



## .02 Im Interview: IT-Compliance im Visier der Wirtschaftsprüfer

24|1|2007



Weltweit gelten mittlerweile mehr als 25.000 Regulierungen und gesetzliche Auflagen zur Kontrolle und Transparenz im Unternehmen oder zur Dokumentationspflicht von Geschäftsabläufen. IT-Governance Experte Holger Schellhaas von evoltas solutions verrät im Gespräch, wie sich GDPdU, GoBS, Basel II, KonTraG, Solvency II, FDA-Compliance oder der Sarbanes-Oxley-Act über alle Branchen hinweg massiv auf die IT auswirken.

**CW: Und wieder ein neuer Begriff, ein neues „Buzzword“ in der IT: Compliance. Was ist das eigentlich?**

**Holger Schellhaas:** Ein Beispiel: Sie wollen, dass mit Hilfe der eingesetzten IT die Geschäftsziele abgedeckt, Ressourcen verantwortungsvoll eingesetzt und Risiken angemessen überwacht werden? Klar, keine Frage! Dann haben Sie bestimmt Grundsätze, Verfahren und Maßnahmen etabliert, die dies garantieren. Wie Sie die Anforderungen ihrer Anwender in Systemlösungen überführen, ihren Systembetrieb aufrechterhalten, ihre IT-Sicherheit im Griff haben - das alles haben Sie dokumentiert und Sie kontrollieren es auch kontinuierlich. Dann haben Sie genau das, was IT-Compliance fordert, bereits weitgehend umgesetzt.

Weltweit gelten mittlerweile mehr als 25.000 Regulierungen und gesetzliche Auflagen zur Kontrolle und Transparenz im Unternehmen oder zur Dokumentationspflicht von Geschäftsabläufen - wie die GDPdU, GoBS, Basel II, KonTraG, Solvency II, FDA-Compliance oder der Sarbanes-Oxley-Act, die sich über alle Branchen hinweg massiv auf die IT auswirken. Bereits auf der zweiten September-Plenartagung am 28. September 2005 in Straßburg stimmte eine breite Mehrheit im Europäischen Parlament für die „EuroSOX“-Richtlinie, so dass sich auch Regelungen, die eigentlich nur für die an der US-Börse notierten Firmen gedacht war, in Europa durchsetzen. Darüber hinaus entstehen Compliance-Erfordernisse durch Anforderungen von nationalen und internationalen Kunden und Lieferanten, wenn beispielsweise ein US-Investor oder ein US-Großkunde dies fordert.

**Was ist konkret zu tun? Was ist „essential - nice-to-have - luxury“?**

Es wird viel Panik vor allem über die neuen Gesetze und Normen verbreitet. Viele Inhalte dieser Gesetze werden aber zumindest teilweise schon längst in den Unternehmen aufgrund bestehender Regelungen befolgt. Vieles gebietet der gesunde Menschenverstand und die unternehmerische Logik, vieles ist allerdings nicht sauber dokumentiert. Wirklich neu ist, dass die IT mittlerweile im Visier der Wirtschaftsprüfer ist - kein Wunder, wenn immer mehr Geschäftsprozesse von der IT durchdrungen sind. Hier liegt auch die Chance des Compliance Managements: Der Zwang zur Transparenz leistet einen nicht unerheblichen Beitrag zur Performance Verbesserung. Compliance rentiert sich also! Wichtig ist, eine IT Compliance Roadmap zu erstellen, anhand der der zuständige Wirtschaftsprüfer oder Auditor sehen kann, dass die IT auf dem richtigen Weg ist. Dann kann man mit

realistischen Schritten die IT Compliance schrittweise umsetzen.

### **Seit COBIT 4.0 ist in der IT die Welt wieder in Ordnung ...**

Das COBIT-Modell (Control Objectives for Information and related Technology) wurde von Revisoren aus der Industrie und dem Berufsstand (ISACA - Information Systems and Control Association) auf Basis bestehender Revisionsrichtlinien, Kontrollmodellen und branchenspezifischen Regularien und Richtlinien entwickelt. Bei der Entwicklung galt es, ein Rahmenmodell zur Verfügung zu stellen, mit dem die Ausrichtung der eigenen IT in Bezug auf die unternehmerischen Ziele messbar und steuerbar ermöglicht wird. Mit der neuen Version 4.0 - an der deutschen Fassung hat die KPMG maßgeblich mitgewirkt - hat sich ein bewährtes Verfahren etabliert, mit dem es gelingt, ein „audit-fähiges“ Kontrollsystem mit vertretbarem Aufwand zu entwickeln und ungeliebte Auflagen letztlich in Erfolgsfaktoren umzumünzen.

Vor der umfassenden Neu-Ausrichtung nach den neuen Gesetzen muss allerdings gewarnt werden. „Wer mit beiden Füßen gleichzeitig läuft, stolpert“ oder:  $E = Q * A$  - Effektivität = Qualität \* Akzeptanz. Gleichzeitig kann aber auch die Einführung von COBIT ohne Berücksichtigung von bestehenden Best Practice-Modellen zum Projektmisserfolg führen. Bei Best Practices ist natürlich vor allem der de facto Standards ITIL hervorzuheben. Beide Ansätze ergänzen sich hervorragend in einem komplementären Sinne, da der Ansatz von COBIT der Kontrollgedanke ist und ITIL den Servicegedanken trägt.

#### **UCS Customers Report**

Jetzt das Whitepaper downloaden. Cisco UCS powered mit Intel® Xeon®  
[www.cisco.com/de/UCS](http://www.cisco.com/de/UCS)

#### **Code Review von Experten**

Führender Anbieter: Sicherheit & Qualität für Java, C#, PHP, uvm.  
[www.optimabit.com](http://www.optimabit.com)

#### **DELL Laptop Preissturz**

Jetzt Business Angebote sichern. Mit Intel® Core™ der 2. Generation.  
[www.DELL.com/de](http://www.DELL.com/de)

#### **Workshops Online-Handel**

Workshops für Geschäftsführer, Inhaber und Führungskräfte.  
[akademie-handel.de](http://akademie-handel.de)

Google-Anzeigen