leiten sich die einzelnen Maßnahmen des Compliance-Programms aus der Compliance-Risikoanalyse ab bzw. sind die Maßnahmen einzelnen institutionellen Anforderungen oder Risiken zugeordnet?			
D.3	Ist festgelegt, dass die einzelnen Maßnahmen in der Anforderungs-Maßnahmen-Matrix bzw. der Risiko-Kontroll-Matrix aufzuführen sind (bzw. beide Matrizen verbindlich zu verwenden sind)?			
D.4	*Wirksamkeit*: Sind die einzelnen Maßnahmen in der Anforderungs-Maßnahmen-Matrix bzw. der Risiko-Kontroll-Matrix aufgeführt (dokumentiert)?			
D.5	Ist festgelegt, dass die Verantwortlichen für die einzelnen Maßnahmen und deren Umsetzung in der Anforderungs-Maßnahmen-Matrix bzw. der Risiko-Kontroll-Matrix aufzuführen (zu dokumentieren) sind?			
D.6	*Wirksamkeit*: Sind die Verantwortlichen für die einzelnen Maßnahmen und deren Umsetzung in der Anforderungs-Maßnahmen-Matrix bzw. der Risiko-Kontroll-Matrix aufgeführt (dokumentiert)?			

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
D.7	*Wirksamkeit*: Sind die im Compliance-Programm enthaltenen Maßnahmen im Einzelnen und insgesamt *geeignet*, mit hinreichender Sicherheit wesentliche Regelverstöße zu verhindern (Prävention) als auch solche rechtzeitig zu erkennen (Aufdeckung) und darauf zu reagieren? → Hinweis: Die *Geeignetheit* misst sich an den Compliance-Zielen, der Größe der Verwaltung / des Unternehmens, Art und Umfang der Verwaltungs-, Geschäftstätigkeit, rechtlichen Anforderungen.			
D.8	*Wirksamkeit*: Sind zu *jedem* CMS-Grundelement geeignete Maßnahmen vorhanden? Gibt es mindestens u.a.: • Compliance-Kodex • Verfahrens-Richtlinie • Compliance-Verantwortliche/r • Angemessenes Compliance-Budget • Wirksames Internes Kontrollsystem • Wirksames Hinweisgebersystem mit Verfahren zur Aufklärung von Hinweisen • Vorgehen zur Reaktion auf Compliance-Verstöße → Hinweis: Die *Geeignetheit* misst sich an den Compliance-Zielen, der Größe der Verwaltung / des Unternehmens, Art und Umfang der Verwaltungs-, Geschäftstätigkeit, rechtlichen Anforderungen.			
D.9	*Wirksamkeit*: Entsprechen die vorhandenen Maßnahmen bestehenden rechtlichen Vorgaben?	X		
D.10	Ist das Compliance-Programm und sind die einzelnen Maßnahmen tatsächlich in der Behörde / im Unternehmen implementiert bzw. in Kraft gesetzt worden?	X		
D.11	*Wirksamkeit*: Sind die einzelnen Maßnahmen den Betroffenen (Maßnahmen- bzw. Umsetzungs-Verantwortlichen) nach Maßgabe ihrer Verantwortung bekannt?			

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
D.12	*Wirksamkeit*: Werden die Compliance-Maßnahmen wirksam umgesetzt, d.h. werden die einzelnen Maßnahmen von den Betroffenen (Maßnahmen- bzw. Umsetzungs-Verantwortlichen) nach Maßgabe ihrer Verantwortung beachtet und tatsächlich umgesetzt?			
E. Compliance - Organisation:				
E.1	Ist die Compliance-Organisation mit Aufbau und Ablauf in der CMS-Beschreibung (z.B. CMS-Richtlinie) vollständig, richtig und angemessen dargestellt?	X		
E.2	Ist die in der CMS-Beschreibung (z.B. CMS-Richtlinie) dargestellte Compliance-Organisation geeignet (im Hinblick auf CMS-Ziele und CMS-Risiken), mit hinreichender Wahrscheinlichkeit wesentliche Regelverstöße zu verhindern (Prävention) als auch solche zu erkennen (Aufdeckung) und darauf zu reagieren (Reaktion)?	X		
E.3	Ist die festgelegte Aufbau- und Ablauforganisation ein integraler Bestandteil der Behördenorganisation?			
E.4	Sind für alle Aufgaben im CMS die Rollen, Verantwortlichen und Zuständigkeiten eindeutig festgelegt? Ist ein Compliance-Beauftragter bestellt?			
E.5	Hat der Compliance-Beauftragte die zur wirksamen Wahrnehmung seiner Aufgaben erforderlichen Befugnisse zugewiesen bekommen? Ist seine Unabhängigkeit und Weisungsungebundenheit sichergestellt und wirksam festgelegt? Ist festgelegt, dass er über die nötigen sozialen und fachlichen Anforderungen verfügen muss?	X		
E.6	*Wirksamkeit*: Verfügt der Compliance-Beauftragte tatsächlich über die nötigen sozialen und fachlichen Anforderungen? Kann er tatsächlich in der Kommune unabhängig, ohne Interessenkonflikte und weisungsungebunden agieren?			
E.7	*Wirksamkeit*: Sind ausreichende Ressourcen einschließlich Budgets für die vorhandene			

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
	Compliance-Organisation und den Compliance-Beauftragten vorhanden?			
E.8	*Wirksamkeit*: Ist die in der CMS-Beschreibung (z.B. CMS-Richtlinie) dargestellte Compliance-Organisation (Aufbau und Ablauf) auch wirksam (bzw. wird sie tatsächlich gelebt)?			
F. Compliance - Kommunikation:				
F.1	Ist die Compliance-Kommunikation in der CMS-Beschreibung (z.B. CMS-Richtlinie) vollständig, richtig und angemessen dargestellt?	X		
F.2	Gibt es ein angemessenes Schulungs-, Sensibilisierungs-, Belehrungs- und Informationskonzept, das sich an den unterschiedlichen Adressaten (Führungskräfte, Mitarbeiter, Funktionsträger etc.) orientiert? Ist darin auch sichergestellt, dass neue Führungskräfte und Mitarbeiter unverzüglich geschult und belehrt werden?	X		
F.3	Ist festgelegt, dass der Compliance-Beauftragte die Führungskräfte, Mitarbeiter und Organisationseinheiten bei der Klärung konkreter Compliance-Fragestellungen berät?			
F.4	*Wirksamkeit*: Wird das Schulungs-, Sensibilisierungs-, Belehrungs- und Informationskonzept tatsächlich umgesetzt? Nimmt der Compliance-Beauftragte seine Beratungsfunktion wahr?			
F.5	*Wirksamkeit*: Sind die (wesentlichen) Compliance-Ziele, Compliance-Risiken und die Compliance-Maßnahmen allen Führungskräften, Mitarbeitern und andere wesentlichen Akteuren tatsächlich bekannt?			
F.6	Ist festgelegt, wann, in welcher Form und über welche Compliance-Aspekte der Compliance-Beauftragte die Behördenleitung (und ggf. weitere interne Stellen, die kommunalen Gremien) zu informieren hat (interne Berichtspflichten)? Sind diese Festlegungen eindeutig?	X		

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
F.7	*Wirksamkeit*: Sind die internen Berichtswege den Verantwortlichen bekannt?			
F.8	*Wirksamkeit*: Werden die internen Berichtspflichten tatsächlich eingehalten?			
F.9	Ist das Verfahren festgelegt, wie Bürger und Presse zu Compliance-Themen informiert werden (öffentliche Kommunikation)?			
F.10	*Wirksamkeit*: Wird das Verfahren für die öffentliche Kommunikation eingehalten?			
F.11	Ist festgelegt, dass und in welcher Form compliance-relevante Informationen systematisch aus anderen mit Risiken befassten Organisationseinheiten (Risikomanagement, Interne Revision, Qualitätsmanagement, Justiziariat, o. ä.) vom Compliance-Beauftragten aufgenommen bzw. ausgetauscht werden?			
F.12	*Wirksamkeit*: Werden compliance-relevante Informationen tatsächlich systematisch aus anderen mit Risiken befassten Organisationseinheiten (Risikomanagement, Interne Revision, Qualitätsmanagement, Justiziariat, o. ä.) vom Compliance-Beauftragten aufgenommen bzw. ausgetauscht?			
F.13	Ist festgelegt, dass alle Hinweise auf Regelverstöße an die zuständigen internen Stellen angemessen und unverzüglich kommuniziert werden? Ist festgelegt, dass akute schwere Regelverstöße bzw. entsprechende Hinweise direkt und unverzüglich an die Leitung berichtet werden (ad hoc)? Gibt es definierte Ereignisse, Schwellenwerte etc. für die ad-hoc-Berichterstattung an die Leitung?	X		
F.14	*Wirksamkeit*: Werden Hinweise auf Regelverstöße tatsächlich an die zuständigen internen Stellen angemessen und unverzüglich kommuniziert? Findet eine direkte und unverzügliche Berichterstattung an die Leitung zur Information über akute Regelverstöße bzw. entsprechende Hinweise (ad hoc) unter Einhaltung der definierten Ereignisse, Schwellenwerte etc. tatsächlich statt?			

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
F.15	Sind die Verfahren und Zuständigkeiten für die Kommunikation von Regelverstößen und entsprechenden Hinweisen mit externen Stellen (u.a. Strafverfolgungsbehörden, Meldestellen nach dem HinSchG, beauftragte Rechtsanwälte) festgelegt?			
F.16	*Wirksamkeit*: Werden die Verfahren und Zuständigkeiten für die Kommunikation von Regelverstößen und entsprechenden Hinweisen mit externen Stellen tatsächlich eingehalten?			
G. Compliance-Überwachung und -Verbesserung:				
G.1	Sind in der CMS-Dokumentation die vorhandenen Maßnahmen zur Überwachung und Verbesserung vollständig und angemessen dargestellt?	X		
G.2	Sind die Überwachungsmaßnahmen in den CMS-Regelungen in compliance-prozessintegrierte Überwachung und compliance-prozessunabhängige Überwachung untergliedert (entsprechend Drei-Linien-Modell)?			
G.3	Ist festgelegt, dass für alle Überwachungsmaßnahmen die Zuständigkeiten, Überwachungspläne (o.Ä.) und ggf. -intervalle festzulegen und zu dokumentieren sind (am besten in Ergänzung der Anforderungs-Maßnahmen-Matrix bzw. der Risiko-Maßnahmen-Matrizen)?	X		
G.4	*Wirksamkeit:* Sind für alle Überwachungsmaßnahmen die Zuständigkeiten, Überwachungspläne (o.Ä.) und ggf. -intervalle festgelegt und dokumentiert?			
G.5	*Wirksamkeit:* Sind die Überwachungsmaßnahmen geeignet, die Angemessenheit und Wirksamkeit des CMS sicherzustellen?			
G.6	*Wirksamkeit:* Ist das vorhandene IKS geeignet, mit hinreichender Wahrscheinlichkeit Regelverstöße zu erkennen?			
G.7	Ist festgelegt, dass eine angemessene prozessunabhängige Überwachung zu erfolgen hat?			

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
G.8	*Wirksamkeit*: Findet eine prozessunabhängige Überwachung in angemessenen Zeitintervallen tatsächlich statt? Ist diese angemessen dokumentiert? Werden darüber Berichte an die Leitung gefertigt?			
G.9	Sind die erforderlichen Berichtswege für die Ergebnisse der Überwachungsmaßnahmen festgelegt?			
G.10	*Wirksamkeit*: Werden die Berichtswege für die Ergebnisse der Überwachungsmaßnahmen tatsächlich eingehalten?			
G.11	Ist festgelegt, wer Hinweise auf Regelverstöße prüft, welche Folgemaßnahmen bei Regelverstößen zu prüfen sind und wer für diese Prüfung und deren Umsetzung zuständig ist? ☞siehe auch H.	X		
G.12	*Wirksamkeit*: Werden die Vorgaben, wer Hinweise auf Regelverstöße prüft und wer für Folgemaßnahmen bei Regelverstößen zuständig ist, tatsächlich eingehalten? ☞siehe auch H.			
G.13	Ist geregelt, dass in den (Prüf-)Berichten zu Regelverstößen auch Maßnahmen zur Verbesserung entdeckter Schwachstellen im CMS oder Internen Kontrollsystem aufzuführen sind? Ist geregelt, dass der Compliance-Beauftragte an der Ausarbeitung von Verbesserungsmaßnahmen zum CMS zu beteiligen ist?			
G.14	*Wirksamkeit*: Werden in den (Prüf-)Berichten zu Regelverstößen auch Maßnahmen zur Verbesserung entdeckter Schwachstellen im CMS oder Internen Kontrollsystem aufgeführt? Werden diese vorgeschlagenen Verbesserungsmaßnahmen von den zuständigen Stellen auch umgesetzt? Wird der Compliance-Beauftragte an der Ausarbeitung der Verbesserungsmaßnahmen beteiligt?			
G.15	*Wirksamkeit*: Stehen beim Compliance-Beauftragten ausreichende Ressourcen für dessen Aufgaben bei der Überwachung und Verbesserung zur Verfügung?			
H. Vorhandensein eines internen Meldesystems (entsprechend der EU-Whistleblower-Richtlinie):				

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
H.1	Ist in der CMS-Beschreibung (z.B. CMS-Richtlinie) ein Hinweisgebersystem für Entgegennahme und Bearbeitung von Hinweisen auf Regelverstöße angemessen dargestellt?	X		
H.2	Ist festgelegt, für welche Hinweise das Hinweisgebersystem zuständig ist (sachlicher Anwendungsbereich)? Umfasst der sachliche Anwendungsbereich den gesetzlichen Mindestumfang nach HinSchG? Ist die Festlegung des sachlichen Anwendungsbereichs in Übereinstimmung mit den Compliance-Zielen?	X (sofern gesetzliche Pflicht)		
H.3	*Wirksamkeit*: Wird der sachliche Anwendungsbereich tatsächlich eingehalten?			
H.4	Ist festgelegt, für welchen Personenkreis das Hinweisgebersystem offensteht? Umfasst der zulässige Personenkreis den gesetzlichen Mindestumfang nach HinSchG? Ist die Festlegung des zulässigen Personenkreises in Übereinstimmung mit den Compliance-Zielen?	X (sofern gesetzliche Pflicht)		
H.5	*Wirksamkeit:* Steht das Hinweisgebersystem tatsächlich dem festgelegten Personenkreis offen? Haben alle Mitarbeiter (und ggf. die weiteren Zielgruppen) Zugang zur internen Meldekanälen?			
H.6	Ist in der Festlegung des Verfahrens des Hinweisgebersystems die Wahrung der Vertraulichkeit der Identität der hinweisgebenden Person mindestens im gesetzlichen Umfang nach dem HinSchG in geeigneter Weise sichergestellt?	X (sofern gesetzliche Pflicht)		
H.7	*Wirksamkeit*: Wird die Vertraulichkeit des Hinweisgebers tatsächlich durchgängig gewahrt? Ist die Vertraulichkeit auch technisch (bei eingesetzten IT-Verfahren) gesichert? Ist sichergestellt, dass nur das in der Meldestelle eingesetzte Personal Zugriff auf die Meldungen und deren Inhalt hat?			
H.8	Sind die Meldekanäle festgelegt? Werden dabei die gesetzlichen Mindestanforderungen an das HinSchG eingehalten?	X (sofern gesetzliche Pflicht)		

Nr.	Prüfungsfragen	X“ = Grundanforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
H.9	*Wirksamkeit*: Stehen die festgelegten Meldekanäle tatsächlich zur Verfügung? Ist die unverzügliche persönliche Zusammenkunft möglich?			
H.10	Ist ein geeignetes Verfahren zur Prüfung von Hinweisen und zum Ergreifen von Folgemaßnahmen festgelegt? Sind dort eindeutige Zuständigkeiten hinterlegt? Sind bei der Festlegung des Verfahrens die Regelungen bzw. Standards nach dem VerbSG (*derzeit liegt ein Gesetzentwurf vor*) eingehalten?	X		
H.11	*Wirksamkeit*: Werden das Verfahren und die Zuständigkeiten zur Prüfung von Hinweisen und zum Ergreifen von Folgemaßnahmen tatsächlich eingehalten?			
H.12	Ist die interne Meldestelle mit den notwendigen Befugnissen (zur Prüfung eingehender Hinweise und Ergreifung von Folgemaßnahmen) nach § 12 Abs. 4 HinSchG ausgestattet?	X (sofern gesetzliche Pflicht)		
H.13	Ist festgelegt, dass die interne Meldestelle den Informationspflichten nach HinSchG gegenüber den hinweisgebenden Personen nachkommt?	X (sofern gesetzliche Pflicht)		
H.14	*Wirksamkeit*: Kommt die interne Meldestelle den Informationspflichten (einschließlich der Fristen) nach HinSchG gegenüber den hinweisgebenden Personen tatsächlich nach? Gibt es interne Arbeitshilfen zur Erfüllung der Informationspflichten (Hinweiseingangsbestätigung und Folgemeldung)?			
H.15	Ist festgelegt, dass bei der internen Meldestelle eingehende Hinweise gem. § 11 HinSchG dokumentiert werden?	X (sofern gesetzliche Pflicht)		
H.16	*Wirksamkeit*: Werden bei der internen Meldestelle eingehende Hinweise tatsächlich gem. § 11 HinSchG dokumentiert? Gibt es interne Arbeitshilfen zur Sicherstellung der Anforderungen an die Dokumentation der Meldungen (Eingang und Bearbeitung)?			
H.17	Sind die Anforderungen an das Personal der internen Meldestelle festgelegt? Werden dabei auch die gesetzlichen Vorgaben nach § 15 HinSchG eingehalten? Ist vorgesehen,	X (sofern gesetzliche Pflicht)		

Nr.	Prüfungsfragen	X“ = Grund-anforderung“	Bewertung (Ergebnis der Prüfung) entsprechend festgelegter Skala (Stufe)	Prüfungshinweise, Erläuterungen, Empfehlungen
	dass das in der Meldestelle eingesetzt Personal regelmäßig geschult wird?			
H.18	*Wirksamkeit*: Werden die Anforderungen an das Personal der internen Meldestelle entsprechend den Festlegungen eingehalten? Gibt es ein Schulungskonzept für das in der Meldestelle eingesetzt Personal?			
H.19	Sind Maßnahmen zur Wiedergutmachung von Schäden festgelegt, die durch Meldungen oder Offenlegungen vorsätzlich oder grob fahrlässig falscher Hinweise entstanden sind (38 HinSchG)	X (sofern gesetzliche Pflicht)		
H.20	*Wirksamkeit*: Werden Maßnahmen zur Wiedergutmachung von Schäden, die durch Meldungen oder Offenlegungen vorsätzlich oder grob fahrlässig falscher Hinweise entstanden sind (§ 38 HinSchG), tatsächlich umgesetzt?			
H.21	Ist festgelegt, dass die Angemessenheit und Wirksamkeit des Hinweisgebersystems regelmäßig evaluiert wird?			
H.22	*Wirksamkeit*: Finden regelmäßige Evaluierungen des Hinweisgebersystems statt?			
H.13	*Wirksamkeit*: Wird die interne Meldestelle dem zulässigen Personenkreis angemessen bekanntgemacht? Sind Informationen zur internen Meldestelle leicht zugänglich und leicht verständlich? Wird aus den kommunizierten Informationen leicht verständlich deutlich, dass hinweisgebenden Personen keine Repressalien zu befürchten haben? Haben alle Beschäftigten (und ggf. die weiteren Zielgruppen) Zugang zu Information und Beratung über Abwehr-/ Unterstützungsmöglichkeiten bei drohenden / bereits eingetretenen Repressalien? Wird aus den kommunizierten Informationen leicht verständlich deutlich, welche Konsequenzen bewusste Falschmeldungen haben können?			
H.14	*Wirksamkeit:* Wird eine positive Haltung der Führungsspitze zu hinweisgebenden Personen und zur internen Meldestelle zum Ausdruck gebracht („tone at the top“)?			

9. Glossar

Anforderungsinventar (institutionelle Compliance-Risiken) [☞ Tz. 83]: Die identifizierten institutionellen Compliance-Risiken bzw. die korrespondierenden *institutionellen Compliance-Anforderungen* werden für die Kommune in Form eines *Anforderungsinventars* (☞ Anlage 2, Abschnitt 8.2) zusammengetragen. Sie lassen sich einzelnen oder mehreren Funktionen eines CMS (Prävention, Aufdeckung, Reaktion) zuordnen. Für jedes Risiko bzw. für jede Anforderung ist ein Verantwortlicher festzulegen. Dies alles ist zu dokumentieren.

Anforderungs-Maßnahmen-Matrix [☞ Tz. 84]: Nach der Risikobewertung wird das bei der Risikoidentifikation erstellte *Anforderungsinventar* um die vorhandenen und im Rahmen des zu erstellenden Compliance-Programms noch zu ergreifenden Maßnahmen zu einer *Anforderungs-Maßnahmen-Matrix* (☞ Anlage 3, Abschnitt 8.3) erweitert.

Antikorruptionsklauseln [☞ Tz. 59]: Vertragsklauseln, die bei Verletzung Vertragsstrafen bzw. Vertragskündigungen vorsehen.

Belehrung der Mitarbeitenden und Dritten [☞ Tz. 123]: *Belehrung* ist die Bestätigung der Mitarbeitenden oder ggf. Dritter, dass sie von den Compliance-Regeln der Kommune (u.a. dem Verhaltenskodex) Kenntnis genommen haben. Die Bestätigung erfolgt u.a. durch Unterschrift, Teilnahmelisten bei Schulungen oder Dienstbesprechungen, Zertifikate an teilgenommenen Online-Schulungen. Belehrungen sollten regelmäßig (z.B. jährlich) wiederholt werden. Eine besondere Form ist die förmliche Verpflichtung von Personen, die nicht Amtsträger sind und öffentliche Aufgaben wahrnehmen, nach dem *Verpflichtungsgesetz*, wonach diese Personen bei Verwirklichung von Amtsträger-Korruptionsstraftatbeständen strafrechtlich Amtsträgern gleichgestellt werden.

CMS-Beschreibung [☞ Tz. 53]: Eine CMS-Beschreibung ist eine zusammenfassende Darstellung der wesentlichen Aspekte des eingerichteten CMS durch die Leitung der Kommune; dies Beschreibung kann auch in der CMS-Richtlinie erfolgen.

CMS-Richtlinie (Dienstanweisung) [☞ Tz. 121]: Die organisatorische Eingliederung der Compliance-Aufgabe in die Gesamtorganisation sowie die zu beachtenden gesetzlichen und internen Vorgaben und die CMS-Grundelemente bilden den Rahmen für die zuzuweisenden Aufgaben und die einzurichtenden Abläufe bzw. Prozesse, die in eine CMS-Richtlinie (Dienstanweisung) aufzunehmen sind.

Compliance [☞ Tz. 29]: Die Verwaltungsorgane einer Kommune haben im Rahmen ihrer Zuständigkeit dafür Sorge zu tragen, dass alle formellen und materiellen Gesetze sowie alle verwaltungsinternen Regelungen eingehalten werden. Sie wirken auf deren wirksame Beachtung in der Kommune hin.

- ➢ Rechtlicher Rahmen für Compliance in der öffentlichen Verwaltung [☞ Tz 35 ff.]

Compliance-Beauftragter [☞ Tz. 107 ff.]: Person, die in der Kommune mit der Compliance-Funktion bzw. dem Aufbau und dem Betrieb eines CMS zur Umsetzung der festgelegten Compliance-Ziele betraut ist. Zur Compliance-Funktion gehören – entsprechend den drei Säulen eines CMS – Aufgaben der Prävention, der Aufdeckung und der Reaktion.

- ➢ Aufgaben [☞ Tz. 108 ff.]
- ➢ Qualifikation / Kompetenzen [☞ Tz. 112 ff.]
- ➢ Rechte und Befugnisse [☞ Tz. 111]
- ➢ Ressourcenausstattung [☞ Tz. 117 ff.]

Compliance-Kommunikation [☞ Tz. 122]: Die Compliance-Kommunikation dient der adressatenorientierten Information aller Akteure eines CMS. Eine wirksame Compliance-Kommunikation besteht mindestens aus den folgenden fünf Elementen: 1.) Information, Belehrung, Sensibilisierung, Beratung und Aus- und Fortbildung der Mitarbeitenden und ggf. Dritten; 2.) Information (potenzieller) Hinweisgeber; 3.) Information der Bürger und Presse (öffentliche Kommunikation); 4.) interne Compliance-Berichterstattung; 5) Kommunikation mit externen Stellen (u.a. Strafverfolgungsbehörden, externen Meldestellen nach dem Hinweisgeberschutzgesetz, beauftragten Rechtsanwälten).

- ➢ Elemente [☞ Tz. 122 ff.]
- ➢ Berichtspflichten [☞Tz. 126]

Compliance-Kultur [☞ Tz. 54]: Gegenstand der Compliance-Kultur - als Teil der bestehenden Organisations- bzw. Unternehmenskultur – ist die Bedeutung, die der Beachtung von Normen, Regelungen und Werten in der Organisation entgegengebracht wird. Herrscht eine „gute" Compliance-Kultur, sind die Mitarbeitenden in hohem Maße intrinsisch motiviert, sich regelkonform zu verhalten bzw. gegenüber Regelverstößen nicht tolerant zu sein.

Compliance Management System – CMS (☞ Tz. 31): Unter einem CMS werden – in Anlehnung an IDW PS 980 – für diesen Prüfungsleitfaden die Gesamtheit aller Regelungen (hinsichtlich Strukturen, Prozesse und Maßnahmen) der Kommune verstanden, die darauf abzielen bzw. sicherstellen sollen, dass die Akteure der Kommune regelkonform handeln und damit wesentliche Regelverstöße verhindert werden (Verwaltungssystem zur Regeleinhaltung). Akteure der Kommune sind: ihre gesetzliche Vertretung wie (Ober-)Bürgermeister, Landrat etc.; ihre Mitarbeitenden; Mitglieder der kommunalen Volksvertretung; Dritte, bei deren Beauftragung von der Kommune Sorgfaltspflichten zu erfüllen sind (u.a. Verwaltungshelfer, Lieferanten); Dritte, die von der Kommune als Zuwendungsgeberin freiwillige zweckgebundene Leistungen erhalten.

- ➢ Ausgestaltung für Kommunen [☞ Tz. 42 ff.]

- ➢ Funktionen (Säulen) eines CMS [☞ Tz. 34]
- ➢ Projekt zur Einrichtung [☞ Tz. 46 ff.]

Compliance-Organisation [☞ Tz. 103]: Die Organisation des CMS umfasst: a.) die verbindliche Festlegung der *Aufbau- und Ablauforganisation* des CMS als integraler Bestandteil der Behördenorganisation; b.) die verbindliche Festlegung der Aufgaben, Rollen und Verantwortlichkeiten im CMS; Bestellung des Compliance-Beauftragten und von Ansprechpersonen für Teilbereiche; c.) die der Compliance-Funktion zugeordneten Mitarbeitenden haben die notwendige Unabhängigkeit, Kompetenz und organisatorische Stellung für eine wirksame Wahrnehmung ihrer Rollen; d.) die Bereitstellung der erforderlichen personellen, technischen (v.a. Hard- und Software) und finanziellen Ressourcen.

Compliance-Programm [☞ Tz. 92]: Auf der Grundlage der Ergebnisse der Compliance-Risikoanalyse sind Maßnahmen einzuführen, die auf die Begrenzung der Compliance-Risiken und damit auf die Vermeidung von Regelverstößen ausgerichtet sind. Des Weiteren sind die bei Compliance-Verstößen zu ergreifenden Maßnahmen festzulegen. Die Maßnahmen ergeben sich aus den Anforderungen aller CMS-Grundelemente bzw. entsprechend der Unterscheidung bei der Compliance-Risikoanalyse aus den für alle Kommunen gleichen *institutionellen* Anforderungen und den konkreten *prozessbezogenen* Compliance-Risiken. Das Compliance-Programm stellt die Gesamtheit aller dieser Maßnahmen dar.

- ➢ Anforderungen [☞ Tz. 94 ff.]
- ➢ Maßnahmen [☞ Tz. 100 ff.]

Compliance-Risiken [☞ Tz. 78]: Compliance-Risiken stellen die bewertete Gefahr bzw. Möglichkeit dar, gegen einzuhaltende Regeln zu verstoßen und damit die festgelegten Compliance-Ziele zu verfehlen. Bezogen auf die einzelnen Compliance-Ziele (insbesondere die dem CMS unterliegenden Teilbereiche) sind anhand einer Compliance-Risikoanalyse die Compliance-Risiken zu identifizieren und zu bewerten. Die Risikobewertung dient als Grundlage für die Ausgestaltung und Festlegung des Compliance-Programms.

- ➢ Analyse der institutionellen Compliance-Risiken [☞ Tz. 81]
- ➢ Analyse der prozessbezogenen Compliance-Risiken [☞ Tz. 85]
- ➢ Risikobewertung, institutionelle Risiken [☞ Tz. 84]
- ➢ Risikobewertung, prozessbezogene Risiken [☞ Tz. 88]
- ➢ Risikoidentifizierung, institutionelle Compliance-Risiken [☞ Tz. 81 ff.]
- ➢ Risikoidentifizierung, prozessbezogene Compliance-Risiken [☞ Tz. 85 ff.]
- ➢ Risikoinventar [☞ Tz. 87]
- ➢ Risiko-Kontroll-Matrix [☞ Tz. 88]
- ➢ Risikomatrix (Risikolandkarte) [☞ Tz. 88]

Compliance-Überwachung und -Verbesserung [☞ Tz. 129 f.]: Es sind Verfahren bzw. Maßnahmen einzuführen, die Angemessenheit und Wirksamkeit des CMS systematisch überwachen und verbessern. Den entsprechenden Rollen für die Überwachung und Verbesserung liegt das *Drei-Linien-Modell* des Institute of Internal Auditors (IIA) zugrunde. Die Compliance-Überwachung und -Verbesserung dient den CMS-Funktionen Aufdeckung und Reaktion. Eine wirksame Compliance-Überwachung und -Verbesserung wirkt auch präventiv.

- ➢ Reaktion auf Regelverstöße [☞ Tz. 135]
- ➢ Überwachung [☞ Tz. 131 ff.]
- ➢ Verbesserung [☞ Tz. 136 ff.]

Compliance-Verantwortung, persönliche [☞ Tz. 41]: Aus den Zuständigkeitsregelungen folgt, dass der gesetzliche Vertreter der Kommune (Bürgermeister, Landrat etc.) als Leiter der Verwaltung aufgrund seiner Gesamtverantwortung für die Einhaltung der Legalitätspflicht (Legalitätskontrollpflicht) in der Kommunalverwaltung für die Einrichtung und Ausgestaltung einer Compliance-Organisation verantwortlich ist. Ebenso hat er als Dienstvorgesetzter die erforderlichen Schritte einzuleiten, wenn ihm eine Verfehlung oder Unregelmäßigkeit zur Kenntnis gelangt. Die Verwaltungsleitung kann Compliance-Aufgaben auf Bedienstete (Compliance-Beauftragter, ☞ Tz. 107 ff.) übertragen, wozu eine ordnungsgemäße Delegation erforderlich ist. In einem solchen Fall besteht bei einer Pflichtverletzung für diese Personen unter Berücksichtigung der Grundsätze der Arbeitnehmer- oder Beamtenhaftung das Risiko einer Regresspflicht.

Compliance-Ziele [☞ Tz. 68 ff.]: Mit den Compliance-Zielen wird festgelegt, was mit dem CMS erreicht werden soll. Die Compliance-Ziele ergeben sich aus den folgenden Fragestellungen: 1.) Welche strategischen Ziele verfolgt die Kommune? 2.) Welche *Teilbereiche* (siehe dort) dieser Institution sollen vom CMS abgedeckt werden (Teilbereichsziele)?

Dezentrale Ansprechpersonen für Compliance [☞ Tz. 115]: Bei größeren Kommunen kann es für eine wirksame Compliance-Organisation sinnvoll sein, Ansprechpersonen für Compliance in dezentralen Organisationseinheiten zu haben. Sie arbeiten dem Compliance-Beauftragten zu, unterstützen ihn und stimmen sich mit ihm ab. Zu den Aufgaben solcher dezentralen Ansprechpersonen für Compliance können gehören: Unterstützung bei der Organisation von Schulungen; erste Anlauflaufstelle bei Fragen zur Compliance im jeweiligen Teilbereich bzw. in der jeweiligen Organisations-Einheit (z. B. beim Umgang mit angebotenen Vorteilen); Unterstützung des Compliance-Beauftragten bei internen Ermittlungen.

Dokumentation des CMS, Pflicht [☞ Tz. 53]: Die Einrichtung und der Betrieb eines CMS mit seinen Grundelementen ist vollständig, für einen objektiven sachverständigen Dritten nachvollziehbar und revisionssicher zu dokumentieren. Die Dokumentation hat die Regelungen der Strukturen (Aufbauorganisation), Prozesse und Maßnahmen, die konkreten Umsetzungshandlungen sowie die jeweils verantwortlichen Personen zu enthalten. Zur CMS-Dokumentation gehören v.a.: 1.) eine CMS-Beschreibung der Leitung der Kommune als zusammenfassende Darstellung der wesentlichen Aspekte des eingerichteten CMS (dies kann auch in Form einer Dienstanweisung Compliance geschehen); 2.) die CMS-relevanten Regelungen der Kommune (u.a. Dienstanweisungen, Zuständigkeitsregelungen, Regelungen zur Aufbauorganisation); 3.) Beschreibungen bzw. Visualisierungen der CMS-Prozesse; 4.) Dokumente zur organisatorischen und prozessualen Ausgestaltung von Compliance-Maßnahmen und deren Umsetzung (u.a. Berichte, Protokolle, Anforderungs-Maßnahmen-Matrix, Risiko-Kontroll-Matrix, Checklisten, Konzepte).

Drei-Linien-Modell [☞ Tz. 129]: Nach dem Drei-Linien-Modell (des Institute of Internal Auditors - IAA) obliegt: 1.) der Leitung und der ersten Linie (v.a. Fach- und Querschnittsämter), Compliance-Maßnahmen (einschließlich prozessintegrierter Kontrollen – Internes Kontrollsystem) umzusetzen; 2.) der zweiten Linie (Beauftragte für bestimmte Bereiche), wozu auch der *Compliance-Beauftragte* gehört, die erste Linie durch Festlegung von Anforderungen, Beratung und Überwachung der Funktionsfähigkeit der Compliance-Maßnahmen zu unterstützen; 3.) der dritten Linie (u.a. die Interne Revision) die prozessunabhängige Überwachung.

Ehrenkodex (Ehrenordnung) für kommunale Vertretungen [☞ Tz. 59]: Mit dem Ehrenkodex bekennen sich die Mandatsträger zu ihrer Verantwortung, das Mandat uneigennützig und zum Wohle der Kommune auszuüben. Nach derzeitiger Rechtslage können solche Ehrenkodexe nur als freiwillige Verpflichtung der Mitglieder des Vertretungsorgans von diesem beschlossen werden; Sanktionierungen bei Verstößen sind nicht möglich.

Geschäftspartnerkodex [☞ Tz. 59]: Ein solcher Kodex legt verbindliche Verhaltensgrundsätze für die Geschäftspartner und ihre Mitarbeitenden fest. Die Befolgung des Verhaltenskodex sollte schriftlich vom Geschäftspartner erklärt bzw. vertraglich vereinbart werden.

Grundelemente eines CMS [☞ Tz. 50]: In Anlehnung an Ziffer 23 des IDW PS 980 (Ziffer 27 des IDW EPS 980 - Entwurf) sollte jedes CMS die folgenden sieben Grundelemente in die Struktur und Abläufe der Organisation einbinden: *Compliance-Kultur, Compliance-Ziele, Compliance-Risiken, Compliance-Programm, Compliance-Organisation, Compliance-Kommunikation sowie Compliance-Überwachung und Verbesserung.*

Hinweisgeberschutzgesetz [☞ Tz. 37, Tz 153. ff.]: Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (HinSchG) – vgl. Deutscher Bundestag, Drucksache 20/6700 vom 09.05.2023, Drucksache 20/5992 vom 14.03.2023, Drucksache 20/4909 vom 14.12.2022. Das HinSchG ist die nationale Umsetzung der *EU-Whistleblower-Richtlinie*.

Hinweisgebersystem [Tz. 153 ff.]: Zweck eines Hinweisgebersystems ist es, Mitarbeitern oder anderen potentiellen Hinweisgebern über Einrichtung von *Meldestellen* einen vertraulichen Kommunikationskanal (Meldekanal) zu eröffnen, um Missstände oder Unregelmäßigkeiten melden zu können. Seit dem Erlass der *Whistleblower-Richtlinie* durch die Europäische Union gibt es verbindliche Vorgaben für die Einrichtung eines solchen Hinweisgebersystems, welche durch die EU-Mitgliedstaaten umzusetzen sind. Die nationale Umsetzung in Deutschland erfolgt durch das *Hinweisgeberschutzgesetz*.

Integritätsaspekte bei Personalauswahl und -entwicklung [☞ Tz. 60]: Bei der Personalauswahl sollte auf die Integrität der Bewerber geachtet werden. Um über die persönliche Einstellung eines Bewerbers ein belastbares Bild zu erhalten, kann eine Organisation auf das Instrument eines professionellen Integritäts-Tests zurückgreifen. Alternativ können den Bewerbern im Personalauswahlgespräch Fragen mit Compliance-Bezug gestellt werden. Des Weiteren sollten bei der Personalauswahl bekannt gewordene Auffälligkeiten berücksichtigt werden

Interessenkonflikte, Vermeidung [☞ Tz. 62]: Ein Interessenkonflikt ist nach der OECD „ein Konflikt zwischen den Amtspflichten und den Privatinteressen eines öffentlichen Bediensteten, bei dem die Interessen, die ein öffentlicher Bediensteter in seiner Eigenschaft als Privatperson hat, die Wahrnehmung seiner amtlichen Pflichten und Verantwortlichkeiten auf unbillige Weise beeinflussen können" (OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung): OECD-Leitlinien für die Behandlung von Interessenkonflikten im öffentlichen Dienst, 2006, S. 8.). Zur Vermeidung von Interessenkonflikten sind die gesetzlichen Regelungen zu Befangenheit und Hinderungsgründen (v.a. Verwaltungsverfahrensrecht, Kommunalrecht), zu Nebentätigkeiten (Arbeits- und Dienstrecht) und zum Verbot der Annahme von Vorteilen (Straf-, Arbeits- und Dienstrecht) zu beachten. Spenden, Sponsoring und sonstige Zuwendungen sind im Hinblick auf mögliche Interessenkonflikte zu prüfen und transparent zu machen. Die Vorgesetzten haben diesbezüglich ihrer Kontrollpflicht nachzukommen.

Interne Ermittlungen (Untersuchungen) (☞ Tz. 159 e): Fällt ein gemeldeter Regelverstoß in den sachlichen Anwendungsbereich der internen Meldestelle und ist stichhaltig (plausibel), so ist bei hinreichenden Verdacht auf Compliance-Verstöße als Folgemaßnahme

die Durchführung interner Ermittlungen in Betracht zu ziehen. Für solche internen Ermittlungen sollte ein Verfahren eingerichtet werden, dass Unparteilichkeit sicherstellt, von qualifiziertem Personal durchgeführt wird und weitere Standards eines fairen Verfahrens berücksichtigt (vgl. Nr. 8.4.1 der ISO 37002) sowie weitere gesetzliche Regelungen und Standards einhält (vgl. § 17 RegE Gesetz zur Stärkung der Integrität in der Wirtschaft - Verbandssanktionengesetz).

Internes Kontrollsystem [☞ Tz. 102]: Ein Internes Kontrollsystem besteht aus systematisch gestalteten organisatorischen (Sicherungs-) Maßnahmen und Kontrollen in der Kommune zur Einhaltung von Richtlinien und zur Abwehr von Schäden, die durch das eigene Personal oder böswillige Dritte verursacht werden können. Die Maßnahmen beruhen auf technischen und organisatorischen Prinzipien. Ein Internes Kontrollsystem dient sowohl der Verhinderung als auch der Aufdeckung von Regelverstößen.

Meldestellen, interne [☞ Tz. 156]: Nach Art. 8 Abs. 1 i. V. m. Abs. 9 Satz 1 und 2 WBRL sind alle Kommunen verpflichtet, bei sich interne Meldestellen zur Mitteilung von Informationen über Regelverstöße (Hinweise) und Verfahren für Folgemaßnahmen einzurichten und zu betreiben, sofern der deutsche Gesetzgeber diese Verpflichtung nicht auf Gemeinden ab 10.000 Einwohner bzw. ab 50 Arbeitnehmer begrenzt.

- ➢ Anforderungen [☞ Tz. 159]
- ➢ Bekanntmachung der Meldestelle [☞ Tz. 159]
- ➢ Dokumentationspflicht [☞ Tz. 159]
- ➢ Einrichtungspflicht für Kommunen [☞ Tz. 156]
- ➢ Informationspflichten [☞ Tz. 159]
- ➢ Vertraulichkeit [☞ Tz. 159]

Meldestellen, externe [☞ Tz. 159, Buchtstabe j]: §§ 19 HinSchG sehen die Einrichtung mehrere externer Meldestellen vor. Danach sind obligatorische Meldestellen beim Bund: Bundesamt für Justiz (vgl. Verordnung über die Organisation der nach dem Hinweisgeberschutzgesetz einzurichtenden externen Meldestelle des Bundes [Hinweisgeberschutzgesetz-Externe-Meldestelle-des-Bundes-Verordnung – HEMBV] vom 7. August 2023), Bundesamt für Finanzdienstleistungsaufsicht (BaFin), Bundeskartellamt. Die Länder können eigene externe Meldestellen einrichten.

Prüfung des CMS [☞ Tz. 161 ff.]: Die Prüfung eines CMS ist eine Systemprüfung. Sie ist nicht darauf ausgerichtet, einzelne Regelverstöße zu erkennen und kann daher auch keine Prüfungssicherheit über die tatsächliche Einhaltung von Regeln geben. Gegenstand bzw. Ausgangspunkt der Prüfung sind die Aussagen zum eingerichteten CMS in der *CMS-Beschreibung*. Es wird hinsichtlich der Prüfungsarten zwischen *Angemessenheitsprüfung* und *Wirksamkeitsprüfung* unterschieden. Eine Angemessenheitsprüfung

kann bereits begleitend zur Einrichtung eines CMS durchgeführt werden; eine Wirksamkeitsprüfung setzt hingegen voraus, dass das eingerichtete CMS bereits für einen bestimmten Zeitraum, der für ein sicheres Prüfungsurteil erforderlich ist, in der Kommune umgesetzt worden ist.

- Angemessenheitsprüfung [☞ Tz. 164]
- Maßnahmenverfolgung [☞ Tz. 185]
- Prüfungsarten [☞ Tz. 163]
- Prüfungsbericht [☞ Tz. 182]
- Prüfungshemmnis [☞ Tz. 183]
- Prüfungsplanung und -durchführung [☞ Tz. 174 ff.]
- Prüfungsurteil [☞ Tz. 183]
- Prüfungsvoraussetzungen [☞ Tz. 172 f.]
- Wesentlichkeit [☞ Tz. 167 ff.]
- Wirksamkeitsprüfung [☞ Tz. 165]

Rotation [☞ Tz. 65]: Durch jahrelang unveränderte dienstliche Verwendungen auf einem Dienstposten können Verbindungen entstehen, die Regelverstöße begünstigen. Der Wechsel von Mitarbeitenden auf andere Dienstposten (Personalrotation) sowie die Umressortierung besonders korruptionsgefährdeter Aufgaben zu einem anderen Dienstposten (Aufgabenrotation) kann dem Entstehen solcher Verbindungen entgegenwirken.

Säulen eines CMS [☞ Tz. 34]: Die drei Funktionen eines CMS - Prävention, Aufdeckung und Reaktion – können als die drei Säulen eines CMS bezeichnet werden.

Sensibilisierung [☞ Tz. 123]: Sensibilisierung der Mitarbeitenden oder ggf. von Dritten in Bezug auf Gefahren für Regelverstöße, die aus bestimmten Situationen entstehen können, durch Schulungen, Informationsmaterial oder auf Dienstbesprechungen, Workshops u.ä., mit dem Ziel, das Verhalten der Akteure im Sinne eines regelkonformen Verhaltens zu beeinflussen.

Tax Compliance Management System (TCMS) (☞ Tz. 139 ff.)*:* Unter einem TCMS ist ein klar abgegrenzter Teilbereich eines CMS zu verstehen, dessen Zweck die vollständige und zeitgerechte Erfüllung steuerlicher Pflichten ist. Auch ein TCMS umfasst die sieben Grundelemente eines CMS.

Teilbereiche eines CMS [☞ Tz. 33]: Ein CMS umfasst in der Regel mehrere nach Rechtsgebieten (und ggf. darunter nach einzelnen Organisationseinheiten) abgrenzbare Teilbereiche, für die eine Analyse der jeweiligen *Compliance-Risiken* durchzuführen ist.

Tone at the top (tone from the top), tone from the middle [☞ Tz. 58]: Die *Compliance-Kultur* wird maßgeblich geprägt durch die Grundeinstellungen und Verhaltensweisen der

Leitung und oberen Führungskräfte („tone at the top") sowie der mittleren Führungsebene („tone from the middle".[151] Hierbei geht es um ein eindeutiges Bekenntnis der Leitung zur Compliance in Wort und im Handeln, dass allen Führungskräften und Mitarbeitenden stetig zu vermitteln ist. Für die Vermittlung des Bekenntnisses sind Maßnahmen der *Compliance-Kommunikation* anzuwenden. Alle Führungskräfte müssen ihre Vorbildfunktion für rechtskonformes und integres Verhalten verinnerlicht haben.

Verbandssanktionengesetz (VerSanG) [☞ Tz. 37]: Das Verbandssanktionengesetz (Gesetz zur Stärkung der Integrität in der Wirtschaft) soll die Verhängung von Sanktionen gegen einen Verband ermöglichen. Voraussetzung hierfür ist eine Straftat, die aus einem Verband (juristische Personen und Personenvereinigungen) heraus begangen wurde (umfasst auch Gebietskörperschaften und sonstige öffentlich-rechtliche Personen, sofern sie wirtschaftlich (nicht hoheitlich) tätig sind). Bisher kann nach geltendem Recht der Verband lediglich mit einer Geldbuße nach dem OWiG geahndet werden. Nach dem ursprünglichen, inzwischen nicht weiter verfolgten Gesetzesentwurf (RegE: Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft, Stand 16.06.2020 (abrufbar unter: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Staerkung_Integritaet_Wirtschaft.html) war eine Sanktionierung u.a. vorgesehen, wenn eine Leitungsperson im Rahmen der Wahrnehmung der Angelegenheiten des Verbands eine Straftat begangen hat, durch die verbandsbezogene Pflichten verletzt worden sind oder durch die der Verband bereichert wurde oder werden sollte.

Verhaltenskodex (Compliance-Kodex) [☞ Tz. 59]: Ziel eines Verhaltenskodex ist es, verbindliche Verhaltensstandards festzulegen, um Verstöße gegen Normen (rechtliche Rahmenbedingungen wie formelle und materielle Gesetze, Regelungen, Richtlinien u. s. w.) und Werte der Organisation vorzubeugen. Solche Verhaltenskodexe sollten zielgruppenorientiert aufgesetzt werden. *Verhaltenskodex für alle Mitarbeitenden der Kommune*: In der öffentlichen Verwaltung sind in unterschiedlichen Gesetzen und kommunalinternen Anweisungen bereits zahlreiche Verhaltensnormen festgelegt (u.a. Arbeits-, Beamtenrecht, Vergaberecht, Haushalts- und Kassenrecht), sodass im Verhaltenskodex auf sie zu verweisen ist. Weitere Verhaltensnormen können aufgenommen werden. Insbesondere sollte auch die Pflicht aller Mitarbeitenden aufgenommen werden, konkrete Verdachtsmomente zu melden. Entsprechend sollten auch Meldewege (Meldekanäle) von Regelverstößen bzw. von Verdachtsfällen angegeben werden. Der Verhaltenskodex sollte sprachlich einfach bzw. auch für Nichtjuristen verständlich formuliert werden. Die

[151] Vgl. IDW PS 980, Tz 23.

Mitarbeitenden sind auf den Verhaltenskodex und seine Verbindlichkeit bei Einstellung und danach regelmäßig zu belehren. Die Belehrung ist zu dokumentieren.

Verpflichtungsgesetzt [☞ Tz. 59, 123]: Personen, die nicht Amtsträger sind und öffentliche Aufgaben wahrnehmen, sollten nach dem Verpflichtungsgesetz förmlich verpflichtet werden, wonach diese Personen bei Verwirklichung von Amtsträger-Korruptionsstraftatbeständen strafrechtlich Amtsträgern gleichgestellt werden.

Whistleblower-Richtlinie (WBRL) [☞ Tz. 153]: Seit dem Erlass der sogenannte *„Whistleblower-Richtlinie*" (im Folgenden „WBRL") durch die Europäische Union (RICHTLINIE (EU) 2019/1937 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, abrufbar im Internet: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L1937&from=DE) gibt es verbindliche Vorgaben für die Einrichtung eines solchen Hinweisgebersystems, welche durch die EU-Mitgliedstaaten umzusetzen sind. Die WBRL dient einem besseren Schutz von Hinweisgebern, die in ihrem beruflichen Kontext Informationen über Verstöße gegen Unionsrecht melden.

10. Literaturverzeichnis

BeckOK Grundgesetz (Beck'scher Online-Kommentar Grundgesetz, Hrsg.: Epping, Volker / Hillgruber, Christian), 47. Edition Stand: 15.11.2021.

BeckOK Kommunalrecht BW (Beck'scher Online-Kommentar Kommunalrecht Baden-Württemberg, Hrsg.: Dietlein, Johannes / Pautsch, Arne), 16. Edition Stand: 01.01.2022.

BeckRS: Rechtsprechungsdatenbank in beck-online.

Bürkle, Jürgen / Hauschka, Christoph E. et al.: Der Compliance Officer, 1. Auflage 2015.

DCGK (2022): Deutscher Corporate Governance Kodex (DCGK) vom 28.04.2022; jeweils aktuelle Fassung: https://www.dcgk.de/de/kodex.html.

Deutscher Städtetag: Tax Compliance in Kommunen - Leitfaden des Deutschen Städtetages für den Aufbau eines Internen Kontrollsystems für Steuern, Stand: 26.04.2017.

Deutsches Institut für Interne Revision e. V. (DIIR), Institut für Interne Revision Österreich (IIA Austria), Schweizerischer Verband für Interne Revision (IIA Switzerland) als Herausgeber der deutschen Auflage der International Professional Practices Framework (IPPF): Internationale Standards für die berufliche Praxis der Internen Revision 2017, Version 6.1 vom 10. Januar 2018, Frankfurt am Main.

Deutsches Institut für Interne Revision e. V. (DIIR) - DIIR-Arbeitskreis „Interne Revision in gesetzlichen Kranken- und Pflegeversicherungen", hier: Checkliste zur Prüfung des Compliance Management Systems in der gesetzlichen Kranken- und Pflegeversicherung, Stand 01.10.2020, im Internet abrufbar: https://www.diir.de/arbeitskreise/interne-revision-in-gesetzlichen-kranken-und-pflegeversicherungen/aufgaben-und-ziele/.

DICO (Deutsches Institut für Compliance): Compliance-Management-Systeme – Übergreifender Standard der DICO-Standard-Reihe, März 2021.

DICO (Deutsches Institut für Compliance): DICO-Studie „Interne Untersuchungen in Deutschland – 2022" vom Arbeitskreis Interne Untersuchungen & Hinweisgebersysteme.

D-PCGM (2022): Deutscher Public Corporate Governance-Musterkodex (D-PCGM), Hrsg. Ulf Papenfuß/Klaus-Michael Ahrend/Kristin Wagner-Krechlok, in der Fassung vom 14.03.2022, https://doi.org/10.13140/RG.2.2.14710.47688.

Eckert, Tilmann / Deters, Heike: Praxiswissen Compliance, 2. Auflage 2018.

Haag, Oliver / Bindschädel Hannah: Das idealtypische Compliance Risk Assessment – Teil 2, in: Compliance-Berater 4/2021

Hauschka, Christoph E. / Moosmayer, Klaus / Lösler, Thomas (Hrsg.): Corporate Compliance, 3. Auflage 2016.

Hülsberg, Frank / Fassbach, Burkhard: Die Versicherbarkeit von Compliance-Risiken im Lichte der strengen Organhaftung. Überlegungen aus Sicht der Beratungspraxis, in: Wirtschaftsprüfung (WPg) 08.2023, S.479-488.

IDR Prüfungsleitlinie L 111 „Die IKS-Prüfung in der Rechnungsprüfung", Stand 29.11.2018.

IDW Praxishinweis 1/2016: Ausgestaltung und Prüfung eines Tax Compliance Management Systems gemäß IDW PS 980, Stand: 31.05.2017.

IDW (Hrsg.): Praxisleitfaden Governance, Risk und Compliance - Ausgewählte Fachbeiträge zur Einrichtung und Prüfung von Corporate-Governance-Systemen; Düsseldorf 2017.

IDW PS 980 (IDW EPS 980): Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen, Stand 11.03.2011 (Entwurf einer Neufassung als IDW EPS 980, Stand 28.10.2021).

Institute of Internal Auditors (IIA), Das Drei Linien Modell des IIA, Juli 2020 (Deutsche Übersetzung durch den DIIR).

ISO 37301: Compliance management systems – Requirements with guidance for use, 13.04.2021 (Nachfolger der ISO 196000).

ISO 37002: Whistleblowing Management Systems – Guidelines (First Edition 2021-07-27).

Konstanz Institut für Corporate Governance (KICG) der Hochschule Konstanz Technik, Wirtschaft und Gestaltung: Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen – KICG CMS-Leitlinie 2 2014 für Unternehmen mit 250 bis 3.000 Mitarbeitern, Stand 04/2014.

Kunze / Bronner /Katz, Alfred et al.: Gemeindeordnung für Baden-Württemberg – Kommentar, Loseblattsammlung, Stand: 30. Lieferung April 2020.

Louis, Jürgen / Glinder, Peter /Waßmer, Martin Paul (Hrsg.): Korruptionsprävention in der öffentlichen Verwaltung – Handbuch für die kommunale Praxis, Stuttgart 2020.

Moosmayer, Klaus: Compliance Praxisleitfaden für Unternehmen, 4. Auflage 2021.

PWC (Hrsg.): Öffentlich-rechtliche Unternehmen der Gemeinden – Länderübergreifende Darstellung, 6. Überarbeitete Auflage, Stuttgart, 2015.

Ruhmannseder, Felix / Behr, Nicolai / Krakow, Georg: Hinweisgebersysteme. Implementierung in Deutschland, Österreich und der Schweiz. 2. Auflage. Heidelberg 2021.

Sachs, Michael (Hrsg.), Grundgesetz GG - Kommentar, 9. Auflage 2021.

Schmigale, Jenny: Compliance Management, Herangehensweise an das Compliance-Risikomanagement, in: https://www.compliance-manager.net/fachartikel/herangehensweisen-das-compliance-risikomanagement-1774965701 (abgerufen am 03.02.2022).

Schoch, Friedrich / Schneider, Jens-Peter (Hrsg.): Verwaltungsverfahrensgesetz, Loseblattsammlung.

Süßmann, Joshua: Die strafrechtliche Haftung kommunaler Amtsträgerinnen und Amtsträger in Baden-Württemberg für Sicherungs- und Überwachungspflichten aus einer Garantenstellung, Bachelorarbeit zur Erlangung des Grades eines Bachelor of Arts (B.A.) im Studiengang gehobener Verwaltungsdienst – Public Management der Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg, September 2021.

Stober, Rolf / Ohrtmann, Nicola (Hrsg.): Compliance, Handbuch für die öffentliche Verwaltung, 2. Auflage 2022.

Transpareny International Deutschland e.V.: Muster eines Verhaltenskodexes für kommunale Mandatsträger*innen, November 2022, https://148262.seu2.cleverreach.com/c/78456107/6c387b7e60c7-rmsggl

Wilmers, Burkhard Wolf / Fahr, Réne: Behavioral Compliance in der Unternehmenspraxis, in: ComplianceBusiness, Ausgabe 4, November 2017, S. 6 – 9.