

ZERTIFIZIERUNGSPROGRAMM FÜR COMPLIANCE-MANAGEMENT NACH DIN ISO 37301:2021

Inhaltsverzeichnis

Einleitung	1
1 Anwendungsbereich	3
2 Normative Verweisungen und mitgeltende Regelungen	3
3 Begriffe	4
4 Zertifizierungsverfahren und -zyklus.....	4
5 Anforderungen der DIN ISO 37301:2021	12
6 Datenschutz und Vertraulichkeit.....	19
7 Änderungen und Ausnahmen.....	19
8 Sanktionen und Folgen bei Nichteinhaltung	19
9 Versionierung und Änderungsverfolgung	19
Anhang A – Begleitende Pflichttabelle.....	20

Einleitung

Dieses Zertifizierungsprogramm beschreibt die Anforderungen an den Kunden im Verfahren zur Zertifizierung eines Compliance-Managementsystems (CMS) nach DIN ISO 37301:2021.

Die Zertifizierung Bau GmbH (ZertBau) ist eine durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) akkreditierte Zertifizierungsstelle und ist berechtigt, Managementsysteme zu zertifizieren und Zertifikatsurkunden mit der DAkkS-Kennzeichnung auszugeben. Die Anforderungsnormen und die jeweiligen Wirtschaftsbereiche, für welche die Zertifizierungsstelle durch die DAkkS akkreditiert ist, sind in der Akkreditierungsurkunde definiert.

Die Vergabe des Zertifikats in Verbindung mit einem Geltungsbereich, der durch die Tätigkeit des Kunden bestimmt ist, und einer einmaligen, rückverfolgbaren Registernummer wird als Zertifizierung verstanden. Der Eintrag in das Unternehmensregister der ZertBau im Internet unter <https://www.zert-bau.de/unternehmenssuche> gilt als Nachweis der Zertifizierung und die Streichung aus dem vorgenannten Verzeichnis als Aussetzung oder Zurückziehung der Zertifizierung.



Zertifizierungsstelle im Sinne dieses Zertifizierungsprogramms ist der Geschäftsbereich Managementsysteme der ZertBau. Andere Zertifizierungs- bzw. Konformitätsbewertungsstellen sind nicht Anwender dieses Programms. Die Anerkennung von Ergebnissen aus anderen Konformitätsbewertungsverfahren ist nicht vorgesehen, sofern dies nicht ausdrücklich in der Zertifizierungsvereinbarung oder im Regelwerk der Zertifizierungsstelle geregelt ist.

Die Zertifizierungsstelle ist unparteilich. Unparteilichkeit bedeutet eine 100 %-ige Objektivität hinsichtlich der Konformitätsbewertungstätigkeit und der Zertifizierungsentscheidung. Das bedeutet, dass keine Vorurteile und keine Interessenkonflikte existieren bzw. dass diese gelöst werden, um die Tätigkeit nicht nachteilig zu beeinflussen.

Alle am Prozess Beteiligten, einschließlich interner Mitarbeiter der Zertifizierungsstelle und externer Auditoren, sind schriftlich zur Vertraulichkeit verpflichtet. Informationen über Zertifizierungen und Auditergebnisse werden nur mit Zustimmung des Kunden weitergegeben, es sei denn, es bestehen gesetzliche Verpflichtungen oder die DAkkS fordert Einblick in Unterlagen im Rahmen der für die Erlangung oder Aufrechterhaltung der Akkreditierungen notwendigen Begutachtungen.

Die Transparenz der ZertBau als Zertifizierungsstelle ist grundlegend für unser Engagement gegenüber unseren Kunden. Wir streben danach, ein offenes und verständliches Umfeld zu schaffen, in dem Kunden vollständige Einsicht in unsere Prozesse und Verfahren haben. Unsere Dokumentationen sind klar strukturiert und leicht zugänglich, und wir stehen jederzeit für Fragen und Erläuterungen zur Verfügung.

Die Gleichbehandlung aller Kunden ist ein zentraler Grundsatz unserer Zertifizierungsstelle. Wir verpflichten uns dazu, jedem Kunden fair und objektiv zu begegnen, unabhängig von Größe, Branche oder Hintergrund. Unsere Bewertungskriterien und Verfahren sind einheitlich und werden ohne Vorurteile angewendet, um sicherzustellen, dass alle Kunden gleichbehandelt werden.

Zur besseren Lesbarkeit wird in diesem Dokument das generische Maskulinum verwendet. Die in dieser Arbeit verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.

Die Ermittlung der Auditzeit sowie die Auditprogrammgestaltung erfolgen nach dokumentierter Methodik der Zertifizierungsstelle unter Berücksichtigung der DIN EN ISO/IEC 17021-1 sowie der einschlägigen verbindlichen IAF-Dokumente, insbesondere IAF MD 1 für Multi-Standort-Organisationen, IAF MD 4 für den Einsatz von Informations- und Kommunikationstechnologien und IAF MD 11 für integrierte Managementsysteme; IAF MD 5 wird berücksichtigt, soweit einzelne methodische Elemente für das Zertifizierungsprogramm anwendbar sind.

Um die fortwährende Eignung und Gültigkeit des Zertifizierungsprogramms zu bestätigen und mögliche Verbesserungsoptionen zu identifizieren, wird das Programm im Rahmen des im Qualitätsmanagementsystem der ZertBau implementierten Prozesses der Internen Audits durch am Zertifizierungsprogramm unbeteiligte Auditoren regelmäßig überprüft, wobei auch stichprobenartig laufende Zertifizierungsverfahren sowie der Umgang mit Abweichungen und Beschwerden ausgewertet und Anregungen interessierter Kreise sowie Beiträge des Fachbeirats im Zusammenhang mit Beschwerden und anderen fachlichen Fragen berücksichtigt werden. Bestandteil des Prozesses der Internen Audits ist auch die Festlegung und

Nachverfolgung geeigneter Maßnahmen zur Behebung von Abweichungen oder Umsetzung erkannter Verbesserungspotenziale.

1 Anwendungsbereich

Dieses Zertifizierungsprogramm regelt die Anforderungen an den Kunden im Verfahren zur Zertifizierung eines Compliance-Managementsystems (kurz: CMS) nach DIN ISO 37301:2021. Es beschreibt insbesondere Mitwirkungspflichten des Kunden, die wesentlichen Schritte des Zertifizierungsverfahrens sowie Fristen und Regelungen im dreijährigen Zertifizierungszyklus.

Das Zertifikat bestätigt die Konformität des CMS mit der DIN ISO 37301:2021 für den im Zertifikat ausgewiesenen Geltungsbereich. Eine Zertifizierung ist kein Nachweis für die vollständige Einhaltung sämtlicher Compliance-Verpflichtungen; sie bestätigt, dass das Managementsystem die Anforderungen der Norm erfüllt und wirksam angewendet wird.

Soweit der Kunde eine Zertifizierung mit mehreren Standorten beantragt, gelten zusätzlich die Anforderungen an Multi-Standort-Organisationen gemäß den einschlägigen IAF-Vorgaben; eine Stichprobenprüfung ist nur zulässig, wenn die Voraussetzungen hierfür erfüllt sind.

2 Normative Verweisungen und mitgeltende Regelungen

Folgende Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen):

- DIN EN ISO 17000 Konformitätsbewertung - Begriffe und allgemeine Grundlagen
- DIN EN ISO/IEC 17021-1 Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren – Teil 1
- DIN EN ISO/IEC 19011 Leitfaden zur Auditierung von Managementsystemen
- DIN ISO 37301:2021 (A1:2024) Compliance-Managementsysteme – Anforderungen mit Leitlinien zur Anwendung
- DIN ISO 37001:2018 (A1:2024)
- IAF MD 5 Ermittlung von Auditzeiten für QMS, UMS und SGA-MS (soweit einzelne methodische Elemente für dieses Zertifizierungsprogramm anwendbar sind)
- IAF MD 1 Auditierung und Zertifizierung von Managementsystemen in Organisationen mit mehreren Standorten (jeweils gültige Ausgabe)
- IAF MD 4 Verwendung von Informations- und Kommunikationstechnologien (IKT) für Audit- und Begutachtungszwecke (sofern anwendbar)
- IAF MD 5 Ermittlung von Auditzeiten für die Auditierung von Qualitätsmanagement-(QMS) und Umweltmanagementsystemen (UMS), sowie Managementsystemen für Sicherheit und Gesundheit bei der Arbeit (SGA-MS) (sofern anwendbar)
- IAF MD 11 Anwendung der ISO/IEC 17021-1 für Audits integrierter Managementsysteme (sofern anwendbar)
- anwendbare Gesetze zur Korruptionsprävention, Geldwäsche und Kartellrecht
- weitere anwendbare gesetzliche, behördliche, vertragliche und freiwillig übernommene Compliance-Verpflichtungen des Kunden
- anwendbare Regelwerke und Vorgabedokumente der DAkkS
- Zertifizierungsvereinbarung
- Regelwerk der Zertifizierungsstelle der ZertBau

3 Begriffe

Eine terminologische Datenbank findet sich unter www.iso.org/obp.

Im Übrigen gelten die Begriffe und Definitionen der DIN ISO 37301:2021 und der DIN EN ISO/IEC 17021-1. Für dieses Zertifizierungsprogramm werden u. a. die folgenden Begriffe verwendet:

- Kunde/Organisation: natürliche oder juristische Person, die die Zertifizierung beantragt oder innehat.
- Standort: Ort, an dem Prozesse/Tätigkeiten unter Kontrolle des Kunden ausgeführt werden; kann Lagerung, Infrastruktur und zugehörige Tätigkeiten umfassen.
- Multi-Standort-Organisation: Organisation mit mehreren Standorten, die einem einzigen Managementsystem unterliegen, das durch eine Zentrale festgelegt und überwacht wird.
- Compliance-Verpflichtungen: Anforderungen, die eine Organisation zwingend erfüllen muss, sowie Anforderungen, denen sie sich freiwillig unterwirft.
- Non-Compliance/Nichtkonformität/Abweichung: Nichterfüllung von Compliance-Verpflichtungen bzw. Nichterfüllung einer Anforderung; Feststellungen werden im Audit nachvollziehbar gegen konkrete Anforderungen aufgezeichnet.

4 Zertifizierungsverfahren und -zyklus

Die nachfolgenden operativen Schritte beschreiben den Ablauf des Zertifizierungsverfahrens nach DIN EN ISO/IEC 17021-1 von der Antragsphase bis zur Aufrechterhaltung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung.

4.1 Tätigkeiten vor der Zertifizierung

4.1.1 Antrag

Der Kunde stellt durch einen bevollmächtigten Vertreter alle für die Antragstellung erforderlichen Informationen bereit. Hierzu gehören insbesondere der gewünschte Geltungsbereich der Zertifizierung, relevante Angaben zur Organisation und zu ihren Standorten, Prozessen und Tätigkeiten, personellen und technischen Ressourcen, Funktionen, Beziehungen sowie maßgebliche Compliance-Verpflichtungen. Ferner sind ausgelagerte Prozesse, die anzuwendenden Normen oder sonstigen normativen Dokumente sowie – soweit zutreffend – bereits erbrachte Beratungsleistungen zum zu zertifizierenden Managementsystem anzugeben.

4.1.2 Antragsprüfung

Die Zertifizierungsstelle prüft den Antrag und ergänzende Informationen. Der Kunde wirkt an der Klärung aller offenen Punkte mit. Eine Annahme des Antrags setzt voraus, dass die Informationen für die Erstellung des Auditprogramms ausreichen, bekannte Verständnisunterschiede geklärt sind und alle für die Zertifizierungstätigkeit maßgeblichen Rahmenbedingungen berücksichtigt werden können. Bei Ablehnung des Antrags werden die Gründe dokumentiert und dem Kunden mitgeteilt. Auf Grundlage der Antragsprüfung werden zudem die für Auditteam und Zertifizierungsentscheidung erforderlichen Kompetenzen bestimmt.

4.1.3 Auditprogramm

Für den gesamten Zertifizierungszyklus wird ein Auditprogramm festgelegt. Dieses umfasst das zweistufige Erstaudit, Überwachungsaudits im ersten und zweiten Jahr nach der Zertifizierungsentscheidung sowie das Re-Zertifizierungsaudit im dritten Jahr vor Ablauf der Zertifizierung. Der erste Überwachungszyklus beginnt mit der Zertifizierungsentscheidung; das erste Überwachungsaudit nach Erstzertifizierung muss spätestens zwölf Monate nach der Zertifizierungsentscheidung stattfinden. Bei der Festlegung und Anpassung des Auditprogramms werden insbesondere Größe, Geltungsbereich und Komplexität des Managementsystems, Ergebnisse früherer Audits, Beschwerden, rechtliche oder regulatorische Änderungen sowie weitere relevante Entwicklungen berücksichtigt. Soweit frühere Zertifizierungen oder Audits anderer Zertifizierungsstellen berücksichtigt werden sollen, hat der Kunde die hierfür erforderlichen Nachweise bereitzustellen.

4.1.4 Ermittlung des Auditzeitaufwandes

Der Kunde stellt alle Informationen vollständig bereit, die zur Ermittlung des Auditzeitaufwandes erforderlich sind. Maßgeblich sind insbesondere die Anforderungen der einschlägigen Normen und Regelwerke, Größe und Komplexität der Organisation und ihres Managementsystems, Compliance-Verpflichtungen und Compliance-Risiken, ausgelagerte Tätigkeiten, Ergebnisse früherer Audits, Anzahl und Lage der Standorte einschließlich temporärer Einsatzorte sowie die mit Produkten, Prozessen, Dienstleistungen oder Tätigkeiten verbundenen Risiken. Die Dauer des Managementsystemaudits und ihre Begründung werden dokumentiert.

Während des dreijährigen Erst-Zertifizierungszyklus sollte die Auditzeit des Überwachungsaudits für eine bestimmte Organisation proportional zu der Auditzeit sein, die für ein Erstzertifizierungsaudit (Stufe 1 + Stufe 2) aufgewendet wurde; die jährlich für Überwachungen aufgewendete Gesamtzeit beträgt dabei etwa ein Drittel der Auditzeit des Erstaudits.

4.1.5 Stichprobenprüfung an mehreren Standorten

Soweit ein Stichprobenverfahren für mehrere Standorte (Multi-Standort-Organisationen) angewendet werden soll, stellt der Kunde die hierfür erforderlichen Informationen vollständig und zutreffend bereit. Die Zertifizierungsstelle entwickelt einen dokumentierten Stichprobenplan, der ein ordnungsgemäßes Audit des Managementsystems sicherstellt. Stichproben sind nur zulässig, wenn die Voraussetzungen des jeweiligen Zertifizierungsprogramms erfüllt sind; bei nicht vergleichbaren Tätigkeiten an den Standorten ist ein Stichprobenverfahren nicht zweckmäßig.

Sofern die Voraussetzungen für ein Stichprobenverfahren erfüllt sind, beträgt die Mindestanzahl zu auditierender Standorte im Erstaudit $y=\sqrt{x}$ (aufgerundet), im Überwachungsaudit $y=0,6\sqrt{x}$ (aufgerundet) und im Rezertifizierungsaudit wie Erstaudit; bei nachgewiesener Wirksamkeit kann im Rezertifizierungsaudit auf $y=0,8\sqrt{x}$ (aufgerundet) reduziert werden. Bei nicht geeignetem Stichprobenverfahren ist ein Auditprogramm vorzusehen, das im Erstaudit und Rezertifizierungsaudit alle Standorte umfasst und bei Überwachungsaudits 30 % aller Standorte pro Kalenderjahr auditiert; die Zentrale wird in jedem Audit auditiert.

4.1.6 Mehrfach-Managementsysteme

Bei Zertifizierungen gegen mehrere Managementsystemnormen muss die Auditplanung ein angemessenes Vor-Ort-Audit sicherstellen. Der Kunde ermöglicht insoweit die wirksame Auditierung aller in die Zertifizierung einbezogenen Managementsystemanforderungen.

4.2 Planen von Audits

4.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien

Die Auditziele, der Auditumfang und die Auditkriterien werden von der Zertifizierungsstelle in Abstimmung mit dem Kunden festgelegt. Die Auditziele umfassen insbesondere die Beurteilung der Konformität des Managementsystems, seiner Fähigkeit zur Erfüllung geltender Compliance-Verpflichtungen sowie seiner Eignung, beabsichtigte Ergebnisse zu erreichen. Der Auditumfang beschreibt Ausmaß und Grenzen des Audits, z. B. Standorte, Organisationseinheiten, Tätigkeiten und Prozesse. Die Auditkriterien bestehen mindestens aus den Anforderungen der zugrunde liegenden Managementsystemnorm und den festgelegten Prozessen sowie dokumentierten Informationen des Managementsystems des Kunden.

4.2.2 Auswahl des Auditteams und Aufgabenzuordnung

Die Zertifizierungsstelle stellt ein Auditteam zusammen, das in seiner Gesamtheit über die für das jeweilige Audit erforderliche Kompetenz verfügt. Größe und Zusammensetzung des Auditteams richten sich insbesondere nach Auditart, Auditumfang, Auditzeit, Zertifizierungsanforderungen sowie sprachlichen und kulturellen Rahmenbedingungen. Die Aufgaben innerhalb des Auditteams werden so verteilt, dass Prozesse, Funktionen, Standorte, Bereiche oder Tätigkeiten wirksam und effizient auditiert werden können.

Der Einsatz von Beobachtern, Fachexperten, Übersetzern, Dolmetschern oder Betreuern ist vor Beginn des Audits mit dem Kunden abzustimmen. Beobachter dürfen Auditverlauf und Auditergebnis nicht unzulässig beeinflussen. Fachexperten unterstützen das Auditteam fachlich, führen jedoch keine eigenständigen Audits durch. Vom Kunden benannte Betreuer dürfen Kontakte herstellen und organisatorisch unterstützen, sie dürfen das Audit jedoch nicht beeinflussen oder bewerten.

4.2.3 Auditplan

Vor jedem im Auditprogramm vorgesehenen Audit wird ein Auditplan erstellt. Er dient als Grundlage für die Durchführung und zeitliche Planung der Audittätigkeiten.

Der Auditplan enthält mindestens die Auditziele, Auditkriterien, den Auditumfang, die zu auditierenden Standorte, Organisationseinheiten, Funktionen oder Prozesse, Termine und Orte der Vor-Ort- oder Remote-Audittätigkeiten, die vorgesehene Dauer der Audittätigkeiten sowie die Rollen und Verantwortlichkeiten der Mitglieder des Auditteams und sonstiger Begleitpersonen.

Die dem Auditteam übertragenen Aufgaben umfassen die Prüfung und Verifizierung von Struktur, Regelungen, Prozessen, Verfahren, Aufzeichnungen und zugehörigen Dokumenten des Kunden sowie die Beurteilung, ob diese die Anforderungen für den beabsichtigten Geltungsbereich der Zertifizierung erfüllen und wirksam eingeführt, umgesetzt und aufrechterhalten werden.

Der Auditplan wird dem Kunden vorab mitgeteilt; die Audittermine werden mit dem Kunden abgestimmt.

Die Zertifizierungsstelle teilt dem Kunden die Namen der vorgesehenen Mitglieder des Auditteams und auf Anforderung deren Hintergrundinformationen mit. Dem Kunden ist ausreichend Zeit einzuräumen, begründete Einwände gegen einzelne Teammitglieder vorzubringen.

Bei Einsatz von Informations- und Kommunikationstechnologien (z. B. Remote-Audit-Anteile) werden diese im Auditplan ausgewiesen; die hierfür aufgewendete Zeit kann zur Gesamtdauer des Audits beitragen.

4.3 Erstzertifizierung

4.3.1 Erstzertifizierungs-Audit

Das Erstzertifizierungsaudit wird in zwei Stufen durchgeführt: Stufe 1 und Stufe 2.

Stufe 1 dient der Bewertung der dokumentierten Informationen des Managementsystems, der standortspezifischen Bedingungen und des Vorbereitungsstands des Kunden auf Stufe 2. Hierzu gehören insbesondere die Bewertung des Verständnisses der Normanforderungen, die Ermittlung notwendiger Informationen zum Geltungsbereich, zu Standorten, Prozessen, Arbeitsmitteln, Lenkungsebenen sowie zu anzuwendenden gesetzlichen und behördlichen Anforderungen, die Bewertung der Ressourcenzuordnung für Stufe 2 sowie die Beurteilung, ob interne Audits und Managementbewertungen geplant bzw. durchgeführt werden. Die dokumentierten Schlussfolgerungen aus Stufe 1 und die Bereitschaft für Stufe 2 werden dem Kunden mitgeteilt. Ergeben sich wesentliche Änderungen oder erhebliche Schwachstellen, kann dies zur Verschiebung, Anpassung oder Wiederholung von Stufe 1 oder zur Verschiebung bzw. Stornierung von Stufe 2 führen.

Stufe 2 dient der Bewertung der Umsetzung und Wirksamkeit des Managementsystems am Standort bzw. an den Standorten des Kunden. Sie umfasst mindestens die Prüfung der Konformität mit den Anforderungen der Norm, die Leistungsfähigkeit des Managementsystems hinsichtlich der Compliance-Verpflichtungen, die operative Lenkung, interne Audits und Managementbewertung sowie die Verantwortung der Leitung für Compliance-Politik, Compliance-Ziele, Compliance-Kultur und Compliance-Funktion.

Das Auditteam analysiert die in Stufe 1 und Stufe 2 gewonnenen Informationen und Auditnachweise, bewertet die Auditfeststellungen und einigt sich auf die Auditschlussfolgerungen als Grundlage für die Zertifizierungsentscheidung.

4.4 Durchführen von Audits

4.4.1 Allgemeines

Die Zertifizierungsstelle verfügt über einen Prozess zur Durchführung von Vor-Ort-Audits. Dieser umfasst eine Eröffnungsbesprechung zu Beginn und eine Abschlussbesprechung am Ende des Audits. Soweit Teile des Audits mit elektronischen Mitteln durchgeführt werden oder virtuelle Standorte betroffen sind, müssen diese Tätigkeiten durch kompetentes Personal

erfolgen; der erlangte Nachweis muss für eine sachgerechte Beurteilung der Konformität ausreichen.

4.4.2 Durchführung der Eröffnungsbesprechung

Zu Beginn des Audits findet eine offizielle Eröffnungsbesprechung mit dem Management des Kunden und gegebenenfalls mit den für die auditierten Funktionen oder Prozesse verantwortlichen Personen statt. Dabei werden insbesondere Auditplan, Geltungsbereich, Auditziele und Auditkriterien, Kommunikationswege, Vertraulichkeits- und Sicherheitsaspekte, Verfügbarkeit von Ressourcen und Begleitpersonen, Berichtswege sowie mögliche Bedingungen für einen Abbruch des Audits erläutert. Der Kunde erhält Gelegenheit, Fragen zu stellen.

4.4.3 Kommunikation während des Audits

Während des Audits bewertet das Auditteam regelmäßig den Fortschritt und tauscht Informationen aus. Der Kunde wird über Fortschritt und Bedenken informiert. Wenn sich zeigt, dass Auditziele nicht erreichbar sind oder ein unmittelbares erhebliches Risiko besteht, werden geeignete Maßnahmen festgelegt; hierzu können Änderungen des Auditplans, des Auditumfangs oder der Auditziele sowie ein Abbruch des Audits gehören. Erforderliche Änderungen des Auditumfangs werden mit dem Kunden besprochen.

4.4.4 Erlangung und Verifizierung von Informationen

Für Auditziele, Auditumfang und Auditkriterien relevante Informationen - einschließlich Schnittstellen zwischen Funktionen, Tätigkeiten und Prozessen - werden durch angemessene Stichproben gewonnen und verifiziert. Hierzu zählen insbesondere Befragungen, Beobachtungen von Prozessen und Tätigkeiten sowie die Auswertung von Dokumentationen und Aufzeichnungen.

4.4.5 Ermittlung und Aufzeichnung der Auditfeststellungen

Auditfeststellungen werden so ermittelt, eingestuft und aufgezeichnet, dass eine fundierte Zertifizierungsentscheidung getroffen oder die Zertifizierung aufrechterhalten werden kann. Nichtkonformitäten werden jeweils gegen eine konkrete Anforderung aufgezeichnet und mit objektiven Nachweisen eindeutig beschrieben. Sie werden mit dem Kunden erörtert, damit Nachweise und Feststellungen verstanden werden. Verbesserungsmöglichkeiten können benannt werden; Nichtkonformitäten dürfen jedoch nicht als Verbesserungsmöglichkeiten dargestellt werden. Nicht auflösbare Meinungsverschiedenheiten werden dokumentiert.

4.4.6 Erarbeiten der Auditschlussfolgerungen

Vor der Abschlussbesprechung bewertet das Auditteam unter Verantwortung des Auditteamleiters die Auditfeststellungen und sonstigen geeigneten Informationen im Hinblick auf Auditziele und Auditkriterien, klassifiziert die Nichtkonformitäten, einigt sich auf erforderliche Folgemaßnahmen und bestätigt die Eignung des Auditprogramms oder benennt erforderliche Änderungen für künftige Audits.

4.4.7 Durchführung der Abschlussbesprechung

Nach Abschluss des Audits findet eine formelle Abschlussbesprechung mit dem Management des Kunden und gegebenenfalls mit den für die auditierten Funktionen oder Prozesse verantwortlichen Personen statt. Die Anwesenheit wird aufgezeichnet. Vorgestellt werden die Auditschlussfolgerungen einschließlich der Empfehlung zur Zertifizierung, die festgestellten

Nichtkonformitäten, der Zeitrahmen für Korrekturen und Korrekturmaßnahmen, die auf Stichproben beruhende Natur der Auditnachweise, das weitere Vorgehen der Zertifizierungsstelle sowie Informationen zu Beschwerde- und Einspruchsverfahren. Der Kunde erhält Gelegenheit zu Fragen; nicht gelöste Meinungsverschiedenheiten werden dokumentiert.

4.4.8 Auditbericht

Für jedes Audit wird ein schriftlicher Auditbericht erstellt. Dieser muss eine zutreffende, knappe und klare Aufzeichnung des Audits enthalten und eine fundierte Zertifizierungsentscheidung ermöglichen. Der Bericht umfasst oder referenziert insbesondere Auditart, Auditkriterien, Auditziele, Auditumfang, Auditzeit, Teamzusammensetzung, Auditorte und -termine, Auditfeststellungen und -schlussfolgerungen, wesentliche Änderungen seit dem letzten Audit, gegebenenfalls ungelöste Punkte sowie die Bestätigung, dass Auditziele erreicht wurden. Verbesserungsmöglichkeiten dürfen benannt, jedoch keine konkreten Lösungen empfohlen werden. Das Eigentum am Auditbericht verbleibt bei der Zertifizierungsstelle.

4.4.9 Analyse der Ursachen von Nichtkonformitäten

Bei festgestellten Nichtkonformitäten muss der Kunde die Ursachen analysieren und innerhalb eines festgelegten Zeitraums die spezifischen Korrekturen sowie die durchgeführten oder geplanten Korrekturmaßnahmen beschreiben.

4.4.10 Wirksamkeit der Korrekturen und Korrekturmaßnahmen

Die Zertifizierungsstelle bewertet die vom Kunden vorgelegten Korrekturen, Ursachenanalysen und Korrekturmaßnahmen auf ihre Annehmbarkeit und verifiziert deren Wirksamkeit. Der Kunde wird über das Ergebnis dieser Prüfung informiert. Soweit erforderlich, kann hierfür ein zusätzliches vollständiges Audit, ein zusätzliches eingeschränktes Audit oder dokumentierter Nachweis verlangt werden.

4.5 Zertifizierungsentscheidung

4.5.1 Allgemeines

Die Entscheidung über Erteilung oder Verweigerung der Zertifizierung, Erweiterung oder Einschränkung des Geltungsbereichs, Aussetzung oder Wiederherstellung, Zurückziehung oder Erneuerung der Zertifizierung wird von hierfür kompetenten Personen oder Gremien getroffen, die nicht an der Durchführung des Audits beteiligt waren. Jede Zertifizierungsentscheidung wird aufgezeichnet.

4.5.2 Maßnahmen vor der Zertifizierungsentscheidung

Vor der Entscheidung wird geprüft, ob die durch das Auditteam bereitgestellten Informationen im Hinblick auf Zertifizierungsanforderungen und Geltungsbereich ausreichend sind, ob Korrekturen und Korrekturmaßnahmen zu wesentlichen Nichtkonformitäten bewertet, angenommen und verifiziert wurden und ob Pläne zu Korrekturen und Korrekturmaßnahmen bei untergeordneten Nichtkonformitäten bewertet und angenommen wurden.

4.5.3 Information über Erteilung der Erstzertifizierung

Für die Zertifizierungsentscheidung zur Erstzertifizierung stellt das Auditteam mindestens den Auditbericht, Anmerkungen zu Nichtkonformitäten und gegebenenfalls zu ergriffenen Korrekturen und Korrekturmaßnahmen, die Bestätigung der in der Antragsprüfung verwendeten Informationen, die Bestätigung der Erreichung der Auditziele sowie eine Empfehlung zur Zertifizierung bereit. Kann die Umsetzung von Korrekturen und Korrekturmaßnahmen zu einer wesentlichen Nichtkonformität nicht innerhalb von sechs Monaten nach dem letzten Tag der Stufe 2 verifiziert werden, ist vor einer Empfehlung zur Zertifizierung eine erneute Stufe 2 durchzuführen.

4.5.4 Informationen zur Erteilung der Re-Zertifizierung

Die Entscheidung über die Erneuerung der Zertifizierung basiert auf den Ergebnissen des Re-Zertifizierungsaudits, der Bewertung des Managementsystems über den gesamten Zertifizierungszeitraum sowie gegebenenfalls eingegangenen Beschwerden von Nutzern der Zertifizierung.

4.6 Aufrechterhaltung der Zertifizierung

4.6.1 Allgemeines

Die Zertifizierung wird aufrechterhalten, wenn der Kunde weiterhin die Anforderungen der Managementsystemnorm erfüllt und dies durch die Zertifizierungsstelle nachgewiesen werden kann.

4.6.2 Überwachungstätigkeiten

Für jedes Überwachungsaudit muss die Zertifizierungsstelle aktualisierte Daten des Kunden bezüglich seines Managementsystems erhalten; die geplante Auditzeit ist mindestens bei jedem Überwachungs- und Rezertifizierungsaudit zu überprüfen, um Veränderungen an der Organisation, am Reifegrad des Systems usw. zu berücksichtigen. Die Zertifizierungsstelle legt Überwachungstätigkeiten so fest, dass maßgebliche Bereiche und Funktionen des zertifizierten Managementsystems regelmäßig überwacht werden. Zu den Überwachungstätigkeiten gehören Vor-Ort-Audits; ergänzend können Anfragen an den Kunden, die Bewertung von Aussagen des Kunden über seine Tätigkeiten, die Anforderung dokumentierter Informationen oder andere geeignete Mittel zur Überwachung der Leistungsfähigkeit gehören.

Überwachungsaudits sind Vor-Ort-Audits, jedoch nicht notwendigerweise vollständige Systemaudits. Sie werden so geplant, dass das Vertrauen in die fortgesetzte Konformität des zertifizierten Managementsystems zwischen den Re-Zertifizierungsaudits aufrechterhalten wird. Jede Überwachung umfasst mindestens interne Audits und Managementbewertung, die Bewertung umgesetzter Maßnahmen zu früheren Nichtkonformitäten, den Umgang mit Beschwerden, die Wirksamkeit des Managementsystems im Hinblick auf Ziele und beabsichtigte Ergebnisse, den Fortschritt kontinuierlicher Verbesserungen, die anhaltende operative Lenkung, die Bewertung von Änderungen sowie die Nutzung von Zertifikatszeichen und sonstigen Verweisen auf die Zertifizierung.

4.6.3 Re-Zertifizierung

Für die Berechnung der Auditzeit für das Rezertifizierungsaudit sollten aktualisierte Informationen des Kunden zugrunde gelegt werden; sie beträgt in der Regel zwei Drittel der Zeit, die für ein Erstzertifizierungsaudit (Stufe 1 + Stufe 2) der Organisation benötigt werden würde, wenn ein solches Erstaudit zum Zeitpunkt der Rezertifizierung durchgeführt würde. Es ist unwahrscheinlich, dass die Dauer eines Rezertifizierungsaudits weniger als einen Audittag umfasst.

Das Re-Zertifizierungsaudit wird so geplant und durchgeführt, dass die kontinuierliche Konformität und Wirksamkeit des Managementsystems als Ganzes sowie seine fortdauernde Bedeutung und Anwendbarkeit für den zertifizierten Geltungsbereich rechtzeitig vor Ablauf des Zertifikats beurteilt werden können. Dabei werden frühere Überwachungsauditberichte und die Leistungsfähigkeit des Managementsystems über den zurückliegenden Zertifizierungszyklus berücksichtigt. Bei signifikanten Änderungen des Managementsystems, der Organisation oder ihres Kontextes kann eine Stufe 1 erforderlich werden.

Das Re-Zertifizierungsaudit umfasst ein Vor-Ort-Audit. Es behandelt insbesondere die Wirksamkeit des Managementsystems in seiner Gesamtheit unter Berücksichtigung interner und externer Änderungen, die fortdauernde Relevanz und Anwendbarkeit des zertifizierten Geltungsbereichs sowie die dargelegte Verpflichtung des Kunden zur Aufrechterhaltung und Verbesserung der Wirksamkeit des Managementsystems. Wird das Re-Zertifizierungsaudit nicht rechtzeitig abgeschlossen oder kann die Umsetzung von Korrekturen und Korrekturmaßnahmen zu wesentlichen Nichtkonformitäten vor Ablauf der Zertifizierung nicht verifiziert werden, darf eine Re-Zertifizierung nicht empfohlen und die Gültigkeit der Zertifizierung nicht verlängert werden. Nach Ablauf der Zertifizierung kann diese innerhalb von sechs Monaten wiederhergestellt werden, sofern die ausstehenden Re-Zertifizierungstätigkeiten abgeschlossen werden; andernfalls ist mindestens eine erneute Stufe 2 durchzuführen.

4.6.4 Audits aus besonderem Anlass

Beantragt der Kunde eine Erweiterung des Geltungsbereichs einer bereits erteilten Zertifizierung, prüft die Zertifizierungsstelle den Antrag und legt die hierfür erforderlichen Audittätigkeiten fest. Die Bewertung kann im Zusammenhang mit einem Überwachungsaudit erfolgen.

Kurzfristig angekündigte oder unangekündigte Audits können erforderlich sein, um Beschwerden zu untersuchen, auf Änderungen zu reagieren oder ausgesetzte Zertifizierungen nachzuverfolgen. Die Bedingungen für solche Audits werden dem Kunden vorab bekannt gemacht. Wegen der eingeschränkten Möglichkeit des Kunden, gegen Teammitglieder Einwände zu erheben, wendet die Zertifizierungsstelle bei der Benennung des Auditteams besondere Sorgfalt an.

4.6.5 Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung

Die Zertifizierungsstelle verfügt über dokumentierte Regelungen und Verfahren für die Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung sowie für die jeweils zu ergreifenden Folgemaßnahmen.

Eine Aussetzung kommt insbesondere in Betracht, wenn das zertifizierte Managementsystem Anforderungen dauerhaft oder schwerwiegend nicht erfüllt, erforderliche Überwachungs- oder

Re-Zertifizierungsaudits nicht zugelassen werden oder der zertifizierte Kunde freiwillig um Aussetzung bittet.

Während der Aussetzung ist die Managementsystemzertifizierung des Kunden vorübergehend nicht gültig.

Die Zertifizierungsstelle stellt eine ausgesetzte Zertifizierung wieder her, wenn die Gründe für die Aussetzung wirksam beseitigt wurden. Werden diese Gründe nicht innerhalb des von der Zertifizierungsstelle festgelegten Zeitraums behoben, führt dies zur Zurückziehung der Zertifizierung oder zur Einschränkung ihres Geltungsbereichs. In der Regel übersteigt eine Aussetzung nicht sechs Monate.

Der Geltungsbereich der Zertifizierung wird eingeschränkt, wenn der zertifizierte Kunde die Zertifizierungsanforderungen für bestimmte Teile des Geltungsbereichs dauerhaft oder schwerwiegend nicht erfüllt. In diesem Fall sind die nicht konformen Teile vom zertifizierten Geltungsbereich auszuschließen.

4.7 Zertifizierungszyklus

Ein regulärer Zertifizierungsszyklus beträgt drei Jahre und umfasst mindestens drei Audits – ein Zertifizierungs- oder Re-Zertifizierungsaudit und zwei Überwachungsaudits.

5 Anforderungen der DIN ISO 37301:2021

5.1 Kontext der Organisation

Die Zertifizierung eines wirksamen CMS setzt eine gut geführte Organisation voraus, die über eine Compliance-Politik verfügt, die zur Erfüllung ihrer gesetzlichen Verpflichtungen und ihrer Verpflichtung zur Integrität durch geeignete Managementsysteme unterstützt wird.

Die Risiken, denen eine Organisation gegenübersteht, hängen von Faktoren wie der Größe, der Organisation, den Standorten und Branchen, in denen die Organisation tätig ist, sowie der Art, dem Umfang und der Komplexität der Aktivitäten der Organisation ab.

Dieses Programm legt Standards fest, die eine Prüfung in angemessenem Verhältnis zu Risiken, denen die Organisation gegenübersteht, gewährleistet.

Die Feststellung der Konformität mit dem Standard aus DIN ISO 37301 kann nicht gewährleisten, dass kein Compliance-Verstoß (Non-Compliance) auftritt oder auftreten wird. Sie bestätigt lediglich, dass die getroffenen Maßnahmen zur Prävention grundsätzlich geeignet sind.

Um ein Instrument in der Organisation zu schaffen, welches die tatsächlichen Risiken aufzeigt, der eine Organisation gegenübersteht, ist zunächst ein Verständnis der Arbeit der Organisation und ihres Umfeldes notwendig.

Dies bedeutet zum einen eine Erfassung der Größe, Standorte, Struktur und des Geschäftsmodells der Organisation, hierauf aufbauend auch der internen und externen Stakeholder. Bei der Ermittlung relevanter interessierter Parteien sind ggf. auch klimabezogene Anforderungen und Erwartungen dieser Parteien zu berücksichtigen. Darüber hinaus muss eine Identifizierung der wichtigsten Stakeholder und Themen erkennbar sein, sowie eine Einordnung der übrigen

Faktoren/Themen aufgrund ihrer Relevanz für die Organisation und anhand der Ausrichtung und Ziele der Organisation.

Im Rahmen der Ermittlung interner und externer Themen hat die Organisation zu bestimmen, ob der Klimawandel ein relevantes externes Thema ist, das die Fähigkeit beeinflusst, die beabsichtigten Ergebnisse des CMS zu erreichen. Das Ergebnis ist zu begründen und nachvollziehbar zu dokumentieren.

Aufgrund der erhobenen Daten soll eine Beurteilung des Risikos erfolgen. Diese wiederum führt zur Schaffung eines entsprechenden Managementsystems zur Compliance. Die Dokumentation des Systems erfasst den Anwendungsbereich, die Werte, Ziele, Strategie und identifizierten Risiken.

Ebenfalls müssen Prozesse angemessen dokumentiert sein, um neue und veränderte Compliance-Verpflichtungen sowie andere Veränderungen (z. B. des Kontextes) zu identifizieren, die Auswirkungen zu bewerten und notwendige Maßnahmen einleiten zu können.

5.2 Führung

Das gesamte Management einer Organisation, insbesondere ihre oberste Leitung/ihr oberstes Organ, muss in Bezug auf Compliance Führung und Verpflichtung zeigen. Es definiert die Politik, stellt die sich hieraus ergebende strategische Ausrichtung sicher, informiert sich über den wirksamen Betrieb, stellt geeignete Ressourcen für diesen Betrieb zur Verfügung und übt die Aufsicht über das vorgenannte aus. Die oberste Leitung hat hierüber die Gesamtverantwortung.

Die oberste Leitung muss eine Politik zur Compliance festlegen, aufrechterhalten und überprüfen, die:

- a) für den Zweck der Organisation angemessen ist,
- b) einen Rahmen zur Festlegung von Compliance – Zielen bietet,
- c) eine Verpflichtung zur Erfüllung zutreffender Anforderungen enthält,
- d) eine Verpflichtung zur fortlaufenden Verbesserung des CMS enthält.

Die Politik zur Compliance muss:

- mit den Werten, den Zielen und der Strategie der Organisation abgestimmt sein,
- die Einhaltung der Compliance-Verpflichtungen der Organisation fordern,
- die Grundsätze der Compliance-Führung unterstützen,
- auf die Compliance-Funktion Bezug nehmen und sie beschreiben,
- die Folgen der Nichteinhaltung der Compliance-Verpflichtungen, Politiken, Prozesse und Verfahren der Organisation beschreiben,
- das Melden von Bedenken fordern und jede Form von Vergeltung verbieten,
- in einfacher Sprache formuliert sein,
- angemessen bekanntgemacht, eingeführt und durchgesetzt sein,

- als dokumentierte Information für Mitarbeitende und interessierte Parteien verfügbar sein.

Die oberste Leitung und das Management stellen sicher, dass die Politik bekannt gemacht und umgesetzt wird, dies wird in der Regel durch ein Compliance-Organ geschehen. Idealerweise ist das Compliance-Organ präventiv tätig, um ein Verhalten zu vermeiden, das den rechtlichen Vorgaben und den ethischen Standards des Unternehmens widerspricht oder noch besser ein Verhalten fördert, das in Übereinstimmung mit den geltenden Rechtsvorschriften steht sowie an ethischen Standards als Unternehmenskultur ausgerichtet ist. Dazu muss die Compliance-Organisation die einzuhaltenden rechtlichen Vorgaben und ethischen Standards festlegen und in den einschlägigen Regelwerken des Unternehmens festschreiben. (Bay/Hastenrath CMS/Daum, 3. Aufl. 2022, § 5 Rn. 7, beck-online)

Die oberste Leitung muss einer **Compliance-Funktion** als Kopf der Compliance-Organisation die Verantwortlichkeit und Befugnis zuweisen für:

- a) die Unterstützung der Identifizierung von Compliance-Verpflichtungen,
- b) die Beaufsichtigung der Gestaltung und Verwirklichung des CMS durch die Organisation sowie die Analyse, Bewertung und Dokumentation des Systems und entsprechende Schulung der Mitarbeitenden,
- c) die Bereitstellung von Beratung und Anleitung des Personals über das CMS und das Bereitstellen von Hinweisgebersystemen,
- d) das Sicherstellen, dass das CMS die Anforderungen dieses Dokuments erfüllt,
- e) das Berichten über die Leistung des CMS an das oberste Organ (wenn vorhanden) und an die oberste Leitung und andere mit der Compliance betraute Funktionen, sofern zutreffend.

Die Compliance-Funktion muss angemessen ausgestattet und einer Person bzw. Personen zugewiesen sein, die in angemessener Weise über Kompetenz, Status, Verantwortung und Unabhängigkeit verfügt bzw. verfügen. Die Compliance-Funktion muss direkten und sofortigen Zugang zum obersten Organ (wenn vorhanden) und der obersten Leitung haben, wenn Themen oder Bedenken in Bezug auf das CMS geklärt werden müssen.

Weiter müssen die Compliance-Funktion oder die oberste Führung dafür sorgen, dass die Verantwortlichkeiten für die Erreichung der aus der Compliance-Politik abgeleiteten Verpflichtungen in der Organisation angemessen zugewiesen sind und die Verpflichtungen in nachgeordnete Politiken, Prozesse und Verfahren integriert werden. Hierzu muss die Compliance-Funktion Zugang zum gesamten Personal sowie sämtlichen erforderlichen dokumentierten Informationen und Daten erhalten.

5.3 Planung

Bei der Planung sind – soweit Klimawandel als relevant bestimmt wurde oder relevante interessierte Parteien entsprechende Anforderungen stellen – daraus resultierende Compliance-Ziele, -Verpflichtungen und -Risiken zu berücksichtigen. Ziele müssen messbar sein und dokumentiert werden. Die Planung und jede spätere Änderung haben sicherzustellen, dass das

CMS seine angestrebten Ergebnisse erreicht, unerwünschte Auswirkungen ausbleiben und eine fortlaufende Verbesserung erzielt wird.

Bei der Planung zum Erreichen der Compliance-Managementsystemziele muss die Organisation bestimmen:

- was getan wird;
- welche Ressourcen erforderlich sind;
- wer verantwortlich ist;
- wann die Maßnahme abgeschlossen ist;
- wie die Ergebnisse bewertet und berichtet werden.

Die Maßnahmen müssen dokumentiert werden.

Planung und Änderungen werden unter Berücksichtigung der folgenden Punkte durchgeführt:

- Zweck der Änderung und mögliche Konsequenzen;
- die Gestaltung und betriebliche Wirksamkeit des CMS;
- Verfügbarkeit angemessener Ressourcen;
- die Zuweisung oder Neuzuweisung von Verantwortlichkeiten und Befugnissen.

In die Planung muss auch die regelhafte Aktualisierung der Maßnahmen einfließen.

5.4 Unterstützung

Die Organisation muss die erforderlichen Ressourcen für den Aufbau, die Verwirklichung, die Aufrechterhaltung und die fortlaufende Verbesserung des CMS bestimmen und bereitstellen.

Personal muss entsprechend kompetent und regelmäßig geschult sein, ggf. ist ein Mentoring notwendig, insbesondere ist die Auswahl des Personals mit der entsprechenden Sorgfalt durchzuführen. Die Einhaltung der Compliance-Verpflichtungen, - Politiken, - Prozesse,- und Verfahren ist von den Mitarbeitenden zu verlangen und ihnen jederzeit zu ermöglichen.

Die Personalverwaltung muss Prozesse zur Schulung, Überwachung der Kompetenz und Disziplinierung leben. Inhalt der Schulungen soll die Schaffung eines Bewusstseins für die Inhalte des CMS und die Herbeiführung einer Akzeptanz der ihm inhärenten Werte sein, Schulungen sind an möglicherweise stattfindende Veränderungen anzupassen und ggf. zyklisch durchzuführen.

Führungspersonen oder das Management einer Organisation sollen Erklärungen mit dem üblichen Inhalt eines Code of Conduct abgegeben haben. Personal darf nicht durch Vorgesetzte oder die Organisation in eine Lage gebracht werden, die rechtswidriges Handeln fördert oder verlangt. Die Organisation muss es den Führungskräften ermöglichen und sie verpflichten, das Bewusstsein der Mitarbeitenden für das CMS zu entwickeln und den Rahmen für ein Compliance-gerechtes Verhalten zu schaffen.

Geschäftspartner müssen von dem CMS in Kenntnis gesetzt werden. Sie sind auf die Einhaltung dieser Normen im Rahmen des Möglichen zu verpflichten und zu überwachen.

Die Organisation muss die interne und externe Kommunikation in Bezug auf das CMS bestimmen und umfassend dokumentieren. Den Mitarbeitenden ist ein gesicherter Weg zum sanktionslosen Vorbringen von Compliance-Bedenken aufzuzeigen.

Das CMS der Organisation muss, abhängig von der Größe der Organisation und der Art ihrer Tätigkeiten, Prozesse, Produkte und Dienstleistungen, der Komplexität ihrer Prozesse und deren Wechselwirkungen, der Kompetenz des Personals beinhalten:

- a) die von diesem Dokument geforderte dokumentierte Information;
- b) dokumentierte Information, welche die Organisation als notwendig für die Wirksamkeit des CMS bestimmt hat.

Bei der Erstellung und Aktualisierung dokumentierter Information muss die Organisation:

- a) die angemessene Kennzeichnung und Beschreibung (z. B. Titel, Datum, Autor oder Referenznummer)
- b) ein angemessenes Format (z. B. Sprache, Softwareversion, Grafiken) und Medium (z. B. Papier, elektronisch)
- c) die angemessene Überprüfung und Genehmigung im Hinblick auf Eignung und Angemessenheit

sicherstellen.

Die für das CMS erforderliche und von diesem Dokument geforderte dokumentierte Information muss gelenkt werden, um sicherzustellen, dass sie:

- a) verfügbar und für die Verwendung geeignet ist, wo und wann sie benötigt wird;
- b) angemessen geschützt wird (z. B. vor Verlust der Vertraulichkeit, unsachgemäßem Gebrauch oder Verlust der Integrität).

Zur Lenkung dokumentierter Information muss die Organisation, falls zutreffend, folgende Aktivitäten berücksichtigen:

- Verteilung, Zugriff, Auffindung und Verwendung;
- Ablage/Speicherung und Erhaltung, einschließlich Erhaltung der Lesbarkeit;
- Überwachung von Änderungen (z. B. Versionskontrolle);
- Aufbewahrung und Bereitstellung.

Dokumentierte Information externer Herkunft, die von der Organisation als notwendig für Planung und Betrieb des CMS bestimmt wurde, muss angemessen identifiziert und gelenkt werden.

5.5 Betrieb

Die betriebliche Planung und Steuerung beinhalten zwingend die Festlegung und fortlaufende Beurteilung der Kriterien für die Prozesse, die Steuerung der Prozesse anhand dieser Kriterien und die entsprechende Dokumentation im notwendigen Umfang. Geplante Änderungen müssen ebenfalls anhand dieser Kriterien gesteuert werden.

Die Beurteilung muss die notwendige gebührende Sorgfalt umfassen, um ausreichende Informationen zur Beurteilung des Compliance-Risikos zu erhalten.

Die Steuerung muss eine finanzielle und eine nicht-finanzielle Steuerung umfassen. Finanzielle Steuerungen sind die von der Organisation verwirklichten Managementsysteme und Prozesse, um ihre finanziellen Transaktionen ordnungsgemäß zu führen und zu steuern und diese

Transaktionen fehlerlos, vollständig und rechtzeitig aufzuzeichnen. Nicht-finanzielle Steuerungen sind die von der Organisation verwirklichten Managementsysteme und Prozesse, die ihr helfen sicherzustellen, dass die Beschaffungs- und Betriebsaspekte, kommerzielle und andere nicht-finanzielle Aspekte ihrer Aktivitäten ordnungsgemäß geführt und gesteuert werden.

Mitarbeitende müssen die Möglichkeit bekommen, im Geschäftsprozess Bedenken zu äußern.

Die Organisation muss dafür Sorge tragen, sicherzustellen, dass auch Geschäftspartner diese Kriterien angemessen beachten. Es sind „red flags“ zum Abbruch von Verhandlungen und Geschäftsbeziehungen zu definieren.

Wirksame interne Richtlinien zur Annahme von Vorteilen, zur internen Ermittlung und zum Whistleblowing sind notwendig und aktiv zu beachten.

Im Einstellungsprozess von Personal und in der Geschäftspartnerakquise sind diese Kriterien ebenfalls sicherzustellen, ggf. ist die Exportkontrolle durchzuführen.

5.6 Bewertung der Leistung

Die Organisation muss bestimmen:

- a) was überwacht und gemessen werden muss;
- b) wer für die Überwachung verantwortlich ist;
- c) die Methoden zur Überwachung, Messung, Analyse und Bewertung, sofern zutreffend, um gültige Ergebnisse sicherzustellen;
- d) wann die Überwachung und Messung durchzuführen ist;
- e) wann die Ergebnisse der Überwachung und Messung zu analysieren und zu bewerten sind;
- f) wem und wie solche Informationen berichtet werden müssen.

Die Organisation muss geeignete dokumentierte Informationen als Nachweis der Methoden und Ergebnisse aufbewahren sowie die Compliance-Leistung und die Wirksamkeit und Effizienz des CMS bewerten.

Es müssen Audits mit dem Ziel der Feststellung der Wirksamkeit des CMS durchgeführt werden. Ebenso müssen die oberste Leitung und der Compliance Officer regelmäßig feststellen, ob sämtliche Mechanismen des CMS wirksam in der Organisation gelebt werden. Sie müssen sich insbesondere über die Ergebnisse der Audits, Korrekturmaßnahmen und interne Ermittlungen informieren.

Ebenfalls muss das oberste Organ/die oberste Leitung das CMS regelmäßig auf seine Angemessenheit, Geeignetheit und Wirksamkeit überprüfen.

Diese Prüfung muss folgende Aspekte behandeln:

- Den Status von Maßnahmen vorheriger Managementbewertungen,
- Veränderungen bei externen und internen Themen, die das CMS betreffen, einschließlich klimabezogener externer Themen (sofern zutreffend),

- Veränderungen bei Bedürfnissen und Erwartungen interessierter Parteien, die das CMS betreffen, einschließlich klimabezogener Anforderungen/Erwartungen interessierter Parteien (sofern zutreffend),
- Informationen über die Compliance-Leistung, einschließlich Entwicklungen bei Nichtkonformität, Non-Compliance und Korrekturmaßnahmen, Ergebnissen von Überwachungen und Messungen sowie den Auditergebnissen,
- Möglichkeiten zur fortlaufenden Verbesserung.

Hierbei muss die Prüfung die Eignung der Compliance-Politik, die Unabhängigkeit der Compliance-Funktion, den Grad, zu dem die Compliance-Ziele erfüllt wurden, die Angemessenheit der Ressourcen, die Risikobeurteilung, Wirksamkeit von Kontrollen und Leistungsindikatoren, Wirksamkeit der Kommunikation und des Berichtssystems enthalten.

Die zu dokumentierende Ergebnisse müssen Entscheidungen zu Maßnahmen enthalten.

5.7 Verbesserung

Die Organisation muss die Eignung, Angemessenheit und die Wirksamkeit des CMS fortlaufend verbessern.

Wenn eine Nichtkonformität auftritt, muss die Organisation:

- 1) darauf reagieren und, falls zutreffend:
 - a) Maßnahmen zur Überwachung und zur Korrektur ergreifen;
 - b) mit den Folgen umgehen;
- 2) die Notwendigkeit von Maßnahmen zur Beseitigung der Ursachen von Nichtkonformitäten bewerten, damit diese nicht erneut oder an anderer Stelle auftreten, und zwar durch:
 - a) Überprüfen der Nichtkonformität;
 - b) Bestimmen der Ursachen der Nichtkonformität;
 - c) Bestimmen, ob vergleichbare Nichtkonformitäten bestehen oder möglicherweise auftreten könnten;
- 3) jegliche erforderliche Maßnahme einleiten;
- 4) die Wirksamkeit jeglicher ergriffener Korrekturmaßnahme überprüfen;
- 5) sofern erforderlich, das CMS ändern.

Korrekturmaßnahmen müssen den Auswirkungen der aufgetretenen Nichtkonformitäten angemessen sein.

Die Organisation muss dokumentierte Informationen aufbewahren, als Nachweis:

- a) der Art der Nichtkonformität sowie jeder daraufhin getroffenen Maßnahme;
- b) der Ergebnisse jeder Korrekturmaßnahme.

6 Datenschutz und Vertraulichkeit

Der Kunde stellt sicher, dass die Verarbeitung personenbezogener Daten im Rahmen des Zertifizierungsverfahrens rechtmäßig erfolgt. Die Zertifizierungsstelle behandelt alle im Zertifizierungsprozess erlangten Informationen vertraulich; eine Weitergabe erfolgt nur mit Zustimmung des Kunden oder auf Grundlage gesetzlicher Verpflichtungen bzw. behördlicher Anforderungen (z. B. Akkreditierungsanforderungen).

7 Änderungen und Ausnahmen

Der Kunde teilt der Zertifizierungsstelle alle geplanten oder eingetretenen Änderungen mit, die den Geltungsbereich, die Standorte, wesentliche Prozesse, die Organisation, das Managementsystem, Compliance-Verpflichtungen, Compliance-Risiken, die Compliance-Funktion oder die Fähigkeit zur Konformität beeinflussen können. Änderungen können eine Anpassung des Auditprogramms, des Geltungsbereichs oder Sonderaudits erforderlich machen.

Ausnahmen von diesem Zertifizierungsprogramm sind nur zulässig, wenn sie durch anwendbare Regelwerke gedeckt und durch die Zertifizierungsstelle dokumentiert sowie - sofern erforderlich - durch die Akkreditierungsstelle akzeptiert sind.

8 Sanktionen und Folgen bei Nichteinhaltung

Bei Nichterfüllung von Mitwirkungspflichten, bei schwerwiegenden oder wiederholten Nichtkonformitäten oder bei Verstößen gegen die Regeln zur Nutzung von Zertifikat/Zeichen kann die Zertifizierungsstelle geeignete Maßnahmen ergreifen. Dies kann u. a. die Forderung von Korrekturen/Korrekturmaßnahmen, zusätzliche Audits, die Einschränkung des Geltungsbereichs, die Aussetzung oder den Entzug der Zertifizierung umfassen.

Im Falle einer Aussetzung oder eines Entzugs der Zertifizierung stellt der Kunde die Nutzung von Zertifikat, Zertifikatszeichen und werblichen Aussagen zur Zertifizierung unverzüglich ein.

9 Versionierung und Änderungsverfolgung

Dieses Zertifizierungsprogramm unterliegt der Dokumentenlenkung der ZertBau. Änderungen werden versioniert, nachvollziehbar dokumentiert und den betroffenen interessierten Parteien bei Bedarf mitgeteilt. Die jeweils gültige Fassung wird durch die Zertifizierungsstelle bereitgestellt.

Anhang A – Begleitende Pflichttabelle

Die nachfolgende Pflichttabelle dient als internes Arbeitspapier zur Nachverfolgung von Pflichten des Kunden im Zertifizierungsprozess.

Nr.	Quelle (Dok/Abschnitt)	Thema	Pflichtentwurf	Klassifi- kation	Frist/Termin	Nachweise
1	ISO/IEC 17021-1	Verfügbarkeit von Informationen	Der Kunde muss der Zertifizierungsstelle alle für Angebot, Auditplanung und Zertifizierungsentscheidung erforderlichen Informationen vollständig, richtig und aktuell bereitstellen.	Muss	vor Vertragsabschluss; laufend	Antragsdaten, Scope, Standortliste, Mitarbeiterzahlen, Prozess-/Tätigkeitsbeschreibung, Angaben zu Compliance-Verpflichtungen und Compliance-Risiken
2	Zertifizierungsprogramm / ISO/IEC 17021-1	Auditzeit und Auditprogramm	Der Kunde muss alle Angaben bereitstellen, die zur Ermittlung der Auditzeit und zur Festlegung des Auditprogramms erforderlich sind, und Änderungen unverzüglich melden, sofern diese Einfluss auf Auditzeit oder Auditprogramm haben.	Muss	vor Auditplanung; bei Änderungen unverzüglich	Mitarbeiterzahlen, Schichtsystem, Komplexität, Standorte/temporäre Standorte, Outsourcing, CMS-Reifegrad, wesentliche Compliance-Risiken
3	DIN ISO 37301:2021, 4.1	Kontext	Der Kunde muss externe und interne Themen bestimmen, die für Zweck und Kontext der Organisation relevant sind und die Fähigkeit beeinflussen, beabsichtigte Ergebnisse des CMS zu erreichen.	Muss	fortlaufend; Aktualisierung anlassbezogen	Kontextanalyse, Strategie-/Geschäftsmodellbeschreibung, Analyse rechtlicher, regulatorischer, wirtschaftlicher, sozialer und

Nr.	Quelle (Dok/Abschnitt)	Thema	Pflichtentwurf	Klassifikation	Frist/Termin	Nachweise
						kultureller Rahmenbedingungen
4	DIN ISO 37301:2021, 4.2	Interessierte Parteien	Der Kunde muss relevante interessierte Parteien, deren Anforderungen und die durch das CMS zu behandelnden Anforderungen bestimmen.	Muss	fortlaufend; Aktualisierung anlassbezogen	Liste interessierter Parteien, Anforderungs- und Relevanzbewertung
5	DIN ISO 37301:2021, 4.3	Anwendungsbereich	Der Kunde muss Grenzen und Anwendbarkeit des CMS bestimmen, den Anwendungsbereich festlegen und als dokumentierte Information verfügbar halten.	Muss	vor Stufe 1; Aktualisierung anlassbezogen	Scope-Dokument, organisatorische/geografische Abgrenzung, Prozess- und Standortabgrenzung
6	DIN ISO 37301:2021, 4.4	CMS-Prozesse	Der Kunde muss ein CMS aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern, einschließlich der benötigten Prozesse und ihrer Wechselwirkungen.	Muss	fortlaufend	CMS-Prozesslandschaft, Prozessbeschreibungen, Wechselwirkungsdarstellung, Wirksamkeitsnachweise
7	DIN ISO 37301:2021, 4.5	Compliance-Verpflichtungen	Der Kunde muss Compliance-Verpflichtungen systematisch identifizieren, deren Auswirkungen auf den Betrieb bewerten, Änderungen erkennen und notwendige Anpassungen einführen.	Muss	fortlaufend; Aktualisierung anlassbezogen	Compliance-Register/Rechtskataster, Änderungsmonitoring, Bewertungs- und Maßnahmenachweise

Nr.	Quelle (Dok/Abschnitt)	Thema	Pflichtentwurf	Klassifikation	Frist/Termin	Nachweise
8	DIN ISO 37301:2021, 4.6	Compliance-Risikobeurteilung	Der Kunde muss Compliance-Risiken identifizieren, analysieren und bewerten, einschließlich Risiken aus ausgelagerten oder durch Dritte ausgeführten Prozessen.	Muss	regelmäßig und bei wesentlichen Änderungen	Compliance-Risikobeurteilung, Risikoregister, Maßnahmen zur Behandlung von Risiken, Bewertungsnachweise
9	DIN ISO 37301:2021, 5.1.1	Führung und Verpflichtung	Das oberste Organ und die oberste Leitung müssen Führung und Verpflichtung zum CMS nachweisen und sicherstellen, dass CMS-Anforderungen in Geschäftsprozesse integriert und Ressourcen bereitgestellt werden.	Muss	fortlaufend	Politik, Zielsystem, Ressourcenfreigaben, Berichtswege, Protokolle/Entscheidungen der Leitung
10	DIN ISO 37301:2021, 5.1.2	Compliance-Kultur	Der Kunde muss eine Compliance-Kultur auf allen Ebenen entwickeln, aufrechterhalten und fördern.	Muss	fortlaufend	Kommunikationsnachweise, Schulungen, Tone-from-the-top, Kultur-/Integritätsmaßnahmen
11	DIN ISO 37301:2021, 5.1.3	Compliance-Führung	Der Kunde muss direkten Zugang, Unabhängigkeit sowie angemessene Befugnis und Kompetenz der Compliance-Funktion sicherstellen.	Muss	fortlaufend	Organigramm, Berichtslinien, Stellen-/Rollenbeschreibungen, Zugangs- und Eskalationsregelungen

Nr.	Quelle (Dok/Abschnitt)	Thema	Pflichtentwurf	Klassifikation	Frist/Termin	Nachweise
12	DIN ISO 37301:2021, 5.2	Compliance-Politik	Der Kunde muss eine Compliance-Politik festlegen, dokumentieren, kommunizieren, durchsetzen und interessierten Parteien soweit angemessen verfügbar machen.	Muss	fortlaufend; Aktualisierung anlassbezogen	Compliance-Politik, Freigabe, Kommunikationsnachweise, Veröffentlichungsnachweise
13	DIN ISO 37301:2021, 5.3	Rollen und Verantwortlichkeiten	Der Kunde muss Verantwortlichkeiten und Befugnisse für CMS-relevante Rollen zuweisen und kommunizieren, einschließlich oberstem Organ, oberster Leitung, Leitung, Compliance-Funktion und Personal.	Muss	fortlaufend; Aktualisierung anlassbezogen	Organigramm, Rollen-/Stellenbeschreibungen, Geschäftsordnung, Delegations- und Vertretungsregelungen
14	DIN ISO 37301:2021, 6.1	Risiken und Möglichkeiten	Der Kunde muss Maßnahmen zum Umgang mit Risiken und Möglichkeiten planen, um beabsichtigte Ergebnisse zu erreichen und unerwünschte Auswirkungen zu verhindern oder zu verringern.	Muss	fortlaufend; mind. jährlich prüfen	Risikoregister, Maßnahmenpläne, Verantwortlichkeiten, Wirksamkeitsbewertung
15	DIN ISO 37301:2021, 6.2	Compliance-Ziele	Der Kunde muss Compliance-Ziele festlegen, planen, überwachen, kommunizieren, aktualisieren und dokumentieren.	Muss	mind. jährlich; anlassbezogen	Zielmatrix, Kennzahlen/Indikatoren, Maßnahmen- und Bewertungsplanung
16	DIN ISO 37301:2021, 6.3	Planung von Änderungen	Der Kunde muss Änderungen am CMS geplant durchführen und Auswirkungen, Ressourcen, Verantwortlichkeiten und Integrität des CMS berücksichtigen.	Muss	vor Umsetzung	Änderungsanträge, Freigaben, Risiko- und Folgenbewertung, Maßnahmenpläne

Nr.	Quelle (Dok/Abschnitt)	Thema	Pflichtentwurf	Klassifikation	Frist/Termin	Nachweise
17	DIN ISO 37301:2021, 7.1	Ressourcen	Der Kunde muss die für Aufbau, Verwirklichung, Aufrechterhaltung und fortlaufende Verbesserung des CMS erforderlichen Ressourcen bestimmen und bereitstellen.	Muss	fortlaufend	Ressourcenplanung, Budget-/Kapazitätsnachweise, Freigaben
18	DIN ISO 37301:2021, 7.2	Kompetenz	Der Kunde muss erforderliche Kompetenz bestimmen, sicherstellen, Wirksamkeit von Maßnahmen bewerten und Kompetenznachweise aufbewahren.	Muss	fortlaufend	Qualifikationsmatrix, Schulungs- und Erfahrungsnachweise, Wirksamkeitsbewertungen
19	DIN ISO 37301:2021, 7.2.2	Beschäftigungsprozess	Der Kunde muss im Beschäftigungsprozess CMS-relevante Anforderungen berücksichtigen, soweit dies für Funktionen und Compliance-Risiken angemessen ist.	Muss	bei Einstellung/Versetzung; fortlaufend	Einstellungs-/Onboarding-Nachweise, Verpflichtungserklärungen, Rollenanforderungen, Due-Diligence-Nachweise soweit zutreffend
20	DIN ISO 37301:2021, 7.2.3	Schulung	Der Kunde muss Schulungen zum CMS bedarfsgerecht planen und durchführen, insbesondere für Personen mit relevanten Compliance-Verantwortlichkeiten oder Compliance-Risiken.	Muss	fortlaufend; gemäß Schulungsplan	Schulungsplan, Teilnehmerlisten, Inhalte, Wirksamkeitsnachweise
21	DIN ISO 37301:2021, 7.3	Bewusstsein	Der Kunde muss Bewusstsein für Compliance-Politik, Compliance-Kultur, eigene Beiträge, Meldemöglichkeiten und Folgen von Non-Compliance sicherstellen.	Muss	fortlaufend	Unterweisungen, Kommunikationsnachweise, Awareness-

Nr.	Quelle (Dok/Abschnitt)	Thema	Pflichtentwurf	Klassifi- kation	Frist/Termin	Nachweise
						Kampagnen, Teilnehmerlisten
22	DIN ISO 37301:2021, 7.4	Kommunikation	Der Kunde muss interne und externe Kommunikation zum CMS festlegen und umsetzen, einschließlich Inhalte, Zeitpunkte, Empfänger und Methoden.	Muss	fortlaufend	Kommunikationsmatrix, Protokolle, Informationsnachweise, Eskalationswege
23	DIN ISO 37301:2021, 7.5	Dokumentierte Information	Der Kunde muss dokumentierte Informationen erstellen, aktualisieren und lenken, einschließlich Zugriff, Schutz, Verfügbarkeit, Aufbewahrung und Änderungskontrolle.	Muss	fortlaufend	Dokumentenlenkung, Versionsnachweise, Aufbewahrungsregelungen, Zugriffskonzepte
24	DIN ISO 37301:2021, 8.1	Betriebliche Planung und Steuerung	Der Kunde muss CMS-relevante Prozesse planen, Kriterien festlegen, Steuerungen umsetzen, Änderungen lenken und ausgelagerte Prozesse steuern.	Muss	fortlaufend	Prozess-/Verfahrens-anweisungen, Kontrollen, Änderungslenkung, Outsourcing-Steuerung
25	DIN ISO 37301:2021, 8.2	Steuerungen und Verfahren	Der Kunde muss angemessene Steuerungen und Verfahren festlegen, um Compliance-Verpflichtungen zu erfüllen und Compliance-Risiken zu behandeln.	Muss	fortlaufend	Kontrollmatrix, Verfahrensbeschreibungen, Genehmigungs-/Freigabeprozesse, Due-Diligence-Unterlagen
26	DIN ISO 37301:2021, 8.3	Äußern von Bedenken	Der Kunde muss ein System zum Äußern und Behandeln von Bedenken bereitstellen,	Muss	fortlaufend; Meldungen	Meldekanäle, Verfahrensregelung, Fallregister, Schutz- und

Nr.	Quelle (Dok/Abschnitt)	Thema	Pflichtentwurf	Klassifikation	Frist/Termin	Nachweise
			das Meldungen ermöglicht, Vertraulichkeit berücksichtigt und Vergeltung untersagt.		unverzüglich behandeln	Vertraulichkeitsnachweise
27	DIN ISO 37301:2021, 8.4	Untersuchungsprozesse	Der Kunde muss Prozesse zur Untersuchung vermuteter oder tatsächlicher Non-Compliance festlegen, durchführen, dokumentieren und daraus erforderliche Maßnahmen ableiten.	Muss	anlassbezogen; unverzüglich nach Meldung/Feststellung	Untersuchungsberichte, Fallakten, Maßnahmenpläne, Eskalationsnachweise
28	DIN ISO 37301:2021, 9.1	Überwachung, Messung, Analyse, Bewertung	Der Kunde muss festlegen, was zur Compliance-Leistung überwacht, gemessen, analysiert und bewertet wird, und dokumentierte Informationen als Nachweis aufbewahren.	Muss	fortlaufend; gemäß Bewertungsplanung	Kennzahlen, Auswertungen, Compliance-Reports, Bewertungsnachweise
29	DIN ISO 37301:2021, 9.1.2-9.1.5	Feedback, Indikatoren, Berichte, Aufzeichnungen	Der Kunde muss geeignete Feedback-Quellen, Indikatoren, Compliance-Berichte und Aufzeichnungen nutzen, um die Leistung des CMS zu bewerten.	Muss	fortlaufend; gemäß Berichtszyklus	Feedbackauswertungen, Indikatoren, Berichte an Leitung/Compliance-Funktion, Aufzeichnungen
30	DIN ISO 37301:2021, 9.2	Interne Audits	Der Kunde muss interne Audits planen, durchführen und dokumentieren; das Auditprogramm muss Risiken, Bedeutung der Prozesse und Ergebnisse früherer Audits berücksichtigen.	Muss	mind. jährlich, gemäß Auditprogramm	Auditprogramm und -planung, Auditberichte, Maßnahmenverfolgung

Nr.	Quelle (Dok/Abschnitt)	Thema	Pflichtentwurf	Klassifikation	Frist/Termin	Nachweise
31	DIN ISO 37301:2021, 9.3	Managementbewertung	Der Kunde muss Managementbewertungen des CMS durchführen und dokumentieren; daraus abgeleitete Maßnahmen sind zu verfolgen.	Muss	mind. jährlich; anlassbezogen	Managementreview, Protokoll zur Managementbewertung, Maßnahmenliste
32	DIN ISO 37301:2021, 10.1	Fortlaufende Verbesserung	Der Kunde muss die Eignung, Angemessenheit und Wirksamkeit des CMS fortlaufend verbessern.	Muss	fortlaufend	Verbesserungsmaßnahmen, Trendanalysen, Maßnahmencontrolling
33	DIN ISO 37301:2021, 10.2	Nichtkonformität und Korrekturmaßnahmen	Der Kunde muss auf Nichtkonformitäten und Non-Compliance reagieren, Ursachen analysieren, Korrekturmaßnahmen umsetzen und deren Wirksamkeit bewerten.	Muss	Fristen gemäß Maßnahmenplan; unverzüglich bei wesentlichen Fällen	Abweichungs-/Falllisten, Ursachenanalysen, Korrekturen, Korrekturmaßnahmen, Wirksamkeitsnachweise
34	Zertifizierungsprogramm / IAF MD 1	Multi-Site, falls zutreffend	Sofern eine Multi-Site-Zertifizierung vereinbart ist, muss der Kunde eine vollständige und aktuelle Standortliste bereitstellen und die Standortstichprobe sowie zentrale Steuerung nachvollziehbar ermöglichen.	Muss	vor Auditplanung; bei Änderungen unverzüglich	Standortliste, zentrale Prozesse, interne Audit-/Review-Nachweise je Standort
35	Zertifizierungsprogramm / IAF MD 4	IKT/Remote, falls zutreffend	Sofern IKT- oder Remote-Methoden eingesetzt werden, muss der Kunde die technischen und organisatorischen Voraussetzungen bereitstellen und Informationssicherheit gewährleisten.	Muss	vor Audit; während Audit	Zugänge, Datenschutz-/IS-Regelungen, Protokolle