

Der Sarbanes-Oxley-Act im Kontext der Informationstechnologie

Wer **kontrolliert** wen?



Infolge des Sarbanes-Oxley-Act rücken IT-Systeme in den Fokus des Interesses der Finanzverantwortlichen. Denn mit Hilfe der Informationstechnologie werden bilanzrelevante Daten ausgewiesen oder weiterverarbeitet, die für den Geschäftsbetrieb von Bedeutung sind. Das hat auch für CIOs deutscher Unternehmen Konsequenzen.

Der Sarbanes-Oxley-Act (SOX) gilt seit dem 15. April 2004 für alle bei der US Securities and Exchange Commission (SEC) registrierten Unternehmen. Seit 2006 unterliegen dem SOX in vollem Umfang auch ausländische Unternehmen, deren Aktien an amerikanischen Börsen notiert sind. Direkt betroffen sind immerhin 38 deutsche Unternehmen, deren Derivate an Börsen in den USA gehandelt werden. Was den IT-Verantwortlichen vieler, scheinbar nicht betroffener, deutscher (Zulieferer-)Unternehmen noch nicht gänzlich bewusst ist: auch für ihre Informationstechnologie ergeben sich beachtliche Rückwirkungen. Denn mittels ihrer IT-Systeme werden bilanzrelevante Daten ausgewiesen oder weiterverarbeitet, die für den Geschäftsbetrieb von genereller Bedeutung sind.

SOX-Checkliste für den CIO

Folgende Punkte sind wichtig für CIOs. Diese prüfen die Aufsichtsbehörden streng:

- Zugangsberechtigungen
- Sicherheitskonzepte
- Betriebskonzepte für die Archivierung
- Betriebskonzepte für den Einsatz von IT-Sicherheitswerkzeugen
- Sicherungs- und Recovery-Konzepte
- Archivierungslösungen

Die prominenten Pleitefälle von ENRON, WorldCom, Parmalat und anderen bilden den Hintergrund für die Entstehung des Sarbanes-Oxley-Act. Mit dem Gesetz reagierte die amerikanische Regierung auf die ins öffentliche Bewusstsein gedrängten „White Collar Crimes“, das heißt Verbrechen der Vorstandsetagen, die durch Manipulationen und Fälschung von Informationen Anleger um Milliarden prellten.

Kern des SOX ist die Haftung seitens des Managements. Die Verantwortung für ein vollständiges und korrektes Finanzberichtswesen wird bei den Geschäftsführern und Vorständen angesiedelt. Diese büßen für jeden betrügerischen Verstoß im Sinne des SOX mit bis zu 20 Jahren Gefängnis und/oder fünf Millionen Dollar Geldstrafe.

Das Gesetz verpflichtet das Management, Prozesse und Kontrollmechanismen einzuführen, damit bilanzrelevante

Daten eindeutig, vollständig und dauerhaft (auch unveränderlich) gespeichert und verarbeitet werden können.

Die CIOs in Stuttgart, Wolfsburg, München, Berlin, Düsseldorf und andernorts sehen sich also direkt mit amerikanischen Regelungen konfrontiert, die tiefgreifende Implikationen für Budgets und Strukturen nach sich ziehen. Auch die Regeln bezüglich der Aufbewahrung von Dokumenten, Datensicherheit und Wiederauffindung sind streng.

Kontrolle durch IT

Der Schwerpunkt der Anforderungen an die Informationstechnologie leitet sich aus den Sektionen 302 „Corporate Responsibility for Financial Reports“ und 404 „Management Assessment of Internal Controls“ ab. Der Abschnitt 302 fordert die Bestätigungen, dass:

- die Geschäftsführung und ihre Beauftragten für die Einrichtung und Kontrolle des Finanzberichtswesens verantwortlich sind,
- die Geschäftsführung und ihre Beauftragten Kontrollmechanismen eingeführt haben, damit die Buchhaltung auf Basis der Grundlagen ordnungsgemäßer Buchführung durchgeführt wird (im Original wird auf GAAP – General Accepted Accounting Principles – verwiesen),
- etwaige Änderungen an internen Kontrollmechanismen vollständig in den SOX-Report eingeflossen sind.

In erster Linie geht es in Sektion 302 also um die Einrichtung und die Überwachung von Kontrollmechanismen des Prozesses für das Finanzberichtswesen. So bahnen sich die SOX-Anforderungen einen Weg auf die Ebene der Informationstechnologie bis hin zu deren Betrieb. Das Finanzberichtswesen ist üblicherweise vollständig mit und durch IT realisiert. Die Geschäftsführungen der betroffenen Unternehmen werden nicht lange brauchen, um herauszufinden, dass die Einrichtung und die Überwachung von Kontrollmechanismen am effektivsten auf der IT-Ebene geschehen. Ein Blick über den großen Teich offenbart einhergehende Probleme, zum Beispiel bei der Definition der Verantwortlichkeiten zwischen CFOs und CIOs.

Chefredakteur:

Ulrich Parthier (-14)

Redaktion:

Silvia Parthier (-26)

Redaktionsassistentin und Sonderdrucke:

Petra Lemke (-10)

Autoren dieser Ausgabe:

Sebastian Asendorf, Khaled Baghban, Tonio Grawe, Bernhard Gröhl, Luis Praxmarer, Lars Schwarze.

Anschrift von Verlag und Redaktion:

IT Verlag für Informationstechnik GmbH,
Rudolf-Diesel-Ring 32, 82054 Sauerlach,
Postfach 1128, 82050 Sauerlach
Tel.: 08104-6494-0, Fax: 08104-6494-22
E-Mail für Leserbriefe: IT-Management@IT-Verlag.de
Homepage: <http://www.IT-Verlag.de>

Alle Autoren erreichen Sie über die Redaktion. Wir reichen Ihre Anfragen gerne an die Autoren weiter.

Manuskripteinsendungen: Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warenamen ohne Gewährleistung in freier Verwendung benutzt.

Herausgeberin: Dipl.-Volkswirtin Silvia Parthier

Grafische Konzeption, Illustrationen, DTP:

G&K Design: Andreas Kreutz, Fiona Kreutz-Güldenpfennig
www.magazinemaker.de

Anzeigenpreise: Es gilt die Anzeigenpreisleiste Nr. 13 vom Dezember 2005

Anzeigenverkauf:

Hans-Jürgen Schellhase
Mittermayrstraße 29, 80796 München
Tel.: 089 30765774, Fax: 089 30765776
E-Mail: schellhase@it-verlag.de

Anzeigenverkauf Großbritannien:

GCA Greg Corbett Associates Ltd.
International Media Sales
5 Lower Belgrave Street London SW1W 0NR
Tel.: +44 20 7730 60 33
Fax: +44 20 7730 66 28
E-Mail: gca@gca-international.co.uk

Anzeigenverkauf USA:

Global Ad-Net
Mr. Ed Ware
80 Elm Street, Suite #2
Petersborough, NH 03458
Tel.: +1 603-924-1040
Fax +1 603-924-1041
E-Mail: ed@globalad-net.com

Objektleitung: Ulrich Parthier (-14)

ISSN-Nummer: 0945-9650

Erscheinungsweise: monatlich

Verkaufspreis: Einzelheft 10 Euro (Inland), Jahresabonnement 100 Euro (Inland), 110 Euro (Ausland), Probe-Abonnement für drei Ausgaben 15 Euro.

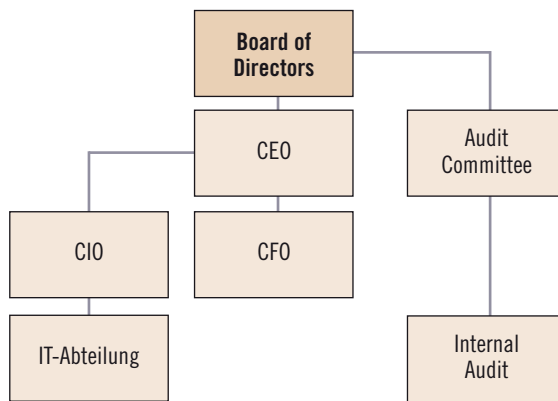
Bankverbindung: VRB Oberhaching-Wolfratshausen eG,
BLZ 701 664 86, Kontonummer 25-23752

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Je 50% des Gesellschaftskapitals halten Silvia und Ulrich Parthier, Sauerlach.

Abonnementservice: Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Bezugsgelder.



Geeignete Unternehmensstruktur



Ein internes Audit kann am effektivsten umgesetzt werden, wenn es direkt an den Aufsichtsrat berichtet. In jedem Fall sollte die IT von dem CFO unabhängig sein.

Zwistigkeiten entstehen, wenn erstere versuchen über die Kontrollhoheit Einfluss auf das IT-Budget zu nehmen.

Die Sektion 404 fordert einen zusätzlichen Bericht, der über den Quartalsbericht und den Jahresabschluss hinausgeht. In diesem muss die Verantwortung der Geschäftsführung zur Einrichtung und Kontrolle des Finanzberichts dokumentiert werden. Damit nicht genug. Weiterhin verlangt die Sektion 404 einen Bericht über die jährliche Prüfung der Wirksamkeit dieser Kontrollmechanismen, gemäß den durch das „Public Company Accounting Oversight Board“ definierten Standards. Diese Kontrollmechanismen wiederum müssen selbst jährlich auf ihre Effektivität geprüft werden. Diese Prüfung kann auch von Dritten durchgeführt werden. Die entsprechenden Kontrollmechanismen müssen natürlich bereits vor der Überprüfung bestehen.

Überprüfungen

Je nach Kontext des Prozesses und der beteiligten Systeme werden die in Abschnitt 302 geforderten Kontrollmechanismen definiert. Hieraus ergeben sich fixe Prüfpunkte, die selbst durch die in Abschnitt 404 geforderten Kontrollen überprüft werden können. Hierzu werden im ersten Schritt die finanz- und damit auch bilanzrelevanten Daten des Unternehmens identifiziert. Daran anschließend wird der Prozess der Verarbeitung dieser Daten nachvollzogen. Dies führt direkt zur Identifikation der beteiligten Anwendungen

und IT-Systeme. Typische Prüfpunkte sind demnach Zugangsberechtigungen zu Systemen und Systemkomponenten, die im Kontext der relevanten Anwendungen bestehen. Auch Sicherheitskonzepte für die Überwachung, Kontrolle und Vergabe der Berechtigungen stehen im Blickpunkt der Aufmerksamkeit. Zudem gilt Beachtung den Betriebskonzepten für die Archivierung der Daten und den Einsatz von IT-Sicherheitswerkzeugen zur Kontrolle sicherheitsrelevanter Ereignisse im Kontext dieser Anwendungen. Ein weiteres Augenmerk richtet sich demnach auf Sicherungs- und Recovery-Konzepte für die Wiederherstellung der finanz- und bilanzrelevanten Daten im Fehlerfall



*Die Informationstechnologie
ist grundlegend für
das Finanzberichtswesen.
Kontrollieren CIOs
also CFOs?*

sowie Archivierungslösungen für alle finanz- und bilanzrelevanten Daten.

Nachweise

Über die Prüfung der Kontrollmechanismen sind, wie mehrfach betont, für die SEC Nachweise zu erbringen. Die Nachweise der Kontrolleure (Auditoren) müssen mindestens fünf Jahre aufbewahrt werden. Sie sind angehalten, von möglichen (wahrscheinlichen) Manipulations- und Fehler-Szenarien auszugehen. Im Einzelfall ist zu prüfen, welchen Umfang die Überprüfung haben soll. Die Nachweise für die Prüfung der Kontrollmechanismen sollen folgenden Charakter haben:

- Eindeutigkeit des überprüften Prüfpunktes.
- Nachvollziehbarkeit der Prüftätigkeit Ergebnis der Prüftätigkeit.
- Entlastung des verantwortlichen Managements durch den erfolgreichen Nachweis der Effektivität der Kontrollmechanismen.

Praktische Anwendung

In der Praxis empfiehlt es sich mit dem Fokus auf die Daten vom Allgemeinen zum Speziellen vorzuarbeiten. Ohne Anspruch auf Vollständigkeit können folgende Fragestellungen helfen:

- Wie werden die Daten erzeugt?
- Wie werden die Daten gelagert und gesichert?
- Wie wird der Zugang zu diesen Daten überwacht?
- Was könnte zu einem Datenverlust führen?
- Was könnte zu einer Manipulation von Daten führen?

Nach einer aktuellen Studie und Berichten in der US-Tagespresse beschäftigen sich die CFOs der prüfungspflichtigen Unternehmen mittlerweile bis zu 40 Prozent ihrer Zeit mit SOX. Im Interesse der allgemeinen Handlungsfähigkeit der Finanzbereiche betroffener Unternehmen ist es wünschenswert, dass die Mechanismen und Kontrollen ihrerseits effektiv und effizient ablaufen und durchgeführt werden.

*Bernhard Gröhl
groehl@lexta.com*