

COMPLIANCE-RISIKOMANAGEMENT IN UNTERNEHMEN

Proaktiv und strategisch die Wertschöpfung steigern und eine widerstandsfähige Governance stärken

Das Compliance-Risikomanagement, ein bekanntes und etabliertes Thema im Finanzsektor, ist auch für grosse Unternehmen und KMUs von zentraler Bedeutung. In einem Umfeld zunehmender Regulierung wirkt es sich auf Produkte, Dienstleistungen, Organisation und Finanzergebnisse aus, erzeugt operative und regulatorische Risiken sowie Kosten im Falle der Nichteinhaltung, aber auch Chancen und erfordert ein hohes Mass an Compliance-Kompetenz.

1. DEFINITION UND ENTWICKLUNG VON COMPLIANCE

Unter «Compliance» versteht man die Einhaltung sowohl betriebsinterner als auch externer Gesetze, Vorschriften, Verfahren, Verhaltenskodizes und Standards. Es handelt sich dabei um die Verpflichtung des Unternehmens und seiner Vertreterinnen und Vertreter (Verwaltungsrat [VR], Geschäftsleitung und Mitarbeitende), alle für die eigene Tätigkeit geltenden Regeln einzuhalten, um rechtliche Risiken, Sanktionen, Reputationsrisiken und nicht zuletzt auch eine Gefährdung der Geschäftskontinuität (z. B. durch Entzug der Betriebsgenehmigung oder Verlust der Reputation) zu vermeiden.

Die Compliance ist Teil eines umfassenderen Unternehmensführungsmodells, das die Governance, das interne Kontrollsystem und die Steuerung aller das Unternehmen betreffenden Risiken umfasst. In einem politischen, wirtschaftlichen und sozialen Umfeld, das sich ständig weiterentwickelt und in dem Veränderungen und Herausforderungen so häufig und intensiv sind wie nie zuvor, müssen Unternehmen mehr denn je ihre Governance und ihr internes Kontrollsystem (einschliesslich Risikomanagement und Compliance) überwachen und anpassen, um diese kontinuierlich effizienter und wirksamer zu machen.

Die Norm ISO 37301 (Compliance-Managementsysteme)^[1] definiert Compliance als «Erfüllung aller Compliance-

Pflichten». Als Pflichten gelten dabei gesetzliche, regulatorische und vertragliche Anforderungen, Verhaltenskodizes und interne Richtlinien. Im COSO-Modell Internal Control – Integrated Framework^[2] hingegen ist Compliance eines von drei grundlegenden Zielen des Internal Control System (zusammen mit Reporting und Operations).

Das Thema Compliance ist nicht über Nacht entstanden, sondern hat sich schrittweise entwickelt als Reaktion auf Systemkrisen, Unternehmensskandale, die Globalisierung der Märkte und die daraus resultierende Regulierungsflut. Das Konzept der Compliance entstand in den 1970er-Jahren in den USA infolge von Korruptionsskandalen in multinationalen Konzernen und der darauffolgenden Einführung des Foreign Corrupt Practices Act (FCPA)^[3] im Jahr 1977. 1985 erfolgte die Gründung der COSO-Initiative, 1992 wurde die erste Version des Internal Control – Integrated Framework veröffentlicht. Nach den Skandalen um Enron, Worldcom und Parmalat (um nur einige zu nennen) verfestigte sich das Thema Compliance in den Jahren 1990 bis 2000 zusätzlich durch den Erlass des Sarbanes-Oxley Act (SOX)^[4] im Jahr 2002. Gleichzeitig entstand die Rolle des Compliance Officer als organisierte, dokumentierte Funktion. Ab Anfang 2000 verbreitete sich das US-Modell weltweit, begleitet von einer Vielzahl neuer Vorschriften auf europäischer und nationaler Ebene – etwa zur Betrugsbekämpfung, zum Datenschutz, zum Wettbewerb und zur Sicherheit am Arbeitsplatz. Die Unternehmen sind aufgerufen, organisatorische Massnahmen zu ergreifen, um empfindliche Verwaltungs- und Strafsanktionen sowie Reputationsschäden zu vermeiden. In den letzten zwanzig Jahren hat sich die Compliance von einem reaktiven zu einem proaktiven Ansatz entwickelt, der auf einer Analyse des Compliance-Risikos sowie international festgelegten und anerkannten Modellen und Rahmenwerken basiert (vgl. *Tabelle 1*).

Verstösse gegen die Compliance sind ernstzunehmende Delikte: In den Medien ist regelmässig von mehr oder we-



SANDRO PROSPERI,
DIPL. WIRTSCHAFTSPRÜFER,
CCSA, CERTIFIED
BOARD MEMBER SUPSI,
GESELLSCHAFTER,
GESCHÄFTSFÜHRER
GOVERNANCE CONSULTING

niger schweren Vorfällen mangelnder Compliance zu lesen – also von Situationen, die Verstösse auf individueller und/oder Unternehmensebene gegen die für bestimmte Tätigkeiten oder Branchen geltenden Vorschriften aufzeigen. Die Risiken sind daher konkret und präsent und die (finanziel-

len und reputationellen) Folgen für die Unternehmen ebenso schwerwiegend – unabhängig von deren Grösse. Hier einige konkrete Beispiele: Das Datenschutzgesetz [5] sieht bei Verstössen Bussen von bis zu CHF 250 000 vor. Wer das Gesetz gegen den unlauteren Wettbewerb [6] nicht befolgt, kann strafrechtlich verfolgt werden.

Allgemein zeichnen sich auf Compliance-Ebene die folgenden Entwicklungen ab:

- Zahlreiche Branchen unterliegen einer zunehmenden Dichte an Gesetzen und Vorschriften, die immer grössere Bereiche betreffen.
- Grosse Unternehmen müssen immer häufiger die Einhaltung der geltenden Vorschriften nachweisen. Das hat auch konkrete Auswirkungen auf die KMUs in ihrer Lieferkette.
- Nichtkonformitäten werden auch dank der Whistleblowing-Prozesse leichter aufgedeckt.
- Nichtkonformitäten werden auf Unternehmensebene und der Ebene persönlicher Verantwortung strenger sanktioniert.
- Aufmerksamkeit und Interesse der Öffentlichkeit (Medien, Investoren, Kundschaft usw.) für Compliance wachsen.

Vor diesem Hintergrund wandelte sich das Thema Compliance, das in der Vergangenheit in bestimmten Sektoren eher unterschätzt wurde, sukzessive zu einem der zentralen Sorgenfaktoren der Unternehmensleitung.

2. COMPLIANCE-BEREICHE UND GELTENDE VORSCHRIFTEN FÜR UNTERNEHMEN

Compliance beschränkt sich nicht auf den Rechtsrahmen eines Unternehmens. Vielmehr betrifft sie alle Unterneh-

Abbildung 1: **UNTERNEHMENSFÜHRUNGSMODELL**

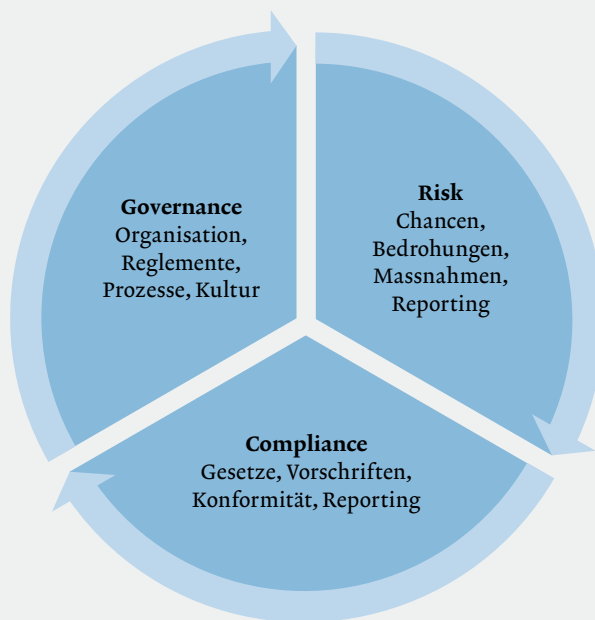


Tabelle 1: **REIFEENTWICKLUNG DER COMPLIANCE-FUNKTION**

Zeitraum	Phase/Ansatz	Hauptfokus	Organisation	Treiber
1970–1990	Rudimentär	Formale Beachtung neuer Regulierungsaufgaben (Checkliste)	Keine spezielle Funktion (Rechtsabteilung, Personalwesen, Qualität)	Erste Vorschriften zu Betrugsbekämpfung, Sicherheit, Datenschutz
1990–2000	Reaktiv und fragmentiert	Schutz vor möglichen Sanktionen	Hybridfunktion (oft Legal & Compliance)	Weltweite Skandale, interne Kontrollmodelle
2000–2010	Proaktiv und risikobasiert	Prävention (von der Checkliste zum Compliance-Managementsystem)	Unabhängige Funktion (getrennt von Legal) und neue Instrumente (Risikobewertung, Überwachungsprogramm, Reporting)	Exponentielle Zunahme der Regulierungskomplexität, internationale Rahmenwerke, Reputationsaspekte
2010–2020	Integriertes System zur Steuerung des Compliance-Risikos	Integration von Governance, Risk und Compliance	Strukturierte und anerkannte selbstständige Funktion, GRC-System, KPI, KCI, Unternehmenskultur (Ethik und Integrität)	Standardisierung durch ISO, Tone at the Top, Datenschutz, ESG, Whistleblowing
2020–heute	Strategisch (Einfluss auf Geschäftsmodell, Lieferantenmanagement, Innovation, ESG, Cybersicherheit, Ethik usw.)	Governance, Ethik, ESG, Unternehmenswert (steigert die Unternehmensresilienz)	Compliance-Zuständigkeiten auf Ebene des VR	Von den Stakeholdern geforderte Transparenz, neue Normen zu Nachhaltigkeit und Due Diligence

mensbereiche – von Produktion und/oder Dienstleistungserbringung über Buchhaltung, Personalwesen, IT, Kundschaft und Wettbewerb bis hin zu Inkasso und Zahlungen.

Angesichts des Umfangs der in *Tabelle 2* (nicht abschliessend) aufgelisteten geltenden Vorschriften könnte man sagen, dass Compliance immer stärker die Grundlage der strategischen und organisatorischen Entscheidungen von Unternehmen einschliesslich KMUs bildet und dass das Nichteinhalten dieser Vorschriften ein erhebliches finanzielles und reputationelles Risiko darstellt. Compliance wird zu einem wichtigen, unverzichtbaren Bestandteil der Verantwortlichkeit des Unternehmens.

3. COMPLIANCE-MANAGEMENTSYSTEM

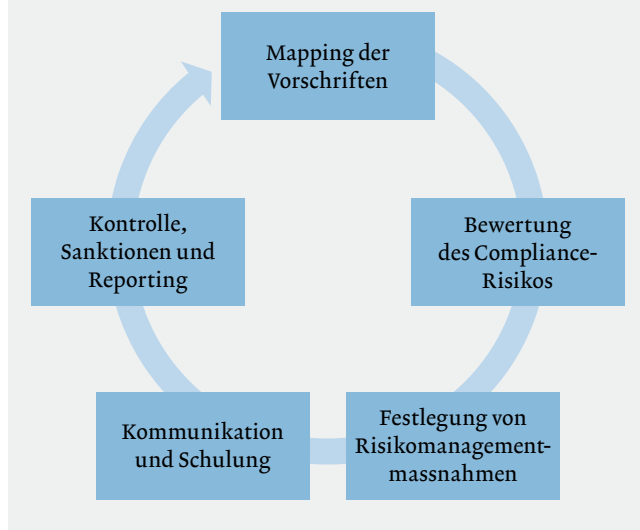
Ein wirksames Compliance-Management bietet Unternehmen folgende Vorteile:

- Einhaltung der für die eigene Tätigkeit geltenden Gesetze und Vorschriften
- Schutz des Unternehmens und der Mitarbeitenden vor Strafsanktionen und hohen Bussen
- Steigerung der eigenen Attraktivität bei Kundschaft, Partnern/-innen, Investoren/-innen, Banken und Mitarbeitenden
- Vorzeitige Identifizierung von Risiken und rechtzeitiges Ergreifen proaktiver Massnahmen gegen jegliche Rechtsverstösse
- Schutz der Reputation und des Unternehmenswerts

3.1 Bestandteile eines Compliance-Managementsystems. Wie lässt sich also Compliance proaktiv und strategisch steuern, sodass sie zu einem Differenzierungsmerkmal und Wettbewerbsvorteil wird? Dies gelingt bspw. mit

Tabelle 2: **GELTENDE VORSCHRIFTEN IM COMPLIANCE-BEREICH**

Compliance-Bereich	Geltende Vorschriften[7]
Corporate Governance	→ Obligationenrecht (OR) – Bestimmungen zu Governance, Rechnungswesen, Verantwortlichkeit der Verwaltungsräte → Swiss Code of Best Practice for Corporate Governance von Economiesuisse (kein Gesetz, aber als nationale Referenz anerkannt)
Produktion/Dienstleistungserbringung	→ Sektorspezifische Gesetze, um eine Betriebsgenehmigung zu erhalten → Bundesgesetz über die Produktesicherheit (PrSG) → Verordnung über die Produktesicherheit (PrSV) → Fachliche Verordnungen (Maschinen, Druckgeräte, Elektrogeräte, Spielzeug usw.) → Umweltschutzgesetz (USG) → Luftreinhalte-Verordnung (LRV) → Verordnung über den Verkehr mit Abfällen (VeVA) → Chemikalien-Risikoreduktions-Verordnung (ChemRRV) → Bundesgesetz über das öffentliche Beschaffungswesen (BöB) → Verordnung über das öffentliche Beschaffungswesen (VöB) → Möglicherweise geltende ausländische Gesetze
Rechnungswesen	→ Geltende Rechnungslegungsgrundsätze → Steuergesetze/Steuern und Abgaben/MWST usw. → Verordnung über Sorgfaltspflichten und Transparenz bezüglich Mineralien und Metallen aus Konfliktgebieten und Kinderarbeit (VSoTr) → Gleichstellungsgesetz (GlG)
Personalwesen	→ Arbeitsgesetz (ArG) und Verordnung zum Arbeitsgesetz (ArGV) → Verordnung über die Unfallverhütung (VUV) → Verordnung über die Sicherheit und den Gesundheitsschutz der Arbeitnehmerinnen und Arbeitnehmer bei Bauarbeiten (BauAV) → Soziale Vorsorge/ Sozialversicherungen → Ethische Grundsätze/Interessenkonflikte/Betrug
IT	→ Datenschutzgesetz (DSG) → Datenschutzverordnung (DSV) → Leitfäden des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) → IT-Sicherheit/Cybersicherheit
Kundschaft/Wettbewerb	→ Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen (KG) → Bundesgesetz gegen den unlauteren Wettbewerb (UWG) → Güterkontrollgesetz (GKG) → Güterkontrollverordnung (GKV) → Embargogesetz (EmbG) → Immaterialgüterrecht
Inkasso/Zahlungen	→ Geldwäschereigesetz (GwG) → Bestechung/Sanktionen

Abbildung 2: **MODELL EINES COMPLIANCE-MANAGEMENTSYSTEMS**

einem systematischen Ansatz zur Steuerung des Compliance-Risikos (vgl. *Abbildung 2*), der folgende Phasen umfasst:

3.1.1 Mapping der für das Unternehmen geltenden Vorschriften: Die für das Unternehmen geltenden Vorschriften und Pflichten werden, nach Bereichen unterteilt, systematisch gemappt (z. B. Produktion und/oder Dienstleistungserbringung, Rechnungswesen, Personalwesen, IT, Kundschaft und Wettbewerb, Inkasso und Zahlungen usw.).

3.1.2 Bewertung des Compliance-Risikos: In diesem Prozess wird für jede Pflicht die Wahrscheinlichkeit eines Verstosses, die Auswirkung (Sanktionen, Produktionsstopp, Reputation, Kosten), die bereits vorhandene Kontrollebene und das Restrisiko bewertet.

3.1.3 Festlegung von Risikomanagementmassnahmen: Dies umfasst Ethikkodex, Reglemente, Verfahren, Prozesse, Verantwortlichkeiten, Zuständigkeiten und interne Kontrollen (Prävention, Identifikation, Korrektur).

3.1.4 Kommunikation und Schulung: Dies soll durch gezielte Schulungsprogramme, Awareness-Kampagnen, Whistleblowing-Instrumente, Integritätskultur erreicht werden.

3.1.5 Kontrolle, Sanktionen und Reporting: In dieser Phase werden Kontrollen der Stufe 2 (durch Compliance-Funktion) mit regelmässigen Berichten an die Spitze (VR, Kontrollausschüsse), Konformitätsindikatoren (KCI), Follow-ups der Risikomanagementmassnahmen und einer kontinuierlichen Aktualisierung des Compliance-Prozesses angewendet.

3.2 Zuständigkeit. Der Verwaltungsrat und die Unternehmensleitung bewerten und genehmigen das Compliance-Managementsystem und vergewissern sich, dass es alle wesentlichen Elemente umfasst. Der Verwaltungsrat und die Unternehmensleitung stellen sicher, dass das System bei Ver-

änderungen des regulatorischen Rahmens oder in der Organisation des Unternehmens umgehend aktualisiert wird. Wie bei jedem Risikoidentifikations- und Steuerungsprozess bildet auch beim Compliance-Risiko die korrekte Ermittlung und Bewertung des Risikos (und der jeweiligen Wechselbeziehungen zwischen den einzelnen Risiken) die Grundlage, um die Risikomanagementmassnahmen und die entsprechenden Kontrollen festzulegen.

4. DIE ROLLE DER COMPLIANCE-FUNKTION

Immer mehr Unternehmen – auch KMUs, sofern das Compliance-Risiko als relevant erachtet wird – schaffen im Rahmen ihrer Organisation eine spezifische Compliance-Funktion. Ziel ist es, Kontrolltätigkeiten und Reporting im Compliance-Bereich zentral zusammenzuführen. Konkrete Beispiele sind:

- Unternehmen, deren Tätigkeit zahlreichen Gesetzen unterliegt (Finanzsektor, Pharma, Lebensmittelbranche usw.)
- Unternehmen mit hohen Umweltauswirkungen
- Unternehmen, die grosse Mengen an Personendaten verarbeiten (Gesundheitssektor)
- Unternehmen, die spezifische Compliance-Risiken haben (Unabhängigkeitserklärung bei der Veröffentlichung von Pharmastudien usw.)

Oft wird die Steuerung solcher Compliance-Risiken (zusammen mit anderen potenziellen Compliance-Risiken) einer Funktion übertragen, die nicht über die erforderlichen Fachkompetenzen verfügt (z. B. CFO, Geschäftsführer/-in, Vertriebsleiter/-in), manchmal unter Beizug zahlreicher externer Berater, was im Falle einer Nichtkonformität erhebliche Konsequenzen und Sanktionen für das Unternehmen nach sich ziehen kann.

Eine interne Compliance-Funktion kann neben einer beratenden Rolle für den Verwaltungsrat und die Unternehmensleitung auch systematisch und koordiniert folgende Tätigkeiten übernehmen:

- Überwachung der geltenden Vorschriften
- Erkennung und Bewertung potenzieller Nichtkonformitätsrisiken
- Definition von Vorfällen und Risikoindikatoren
- Unterstützung bei der Planung von Risikomanagementmassnahmen
- Kommunikation und Schulung der Mitarbeitenden
- Unabhängige Durchführung von Kontrollen der Stufe 2, um die korrekte Funktion des Prozesses zur Steuerung des Compliance-Risikos zu überprüfen
- Berichterstattung an Verwaltungsrat und Unternehmensleitung sowie kontinuierliche Aktualisierung des Prozesses zur Steuerung des Compliance-Risikos

Diese spezielle Funktion im Unternehmen – die Compliance-Funktion (oder der/die sog. Compliance Officer) – kann dem Unternehmen Instrumente zur Unterstützung der eigenen Tätigkeit zur Verfügung stellen, wie etwa eine Aufstellung der geltenden Vorschriften, eine Datenbank mit den möglichen Compliance-Risiken, eine Datenbank mit möglichen Kontrollen der Stufe 2 oder ein standardisiertes Reporting-

Tabelle 3: **ROLLE DER COMPLIANCE-FUNKTION IM REGULATORISCHEN BEREICH**

Identifizierung und Bewertung der Vorschriften	Umsetzung der organisatorischen Lösungen	Kontrolle und Reporting	Kommunikation, Unterstützung und Schulung
Identifizierung des Betriebsumfangs und der Referenzvorschriften	Erstellung von Leitlinien/Richtlinien zu diesem Thema und Festlegung organisatorischer Massnahmen	Ermittlung und Bemessung der Compliance-Risiken	Bekanntmachung der Vorschriften und der relevanten Dokumente
Überwachung und Steuerung der regulatorischen Entwicklungen	Erstellung von Richtlinien, Verfahren oder Reglementen	Überprüfung der Einhaltung der rechtlichen Anforderungen	Beratung der Unternehmensbereiche bei der Anwendung von Normen und Verhaltenskodizes
Identifizierung der betroffenen Tätigkeiten	Entwicklung und Freigabe von Prozessen/IT-Anwendungen, wo erforderlich	Risikominderung und Berichterstattung an VR und Unternehmensleitung	Bearbeitung von Meldungen zu Verstössen gegen Compliance-Vorschriften innerhalb der Unternehmensbereiche sowie Ausarbeitung von Lösungen und organisatorischen Änderungen
Überprüfung des Compliance-Niveaus und Festlegung von Korrekturmassnahmen	Überprüfung der organisatorischen Lösungen	Kontaktmanagement mit den zuständigen Behörden	Schulung der Mitarbeitenden

Modell für den Verwaltungsrat und die Unternehmensleitung (vgl. auch *Tabelle 3*).

5. FAZIT

Auch wenn nicht alle Unternehmen, insb. solche mit weniger als 50 Mitarbeitenden, über die Ressourcen verfügen, um eine eigene, unabhängige interne Compliance-Funktion zu schaffen, sollten alle Unternehmen, sofern noch nicht geschehen, dazu übergehen, das Compliance-Risiko systematisch zu bewerten.

Dazu könnte jedes Unternehmen zunächst die folgenden Schritte umsetzen:

→ Beauftragen mindestens einer spezifischen Person im Unternehmen, die sich mit den Compliance-Aktivitäten befasst. Es ist wichtig, dass diese Person in entsprechenden externen Seminaren geschult wird, wie die Compliance-Funktion auszuüben ist. Zudem ist es erforderlich, die Rolle und die Tätigkeiten der Compliance-Funktion allen Mitarbeitenden ge-

genüber zu kommunizieren. Schliesslich ist ein Ethikkodex unerlässlich, der sämtliche Verhaltensregeln für alle Mitarbeitenden des Unternehmens einschliesslich der Spitze enthält.

→ Durchführen einer Bewertung des Compliance-Risikos, um die wichtigsten Risiken zu ermitteln. Dies dient als Grundlage, um geeignete Massnahmen zur Minderung möglicher Risiken für das Unternehmen zu entwickeln.

→ Bereitstellen eines Kanals für die Mitarbeitenden, über den sie Rechtsverstösse auch anonym melden können (Whistleblowing).

→ Last but not least: Fördern einer ethischen Unternehmenskultur auf der Grundlage von Transparenz und Integrität durch Kommunikation und regelmässige Schulungen für Mitarbeitende und Führungskräfte.

Die Einführung eines systematischen Prozesses zur Steuerung des Compliance-Risikos ist eine Investition in eine nachhaltige, resiliente Zukunft des eigenen Unternehmens. ■

Fussnoten: 1) International Organisation for Standardisation (ISO). 2) Committee of Sponsoring Organisations of the Treadway Commission (COSO). 3) United States Congress, Criminal Division, Foreign Corrupt Practices Act Unit, <https://www.justice.gov/criminal/criminal-fraud/foreign-corrupt-practices-act>. 4) United States Congress, Sarbanes-Oxley Compliance Professionals Association (SOXCPA), Sarbanes-Oxley Act, <https://www.sarbanes-oxley-act.com>. 5) Bundesgesetz über

den Datenschutz (DSG) vom 25. September 2020. 6) Bundesgesetz gegen den unlauteren Wettbewerb (UWG) vom 19. Dezember 1986. 7) Liste ohne Anspruch auf Vollständigkeit.

den Datenschutz (DSG) vom 25. September 2020. 6) Bundesgesetz gegen den unlauteren Wettbewerb (UWG) vom 19. Dezember 1986. 7) Liste ohne Anspruch auf Vollständigkeit.