Olaf Mußmann

Die ISO 37301 – eine Norm für Compliance-Managementsysteme

Entwicklung, Aufbau, Anwendung

Die ISO 37301 der *International Organization for Standardization* ist eine weltweit geltende Norm für Compliance-Managementsysteme, welche der Sicherstellung von Organisationsverantwortung und rechtskonformem Verhalten dient. Ihre Entstehung ist eng mit der zunehmenden Bedeutung unternehmensethischer Fragen und der Notwendigkeit effektiver Regeltreue in einem zunehmend komplexen regulatorischen Umfeld verbunden.

Entwicklung

Die ISO 37301 löste 2014 die ISO 19600 ab, eine Leitlinie für Compliance-Managementsysteme, die als nicht-zertifizierbarer Standard konzipiert war und primär der Orientierung diente. Aufgrund zunehmender Nachfrage nach einer verbindlicheren und auditierbaren Norm beschloss die Internationale Organisation für Normung (ISO), eine neue Version zu entwickeln. So wurde 2021 die ISO 37301:2021 unter dem Titel „Compliance Management systems – Requirements with guidance for use“ veröffentlicht. Sie ersetzte die ISO 19600 und ist im Gegensatz zu dieser als zertifizierbarer Standard ausgelegt.[1]

Aufbau

Die ISO 37301 basiert auf der High-Level Structure (HLS) der ISO und ist damit kompatibel mit anderen Managementsystemnormen wie ISO 9001 (Qualitätsmanagement) oder ISO 14001 (Umweltmanagement). Die auf das Compliance-Managementsysteme ausgerichtete HLS-Struktur sieht folgendermaßen aus:

1 Anwendungsbereich
2 Normative Verweisungen
3 Begriffe
4 Kontext der Organisation
 4.1 Verstehen der Organisation und ihres Kontextes
 4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien
 4.3 Festlegen des Anwendungsbereichs des Compliance-Managementsystems
 4.4 Compliance-Managementsystem
 4.5 Compliance-Verpflichtungen
 4.6 Compliance-Risikobeurteilung
5 Führung
 5.1 Führung und Verpflichtung
 5.1.1 Oberstes Organ und oberste Leitung
 5.1.2 Compliance-Kultur
 5.1.3 Compliance-Führung
 5.2 Compliance-Politik
 5.3 Rollen, Verantwortlichkeiten und Befugnisse
 5.3.1 Oberstes Organ und oberste Leitung
 5.3.2 Compliance-Funktion
 5.3.3 Leitung
 5.3.4 Personal
6 Planung
 6.1 Maßnahmen zum Umgang mit Risiken und Möglichkeiten
 6.2 Compliance-Ziele und Planung zu deren Erreichung
 6.3 Planung von Änderungen
7 Unterstützung
 7.1 Ressourcen
 7.2 Kompetenz
 7.2.1 Allgemeines
 7.2.2 Beschäftigungsprozess
 7.2.3 Schulung
 7.3 Bewusstsein
 7.4 Kommunikation

Hannover, 2024, veröffentlicht unter https://mussmann-partner-consulting.net/download

7.5 Dokumentierte Information
7.5.1 Allgemeines
7.5.2 Erstellung und Aktualisierung dokumentierter Information
7.5.3 Lenkung dokumentierter Information
8 Betrieb
8.1 Betriebliche Planung und Steuerung
8.2 Festlegung der Steuerungen und Verfahren
8.3 Äußern von Bedenken
8.4 Untersuchungsprozesse
9 Bewertung der Leistung
9.1 Überwachung, Messung, Analyse und Bewertung
9.1.1 Allgemeines
9.1.2 Feedback-Quellen zur Compliance-Leistung
9.1.3 Entwicklung von Indikatoren
9.1.4 Compliance-Berichte
9.1.5 Aufzeichnungen
9.2 Internes Audit
9.2.1 Allgemeines
9.2.2 Programm des internen Audits
9.3 Managementbewertung
9.3.1 Allgemeines
9.3.2 Eingaben für die Managementbewertung
9.3.3 Managementbewertungsergebnisse
10 Verbesserung
10.1 Fortlaufende Verbesserung
10.2 Nichtkonformität und Korrekturmaßnahmen

Diese Struktur erleichtert es Organisationen, integrierte Managementsysteme aufzubauen, in denen Compliance als Querschnittsfunktion verankert ist.[2]

Die Norm betont nicht nur die Einhaltung gesetzlicher Vorgaben, sondern auch freiwilliger Verpflichtungen, ethischer Grundsätze und interner Richtlinien.

Inhaltlich deckt die Norm ein breites Spektrum ab: Von der Analyse des organisatorischen Kontexts über Führungsverantwortung, Planung, Unterstützung und Betrieb bis hin zur Leistungsbewertung und kontinuierlichen Verbesserung. Besonders hervorgehoben wird die Verantwortung der obersten Leitung und die Notwendigkeit einer gelebten Compliance-Kultur.[3]

Anwendung

Die Anwendungsfelder der ISO 37301 sind vielfältig. Ursprünglich auf Unternehmen ausgerichtet, hat sich die Norm auch in der öffentlichen Verwaltung, bei Non-Profit-Organisationen und in internationalen Organisationen etabliert. Besonders Branchen mit hohem Regulierungsdruck – wie Finanzdienstleistungen, Energieversorgung, Gesundheitswesen oder die öffentliche Auftragsvergabe – profitieren von der strukturierten Herangehensweise an Regel-konformität. Aber auch kleine und mittlere Unternehmen (KMU) nutzen die ISO 37301 zunehmend als Grundlage für ein systematisches Compliance-Management.[4]

Anwendungsbeispiele

In der Anwendung ist die Norm recht offen, und sie ist auf unterschiedlichste Organisationen anwendbar.[5]

So implementierte etwa eine internationale Großbank mit Hauptsitz in Frankfurt am Main die ISO 37301, um ihre internen Kontrollsysteme mit regulatorischen Anforderungen der Europäischen Zentralbank (EZB) zu harmonisieren. Die Norm wurde genutzt, um bestehende Prozesse zu konsolidieren, insbesondere im Hinblick auf Geldwäscheprävention, Markt-missbrauch und Interessenkonflikte. Die Bank konnte durch externe Zertifizierung ihr Vertrauen bei Aufsichtsbehörden und Investoren signifikant steigern.

In Österreich führte eine Stadtverwaltung ISO 37301 ein, um die Compliance mit dem Vergaberecht, Datenschutzbestimmungen und Transparenzvorgaben zu stärken. In Kombination mit einem Whistleblower-System und

Schulungsmaßnahmen für Führungskräfte konnte das Fehlverhalten in Vergabeverfahren reduziert werden. Die Zertifizierung diente auch als Referenzrahmen für andere kommunale Einrichtungen.

Eine international tätige Nichtregierungsorganisation (NGO) mit Fokus auf Umwelt- und Klimaschutz nutzte ISO 37301 zur Professionalisierung ihrer Governance-Strukturen. Mit Hilfe der Norm wurden Richtlinien zu Spendenverwendung, Partnerauswahl und Lobbyarbeit systematisiert. Die Anwendung half, das Vertrauen von Fördermittelgebern und Kooperationspartnern zu erhöhen, ohne die operative Flexibilität einzuschränken.

Die ISO 37301 trägt somit nicht nur zur Risikominimierung und Rechtssicherheit bei, sondern stärkt auch das Vertrauen von Stakeholdern in verantwortungsbewusstes und regelkonformes Handeln. Sie fördert die Entwicklung einer nachhaltigen und ethisch ausgerichteten Unternehmensführung – über sektorale und geographische Grenzen hinweg.

Endnoten - Literatur

[1] Pieper, T. (2022): Normbasiertes Compliance Management: Die ISO 37301 im Vergleich zur ISO 19600. In: Zeitschrift für Corporate Compliance (ZCC), 3(2), S. 55–61.

[2] Becker, S. (2022): Integrierte Managementsysteme in der Praxis. 3. Aufl., Berlin: Erich Schmidt Verlag.

[3] Hildebrandt, M. (2021): Compliance-Management: Organisation, Kontrolle, Kultur. Wiesbaden: Springer Gabler.

[4] Dillerup, R. / Stoi, R. (2023): Unternehmensführung. 7. Aufl., München: Vahlen.

[5] Walter Schlegel, Stefan Pawils – Die ISO 37301:2021: Interpretation der Anforderungen Herausgeber: TÜV Media GmbH, 2021