Teil 7

ISO 9001:2015 für KMU: sinnvoll, unkompliziert, vorteilhaft!

Im siebten Teil unserer Leitfadenreihe geht es um das Einhalten interner und externer Anforderungen sowie anderer bindender Verpflichtungen an das Unternehmen. Welches sind die zentralen Aspekte von „Compliance" und welche Rolle spielt Compliance für das Unternehmen und wie sieht der Weg dahin aus? Kann man zu 100% compliant werden?

Der englische Begriff „Compliance" taucht in der DIN EN ISO 9001:2015 gar nicht auf. Er bedeutet die Einhaltung von Gesetzen, Regeln und Normen.[1] Übersetzt in die Normsprache ISO 9001 entspräche das dem Einhalten von Kundenanforderungen und relevanten gesetzlichen und behördlichen Bestimmungen.

Grundgedanke der ISO 9001:2015 ist, dass Unternehmen für langfristigen Erfolg die Anforderungen und Erwartungen ihrer relevanten interessierten Parteien kennen, verstehen und erfüllen müssen. Zunächst sollen Gruppen identifiziert werden, die die Leistung im jeweiligen Bereich beeinflussen können bzw. von der Tätigkeit und Leistung im entsprechenden Managementbereich betroffen sind oder beeinflusst werden können (siehe Teil 5). Das können für das Thema Qualität andere sein, als etwa im Bereich Umwelt oder Arbeitssicherheit. Neben Kunden gehören dazu z. B. auch Lieferanten, Eigentümer, Mitarbeitende, Behörden, Geschäftspartner oder sogar Wettbewerber, etc.

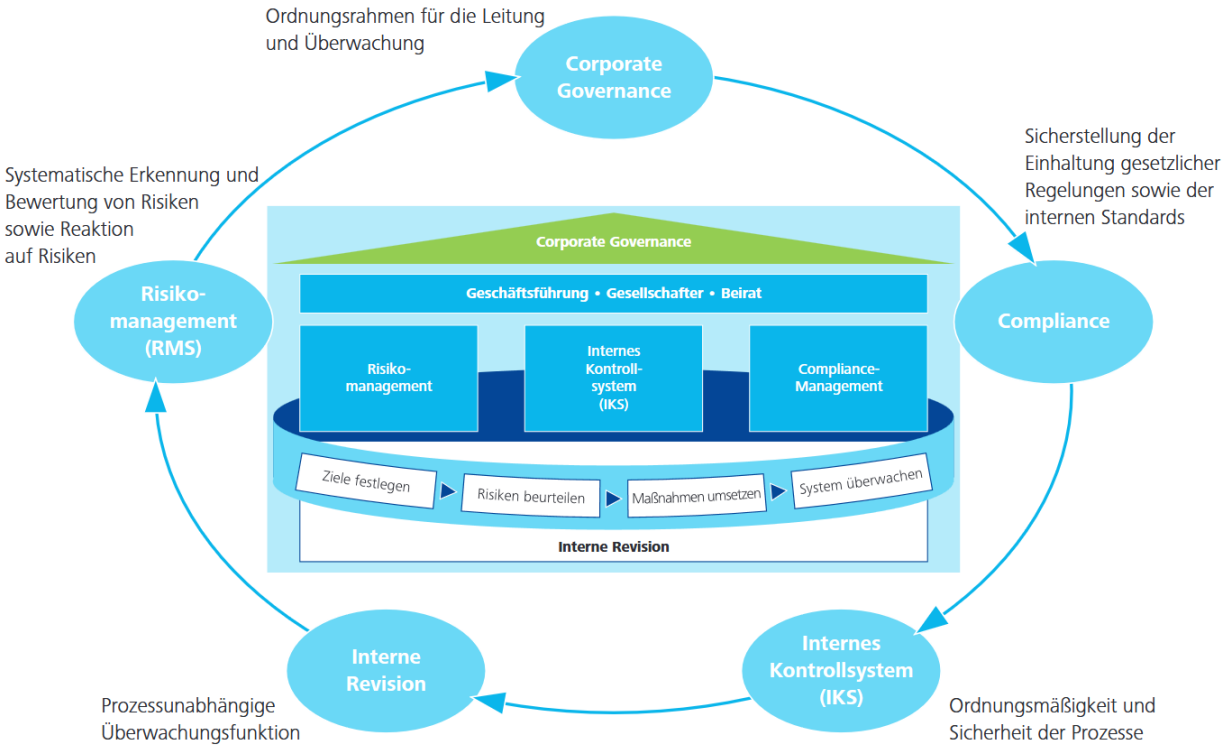
Interessierte Parteien erwarten, dass neben ausdrücklich für die Produkte festgelegten Anforderungen auch implizite Anforderungen wie gesetzliche Vorschriften, technische Normen und Standards sowie Sicherheits- und Gebrauchsfähigkeitskriterien erfüllt werden. Darüber hinaus haben sie eigene Anforderungen an ihre Lieferanten. Werden diese nicht erfüllt, werden Lieferketten unterbrochen und Kunden können ggf. Haftungsansprüche geltend machen.

Ein Compliance-Management-System beinhaltet sämtliche Grundsätze und Maßnahmen eines Unternehmens, um regelkonformes Verhaltens zu gewährleisten: Es stellt die gezielte Planung, Steuerung und Überwachung der Compliance-Aktivitäten des Unternehmens dar. In dieser Funktion ist es Teil der Unternehmensüberwachung, die sich aus Corporate Governance, Compliance, internem Kontrollsystem, interner Revision und Risikomanagement zusammensetzt. Das proaktive Vorgehen der Geschäftsführung ist hier erforderlich.

Inzwischen gibt es für Compliance-Management-Systeme sogar eine eigene Management-Systemnorm: die ISO 37301:2021. Sie orientiert sich – wie alle anderen ISO-Managementsystemnormen – an der Harmonized Structure und ist deshalb leicht in ein QM-System nach ISO 9001 zu integrieren.

[1] https://wirtschaftslexikon.gabler.de/definition/compliance-27721

Die folgende Abbildung von Deloitte stellt Compliance als Teil der Unternehmensüberwachung dar:



Quelle: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Mittelstand/Studie-Compliance-im-Mittelstand.pdf

Die Organisation **muss**:

- geltende rechtliche Vorschriften und andere Anforderungen identifizieren, umsetzen und zugänglich machen
- festlegen, wie diese Anforderungen auf die Organisation zutreffen
- sicherstellen, dass die Vorschriften bei Aufbau, Implementierung und Aufrechterhaltung des Managementsystems berücksichtigt werden und zur kontinuierlichen Verbesserung beitragen
- dokumentierte Informationen über ihre Verpflichtungen aufrechterhalten
- das Einhalten ihrer Verpflichtungen regelmäßig überprüfen
- Kenntnisse und Verständnis über ihren Status hinsichtlich der Einhaltung der Verpflichtungen (Compliance) beibehalten
- dokumentierte Nachweise über die Ergebnisse der Bewertung zur Einhaltung der Verpflichtungen aufbewahren

Teil 7

Warum ist Compliance bei der ISO 9001 wichtig?

Compliance ist aus mehreren wichtigen Gründen von Bedeutung:

- **Kundenzufriedenheit:** Der Hauptschwerpunkt der ISO 9001 ist das Erfüllen der Kundenanforderungen und die Steigerung der Kundenzufriedenheit. Zur Erfüllung der Kundenanforderungen gehören jedoch nicht nur die vom Kunden explizit geforderten Spezifikationen, sondern auch alle relevanten gesetzlichen und behördlichen Regelungen.
- **Risikomanagement:** Werden gesetzliche bzw. behördliche Anforderungen nicht erfüllt, ist das immer ein Risiko für ein Unternehmen. Mögliche Folgen reichen von Kundenunzufriedenheit oder -verlust über Imageverlust und kostspielige Rückrufaktionen für nicht konforme Produkte, bis hin zu behördlich angeordneten Unterlassungen oder sogar Standortschließungen. Das proaktive Erkennen und Umsetzen künftiger regulativer Anforderungen ist somit eine Chance, neue Produkte oder Dienstleistungen am Markt frühzeitig zu positionieren und so neue Kunden und Marktanteile zu gewinnen.

Welche Anforderungsbereiche gibt es?

Die Anforderungen an Unternehmen sind in den letzten Jahren immer komplexer geworden. Der Umfang der relevanten Regelungen hängt dabei stark von der jeweiligen Branche ab und ist teilweise länderspezifisch oder vom beteiligten Rechtsraum abhängig. Ausgehend vom Umfeld des Unternehmens gibt es unterschiedliche Anforderungsbereiche:

- Behörden, Ämter, Stadt, Gemeinde, Kreis
- Lieferanten
- Gesellschafter
- Verbundene Unternehmen (Konzernzugehörigkeit)
- Banken und Versicherungen
- Gesetzgeber
- Kunden, Kundengruppen (B2B, B2C)
- Umgebung, Nachbarschaft (Gewerbegebiet, Naturschutzgebiet, etc.)
- Freiwillige Prinzipien und Verfahrensregeln
- Gepflogenheiten des Marktes
- Freiwillige Anforderungen der Stakeholder, etc.

Tipp: Verwenden Sie zur Identifikation der Anforderungen die KIP-Analyse/PESTEL-Kriterien. Hier werden die Anforderungen als „Einflussfaktoren auf die Organisation" gesehen.

Die Sammlungen von neuen, bzw. geänderten Vorschriften findet man bei Kanzlei-Services wie etwa juris.de oder bei Online-Diensten wie z.B. online-rechtskataster.de. Eine Reihe von Expertendatenbanken (Rack, GeOrg, VISTRA) sowie Vereins- oder Verbandsnewsletter liefern häufig ebenfalls aktuelle, umfassende Information.

Bei der ISO 9001 bezieht sich der Begriff „freiwillige Verpflichtungen" auf Anforderungen, die sich eine Organisation **freiwillig** auferlegt hat, um bestimmte Qualitätsziele oder Standards zu erreichen, die über die **gesetzlichen Anforderungen** hinausgehen.

Freiwillige Verpflichtungen können durch die Organisation jederzeit wieder aufgehoben werden. Sie ergeben sich aus gesellschaftlichen und ethischen Standards und sollten bei der Umsetzung des QMS berücksichtigt werden. Im Grundsatz sollte zur Verbesserung der Nachhaltigkeit die gesamte Lieferkette hinsichtlich sozialer und ökologischer Leistungen betrachtet werden.

Beispiele für **freiwillige Verpflichtungen** könnten sein:

- Ein Unternehmen entscheidet sich, zusätzlich zu den gesetzlichen Vorgaben bestimmte Umweltstandards einzuhalten.
- Es werden zusätzliche Kundenvorgaben oder Branchenstandards integriert, die rechtlich nicht zwingend vorgeschrieben sind.

Kurz gesagt, es handelt sich um freiwillige Vereinbarungen oder Standards, die ein Unternehmen als Teil seines Qualitätsmanagementsystems übernimmt, um höhere Qualitäts- oder Leistungserwartungen zu erfüllen.

Tabelle 1: Beispiele für mögliche Anforderungen

Anforderungen	Beispiele
Kundenanforderungen	Produkt- und Dienstleistungsqualität, Übereinstimmung mit Spezifikationen, Einhaltung gesetzlicher und regulatorischer Anforderungen, pünktliche Lieferung, Kosteneffizienz, Sicherheit und Zuverlässigkeit, Benutzerfreundlichkeit, Ergonomie, Kundendienst und Support, Anpassungsfähigkeit und Flexibilität, Nachhaltigkeit und Umweltfreundlichkeit
Internationale Regelungen	ISO-Normen (z.B. DIN EN ISO 9001), internationale Handelsvereinbarungen, Produktsicherheitsvorschriften, etc.
Nationale Regelungen	Gesetze und Verordnungen, nationale Standards, branchenspezifische Vorschriften (BinSchG, WHG, Ahorn Rechtspflichtenservice), VDI-Richtlinien, Best Practice
Lokale Regelungen	Kommunale Vorschriften, regionale Vorschriften, Arbeits- und Gesundheitsschutz
Gesetzliche und regulatorische Anforderungen	Arbeitsschutz, Umweltrecht, Datenschutzrecht, z.B.: Lieferkettensorgfaltspflichtengesetz (LkSG), Produktsicherheitsgesetz (ProdSG), Datenschutz und Informationssicherheit (DSGVO, BDSG), branchen- und produktspezifische Vorschriften
Unternehmensinterne Regelungen und Richtlinien	Code of Conduct, dokumentierte interne Prozesse, Genehmigungen, Verträge

Tipp: Zur verbesserten Umsetzung der verschiedenen Forderungen hat sich das Erstellen eines für das Unternehmen maßgeschneiderten **Rechtskatasters** etabliert. Er umfasst die für den jeweiligen Betrieb individuell zusammengestellten rechtliche Vorgaben und die davon abgeleiteten Handlungspflichten und -anweisungen mit den festgelegten Verantwortlichkeiten und dem zeitlichen Rahmen.

In Deutschland gibt es aktuell über 5.000 Gesetze und Verordnungen. Natürlich sind nicht alle für das Unternehmen, die Tätigkeit oder das Produkt / die Dienstlesitung relevant.

Teil 7

Jedes Unternehmen muss selbst bestimmen, welche Gesetze Bezug zu Tätigkeiten, Produkten, Anlagen oder verwendeten Materialen haben.

Anbindung von Compliance an das QM-System ISO 9001:2015

Die Integration von Compliance in ein QM-System ist entscheidend, um sicherzustellen, dass alle relevanten gesetzlichen und regulatorischen Anforderungen systematisch erfasst, überwacht und eingehalten werden.

Die ISO 9001:2015 fordert das Bekenntnis zur Compliance in der Unternehmenspolitik. Auch soll ein compliance-relevantes Verfahren im Dokumentensystem festgelegt werden:

- Wie wird das Rechtsregister erstellt? (Quellen, Häufigkeit und Art der Aktualisierung etc.)
- Wer ist verantwortlich für die Erstellung, Pflege und Überprüfung der Rechtskonformität?
- Wie ist die organisatorische Einbindung gestaltet?
- Welche dokumentierten Informationen (Verfahren und Nachweise) sind erforderlich?

Die Einführung eines Compliance-Management-Systems ermöglicht es, relevante Informationen vollumfänglich zu erfassen und alle Unternehmensteile aktiv in die Umsetzung einzubinden.

Tabelle 2 verdeutlicht, wie Compliance-Anforderungen in ein Qualitätsmanagementsystem nach ISO 9001 integriert werden können, indem relevante Prozesse und Nachweise für verschiedene Normkapitel erfasst werden:

Normkapitel	Prozesse	Nachweise
4. Kontext der Organisation	Organisation muss die für QMS relevanten interessierten Parteien und ihre Anforderungen sowie rechtliche Aspekte je nach Strategie/Tätigkeit ermitteln	Business-Plan, Strategiepläne, Analyse der Wettbewerber, Wirtschaftsberichte aus den Geschäftsbereichen, SWOT-Analysen, Risikoanalysen, Berichte, Liste der interessierten Parteien
5. Führung	Festlegen der Unternehmenspolitik, Sicherstellen der Einhaltung der Compliance, Sicherstellen der Kundenanforderungen und-zufriedenheit	Unternehmenspolitik, Compliance-Strategie, Kundenumfragen, Reklamationsberichte
6. Planung	Risiko- und Chancenbewertung, Planen von Maßnahmen	Risikomanagementberichte, Maßnahmenpläne
7. Unterstützung	Schulen und Qualifizieren von Mitarbeitenden, Sensibilisierung für Compliance-Anforderungen, Erstellen und Lenken von Dokumenten und Aufzeichnungen	Schulungsnachweise, Kompetenzmatrix, Schulungsunterlagen, Teilnahmezertifikate, Verfahrensanweisungen, Auditprotokolle
8. Betrieb	Ermitteln und Lenken von Kundenanforderungen, Lieferantenbewertung und-überwachung	Lastenhefte, Pflichtenhefte, Vertragsunterlagen, Lieferantenbewertungen, Auditberichte
9. Bewertung der Leistung	Durchführen internet Audits und Managementbewertungen, Regelmäßige Überprüfung der QMS-Leistung und Compliance	Auditberichte, Managementreview-Protokolle, Auditpläne, Auditprotokolle
10. Verbesserung	Identifikation und Beheben von Nichtkonformitäten	Korrekturmaßnahmenberichte, Fehlanalysen

Schritte zur Einführung und Sicherstellung der Compliance bei ISO 9001

1. **Analyse der Compliance-Anforderungen**: Identifizieren relevanter gesetzlicher und behördlicher Anforderungen, Verpflichtungen sowie branchenspezifischer Standards, die für das Unternehmen gelten. Diese bilden die Grundlage für die Integration von Compliance in das Qualitätsmanagementsystem.
2. **Führung und Verpflichtung der Unternehmensleitung**: Die Geschäftsleitung muss sich aktiv für die Einhaltung von Compliance engagieren. Dies umfasst das Festlegen einer Compliance-Aussage (z.B. als Bestandteil einer umfassenden Unternehmenspolitik), die die Verpflichtung des Unternehmens zur Einhaltung gesetzlicher Anforderungen und Standards deutlich macht.
3. **Bewertung und Management von Risiken und Chancen**: Durchführen einer gründlichen Risikobewertung, um potenzielle Compliance-Risiken zu identifizieren, Erkennen von Chancen für die Weiterentwicklung von Produkten und Dienstleistungen und Entwickeln entsprechender Maßnahmen, um Risiken zu mindern und Chancen zu nutzen.
4. **Integration von Compliance in die Prozesse des QMS**: Bestehende Prozesse des Qualitätsmanagementsystems (QMS) werden überprüft und angepasst, um die Compliance-Anforderungen zu berücksichtigen. Dies kann auch das Überarbeiten von Verfahrensanweisungen, Arbeitsanweisungen und anderen Dokumenten umfassen.
5. **Schulung und Sensibilisierung der Mitarbeiter**: Schulungen sind entscheidend, um sicherzustellen, dass alle Mitarbeitenden verstehen, was Compliance bedeutet und wie sie dazu beitragen können. Schulungsprogramme sollten regelmäßig aktualisiert werden, um neue Compliance-Anforderungen und Änderungen in den Prozessen zu berücksichtigen.

Im Rahmen der Erstellung des Rechtskarasters sind bei der Zuordnung der Rechtspflichten folgende Punkte zu beachten:

- Aufbau einer unternehmensinternen Kommunikationslinie (inkl. Kommunikationsregeln)
- Einpflegen von Pflichten, Aufgaben und Verantwortlichkeiten
- Unterweisen der betroffenen Mitarbeitenden über Rechtspflichten
- Verfahren zur Bewertung der Einhaltung der einschlägigen rechtlichen Verpflichtungen
- Umgang mit den Ergebnissen der Bewertung
- Regelmäßige Kontrolle zum Einhalten und Umsetzen der delegierten Pflichten
- Regelmäßige Kontrolle von Neuerungen und Änderungen mit anschließender Aktualisierung von Rechtspflichten

6. **Interne Compliance-Audits durchführen**: Regelmäßige interne Compliance-Audits sind notwendig, um sicherzustellen, dass die Compliance-Anforderungen effektiv umgesetzt werden. Außerdem können Compliance-Risiken dadurch früh erkannt und Compliance-Verstöße aufdeckt werden. Werden die Abweichungen im Audit festgestellt, müssen entsprechende Maßnahmen ergriffen werden. Die Korrekturmaßnahme muss festgelegt, im Bericht dokumentiert und in den Korrektur-Maßnahmen-Plan aufgenommen werden. Im nächsten Compliance-Audit wird die Wirksamkeit der Maßnahme geprüft.

7. **Managementbewertung**: Die Geschäftsleitung sollte regelmäßig die Leistung des QMS und die Einhaltung der Compliance überprüfen. Diese Managementbewertungen dienen dazu, Verbesserungsmöglichkeiten zu identifizieren und sicherzustellen, dass das QMS den aktuellen Anforderungen entspricht.
8. **Kontinuierliche Verbesserung:** Wichtig ist das Implementieren eines Prozesses für kontinuierliche Verbesserung, um sicherzustellen, dass das QMS und die Compliance-Praktiken ständig optimiert werden. Dies kann durch die Analyse von Daten, Kundenfeedback, interne Audits und andere Feedback-Mechanismen erreicht werden.

Im Zertifizierungsaudit nach ISO 9001 werden folgende Fragen gestellt:

- Haben Sie ein Rechtskataster oder eine Dokumentation aller relevanten gesetzlichen und regulatorischen Anforderungen? Wie wird dieses Rechtskataster gepflegt und aktualisiert? Welche Gesetze und Vorschriften sind für Ihr Unternehmen besonders relevant?
- Welche internen Richtlinien und Verfahren haben Sie implementiert, um die Einhaltung gesetzlicher Anforderungen sicherzustellen? Wie werden diese Richtlinien dokumentiert und kommuniziert?
- Wie schulen Sie Ihre Mitarbeitenden in Bezug auf die Einhaltung gesetzlicher und regulatorischer Anforderungen? Gibt es Schulungsprogramme oder regelmäßige Trainings zu Compliance-Themen? Gibt es Nachweise über durchgeführte Schulungen?
- Wer ist in Ihrem Unternehmen für das Einhalten der gesetzlichen Anforderungen verantwortlich? Sind die Verantwortlichkeiten klar zugewiesen und dokumentiert?
- Wie überwachen Sie die Einhaltung der gesetzlichen und regulatorischen Anforderungen? Werden interne Audits oder Überprüfungen durchgeführt? Wie dokumentieren Sie die Ergebnisse dieser Überprüfungen?
- Wie gehen Sie mit Verstößen gegen gesetzliche Anforderungen um? Gibt es ein Verfahren zur Meldung und Bearbeitung von Verstößen? Wie wird sichergestellt, dass Maßnahmen zur Behebung von Verstößen ergriffen werden?
- Wie stellen Sie sicher, dass Ihr Compliance-Management-System kontinuierlich verbessert wird? Gibt es Prozesse zur regelmäßigen Überprüfung und Anpassung des Systems?
- Wie integrieren Sie Änderungen in den gesetzlichen Anforderungen in Ihr Compliance-Management-System? Gibt es Mechanismen, um sicherzustellen, dass neue oder geänderte Vorschriften zeitnah umgesetzt werden?

Teil 7

Fazit Teil 7

Compliance gewährleistet die Einhaltung internationaler Qualitätsstandards, was die Kundenzufriedenheit erhöht, die betriebliche Effizienz verbessert und das Unternehmen rechtlich absichert. Die Anforderungsbereiche umfassen u. a. die Dokumentation von Prozessen, interne Audits und das Risikomanagement. Zur Einführung und Sicherstellung der Compliance in Ihrem QM-System nach ISO 9001 sollten Unternehmen schrittweise vorgehen, indem sie zunächst die Normanforderungen verstehen, notwendige Maßnahmen umsetzen und sich auf das Zertifizierungsaudit vorbereiten, in dem spezifische Fragen zur Erfüllung der ISO 9001:2015-Kriterien gestellt werden.

In Teil acht der Publikationsreihe wird es um das Thema Führungsverantwortung gehen und die wesentliche Rolle des Managements bei der Umsetzung eines QMS. Sie erfahren, welche Rolle das Festlegen und Kommunizieren von Verantwortlichkeiten in der ISO 9001 spielt.

-

Ihre Ansprechpersonen:

Miroslava Dubinetska

+49 30 233 20 21 – 533 | miroslava.dubinetska@gut-cert.de

Andreas Lemke | Leiter der Zertifizierungsstelle

+49 30 233 20 21 – 41 | andreas.lemke@gut-cert.de