



Compliance Management

Ein Praxisleitfaden zur erfolgreichen Umsetzung

von Martin Schwarzbartl und Andreas Pyrcek
Linde © 2013
111 Seiten

Fokus

Führung & Management
Strategie
Marketing & Verkauf
► **Finanzen**
Personalwesen
IT, Produktion & Logistik
KMU
Wirtschaft & Politik
Branchen
Business weltweit
Karriere & Selbstmanagement
Verwandte Themen

Take-aways

- Compliance steht als Begriff für die Einhaltung von Regeln, sowohl gesetzlicher Bestimmungen als auch interner Richtlinien.
- Compliance-Management-Systeme (CMS) zielen darauf ab, rechtskonformes, an ethischen Werten des Unternehmens orientiertes Verhalten zu steuern und sicherzustellen.
- Wichtigste Grundlage für ein CMS ist die Unternehmenskultur: die Gesamtheit der Werte, Normen und Einstellungen, die ein Unternehmen prägen.
- Das Management ist dafür verantwortlich, die Unternehmenskultur zu formulieren und glaubhaft vorzuleben.
- Die Position des Compliance-Officers erfordert hohe persönliche Kompetenz.
- CMS beruhen auf drei Grundpfeilern: Vermeidung, Früherkennung und Reaktion.
- Die effektivste Form der Prävention sind fortlaufende Schulungen der Mitarbeiter.
- Die effektivste Maßnahme für die Früherkennung sind Hinweisstellen, die die Informationen von Hinweisgebern professionell und systematisch auswerten.
- Compliance ist nur dann glaubwürdig, wenn Verdachtsmomente entschlossen nachverfolgt und Verstöße konsequent sanktioniert werden.
- Wirtschaftskriminelles Verhalten wird durch das Zusammentreffen von drei Faktoren besonders begünstigt: Gelegenheit, Anreiz oder Druck und Rechtfertigung der Tat.

Bewertung (bester Wert: 10)

Gesamtbewertung	Umsetzbarkeit	Innovationsgrad	Stil
7	8	6	7

Relevanz

Das lernen Sie

Nach der Lektüre dieser Zusammenfassung wissen Sie: 1) warum Compliance wichtig ist und 2) wie Sie ein Compliance-Management-System in Ihrem Unternehmen implementieren können.

Empfehlung

Die in den Sonntagsreden gerne beschworenen ethischen Werte lassen sich im Alltagsgeschäft häufig kaum wiederfinden. Compliance ist Ethik zum Anfassen und Compliance-Management-Systeme bringen die Orientierung an ethischen Werten auf den Boden der Büroräume zurück. Das Buch *Compliance Management* ist von Praktikern für die Praxis geschrieben; der eigene Anspruch, einen anwendungsorientierten Leitfaden vorzulegen, wird von den Autoren in vorbildlicher Weise erfüllt. Kurz, sehr gut strukturiert und verständlich formuliert, werden die wesentlichen Informationen zur Implementierung eines Compliance-Management-Systems vermittelt. Zahlreiche Fallbeispiele vertiefen das Verständnis, wichtige Informationen sind grau unterlegt und damit schnell erfassbar, gut aufbereitete Grafiken veranschaulichen das Beschriebene. Die Autoren geben darüber hinaus zahlreiche Tipps, wie Fallstricke zu vermeiden sind, und reißen hin und wieder auch spezielle Fragestellungen an. *getAbstract* empfiehlt das Werk darum allen, die beruflich mit dem Thema zu tun haben, als knappes Vademecum. Es ist jedoch auch für alle geeignet, die sich zum ersten Mal mit Compliance befassen und nach dem roten Faden im überdimensionalen Wollknäuel suchen.

Zusammenfassung

Skandale und kein Ende

Allein nach der US-amerikanischen Antikorruptionsgesetzgebung, der strengsten weltweit, wurden zwischen 2008 und 2011 Unternehmen zu Strafzahlungen von insgesamt mehr als 3,5 Milliarden Dollar verurteilt, unter ihnen so klingende Namen wie Siemens, die Deutsche Telekom, Daimler, Halliburton/KBR oder Johnson & Johnson. Die mit 800 Millionen Dollar höchste jemals zu zahlende Strafe hatte Siemens zu entrichten. Ihr lag eine der größten Korruptionsaffären der Nachkriegsgeschichte zugrunde.

Ein funktionierendes Compliance-Management-System (CMS) ist also alles andere als ein Nebengeschäft. Compliance bedeutet so viel wie Regelkonformität und CMS sind Strukturen und Prozesse, die ein rechtskonformes und an den ethischen Werten des Unternehmens orientiertes Verhalten systematisch steuern und sicherstellen. Orientiert an ähnlichen Systemen in Medizin und Pharmazie sind die Grundpfeiler eines CMS:

- **Prävention:** Vermeidung von Fehlverhalten,
- **Früherkennung:** möglichst frühzeitige Identifikation potenzieller Risikofaktoren,
- **Reaktion:** planvolles Vorgehen bei Verdachtsmomenten.

Ein CMS muss dem jeweiligen Unternehmen auf den Leib geschneidert werden, denn die Risiken für Regelverstöße sind abhängig von Branche, Unternehmensgröße und anderen Faktoren. Klassischerweise wird der Bereich der Antikorruption behandelt. Doch zusätzlich geraten ständig weitere Risiken in das Visier der CMS, sodass sich das zu steu-

„Der wesentlichste und wichtigste Bestandteil eines CMS ist die Unternehmenskultur.“

„Die Kultur und die Werte stellen den Orientierungsrahmen für jegliche Handlung im Unternehmen dar und sind somit der essentielle Bestandteil zur Unternehmensführung und jeglicher Geschäftsentscheidung.“

„Sollte das Topmanagement nicht den tatsächlichen Willen haben, compliance-konform zu handeln, so sollte man generell davon Abstand nehmen, eine derartige Organisation im Unternehmen aufzubauen.“

„Jegliches Handeln und Vorbildverhalten haben einen direkten Einfluss auf die Unternehmenskultur und die direkte Umsetzung im Wertschöpfungsprozess im Unternehmen.“

„Ziel ist es nicht, Mitarbeiter umfassend über Details der juristischen Sachlage zu informieren, sondern aufbauend auf einem Kernrisiko die individuelle Konsequenz für das tägliche Handeln zu beschreiben.“

„Es ist essenziell für die Durchsetzung von Compliance und Integrität, dass die Unternehmensleitung eine Rolle im Rahmen von Compliance-Trainings wahrnimmt. Über diesen Kanal kann die Relevanz des Themas in die Organisation getragen werden.“

ernde Risikoportfolio ständig erweitert und spezifiziert. Die Globalisierungs- und Regularisierungstendenzen liefern zahllose Ansatzpunkte: wettbewerbs- und kartellrechtliche Themen, Datenschutz und Datensicherheit, Export, Geldwäsche, Umweltrisiken und Gesundheitsschutz.

CMS im Herzen der Struktur

Die wesentlichen Faktoren bei der Konzeption und Implementierung von CMS sind Unternehmensgröße und -komplexität, Eigentümerstruktur, Risikoumfeld und Branchenrisiko. Ausgehend von der Compliance-Kultur des Unternehmens, also seinen grundlegenden ethischen Werten, werden in einem ersten Schritt die Compliance-Ziele definiert. Bei der Umsetzung dieser Ziele werden dann die drei Bereiche Prävention, Früherkennung und Reaktion unterschieden. Interne und externe Kommunikationsstrategien sowie fortlaufende Überprüfungen des CMS runden das Konzept ab. Das CMS sollte als integraler Teil der bestehenden risikorelevanten Abteilungen und Funktionen im Unternehmen positioniert werden. Wichtig dabei: eine enge Zusammenarbeit mit der internen Revision und dem Risikomanagement sowie deren Kontrollsystemen. Die Compliance-Abteilung ist innerhalb dieses Systems zuständig für die Sicherstellung der Regelkonformität.

Compliance-Kultur bildet die Grundlage

Der wichtigste Bestandteil eines CMS lässt sich nicht auf Knopfdruck implementieren, entwickeln oder verändern: die Unternehmenskultur. Sie entsteht in einem langen, fortlaufenden Prozess. Sie spiegelt sich wider in materiellen Dingen wie Raumgestaltung, Kleiderordnung, Umgangston oder Parkplatzregelungen, aber auch in immateriellen Dingen wie kollektiven Werten, Normen, Einstellungen, die sich in Denk- und Handlungsmustern oder in Firmengeschichte, Mythen und Werthaltungen äußern. Das grundlegende Menschen- und Weltbild, das in einem Unternehmen gepflegt wird, zeigt sich beispielsweise in der Art und Weise, wie das Verhältnis des Unternehmens zu Umwelt und Gesellschaft gestaltet wird. Compliance ist zwar die Aufgabe jedes und jeder Einzelnen, dennoch spielt das Management eine zentrale Rolle. Es ist dafür verantwortlich, die Unternehmenskultur in eine bestimmte Richtung zu lenken und in Leitbildern zu formulieren. Vor allem aber muss die Unternehmensspitze dies glaubhaft vorleben.

Zur Durchsetzung ist kommunikative Kompetenz gefragt

Die Ziele der Compliance sind nicht nur nach innen, sondern auch nach außen gerichtet und sollen die strategische Grundausrichtung des Unternehmens widerspiegeln. Sie können zum Beispiel verdeutlichen, dass es nicht nur um die Sicherstellung der Regelkonformität geht, sondern auch darum, eine Unternehmenskultur zu entwickeln und zu erhalten, die sich ethischen Grundwerten verpflichtet sieht. Ab einer gewissen Unternehmensgröße ist es sinnvoll, einen eigenen Compliance-Verantwortlichen einzusetzen. Alternativ kann die Funktion auch von der Leitung der Rechts- oder Personalabteilung betreut werden.

Entscheidend ist immer, dass der Compliance-Officer unabhängig und weisungsfrei agieren kann. In jedem Fall ist an Ausstattung und Positionierung der Compliance-Abteilung sehr klar ablesbar, wie ernsthaft ein Unternehmen das Thema angeht. Die Position des verantwortlichen Mitarbeiters erfordert neben fachlichem und technischem Know-how ein hohes Maß an kommunikativer und persönlicher Kompetenz. Klassische High Potentials, die direkt von der Universität kommen, sind eher nicht geeignet.

Prävention: Vermeidung ist die beste Vorsorge

Die Arbeit des Compliance-Officers hat zwei Ziele: Zum einen muss er Regeln und Richtlinien konzeptioniert und verständlich formulieren. Zum anderen ist er dafür verantwort-

*„Es kann nur ange-
raten werden, ein
geeignetes Hinweis-
gebersystem in ei-
nem Unternehmen
zu implementieren.“*

*„Um ein Compli-
ance-System glaub-
würdig in einem
Unternehmen um-
zusetzen, ist es
unumgänglich, po-
tenziellen Verstößen
nachzugehen.“*

*„Interne Unters-
uchungen dienen vor-
rangig dem Zweck,
ausreichend In-
formationen über
fraudulente An-
schuldigungen zu
generieren, um Ent-
scheidungen über
mögliche Conse-
quenzen zu treffen.“*

*„Entscheidend bei
der Erstevaluierung
ist der Umstand,
dass es sich um die
Plausibilisierungs-
maßnahmen der be-
kannten Vorwürfe
handelt, welche für
außenstehende Drit-
te nicht als solche
erkennbar sind.“*

lich, dass die Mitarbeiter so informiert und motiviert werden, dass sie diese Regelungen verstehen und in ihrer täglichen Arbeit anwenden können. Man unterscheidet sogenannte regelbasierte (rule-based) Compliance und verhaltensbasierte (behavior-based) Compliance. Wichtigster Vorteil der regelbasierten Systeme ist, dass sie eindeutig sind und leicht Sanktionen abgeleitet werden können. Und das ist auch gleichzeitig ihr Nachteil, denn sie sind wenig flexibel und können, da sie zu wenig an das Verstehen appellieren, schnell inhaltsleer und formal werden. Die Vorteile verhaltensbasierter Systeme sind, dass ihre Regeln leichter verständlich sind als die häufig an komplexen juristischen Vorgaben orientierten regelbasierten Systeme. Sie sind dadurch flexibler zu handhaben. Da sie aber auf die individuelle Verantwortlichkeit zielen und uneindeutig sind, sind eine Effektivitätskontrolle und Sanktionierungen schwierig.

Neben der Entwicklung und Formulierung der Richtlinien geht es vor allem darum, diese in die Köpfe der Leute zu bringen. Die effektivste Form dafür sind Schulungen, die fortlaufend durchgeführt werden sollten. Wichtig dabei ist, Planung, Organisation und Durchführung in den Händen der CMS-Abteilung zu belassen und auch das Monitoring nicht zu vergessen. Neben laufenden Schulungen sollte die Compliance-Abteilung auch eine permanente Consulting-Dienstleistung im Unternehmen anbieten. Hier gilt es, eine klassische Falle zu vermeiden, in die CMS-Abteilungen schnell geraten, nämlich als Geschäfts-Verhinderer zu gelten. Achten Sie daher darauf, immer unmissverständlich zu kommunizieren, dass die Verantwortung für die getroffenen Entscheidungen beim jeweiligen Management liegt.

Ein oft vernachlässigtes Feld ist die Frage der Incentivierung. Gemeint sind variable, von der Erreichung definierter Ziele abhängige Bestandteile der Vergütung. Klar ist, dass nicht das regelkonforme Verhalten an sich bereits honorierungswürdig ist. Umgekehrt aber muss Fehlverhalten arbeitsrechtlich durchsetzbare Sanktionierungen auf der Seite der variablen Vergütung nach sich ziehen. Darüber hinaus sollten Sie die Vergütungssysteme generell einer Analyse unter Compliance-Gesichtspunkten unterziehen: Einzelne Zieldefinitionen, wie die zu starke Ausrichtung an Verkaufszielen, können zu höheren Risiken führen.

Frühwarnsysteme: Je früher, desto besser

Neben einem funktionierenden Präventionssystem muss die Compliance-Abteilung ein Früherkennungssystem entwickeln und fortlaufend pflegen. Basis dafür ist eine grundlegende Risikoanalyse, das heißt, alle Bereiche des Unternehmens werden auf mögliche Risikopotenziale hin überprüft. Dabei kann eine sogenannte Risikomatrix hilfreich sein, in die Risiken jeweils nach ihrer Eintrittswahrscheinlichkeit und der Stärke der Auswirkungen eingetragen werden. Ein weiterer Bereich ist die Definition und fortlaufende Analyse relevanter Datenbestände. Auch wenn sie in manchen Unternehmen einen schlechten Ruf haben: Die Informationen von Hinweisgebern sind die wichtigsten Faktoren für die Entdeckung von Regelverstößen. Es ist deshalb ratsam, Anlaufstellen für Hinweisgeber einzurichten, die einen professionellen Umgang damit sicherstellen und als effektivstes Mittel für die Früherkennung gelten können.

Reaktion: konsequent nachverfolgen – entschlossen sanktionieren

Compliance ist nur glaubwürdig und wirksam, wenn potenzielle Verstöße entschlossen nachverfolgt und konsequent sanktioniert werden. Das probate Mittel der Nachverfolgung sind interne Untersuchungen, die von einer kleinen Hintergrundrecherche bis zu komplexen Ermittlungsprozessen reichen können. Vielfach wird argumentiert, dass solche Untersuchungen unnötig seien, dies sei Angelegenheit der staatlichen Ermittlungsbehörden. Es

„Verweigert man gänzlich die Stellungnahme bei Medienanfragen, hat dies meist negative Auswirkungen auf die Berichterstattung. Man sollte zumindest zu jeder Zeit auch gegenüber den Medien einen gewissen Kooperationswillen zeigen, ohne zu sehr ins Detail zu gehen.“

„Die Vision, dass mit der Installation eines Compliance-Verantwortlichen und eines Systems alle wesentlichen Compliance-Risiken minimiert sind, ist leider nicht begründet.“

ist aber dringend anzuraten, Verdachtsfälle zunächst intern zu prüfen, da möglicherweise die gemeldeten Verdachtsmomente nicht für staatsanwaltliche Ermittlungen ausreichen oder im Gegenteil so massiv sind, dass die Polizei umgehend mit einem Hausdurchsuchungsbefehl anrückt. Im ersten Fall bleiben Regelverstöße möglicherweise unentdeckt, weil Verdachtsmomente nicht nachverfolgt werden. Polizeiliche Ermittlungen hingegen ziehen meist intern wie auch extern negative und nicht mehr kontrollierbare Reaktionen nach sich.

Das Betrugsdreieck aufbrechen

Die Techniken solcher internen Falluntersuchungen orientieren sich an den Einsichten des Kriminologen Donald R. Cressey, der als einer der Pioniere bei der Erforschung von Wirtschaftskriminalität gilt. Er entwickelte das „Fraud Triangle“ (Betrugsdreieck), das besagt, dass Regelverstöße durch das Zusammentreffen dreier Bedingungen begünstigt werden:

- **Gelegenheit** macht Diebe, das gilt auch im Fall der Wirtschaftskriminalität. Der potenzielle Täter muss zunächst einmal eine Gelegenheit zur kriminellen Handlung haben, etwa weil das Kontrollsystem Schwachstellen hat.
- **Anreiz oder Druck** muss gegeben sein. Der Täter braucht ein Motiv, sei es, dass er sich persönlich bereichern oder auch unrealistische Zielvorgaben erfüllen möchte.
- **Möglichkeiten der Selbstrechtfertigung** sind als letzter Faktor essenziell. Der Täter braucht eine Argumentation, die begründet, warum sein Verhalten eigentlich nicht kriminell ist, beispielsweise weil der Betrug ja nur sein zu niedriges Gehalt aufbessert.

Bevor die Polizei kommt ...

Bereits vor dem Auftauchen von Verdachtsmomenten sollte ein Ablaufplan für interne Untersuchungen als Standardprozess vorliegen. Dieser klärt vorab, ob oder in welchen Fällen diese Untersuchungen von internem oder externem Personal durchgeführt werden oder wer intern den Prozess koordiniert. In der Regel wird dieser Plan eine Erstevaluierung festlegen, also eine Analyse der Ausgangssituation, indem intern Fakten gesammelt und ausgewertet werden, ohne dass für andere erkennbar ist, auf welche konkrete Person sich die Ermittlungen beziehen.

Auf dieser Basis sollte in einem zweiten Schritt ein Untersuchungsplan erstellt werden, der festlegt, welche konkreten Maßnahmen durchgeführt werden sollen. In einem dritten Schritt werden die relevanten Daten identifiziert, gesammelt und sichergestellt. Das können elektronische oder physische Daten sein, aber auch Interviews mit Informationsgebern. Die Ergebnisse werden in einem formellen Bericht niedergelegt, aus dem auch Maßnahmen abgeleitet werden, etwa eine Entlassung oder auch eine Anzeige bei den Strafbehörden. Nicht zuletzt sollten die externen wie internen Kommunikationsstrategien bereits vor dem Eintreten kritischer Situationen minutiös geplant sein, damit sie im Notfall abgerufen werden können.

Über die Autoren

Martin Schwarzbartl ist Chief Compliance Officer bei den Österreichischen Bundesbahnen und **Andreas Pyrcek** ist Senior Manager im Bereich Compliance bei Ernst & Young.