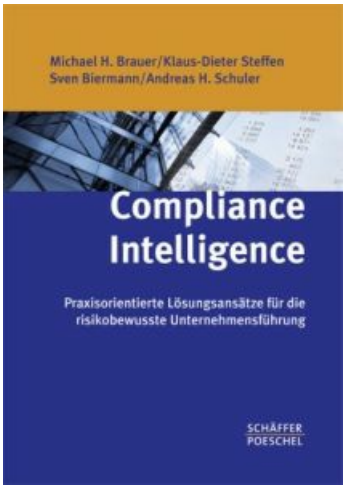

Buch Compliance Intelligence

Praxisorientierte Lösungsansätze für die risikobewusste Unternehmensführung

Michael H. Brauer, Klaus-Dieter Steffen, Sven Biermann und Andreas H. Schuler
Schäffer-Poeschel, 2009

Rezension

2007 war ein düsteres Jahr für den Weltkonzern Siemens: Über ein weit verzweigtes System schwarzer Kassen waren mehr als eine Milliarde Euro an Schmiergeldern geflossen. Reputation und Aktienkurs des ehemaligen Vorzeigeunternehmens waren am Boden. Das im Buch vorgestellte Konzept stammt aus dieser Zeit, das Unternehmen wird allerdings nicht namentlich erwähnt. Die Autoren standen vor der gigantischen Aufgabe, potenziellen Falschspielern in über 1000 Geschäftseinheiten weltweit auf die Finger zu klopfen. Zufallskontrollen, so ihre Erkenntnis, wären da nur ein Tropfen Wasser auf den Wüstensand. Stattdessen sollte ein ausgeklügelter IT-Bulldozer die ganze Wüste umpflügen und sie Tag für Tag, Sandkorn für Sandkorn nach Unregelmäßigkeiten durchsuchen. Klingt einfach, ist aber ebenso wie die Lektüre dieses Fachbuches recht kompliziert. Offen bleibt zudem die Frage, wie ein System formaler Berechtigungs- und Funktionstrennungen auf der Vorstandsebene funktionieren soll. *BooksInShort* empfiehlt das Buch CEOs und CFOs, Aufsichtsräten, Compliance-Officers und Wirtschaftsprüfern, die nach neuen Wegen in der Finanzaufsicht suchen.

Take-aways

- Corporate Governance hat sich zu einem K.-o.-Kriterium für global tätige Unternehmen entwickelt.
- Manuelle Kontrollen reichen nicht aus, um die Einhaltung interner und gesetzlicher Vorschriften zu garantieren.
- Compliance-Intelligence führt IT-Systeme und Prüfmethoden so zusammen, dass Kontrollen automatisch ablaufen.
- Die meisten Mitarbeiter übertreten Regeln, weil sich ihnen die Gelegenheit dazu bietet.
- Interne Kontrollsysteme müssen Versuchungen aufspüren und abbauen, z. B. sollten Mitarbeiter nicht zugleich Bestellungen aufgeben und Rechnungen bezahlen.
- Bieten Sie Ihren Mitarbeitern die Möglichkeit, Missstände anonym zu melden.
- Ergänzen Sie präventive Kontrollen um detektivische und führen Sie beide in einem kontinuierlichen Verbesserungsprozess zusammen.
- Kontinuierliches Information-Mining deckt Ineffizienzen in Arbeitsprozessen auf.
- Im CFO-Monitoring-Cockpit verfolgen Sie die Wirksamkeit der Maßnahmen und passen Kontrollregelwerke an.
- Transparenz ist Trumpf: Compliance-Systeme spionieren nicht, sondern dienen dem Wohl aller.

Zusammenfassung

Aktives Risikomanagement

Globale Geschäftstätigkeit ist eine komplexe Angelegenheit. Angesichts der kommunikativen Vernetzung kann es passieren, dass der Ruf eines Unternehmens in Gegenden ruiniert wird, in denen es nicht einmal präsent ist. Compliance, d. h. die Einhaltung gesetzlicher Pflichten und interner Leitlinien, ist heute wichtiger denn je, auch weil sie sich direkt auf den Unternehmenswert auswirkt. Grobe Verfehlungen haben nicht wenige Unternehmen an den Rand des Abgrunds gebracht. Die multipolare Welt bietet zwar viele Chancen, etwa den Zugang zu neuen Märkten, aber es drohen auch neue Risiken wie steigende regulatorische Anforderungen, politische und soziale Unruhen oder abnehmende Mitarbeiterloyalität. Ein aktives Risikomanagement ist heute unerlässlich.

> „Compliance nur als notwendiges Übel oder gar als Bedrohung aufzufassen, scheint den Autoren zu kurz gegriffen. Sie ist, wie andere Herausforderungen auch, mit Chancen verbunden, wenn man ihr nicht nur defensiv begegnet."

Governance-Programme bieten im Dschungel gesetzlicher und freiwilliger Vorschriften Orientierung. Sie sind der „Knigge“ jedes Unternehmens. Ermöglichen Sie Ihren Mitarbeitern, Missstände anonym zu melden und führen Sie scharfe Sanktionen bei Zuwiderhandlungen ein. Einfache Tätigkeiten, die sich mit Transaktionen befassen, können Sie intern konzentrieren oder in Länder mit niedrigen Lohnkosten auslagern. Hoch spezialisierte Tätigkeiten wie die zentrale Berichterstattung, M&A-Aktivitäten und das Risikomanagement sollten Sie hingegen in der Finanzabteilung zusammenführen. Compliance-Intelligence hilft dieser, bestehende Informationstechnologie und Prüfmethoden so zusammenzubringen, dass Kontrollen automatisch ablaufen.

Kontrolle ist besser

Ein Vertrauensverhältnis zu Mitarbeitern und Geschäftspartnern ist Gold wert – sich allein darauf zu verlassen jedoch naiv. Die meisten Gelegenheitsbetrüger im Job würden sich niemals als kriminell bezeichnen. Vielmehr geraten sie kurzfristig privat oder beruflich unter Druck, es bietet sich die Möglichkeit zur unbemerkten Regelwidrigkeit, und sie finden einen Weg, ihre Tat einigermaßen rational zu rechtfertigen. Ziel der Compliance-Intelligence ist es, solche Gelegenheiten zu reduzieren. Wenn etwa vor Schulanfang die Bestellungen für Bürobedarf stark ansteigen, ist das ein Hinweis darauf, dass es zu viele Möglichkeiten zum Schummeln gibt. Manuelle Kontrollen greifen zu kurz und sind zu kostspielig. Demgegenüber haben automatisierte Systeme viele Vorteile:

- Die Bestimmung von Stichprobenkriterien und Stichtagen entfällt. Kontrolliert wird kontinuierlich, nicht nur innerhalb begrenzter Zeiträume.
- Die Frage, ob es sich bei Unregelmäßigkeiten um Einzelfälle handelt, wird obsolet.
- Das Unternehmen mit all seinen Geschäftseinheiten und Schnittstellen wird abgedeckt.
- Die Ausgaben sinken langfristig, da nach der Einführung kaum Folgekosten anfallen.
- Intelligente Systeme decken Prozessineffizienzen und Optimierungspotenziale auf.

Information-Mining lohnt sich

Die Hauptaufgabe interner Kontrollsysteme liegt im „Information-Mining“, d. h. in der automatisierten Suche nach Prozessineffizienzen, Risiken und unrechtmäßigen Handlungen in großen Datenbeständen. Ein Beispiel für Ineffizienzen sind versehentliche Doppelzahlungen an Lieferanten. Ein Risiko liegt vor, wenn etwa ein Mitarbeiter eine Bestellung gleichzeitig aufgeben und annehmen kann. Von unrechtmäßigem Handeln spricht man z. B., wenn Angestellte bestimmte Lieferanten bevorzugt behandeln oder Leistungen für den eigenen Gebrauch bestellen. Weiter liefert das Information-Mining Hinweise darauf, wie effizient insgesamt gewirtschaftet wird. Z.B. könnte die Volumenverteilung auf unterschiedliche Lieferanten nahelegen, dass deren Zahl reduziert wird. Ohne großen zusätzlichen Aufwand erhalten Sie so Informationen mit hohem Mehrwert. Die Investition in ein intelligentes System zahlt sich immer aus. Laut einer Studie haben Unternehmen mit durchschnittlichen Finanzfunktionen von bis zu 44 % mehr Compliance-Mitarbeiter und zahlen bis zu 47 % mehr für externe Prüfungen als diejenigen mit den besten Finanzfunktionen.

Regelwerke erarbeiten

So führen Sie Compliance-Intelligence in Ihrem Unternehmen ein:

1. **Analysieren Sie den Geschäftsprozess**, und zwar im Hinblick auf Übergabepunkte: Zwischen Einkauf und Buchhaltung oder zwischen Bestellung und Rechnungsstellung liegen die größten Gefahren für Unregelmäßigkeiten.
2. **Identifizieren Sie die Kernrisiken**. Welche sind die gefährlichsten? Beispiele sind Unstimmigkeiten zwischen Leistung und Gegenleistung oder die fehlende Trennung von Verantwortlichkeiten. Kein Mitarbeiter sollte unautorisiert in den Prozess eingreifen oder Kontrollpunkte umgehen können.
3. **Entwickeln Sie die Kontrollstrategie**, indem Sie Ziele definieren: Unter welchen Umständen kann eine Unregelmäßigkeit gar nicht erst auftreten? Definieren Sie die Aktivitäten, die das Erreichen dieser Ziele kontrollieren. Die Aktivitäten fassen Sie zu unternehmensweiten Kontrollregelwerken zusammen.
4. **Passen Sie das Regelwerk an lokale Spezifika an**: Nicht alle Geschäftseinheiten in allen Ländern lassen sich über einen Kamm scheren. Unterschiedliche Datenverarbeitungssysteme sind nur eine von vielen Herausforderungen.

   „Die praktische Umsetzung von Compliance-Intelligence ist sicherlich anspruchsvoll, aber auch der finanzielle und personelle Aufwand für manuelle Kontrollen ist bei einem großen Unternehmen dauerhaft hoch.“

Präventive Kontrollen verhindern, dass überhaupt ein Risiko besteht. Bei der Vergabe einer Berechtigung können Sie automatisch prüfen lassen, ob diese mit einer bereits bestehenden im Konflikt steht. Detektivische Kontrollen liefern Hinweise auf mögliche Unregelmäßigkeiten. Ein Beispiel wäre eine hohe Zahl von Buchungen am Monatsende, die kurz darauf storniert wird. Wohl gemerkt: Eine Zuwiderhandlung ist damit nicht bewiesen. Aber der Fall sollte weiter verfolgt werden. Detektivische und präventive Maßnahmen ergänzen einander in einem kontinuierlichen Verbesserungsprozess, da erstere die Ideen für letztere liefern.

Mitarbeiter schützen

Auf der Mitarbeiterebene geht es in erster Linie um Prävention. Prüfen Sie zunächst die kritischen Einzelberechtigungen. Dann verteilen Sie wichtige Funktionen auf so viele Schultern wie möglich. Mit einer konsequenten „Segregation of Duties“ (SoD) wird verhindert, dass z. B. ein IT-Mitarbeiter, der für Archivierung und Systemkonfiguration gleichzeitig zuständig ist, Daten so verfälscht, dass sie nicht mehr geprüft werden können. Erstellen Sie ein Kontrollregelwerk, das SoD-konforme Berechtigungen in sämtliche Prozesse des Unternehmens integriert. Mitarbeiter, die ihren Aufgabenbereich wechseln, müssen alte Berechtigungen verlieren, wenn diese mit den neuen im Konflikt stehen. Selbstverständlich müssen Sie dafür sorgen, dass die gewonnenen Daten nicht für personenbezogene Auswertungen missbraucht werden. Compliance-Intelligence ist keine unternehmerische Geheimpolizei, sondern ein Instrument zur Vorbeugung. Es geht um das Wohl des Mitarbeiters und aller Interessengruppen – und genau so sollten Sie es kommunizieren.

Aktionen auswerten

Auf der Aktionsebene wird detektivisch gearbeitet. Tag für Tag überprüft der „Prozessdetektiv“ Geschäftstransaktionen, Stammdaten und die präventive Funktionstrennung auf ihre Ordnungsmäßigkeit. Zudem liefert er Informationen, die Ihnen helfen, Prozesse zu verbessern. Werden alle vertraglichen Konditionen, etwa der Skontoabzug, genutzt? Wie lange dauern bestimmte Handlungen und an welchen Stellen könnte der Ablauf beschleunigt werden? Continuous-Controls-Monitoring

(CCM), die kontinuierliche Analyse von Transaktionsdaten und Kontrollen, ermöglicht das Erreichen dieser Ziele. Die Rohdaten aus den Vorsystemen werden mithilfe standardisierter Methoden analysiert und auf die CCM-Plattform übertragen.

IT-Schutzschilde

Die dritte Kontrollebene ist die der Applikationen. Applikationskontrollen sind IT-gestützte Schutzschilde, die anonyme oder unberechtigte Datenverarbeitung verhindern und Manipulationen in der Datenverarbeitungslogik abwehren, z. B. mithilfe der Anlegung komplexer Passwörter. Sämtliche Sicherheitsmaßnahmen auf der Mitarbeiterebene sind wertlos, wenn es Betrügern gelingt, sich unter dem Namen anderer in das System einzuschleichen. Unrechtmäßige Handlungen wie das Zahlen zu hoher Mitarbeiterbezüge können Sie mithilfe einer entsprechenden IT-Konfigurierung verhindern. Das Konzept der PACs (Preventative-Application-Controls) ist nicht neu. Es gibt sie schon seit den Anfängen kaufmännischer Software. Oft sind sie jedoch gar nicht aktiviert oder gehen an den spezifischen Bedürfnissen eines Unternehmens vorbei. Die Herausforderung besteht in einer intelligenten Anpassung mithilfe so genannter PAC-Kontrollmonitoren. Diese kontrollieren die Wirksamkeit aller PACs und koordinieren sie untereinander.

Ein Praxisbeispiel

Die Herausforderung war gewaltig: Das Projektteam musste Compliance-Intelligence innerhalb kürzester Zeit in einem deutschen Industriekonzern mit rund 1000 Geschäftseinheiten im In- und Ausland einführen. Grundvoraussetzung war absolute Transparenz: Das Team berichtete wöchentlich an den Entscheidungsausschuss und führte monatliche Review-Sessions mit den Geschäftseinheiten durch. Im Intranet-basierten „Rollout-Tracker“ waren alle relevanten Termine jederzeit einsehbar.

> „Würden alle nur denkbaren Maßnahmen und Regelungen, die eine spezifische Risikosituation betreffen, im Unternehmen vollständig umgesetzt, käme die Geschäftstätigkeit praktisch zum Erliegen.“

Der Rollout selbst hing von der Risikopriorisierung ab: Ein Indikator für das Risikopotenzial einer Geschäftseinheit war z. B. das Korruptionsranking von Transparency International. Zunächst musste jede Geschäftseinheit detaillierte Fragebögen über ihre Arbeitsprozesse und ihre IT-Systeme ausfüllen – der erste von vielen Meilensteinen, die über den Projektverlauf hinweg gesetzt wurden. Nach einigen Testdurchläufen lief dann die „CCM factory“ an, eine automatisierte Datenanalyse-Plattform, welche die wichtigsten Informationen herausfilterte. Anschließend folgten die ersten präventiven Kontrollen. Zu berücksichtigen waren lokale Besonderheiten: Kleine Geschäftseinheiten hätten etwa eine strikte Funktionstrennung nur durch zusätzliches Personal gewährleisten können. In solchen Fällen galt es, alternative Lösungen zu finden. Ein entscheidender Schritt war die Harmonisierung der Stammdaten.

> „Kommt die Zentrale mit zusätzlichen Anforderungen, ist als erste Reaktion durchaus die Aussage zu hören: ‚Wir müssen auch noch Geschäfte machen!‘“

Um zu vermeiden, dass Geschäftspartner in unterschiedlichen Schreibweisen mehrfach geführt wurden, teilte man jedem eine unternehmensweite Identifikationsnummer zu. Das Mitarbeiterverzeichnis wurde um Funktionsbezeichnungen erweitert, damit die Einhaltung der SoDs überprüft werden konnte. Im Web-basierten CFO-Monitoring-Cockpit wurden alle Ergebnisse zusammengefasst. Der CFO kann darin durch Auswahl der Region, der Geschäftseinheit oder der Zeiträume recherchieren, wie welche Maßnahme wo am besten greift – oder auch nicht.

> „Letztendlich wird aber jedes risikobewusste Kontrollsystem, das dauerhaft bestehen soll, an zwei Grundprinzipien gemessen: Wirksamkeit und Wirtschaftlichkeit.“

Eskalationsmechanismen sorgen dafür, dass die Mitarbeiter ein identifiziertes Problem unverzüglich bearbeiten. Je länger sie es ignorieren, desto höher steht der CFO, der davon erfährt, in der Unternehmenshierarchie. Noch während des Rollouts übertrug das Projektteam das notwendige Know-how an die lokalen Geschäftseinheiten. Compliance-Intelligence ist nun fester Bestandteil des globalen, operativen Betriebs.

Über die Autoren

Michael H. Brauer ist Vice President und **Klaus-Dieter Steffen** Director der Abteilung Corporate IT bei Siemens. Sie waren zuletzt für die konzernweite Einführung eines Compliance-Projekts verantwortlich. **Sven Biermann** und **Andreas H. Schuler** sind Unternehmensberater mit den Schwerpunkten Finance- und Performance-Management.