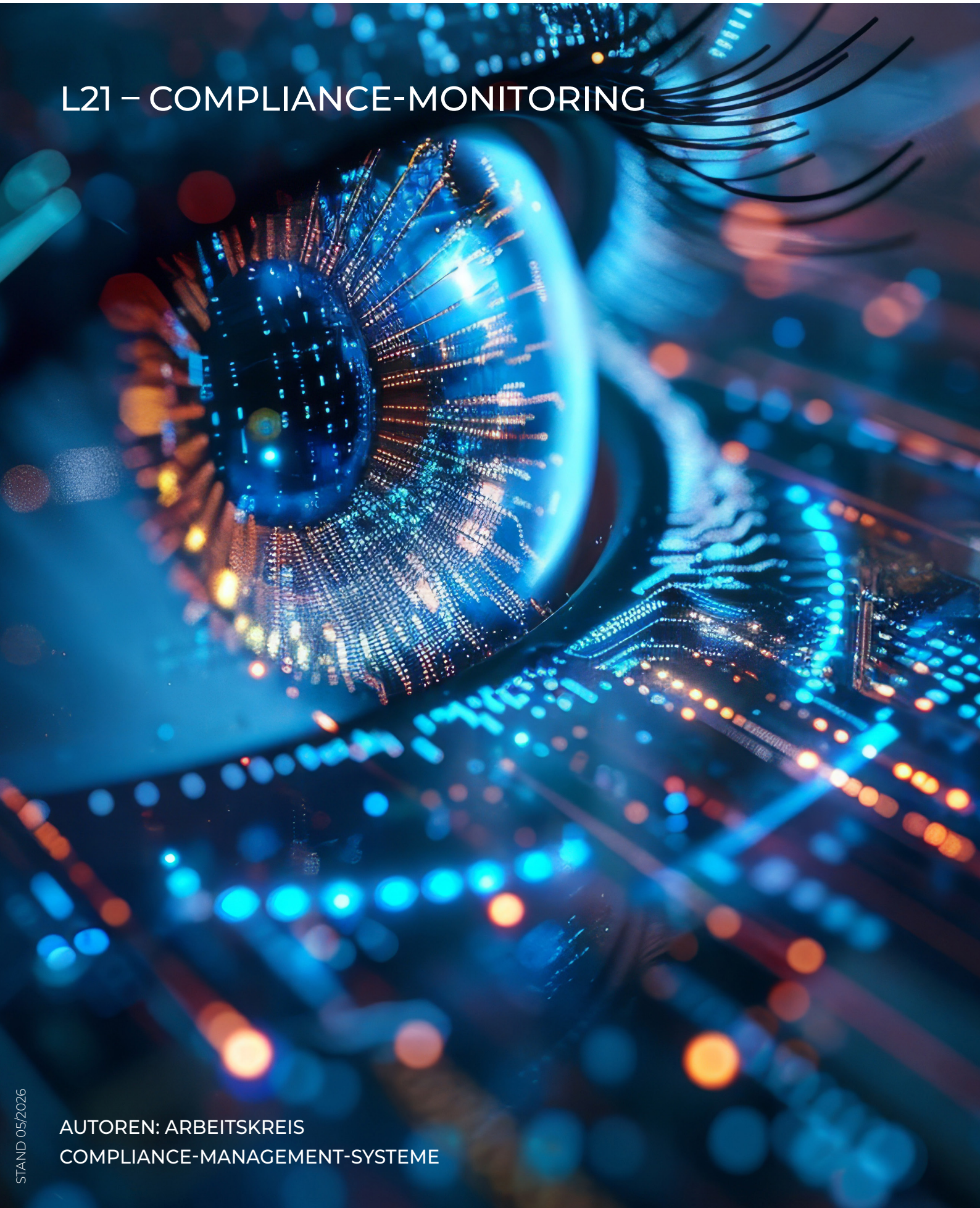
Deutsches Institut für Compliance

DICO LEITLINIE

L21 – COMPLIANCE-MONITORING



AUTOREN: ARBEITSKREIS
COMPLIANCE-MANAGEMENT-SYSTEME

STAND 05/2026

Stand: Mai 2026

Disclaimer

DICO Leitlinien richten sich an Compliance-Praktiker. Sie sollen einen Einstieg in das Thema erleichtern und einen Überblick verschaffen. Es wird daher bewusst darauf verzichtet, juristische Sonderfälle und Ausnahmeregelungen aufzuzeigen.

DICO Leitlinien bieten dem geneigten Leser praxistaugliche und umsetzbare Empfehlungen für ausgewählte Compliance-Themen. Mit Veröffentlichung einer Leitlinie soll zugleich eine Diskussion zum jeweiligen Themenkreis angestoßen werden mit dem Ziel, darauf aufbauend einen Standard zu entwickeln, der von Compliance-Praktikern anerkannt wird.

Senden Sie Ihre Anregungen und Beiträge an leitlinien@dico-ev.de. Wir freuen uns auf eine lebhafte Diskussion und bedanken uns für Ihre konstruktive Unterstützung!

1. VORWORT

Die Unternehmensleitung hat im Rahmen der allgemeinen Sorgfaltspflicht die Einhaltung gesetzlicher Bestimmungen durch Errichtung entsprechender Maßnahmen sicherzustellen und hierfür unternehmensinterne Regeln und Kontrollmechanismen zu etablieren. Verstöße können empfindliche Strafen für ein Unternehmen und seine Organe nach sich ziehen. Zur Abwendung von Schäden für das Unternehmen und zur Vermeidung einer persönlichen Haftung von Organmitgliedern (Aufsichtsrat, Vorstand, Geschäftsführung) bedarf es einer regelmäßigen Überprüfung, ob das Compliance Management System (CMS) des Unternehmens den regulatorischen Anforderungen entspricht sowie angemessen und effektiv ist.

Eine derartige regelmäßige Überwachung und Bewertung der Wirksamkeit von Compliance Management Systemen (CMS) wird daher auch ausdrücklich in externen Standards wie der DIN ISO 37301:2021 oder dem Prüfungsstandard IDW PS 980 gefordert.

Die DIN ISO 37301:2021 „Compliance-Managementsysteme – Anforderungen mit Leitlinien zur Anwendung“[1] sieht u.a. die Einführung von Kontrollmechanismen vor, um den Erfolg des CMS regelmäßig zu überwachen und Schwachstellen zu identifizieren. Ebenso soll eine regelmäßige und konsequente Überwachung und Untersuchung von Fällen der Nichteinhaltung von Compliance-Vorgaben erfolgen.

In regulierten Branchen bestehen Vorschriften zur regelmäßigen Überwachung des CMS, insbesondere durch Vorgaben der BaFin und der MaRisk[2], die ein risikoorientiertes Monitoring sowie eine kontinuierliche Kontrolle der Einhaltung relevanter Regelwerke verlangen.

Auch der Prüfungsstandard 980 für Wirtschaftsprüfer (IDW PS 980 (09.2022))[3] sieht das Grundelement „Compliance-Überwachung und -Verbesserung“ vor. Im betreffenden Grundelement sollen die Angemessenheit und Wirksamkeit des CMS in geeigneter Weise überwacht werden. Es sollen CMS-Schwachstellen und Regelverstöße nach erfolgter Ursachenanalyse an die relevanten Stellen im Unternehmen berichtet und etwaige Mängel beseitigt sowie das CMS verbessert werden.

Das international anerkannte „Prevent – Detect – Respond“-Modell[4] unterstreicht im Bereich „Detect“ die Bedeutung von Mechanismen zur Identifikation von Schwachstellen des CMS und zur Aufdeckung von Compliance-Verstößen. In dieser Säule sollen auch Prozesskontrollen verortet werden.[5]

Auch das CMS-Modell, das DICO in seinem DICO-Standard 12 – CMS darstellt, sieht eine regelmäßige Überwachung der Implementierung des CMS vor.

1 Entgeltlich anforderbar über https://www.dinmedia.de/de/norm/din-iso-37301/344577424 oder https://www.iso.org/standard/75080.html.
2 Vgl. hierzu Rundschreiben MaRisk vom 06/2024 BaFin - Rundschreiben - Rundschreiben 06/2024 (BA) - MaRisk (PDF-Version).
3 Entgeltlich anforderbar über IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen (IDW PS 980).
4 Siehe etwa Kahlenberg/Schäfer/Schieffer, in: Busch/Hoven/Pieth/Rübenstahl, Kap. 33, Rn. 36 ff.; Moosmayer, Rn. 364 ff.; Seyfarth, ZGR-Sonderheft 22/2020, 87 (97); Schieffer, in: Minkoff/Sahan/Wittig, § 28 Rn. 48 ff.; DICO: Checkliste_Compliance_in_Krisenzeiten.pdf.
5 DICO Standard | Compliance-Management-Systeme S. 17, Ziff. 2.3.

Über DICO:

DICO – Deutsches Institut für Compliance e.V. wurde im November 2012 in Berlin auf Betreiben führender Compliance-Praktiker und -Experten gegründet und hat als gemeinnütziger Verein Mitglieder aus allen Branchen in Deutschland, darunter namhafte DAX-Unternehmen, Wirtschaftsprüfungs- und Beratungsgesellschaften sowie aus der Wissenschaft. DICO versteht sich als unabhängiges interdisziplinäres Netzwerk für den Austausch zwischen Wirtschaft, Wissenschaft, Politik und Verwaltung und sieht sich als zentrales Forum für die konsequente und praxisbezogene Förderung und Weiterentwicklung von Compliance in Deutschland.

DICO fördert Compliance in Deutschland, definiert in diesem Bereich Mindeststandards, begleitet Gesetzgebungsvorhaben und unterstützt zugleich die praktische Compliance-Arbeit in privaten und öffentlichen Unternehmen, fördert Aus- und Weiterbildung und entwickelt Qualitäts- sowie Verfahrensstandards.

DICO

DICO – Deutsches Institut für Compliance
Bergstraße 68
D-10115 Berlin
info@dico-ev.de
www.dico-ev.de