

Wenn Compliance bei der IT landet

Compliance ist ein Schlüsselthema. Nicht zuletzt, weil es **persönliche Haftungsrisiken von Führungskräften** betrifft und eine entsprechende Priorität auf deren Agenda besetzt. Das zeigt **Wirkung in den Unternehmen**.

Von Prof. Peter Bienert, Forte Advisors

Compliance als Kostenfalle: Unter compliance-getriebenen Investitionen leidet das Unternehmens-Budget.

Nicht selten hört man in der IT, von der Finanzindustrie würden Budgets überwiegend zu Compliance-Themen bestimmt. Einer Studie von Deloitte mit dem Titel „Compliance im Wandel – Integrated Compliance and Risk Management als Ansatz für die Zukunft“ entnehmen wir: „Weltweit stiegen die durchschnittlichen Compliance-Kosten vom Jahr 2002 zum Jahr 2006 um 159 Prozent. Für die untersuchten Unternehmen beliefen sich die absoluten geschätzten Kosten des Compliance-Managements unternehmensintern in der Spanne von 200 bis 400 Millionen US-Dollar pro Jahr.“

VERANTWORTUNG VERSCHIEBEN

Deloitte US betrachtet diese Zahlen als eher konservativen Ansatz. „Aus eigenen Beobachtungen heraus könnten die Schätzungen immer noch bis 30 Prozent zu niedrig liegen.“ Compliance-Management dreht sich

um Maßnahmen für die Einhaltung von Vorschriften und Normen, denen ein Unternehmen ausgesetzt ist. Auch wenn der Fokus häufig auf externe, meist gesetzliche Normen gelegt wird – diese Definition umfasst alle, also auch interne Normen und Betriebsvorschriften aller Art. Schließlich erfordert die Einhaltung externer Regularien deren Übersetzung auf entsprechende interne Regelwerke.

Gerne tendiert der Zeitgeist zum Glauben, absolute Sicherheit zu erreichen oder zu gewährleisten, sei möglich. In Bezug auf Compliance führt dies in Politik und Wirtschaft zu einem reichlich naiven Handlungsmuster, wodurch die Einführung erweiterter Regularien automatisch zu einer Verringerung unerwünschter Risiken führt. Erfahrungsgemäß nutzt es aber nichts, Fehler zu verbieten. Abweichungen von Vorschriften wird es immer geben. Menschen werden immer Fehler machen.

Somit dreht sich Compliance genauer betrachtet um die Frage, wer die Haftung übernimmt, wer das Risiko einer Abweichung von der Vorschrift und der daraus entstehenden Folgen trägt. Dies führt schlimmstenfalls zu einem gigantischen Verschiebeparkplatz für Verantwortung.

Manche Unternehmensführung scheint weniger damit beschäftigt zu sein, an der Verringerung der Risiken zu arbeiten. Vielmehr scheint es darum zu gehen, durch entsprechende Organisationsreglements sicherzustellen, dass sie die eigene Sorgfaltspflicht nachweisen und dabei zugleich die Verantwortung in die Linienorganisation verlagern kann.

Dabei ist insbesondere die IT ein beliebtes Ziel für diesen internen Delegationsprozess. Die weitgehende Prozessabbildung des operativen Geschäftes mittels der IT bietet einen verführerischen Ansatzpunkt, Compliance alleine durch die Abbildung auf

↳ Prozessmuster der IT in den Griff bekommen zu wollen. Aus Sicht der IT gilt:

- IT kann das Verhältnis zwischen Conformance und Performance verbessern: Der Aufwand für Compliance lässt sich durch geeigneten Einsatz von IT verringern.
- IT ist für manche Compliance-Anforderungen unabdingbar, da deren Komplexität ohne sie gar nicht handhabbar wäre.
- IT und die weitgehende Abbildung des Unternehmens auf digitale Systeme und digitale Daten ist selbst ein Compliance-Risiko.

IT ALS COMPLIANCE-ENABLER

Die zunehmende Volatilität und gegenseitige Abhängigkeit von Compliance-Anforderungen steigert die Komplexität. Der Lebenszyklus von Vorschriften und den daraus resultierenden Modellen, IT-Funktionalitäten und -Prozessen erfordert zwingend den Einsatz geeigneter IT-Instrumente. Für viele Unternehmen besteht hier enormer Nachholbedarf. Compliance lässt sich nicht mehr länger mit Flat Files, Vorschriftendokumenten und Excel-Tabellen abbilden. Ähnlich wie im Falle des Vertragsmanagements, jedoch deutlich komplexer, erfordert ein geeignetes Verfahren ein generisches Unternehmensmodell und dessen Abbildung auf die betroffenen Normen und Vorschriften. Neben der ungewohnten Herausforderung einer digitalen Modellbildung für die Rechtsabteilung, die den ausgebildeten Juristen unvorbereitet trifft, macht sich hier das krasse Missverhältnis zwischen der heute üblichen IT-Unterstützung von Durchführungsprozessen gegenüber jener von Führungsprozessen bemerkbar.

— ANZEIGE —


powered by
IT-BUSINESS
ANZEIGEN

 Akademie
SearchNetworking.de

Praxistag IPv6 2011
Individuelle
Lösungskonzepte
und Praxis-Tipps
für die sichere
IPv6-Migration

NUR NOCH WENIGE
PLATZE FREI!

18.02. Frankfurt/Main



Jetzt anmelden:
www.searchnetworking.de/ipv6-praxis

IT-Verantwortliche müssen vorsichtig sein, keinesfalls das implizite Versprechen vollständiger Sicherheit abzugeben. Wird vollständige Sicherheit für grundsätzlich möglich gehalten, gilt ein tatsächlicher Fehler nicht mehr als Folge eines unvermeidbaren Restrisikos. Wenn absolute Sicherheit möglich ist, muss doch jeder Fehler die Konsequenz eines persönlichen oder organisatorischen Fehlverhaltens sein. Die IT ist hier oft das letzte Glied in der Kette von Zugangssystemen, Identity- und Access-Management, Datensicherung und Datensicherheit sowie Recovery-Management und bildet letztlich die technische Plattform für die breite Mehrheit von Compliance-Verfahren.

IT ALS COMPLIANCE-RISIKO

Unternehmen ohne den Einsatz von Informationstechnik sind nicht mehr denkbar. Mit der Abhängigkeit des Geschäfts von digitalen Daten und Prozessen steigt der Anteil der IT als Risikofaktor. In Bezug auf Datensicherheit und Disaster Recovery ist das Bewusstsein in den Unternehmen inzwischen ausgeprägt und sensibilisiert. Werden jedoch zusätzlich Verfahren zur Einhaltung von Compliance-Vorgaben auf die IT abgebildet, potenziert sich die IT-Risikoposition des Unternehmens gleichsam.

Ein Beispiel: Der Zugriff auf kursrelevante Informationen muss in einer börsennotierten Gesellschaft einem kleinen, klar identifizierbaren und autorisierten Personenkreis vorbehalten bleiben. Dies liegt in der Verantwortung der Unternehmensführung. Banken sind gehalten, den Schutz der Kundendaten gegen unbefugte Zugriffe zu garantieren. In beiden Fällen spielt die Zugangssicherung über ein Rollen- und Identitätskonzept der IT eine zentrale Rolle. Die Verantwortung (zumindest im Innenverhältnis) geht an die IT über. Das Identitäts- und Zugangsmanagement wird damit aber selbst zur zentralen Risikokomponente. Wer diesen „Single Point of Failure“ besetzt, hebt an einer einzigen Stelle das komplette Sicherheitskonzept aus. □



IT Guidelines

In der Kommunikation mit der Unternehmensführung sind drei Ebenen der IT für einen Beitrag zur Compliance zu unterscheiden:

1. Regel-Ebene: IT muss sich aktiv an der Ausgestaltung von Systemen beteiligen, die das Lifecycle-Management von Compliance-Vorgaben erst ermöglichen.
2. Awareness-Ebene: IT kann Verfahren einklagen und mitentwickeln, die dazu beitragen, das Bewusstsein der Mitarbeiter in einem sensiblen Kontext zu schärfen.
3. Audit- und Forensik-Ebene: IT muss einen Beitrag leisten, um die Sicherheit im Unternehmen auditierbar zu machen. Weiterhin sind Mechanismen vorzusehen, mit denen ein Bruch der Regeln schnell offenkundig und nachverfolgbar wird (Forensik).

Als letzte Regel und Erfahrung der Praxis gilt: Risiken lassen sich zwar verringern, niemals aber verhindern. Risikomanagement muss daher immer ein vollständiges Reaktionsmuster für jenen Fall enthalten, dass das Risiko tatsächlich eintritt.

Der Autor



PROF. PETER BIENERT ist Gründer und Präsident des Verwaltungsrates der Forte Advisors AG in Glatttowers/Schweiz. Prof. Bienert ist Buchautor zu Themen wie IT-Governance und hat an

der Hochschule St. Gallen das Modell „New Corporate Governance“ entwickelt.

WEB | WWW.FORTE-ADVISORS.COM