

# DAS 5-SÄULEN-MODELL

## EIN INTEGRIERTES COMPLIANCE MANAGEMENT SYSTEM (CMS)

### LEADERSHIP

#### Führungskräfte

- Die Haltung und das Verhalten der Führungskräfte sind compliant
- Das Compliance-Programm wird von den Führungskräften getragen
- Alle Führungskräfte haben ein Grundverständnis für Compliance
- Alle Führungskräfte leben und verantworten Compliance nach innen und nach außen

#### Kulturelle Aspekte

- Der Umgang miteinander ist von Vertrauen geprägt
- Das Compliance-Verhalten der Mitarbeiter wird bei Beurteilungen und Beförderungen berücksichtigt
- Es wird mit Fehlern sachlich und berechenbar umgegangen
- Compliance-Verstöße führen zu vorhersehbaren Konsequenzen

#### Geschäftsmodell

- Das Geschäftsmodell und die Zielvorgaben sind mit Compliance vereinbar
- Compliance ist als Teil der Wertschöpfung und des Kundennutzens anerkannt
- Es ist ein passender Anspruch an die Qualifikation aller Mitarbeiter definiert
- Die Geschäftspartner und die Infrastruktur genügen den Anforderungen von Compliance

#### Strategie

- Compliance-Ziele werden bei der Entwicklung der Unternehmensstrategie berücksichtigt
- Alle Zielvereinbarungen sind im Einklang mit Compliance

### RISK ASSESSMENT

#### Risikobetrachtung

- Der inhaltliche Umfang der Risikobetrachtung wird durch das Geschäftsmodell, den Katalog der anwendbaren (rechtlichen) Vorgaben und den Kontext der Geschäftstätigkeit, einschl. aller Stakeholder, festgelegt
- Es werden die Vergangenheit, der Status quo und mögliche zukünftige Veränderungen berücksichtigt
- Es wird eine Soll-Ist-Betrachtung durchgeführt, die mindestens folgende Dimensionen umfasst:
  - Aufbauorganisation
  - Ablauforganisation
  - Vollständige Liste aller (Geschäfts-) Tätigkeiten
  - Mitarbeiter
  - Kunden, Lieferanten, sonstige Geschäftspartner
  - Ausstattung und Arbeitsmittel
  - Die Zuständigkeiten und Verantwortlichkeiten sind definiert

#### Risikobewertung

- Risiko = potenzielle Schadensgröße x Eintrittswahrscheinlichkeit
- Die Risikobewertung erfolgt qualitativ oder quantitativ und berücksichtigt Gegenmaßnahmen

#### Maßnahmen

- Für jedes Risiko ist eine angemessene Risikostrategie zu definieren
- Ein Maßnahmenkatalog mit Terminen, Verantwortlichen und einer geregelten Kontrolle der Umsetzung wird erstellt

### STANDARDS & CONTROLS

#### Compliance-Organisation

- Geführt von einem Compliance-Beauftragten mit direkter Anbindung an die oberste Geschäftsführung
- Unabhängig vom operativen Geschäft, nur an die Weisungen der obersten Geschäftsleitung gebunden
- Geregelt sind die Zuständigkeiten und Verantwortlichkeiten, die Prüf- und Entscheidungskompetenz sowie die Zusammenarbeit mit Aufsichtsorganen
- Festgelegte Einbindung in Prozesse
- Angemessene Ausstattung mit Budget und Ressourcen (Personal- und Sachressourcen)

#### Compliance-System

- Alle Managementsysteme der Organisation folgen einer einheitlichen Systematik und regeln Verantwortlichkeiten und Zuständigkeiten eindeutig und vollständig
- Das operative Managementsystem und das CMS sind integriert bzw. widersprechen sich nicht
- Es existiert ein Compliance Management System, das in einem Managementhandbuch beschrieben ist
- Interessenkonflikte sind möglichst vollständig zu identifizieren

- Unvereinbare Tätigkeiten sind zur Vermeidung von Interessenkonflikten getrennt

- Ausreichende Ausstattung an Ressourcen zur Etablierung und Weiterentwicklung des Systems

- Hinweise gegen (mögliche) Verstöße können gemeldet werden (Hinweisgebersystem/„Whistleblower“)

#### Schriftlich fixierte Ordnung

- Es existiert eine schriftlich fixierte Ordnung (SFO), freigegeben durch die zuständige Managementebene
- Typische Elemente einer SFO sind:
  - Katalog der relevanten Anforderungen
  - Unternehmenspolitik, Verhaltenskodex und sonstige Leitlinien
  - Arbeitsanweisungen und Prozessbeschreibungen
  - Die Lenkung und Aufbewahrung von Dokumenten und Aufzeichnungen ist geregelt

#### Kontrollen

- Kontrollplan aufbauend auf der Risikoanalyse
- Einheitliches System zur Durchführung von Audits
- Regelmäßige Kontrollhandlungen

### TRAINING & COMMUNICATION

#### Schulungskonzept

- Ableitung und regelmäßige Aktualisierung der Schulungsinhalte z. B. auf Basis von Risikoanalyse, Feedback und externen Anforderungen
- Etablierung eines Prozesses für die Einarbeitung
- Einführung eines Schulungsplans basierend auf einer Qualifikationsanalyse
- Systematische Dokumentation der Schulungen als Nachweise

#### Schulungsmethoden

- Zielgruppenorientierte Schulungen für Mitarbeiter und Führungskräfte
- Schulungen erfolgen intern und/oder extern als Präsenzschiulung und/oder E-Learning
- Schulungen für Geschäftspartner erfolgen im Bedarfsfall

#### Kommunikation

- Konzept für die interne und externe Kommunikation
- Einbindung der Führungskräfte
- Offenheit für und systematisches Einholen von Feedback
- Präsenz im Unternehmen und Erreichbarkeit
- Möglichkeit zur Transparenz gegenüber Dritten
- Adressaten- und sinnreiche Kommunikation
- Change Management

#### Integration

- Integration von Compliance(-Inhalten), wo immer möglich/erforderlich, in fachliche Aus- und Fortbildungen und Meldungen/ Berichterstattungen

### MONITORING, AUDITING & RESPONSE

#### Überwachung & Prüfung

- Kontinuierliche Überwachung der (risikobehafteten und kritischen) Prozesse und Geschäftsvorgänge
- Kontinuierliche Auswertung von Zahlen, Daten und Fakten
- „Audit committee“ i. S. des UK Bribery Act

#### Berichtslegung

- Die Berichtswege sind definiert
- Mindestens jährliche Berichterstattung an die oberste Geschäftsleitung
- Ad-hoc-Berichterstattungen erfolgen, sofern erforderlich, unmittelbar
- Mindestens jährliche Analyse und Bewertung der Leistungsfähigkeit des CMS durch die oberste Geschäftsleitung
- Die Aufbereitung aller relevanten Informationen eignet sich für die Risikobewertung
- Die Berichterstattung nach außen, sofern relevant

#### Reaktion

- Eine Regelung zur Behandlung von Abweichungen und Regelverstößen, soweit anwendbar gemäß den gesetzlichen/ vertraglichen Vorgaben
- Etablierung von Verfahren für Korrektur- und Vorbeugemaßnahmen
- Ad-hoc-Ausschüsse zur Behandlung von Einzelfällen
- Ad-hoc-Maßnahmen, einschließlich Berichterstattung an zuständige Stellen und Schulungen