



Sophia Steinle



Hannah Müller

Revision 4.0

Compliance-Management-Systeme in KMU – Eine strukturierte Handlungshilfe auf Basis der DIN SPEC 91524

1 Einleitung

Kleine und mittlere Unternehmen (KMU) sehen sich in den vergangenen Jahren einer erheblich verdichteten regulatorischen Landschaft ausgesetzt. Während Compliance-Systeme lange Zeit primär als Instrumente für Großunternehmen und Konzerne galten, hat sich das Risikoprofil mittelständischer Unternehmen signifikant verändert. Nationale und europäische Gesetzgebung, verschärfte Bußgeldregime – etwa im Zuge der EU-Datenschutz-Grundverordnung (EU-DSGVO¹) – zunehmende Haftungsdurchgriffsmöglichkeiten sowie die Ausweitung unternehmerischer Sorgfaltspflichten führen dazu, dass auch KMU faktisch denselben materiellen Anforderungen unterliegen wie größere Marktteilnehmer.

Parallel hierzu verschärft sich die haftungsrechtliche Erwartungshaltung. Die Rechtsprechung verlangt zunehmend eine nachweisbare, dokumentierte Compliance-Organisation als Ausprägung der unternehmerischen Organisationspflicht. Eine bloß informelle „Kultur der Rechtstreue“ genügt nicht mehr. Vielmehr wird erwartet, dass Unternehmen ihre Risikosteuerung strukturell verankern, Zuständigkeiten definieren, Kontrollmechanismen implementieren und ihre Maßnahmen dokumentieren können.²

Für KMU bestehen zentrale Herausforderungen in begrenzten Ressourcen, personellen Abhängigkeiten und fehlender Systematik, da Compliance-Maßnahmen häufig nicht als integriertes Managementsystem ausgestaltet sind.

¹ VO (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), ABl. L 119 vom 4.5.2016

² BGH, Urt. v. 27.4.2022 – 5 StR 278/21; OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19.

Dieser Beitrag verfolgt das Ziel, die Inhalte der DIN SPEC 91524³ in eine systematische, praxisorientierte und unmittelbar umsetzbare Handlungshilfe für KMU zu überführen. Im Mittelpunkt steht die Frage, wie ein angemessenes, verhältnismäßiges und wirksames Compliance-System implementiert werden kann – nicht als bürokratische Last, sondern als strategisches Steuerungsinstrument zur nachhaltigen Sicherung und Weiterentwicklung des Unternehmens.

2 Überblick über das Implementierungskonzept

Die Implementierung eines Compliance-Management-Systems (CMS) in KMU folgt einem klar strukturierten, aber bewusst schlanken Grundmodell. Die einschlägige Literatur (u. a. DIN ISO 37301, IDW PS 980, ISO 31000) betont übereinstimmend, dass ein CMS risikoorientiert, verhältnismäßig und an Größe, Komplexität des Geschäftsmodells sowie Gefährdungspotenzial des Unternehmens angepasst sein muss. Für KMU bedeutet dies: kein komplexes Konzernsystem, sondern ein funktionsfähiger Minimalstandard.^{4 5}

Dieser Ansatz lässt sich auf vier Kernelemente reduzieren:

2.1 Klare Verantwortlichkeit auf Leitungsebene.

Die Geschäftsleitung übernimmt sichtbar Verantwortung („Tone from the Top“) und benennt eine zuständige Person. Mehr ist strukturell zunächst nicht erforderlich – entscheidend ist die eindeutige Zuordnung.

2.2 Fokussierte Risikoanalyse.

Die Risikoanalyse bildet nach allen anerkannten Standards das konzeptionelle Fundament eines Compliance-Management-Systems.⁶ Sowohl die DIN ISO 37301 als auch ISO 31000 stellen klar, dass Maßnahmen nur dann angemessen sein können, wenn sie auf einer strukturierten Identifikation und Bewertung von Risi-

3 DIN SPEC 91524:2023-09, Compliance-Management-Systeme für kleine und mittlere Unternehmen (KMU) – Leitfaden, Beuth Verlag, Berlin 2023

4 DIN EN ISO 37301:2021-11, Compliance-Management-Systeme – Anforderungen mit Leitlinien zur Anwendung; IDW PS 980 n.F. (2022), Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen; ISO 31000:2018, Risk Management – Guidelines.

5 Schröer, Risikomanagement in kleinen und mittleren Unternehmen (KMU), ZRFC 2013, 206 (208 f.) – zur risikoadäquaten und ressourcenschonenden Ausgestaltung von Managementsystemen im Mittelstand.

6 Zenke/Schäfer/Brocke, *Corporate Governance: Risikomanagement, Organisation, Compliance für Unternehmer*, 3. Aufl., De Gruyter Praxishandbuch, Berlin/Boston 2025.

ken beruhen. Auch der Prüfungsstandard IDW PS 980 definiert die Risikoanalyse als zentrales Element eines wirksamen CMS.

Es werden die wesentlichen, tatsächlich relevanten Risiken identifiziert und priorisiert. Die Risikoidentifikation kann zum Beispiel als Bestandteil in Jour Fixes von Abteilungsleitermeetings aufgenommen und dokumentiert werden.

Die Bewertung erfolgt dabei in reduzierter Form anhand dreier Kriterien:

1. **Eintrittswahrscheinlichkeit** (Wie realistisch ist das Risiko?)
2. **Schadenspotenzial** (Welche finanziellen, rechtlichen oder reputativen Folgen drohen?)
3. **Tragweite der Auswirkungen** (Beeinträchtigt das Risiko nur einen Teilbereich oder die Existenz des Unternehmens?)

2.3 Grundlegende Präventions- und Kontrollmechanismen.

Auf Basis der priorisierten Risiken werden zentrale Maßnahmen implementiert: Ein verständlicher Verhaltenskodex, einfache Zuständigkeitsregelungen, gegebenenfalls ein Hinweisgebersystem sowie elementare Kontrollmechanismen (z. B. Vier-Augen-Prinzip, Dokumentation wesentlicher Entscheidungen).

2.4 Regelmäßige Überprüfung.

In angemessenen Abständen wird geprüft, ob die identifizierten Risiken noch zutreffen und ob die Maßnahmen funktionieren. Ein formales Auditregime ist für den Minimalansatz nicht erforderlich; eine dokumentierte jährliche Überprüfung genügt regelmäßig.

Der Fokus liegt damit auf einem **angemessenen, praktikablen Basissystem**, das Haftungsrisiken reduziert und Transparenz schafft, ohne organisatorische Überlastung zu erzeugen.

3 Struktur und Prüfllogik eines CMS-Handbuchs für KMU

Ein Compliance-Handbuch für KMU muss zwei Anforderungen erfüllen: Es soll einerseits als internes Steuerungsdokument dienen und andererseits im Haftungs- oder Prüfungsfall die Angemessenheit des Systems nachweisen. Dabei gilt der Grundsatz der Verhältnismäßigkeit: Das Handbuch soll klar, strukturiert und praxistauglich sein – kein juristisches Kompendium.

Auf Basis der DIN SPEC 91524 der DIN ISO 37301 und des risikoorientierten Ansatzes nach ISO 31000

lässt sich eine sinnvolle, schlanke Struktur in fünf Kernkapiteln entwickeln.

Diese nachfolgende Struktur bildet zugleich die Prüflogik des Systems.

Kapitel 1: Grundverständnis und Zielsetzung

Dieses Kapitel definiert Zweck, Geltungsbereich und Verantwortungsrahmen des CMS. Es beantwortet die grundlegende Frage: Warum existiert das Compliance-Management-System im Unternehmen?

Konkret enthalten sein sollten:

- Zielsetzung des CMS (Haftungsreduktion, Transparenz, Risikosteuerung)
- Geltungsbereich (Unternehmen, Tochtergesellschaften, Mitarbeitende)
- Verweis auf normative Grundlagen (DIN SPEC 91524, DIN ISO 37301)
- Klare Positionierung der Geschäftsleitung („Tone from the Top“)

Prüflogik:

Ist die Verantwortung eindeutig der Geschäftsleitung zugeordnet, und ist der Zweck des Systems nachvollziehbar dokumentiert?

Kapitel 2: Governance und Organisationsstruktur

Dieses Kapitel beschreibt, wie Compliance organisatorisch verankert ist.

Konkret geregelt werden sollten:

- Benennung eines Compliance-Verantwortlichen
- Delegations- und Vertretungsstruktur
- Berichtspflichten gegenüber der Geschäftsleitung
- Grundzüge der Kontrollarchitektur

Das Ziel ist keine komplexe Organigramm-Darstellung, sondern Transparenz: Wer ist wofür verantwortlich und wer kontrolliert wen?

Prüflogik:

Sind Zuständigkeiten klar geregelt und dokumentiert, und existiert ein nachvollziehbarer Berichtsweg?

Kapitel 3: Risikoanalyse und Priorisierung

Dieses Kapitel bildet das inhaltliche Kernstück des Handbuchs. Es beschreibt:

- Die Methodik der Risikoidentifikation
- Die Bewertungslogik (Eintrittswahrscheinlichkeit × Schadenspotenzial × Tragweite)
- Die priorisierten Hauptrisikofelder des Unternehmens

Es genügt eine übersichtliche Darstellung der wesentlichen Risikobereiche (z.B. Korruption, Arbeitsschutz, Datenschutz, Arbeitsrecht, IT-Sicherheit, Lieferkette), ergänzt um eine kurze Begründung, warum diese für das konkrete Unternehmen relevant sind.

Prüflogik:

Sind die wesentlichen Risiken identifiziert, priorisiert und dokumentiert, und ist erkennbar, warum bestimmte Risiken als wesentlich eingestuft wurden?

Kapitel 4: Maßnahmen und Kontrollmechanismen

Hier wird dargestellt, wie auf die priorisierten Risiken reagiert wird. Die Darstellung folgt einer einfachen Systematik:

- Prävention (Kodex, Schulungen, Zuständigkeiten)
- Detektion (Kontrollen, Hinweisgebersystem)
- Reaktion (Untersuchungsverfahren, Sanktionen)

Es genügt, die zentralen Maßnahmen je Risikofeld zu benennen – keine vollständige Prozessbeschreibung. Entscheidend ist der Zusammenhang zwischen Risiko und Maßnahme.

Beispielhafte Logik:

- Risiko: Korruption → Maßnahme: Geschenkeregelung + Vier-Augen-Prinzip
- Risiko: Datenschutz → Maßnahme: Verarbeitungsverzeichnis + Berechtigungskonzept

Prüflogik:

Gibt es für jedes wesentliche Risiko eine nachvollziehbare Gegenmaßnahme und sind Kontrollpunkte definiert?

Kapitel 5: Überwachung und Weiterentwicklung

Dieses Kapitel beschreibt, wie das CMS aktuell gehalten wird:

- Regelmäßige Überprüfung der Risikoanalyse
- Dokumentation von Vorfällen
- Jährliche Management-Bewertung
- Anpassung bei regulatorischen Änderungen

Für KMU reicht regelmäßig eine dokumentierte jährliche Überprüfung mit kurzer Bewertung der Wirksamkeit.

Prüflogik:

Wird das System regelmäßig überprüft, und werden Erkenntnisse aus Vorfällen in das System zurückgespielt?

4 Vom Handbuch zur Überprüfung der Umsetzung

Die vorstehend dargestellte Struktur eines Compliance-Handbuchs legt Aufbau, Verantwortlichkeiten und Prüflogik eines angemessenen CMS fest. Sie schafft den konzeptionellen Rahmen und stellt sicher, dass das System nachvollziehbar und dokumentierbar ist.

Für die praktische Umsetzung im Unternehmensalltag ist jedoch eine weitere Konkretisierung erforderlich. Die strukturellen Elemente müssen in überprüfbare Einzelfragen und konkrete Handlungsschritte übersetzt werden.

Gerade für KMU dient die folgende Checkliste daher als kompaktes Selbstbewertungs- und Steuerungsinstrument. Sie ermöglicht es, systematisch zu prüfen,

- ob die wesentlichen Anforderungen tatsächlich umgesetzt sind,
- wo strukturelle Lücken bestehen,
- welche Maßnahmen priorisiert werden müssen und
- ob das System insgesamt angemessen und wirksam ausgestaltet ist.

Die nachfolgende Checkliste folgt dabei der zuvor dargestellten Systemlogik und überführt diese in eine praxistaugliche Prüfroutine.

Bereich	Kurzprüfung (Je Punkt 1–10 bewerten)	Ø-Wert	Risikoeinstufung
1. Governance & Verantwortung	<ul style="list-style-type: none"> ■ Prozesse dokumentiert? ■ Zuständigkeiten klar geregelt? ■ Leitung übernimmt sichtbare Verantwortung? ■ Kontrollmechanismen vorhanden? 		
2. Risikoanalyse	<ul style="list-style-type: none"> ■ Wesentliche Risiken identifiziert? ■ Bewertung nach Eintritt × Schaden? ■ Priorisierung dokumentiert? ■ Jährliche Aktualisierung? 		
3. Einkauf & Lieferkette	<ul style="list-style-type: none"> ■ Korruptions- oder Kartellrisiken adressiert? ■ Lieferantenprüfung vorhanden? ■ Dokumentiertes Vergabeverfahren? ■ Außenwirtschaftsprüfung? 		
4. Vertrieb & Marktverhalten	<ul style="list-style-type: none"> ■ Kartellrechtliche Sensibilisierung? ■ Geschenkeregelung? ■ Export-/Embargoprüfung? ■ Verbraucherschutz beachtet? 		
5. Produktion & Umwelt	<ul style="list-style-type: none"> ■ Produkthaftungsrisiken kontrolliert? ■ Arbeitsschutz umgesetzt? ■ Umweltauflagen eingehalten? ■ Dokumentierte Kontrollen? 		
6. Personal & Datenschutz	<ul style="list-style-type: none"> ■ DSGVO-konformes Verarbeitungsverzeichnis? ■ Arbeitszeit/Mindestlohn geregelt? ■ Offboarding-Prozess? ■ Schulungen dokumentiert? 		
7. IT & Informationssicherheit	<ul style="list-style-type: none"> ■ IT-Sicherheitskonzept? ■ Rollen-/Rechtemodell? ■ Technische & organisatorische Maßnahmen? ■ Notfallplanung vorhanden? 		
8. Finanzen & Vermögensschutz	<ul style="list-style-type: none"> ■ Funktionstrennung bei Zahlungen? ■ Steuer-Compliance geregelt? ■ Budgetkontrollen? ■ Schutz vor Vermögensdelikten? 		
9. Hinweisgeber & Reaktion	<ul style="list-style-type: none"> ■ Hinweisgebersystem vorhanden? ■ Vorfalldokumentation? ■ Sanktionensystem klar? ■ Lessons-Learned-Prozess? 		

Bewertungslogik der Themenfelder in der Kurzprüfung je Punkt:

- 1–3 Struktur klar geregelt, dokumentiert und wirksam umgesetzt
 4–6 Teilweise geregelt, jedoch Lücken in Dokumentation, Zuständigkeit oder Kontrolle
 7–10 Fehlende oder unzureichende Regelung; strukturelle Schwächen erkennbar

Einstufung Durchschnittswert:

- Ø-Wert ≤ 3: System angemessen ausgestaltet → Risikoeinstufung: Niedriges Risiko
 Ø-Wert 4–6: Strukturüberprüfung empfohlen → Risikoeinstufung: Mittleres Risiko
 Ø-Wert ≥ 7: Priorisierte Maßnahmen erforderlich → Risikoeinstufung: Hohes Risiko

5 Fazit und Ausblick

Compliance ist für KMU längst kein optionales Zusatzthema mehr, sondern Bestandteil verantwortungsvoller Unternehmensführung. Angesichts zunehmender regulatorischer Anforderungen und verschärfter Haftungsmaßstäbe dient ein strukturiertes Compliance-Management-System nicht nur der Normerfüllung, sondern der gezielten Risikosteuerung und Stabilisierung der Unternehmensorganisation. Die DIN SPEC 91524 zeigt, dass hierfür kein komplexes Konzernmodell erforderlich ist, sondern ein verhältnismäßiger, risikoorientierter Ansatz genügt. Mit diesem Ansatz wird Compliance KMU-tauglich.

Abschließende Empfehlung

Für KMU empfiehlt sich ein dreistufiger Implementierungsansatz:

1. Minimalstandard

Ein belastbares Basissystem mit Risikoregister, Verhaltenskodex, Schulungskonzept und – soweit erforderlich – Hinweisgebersystem.⁷

2. Strukturphase

Integration der Compliance-Anforderungen in die wesentlichen Unternehmensprozesse, ergänzt um klare Dokumentation und grundlegende Kontrollmechanismen.

3. Reifegradphase

Weiterentwicklung hin zu Auditfähigkeit, KPI-gestütztem Monitoring und kontinuierlicher Verbesserung.

Ein solches schrittweises Vorgehen ermöglicht es KMU, ein angemessenes und wirksames Compliance-System aufzubauen – nicht als bürokratische Last, sondern als strategisches Instrument zur nachhaltigen Sicherung und Weiterentwicklung des Unternehmens.

Quellen

VO (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), ABl. L 119 vom 4.5.2016

BGH, Urt. v. 27.4.2022 – 5 StR 278/21, ; OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19.

DIN SPEC 91524:2023-09, Compliance-Management-Systeme für kleine und mittlere Unternehmen (KMU) – Leitfaden, Beuth Verlag, Berlin 2023

⁷ RL (EU) 2019/1937; Hinweisgeberschutzgesetz vom 31.5.2023.

DIN EN ISO 37301:2021-11, Compliance-Management-Systeme – Anforderungen mit Leitlinien zur Anwendung; IDW PS 980 n.F. (2022), Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen; ISO 31000:2018, Risk Management – Guidelines.

Schröder, Risikomanagement in kleinen und mittleren Unternehmen (KMU), ZRFC 2013, 206 (208 f.) – zur risikoadäquaten und ressourcenschonenden Ausgestaltung von Managementsystemen im Mittelstand.

Zenke/Schäfer/Brocke, Corporate Governance: Risikomanagement, Organisation, Compliance für Unternehmer, 3. Aufl., De Gruyter Praxis-handbuch, Berlin/Boston 2025.

RL (EU) 2019/1937; Hinweisgeberschutzgesetz vom 31.5.2023.



Sophia Steinle ist Wirtschaftsjuristin bei Menold Bezler in Stuttgart. Ihr Tätigkeitsschwerpunkt liegt in der Durchführung und Begleitung interner Revisionen, insbesondere im Rahmen von Co- und Outsourcing-Modellen. Sie berät und unterstützt Unternehmen sowie öffentliche Einrichtungen an der Schnittstelle zwischen Steuerwesen und Prozessprüfung, wo sie steuerliche Themen – insbesondere Umsatz-, Energie- und Stromsteuer – mit prozessualen und regulatorischen Anforderungen verknüpft. Zuvor war sie von 2018 bis 2023 bei einer Big Four-Gesellschaft im Bereich Indirect Tax tätig. Seit 2024 ist sie bei Menold Bezler als Managerin tätig und verantwortet unter anderem Revisions- und Beratungstätigkeiten für Energieversorger und mittelständische Unternehmen.



Hannah Müller ist Qualitätsingenieurin bei der Mercedes-Benz AG. Ihr Tätigkeitsschwerpunkt liegt in der Qualitätsmethodenentwicklung sowie in Governance-Themen, wo sie Qualitätsstandards (weiter-)entwickelt und deren strukturierte Umsetzung im Unternehmen unterstützt. Zuvor war sie mehrere Jahre beim Steinbeis Center of Management and Technology (SCMT GmbH) im Qualitätsmanagement tätig. Dort verantwortete sie den Aufbau und die Weiterentwicklung eines Qualitätsmanagementsystems nach ISO 9001:2015, begleitete Zertifizierungs- und Überwachungsaudits und führte interne Systemaudits durch. Weitere Schwerpunkte lagen im Risiko- und Prozessmanagement, in der Einführung eines Datenschutzmanagementsystems nach EU-DSGVO sowie im Aufbau eines Wissensmanagementsystems.