

# Alles wie immer?!

## Wie viel Neues bringt „Euro-SOX“ für das IT-Risikomanagement?

**Bei genauer Betrachtung erweist sich die häufig als Euro-SOX bezeichnete 8. EU-Richtlinie vor allem als „Meta-Richtlinie“, die kaum Neues und Konkretes zum IT-Risikomanagement enthält, aber wichtige Rahmenbedingungen festschreibt. Neben einem Blick in die jetzt in Kraft getretene Regelung liefert der vorliegende Beitrag eine grundlegende Zusammenfassung anzuwendender Regularien.**

*Von Reinhard Vossbein, Wuppertal*

Seit Anfang 2008 ist die 8. EU-Richtlinie in Kraft, die umgangssprachlich häufig Euro-SOX genannt wird. Offiziell trägt sie die Bezeichnung „Richtlinie des Europäischen Parlaments und des Rates über die Prüfung des Jahresabschlusses und des konsolidierten Abschlusses und zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates“. Die Bezeichnung Euro-SOX ist insofern irreführend, als sich die 8. EU-Richtlinie im Gegensatz zu ihrem US-amerikanischen Pendant nicht mit exakten Fragestellungen der Bewältigung von Risiken im Unternehmen befasst. Sie legt vielmehr fest, nach welchen Kriterien Unternehmen eine Institutionalisierung des Risikomanagements (mindestens) vornehmen müssen und welche Voraussetzungen Wirtschaftsprüfer zu erfüllen haben, um das Risikomanagement effizient kontrollieren zu können.

Das Risikomanagement selbst muss jedoch gemäß bereits bestehenden Gesetzen erfolgen – die Richtlinie gibt lediglich Hinweise im Hinblick auf Ordnungsmäßigkeitsvorgaben zu Management und Prüfung. Im Prinzip bedeutet dies, dass Unternehmen, die bisher schon ein ordnungsgemäßes Risikomanagement installiert haben, wegen der Inhalte der Richtlinie kaum Veränderungen vornehmen müssen. Um das genauer zu erörtern, sollen im Folgenden zunächst einige Aussagen der Richtlinie selbst in Augenschein genommen und anschließend konkretere Vorgaben zum IT-Risikomanagement aus verschiedenen Regularien rekapituliert werden.

Sucht man in der Richtlinie risikorelevante Aussagen, so findet man zunächst folgende Zweckbestimmung: „Durch ein wirksames internes Kontrollsystem werden finanzielle und betriebliche Risiken sowie das Risiko von

Gesetzesverstößen auf ein Mindestmaß beschränkt und die Qualität der Rechnungslegung verbessert. .... Der Prüfungsausschuss hat darüber zu wachen, dass Kontrollen durchgeführt werden und bei Verstößen gegen interne Kontrollregelungen oder Rechts- und Verwaltungsvorschriften geeignete Meldeverfahren greifen. Der kollektiven Verantwortung des Vorstandes für Betrieb, Prüfung und Offenlegung des internen Kontrollsystems darf dies jedoch keinesfalls Abbruch tun.“

### Auszüge der 8. EU-Richtlinie

Im Übrigen heißt es: „Prüfungsausschüsse und ein wirksames internes Kontrollsystem tragen dazu bei, finanzielle und betriebliche Risiken sowie das Risiko von Vorschriftenverstößen auf ein Mindestmaß zu begrenzen und die Qualität der vorgelegten Abschlüsse zu verbessern.“ Somit müssen Prüfungsausschüsse auf höchster Ebene sowie ein wirksames internes Kontrollsystem (IKS) zum Management von finanziellen, betrieblichen und rechtlichen Risiken als unabdingbare Voraussetzung für ein effizientes Risikomanagement gelten.

Wirtschaftsprüfungsgesellschaften haben die Qualität des internen Kontrollsystems – gestützt auf die Arbeit der Prüfungsausschüsse – zu prüfen. Rechnungsprüfer müssen im Rahmen ihrer Eignungsprüfung eine entsprechende Befähigung nachweisen. Die Richtlinie fordert hierzu, dass die im Rahmen der Eignungsprüfung (für Wirtschaftsprüfer) durchgeführte theoretische Prüfung insbesondere auch das Sachgebiet „Risikomanagement und interne Kontrolle“ umfasst.

Als Aufgaben des Prüfungsausschusses nennt die Richtlinie unter anderem:

- \_\_\_\_\_ den Rechnungslegungsprozess zu überwachen und
- \_\_\_\_\_ die Wirksamkeit der internen Kontrolle, gegebenenfalls der Innenrevision und des Risikomanagements des Unternehmens zu kontrollieren.

### Allgemeine Regularien

Das Risikomanagement eines Unternehmens wird jedoch letztlich erst durch die jeweils geltenden gesetzlichen Regelungen vorgegeben und durch Wirtschaftsprüfer im Hinblick auf seine Ordnungsmäßigkeit geprüft. Die 8. EU-Richtlinie setzt voraus, dass Unternehmen die entsprechenden Gesetze kennen und einhalten und

Wirtschaftsprüfer diese Einhaltung in der Jahresabschlussprüfung kontrollieren. Aus der Vielzahl der Regularien, die Vorgaben zum Risikomanagement enthalten, sollen daher die wichtigsten im Folgenden kurz dargestellt werden.

## KonTraG

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (kurz KonTraG) hat zum Ziel, Unternehmensführungsmethoden zu installieren, die ermöglichen Entwicklungen frühzeitig zu erkennen, die den Fortbestand des Unternehmens gefährden könnten. Als mögliche existenzgefährdende Entwicklungen nennt das KonTraG:

- \_\_\_\_\_ risikobehaftete Geschäfte,
- \_\_\_\_\_ Unrichtigkeiten der Rechnungslegung sowie
- \_\_\_\_\_ Verstöße gegen gesetzliche Vorschriften.

Hierbei ist als Zusatzbedingung erwähnt, dass die betreffenden Risiken Auswirkungen auf die Vermögens-, Ertrags- und Finanzlage haben sollen. Somit sind IT-Risiken aufgrund ihrer Auswirkungen auf die Vermögens-, Ertrags- und Finanzlage wesentliche Bestandteile der Betrachtung.

Das KonTraG fordert von Unternehmen, Risikofrüherkennungssysteme, Risikomanagement- und -steuerungssysteme zu installieren sowie potenzielle Risikofelder zu beobachten und den davon ausgehenden Risiken gegenzusteuern.

Die zunehmende Abhängigkeit der meisten Unternehmen von einem funktionierenden Informationswesen, Computerunterstützung als Faktor im Wett-

bewerb, unternehmensübergreifende Kommunikation als Möglichkeit, innovativ im Markt aufzutreten und Kommunikationsprozesse als Erfolgsfaktor zu begreifen, machen die Bedeutung der Informationstechnik und ihres Einsatzes als ein beachtliches Risikofeld offenkundig.

## Basel II

Die EU-Eigenkapitalrichtlinie (Capital Requirements Directive – CRD), meist kurz „Basel II“ genannt, hat zum Ziel, die Stabilität im Kreditwesen zu erhöhen. Die Hinterlegung mit Eigenkapital bei den Kreditinstituten berücksichtigt die Risiken des einzelnen Kreditengagements. Die Höhe des zur Absicherung von Krediten einzusetzenden Eigenkapitals hängt dabei wesentlich von der Bonität und den Zukunftsaussichten der Kreditnehmer ab. Hierbei werden auch „weiche“ Faktoren wie Strategie, Marktkennntnis, Managementqualität, Sicherheit der Planung sowie Geschäftsprozesse, Reaktion auf Abweichungen und vieles mehr in den kreditnehmenden Unternehmen überprüft und bewertet. Schließlich wirken sich alle unternehmerischen Entscheidungen über kurz oder lang auf die Zahlen des Jahresabschlusses aus – die Banken wollen Chancen und Risiken der Unternehmen im Voraus erkennen und bewerten.

Relevante Fragen zum Risikomanagement sind bei Basel II unter anderem:

- \_\_\_\_\_ Sind die Ziele für das Risikomanagement definiert?
- \_\_\_\_\_ Verfügt das Unternehmen über eine Unternehmensstrategie?
- \_\_\_\_\_ Existiert eine Risikostrategie?
- \_\_\_\_\_ Ist die Risikostrategie aus der Unternehmensstrategie abgeleitet?

\_\_\_\_\_ Ist ein einheitliches Risikomanagement im Unternehmen umgesetzt?

\_\_\_\_\_ Besteht in allen Unternehmensbereichen ein Risikomanagement-Verständnis und Risiko-Bewusstsein?

Die Überprüfung von qualitativen Kriterien stellt dabei einen Frühwarnindikator dar, mit dessen Hilfe Gefahrenpotenzial erkannt werden soll. Zur Ermittlung und Bewertung von Risiken wird dabei auf so genannte Ratings zurückgegriffen. Es geht in diesem Zusammenhang um die Herleitung eines Konzepts für ein IT-Risikomanagement und IT-Securitymanagement, aus dem sich ein positiver Einfluss auf das Rating des Unternehmens durch die Banken ergeben soll: So wie ein Unternehmen durch eigene Entscheidungen, Maßnahmen und Aktivitäten sein Rating positiv beeinflussen und damit seinen Handlungsspielraum (bezüglich der auf Fremdkapital beruhenden finanziellen Möglichkeiten) aktiv gestalten kann, so ist auch die Gestaltung der sicheren und zuverlässigen organisatorisch-technischen Abwicklung der Geschäftsprozesse Aufgabe des zu entwickelnden IT-Risiko- und -Securitymanagements.

## SOX

Obwohl der US-amerikanische Sarbanes-Oxley-Act (SOX) nicht direkt für deutsche Unternehmen gilt, ist zu erwarten, dass viele seiner Anforderungen über kurz oder lang in europäisches Recht einfließen und auch in der deutschen Rechtsprechung zukünftig berücksichtigt beziehungsweise von global operierenden Unternehmen vorzeitig in ihre Überlegungen einbezogen werden. Hierin liegt ein wesentlicher Unterschied zur 8. EU-Richtlinie.

Für Authentifizierung, Zugriffskontrolle und Benutzermanagement empfiehlt das IT Governance Institute die Control Objectives for Information and related Technology (COBIT). Dieser Standard nimmt eine ganzheitliche Sicht auf die IT ein. Er unterstützt das Management und vor allem die interne Revision bei der Wahrnehmung ihrer Verantwortung für das Erreichen der Geschäftsziele, die Kontrolle der dabei verwendeten Ressourcen hinsichtlich Effektivität und Effizienz, die Einhaltung rechtlicher Rahmenbedingungen sowie die Handhabung der mit der Geschäftstätigkeit und dem Ressourceneinsatz verbundenen Risiken (z. B. Sicherheitsrisiken).

Die Revisionsicht auf die IT enthält den Aspekt der „einheitlichen Grundlage für die Wertung der internen Kontrollen“ (so die 8. EU-Richtlinie). Damit werden die Ziele der IT-Governance im Unternehmen unterstützt: Ausrichtung der IT auf die Geschäftstätigkeit (Nutzenmaximierung), wirtschaftlicher Einsatz von IT-Ressourcen (Daten, Anwendungen, Technologie, Anlagen, Personal) und angemessenes Risikomanagement IT-bezogener Risiken.

SOX verlangt in Section 302 Kontrollen und Verfahren für korrekte Veröffentlichungen der Finanzdaten: Dies erfordert ein korrektes Erfassen und Verarbeiten aller relevanten Informationen im Unternehmen. Es muss durch entsprechend ausgeprägte Maßnahmen verhindert werden, dass mangelhafte Kontrollen und dadurch bedingte falsche oder unvollständige Informationen die Finanzdaten verfälschen. Dieser Ansatz korrespondiert mit dem KonTraG und dem Handelsgesetzbuch (§§ 317 ff. HGB).

SOX Section 404 legt für das Management weitere reichende Konsequenzen fest: Das Management hat die Wirksamkeit des IKS jährlich zu bewerten und muss dies mit Beweismaterial und einer Dokumentation nachweisen können, wie es auch die 8. EU-Richtlinie fordert. Allerdings ist in SOX die persönliche Haftung der Verantwortlichkeiten eindeutig definiert, was das US-Gesetz deutlich von der 8. EU-Richtlinie unterscheidet.

## IDW PS 330

Das Institut der Wirtschaftsprüfer (IDW) hat im Laufe der letzten Jahre eine Vielzahl von Prüfungsstandards (PS) erlassen; diese sind auch Grundlage der von Wirtschaftsprüfern vorzunehmenden Prüfungshandlungen im Sinne der 8. EU-Richtlinie. Im IT-Umfeld ist vor allem der Prüfstandard IDW PS 330 relevant, der Abschlussprüfungen bei Einsatz von Informationstechnik erfasst (vgl. <kes> 2006#6, S. 79). Er enthält Richtlinien für:

- \_\_\_\_\_ Ziele und Umfang von IT-Systemprüfungen,
- \_\_\_\_\_ Durchführung von IT-Systemprüfungen,
- \_\_\_\_\_ IT-gestützte Prüfungstechniken sowie
- \_\_\_\_\_ Produktdokumentation und Berichterstattung.

Der Standard wird im Hinblick auf die zu prüfenden Gebiete durch weitere IDW-Prüfstandards und so genannte Grundsätze ergänzt, allem voran IDW RS FAIT 1 „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (siehe [www.idw.de/idw/portal/d302224/](http://www.idw.de/idw/portal/d302224/)): In ihm sind die Grundlagen zur Prüfung eines IT-gestützten Rechnungslegungssystems im Hinblick auf die Erfüllung der gesetzlichen Anforderungen dargestellt.

Aus dem IDW PS330 lassen sich im Hinblick auf das Risikoproblem folgende Risikofelder ableiten:

- \_\_\_\_\_ IT-Umfeldrisiken,
- \_\_\_\_\_ IT-Organisationsrisiken,
- \_\_\_\_\_ IT-Infrastrukturrisiken,
- \_\_\_\_\_ IT-Anwendungsrisiken,
- \_\_\_\_\_ IT-Geschäftsprozessrisiken,
- \_\_\_\_\_ IT-Überwachungsrisiken sowie

\_\_\_\_\_ IT-Outsourcingsrisiken (genauer im Prüfstandard IDW PS331 dargestellt).

Diese Risiken sind Gegenstand des Prüfungsvorgehens. Es ist ersichtlich, dass eine nach den Prinzipien der Risikoinventur vorgenommene Risikobewertung diese Risikofelder abdecken muss, sodass bei einer Prüfung durch den Wirtschaftsprüfer diesem die Vorlage des Risikomanagementberichtes als Grundlage für sein weiteres Vorgehen dienen kann. Es sei darauf hingewiesen, dass nach der oben dargestellten Struktur des IDW PS330 die Dokumentation (und natürlich auch die hierauf aufbauende Dokumentationsprüfung) ein wesentlicher Bestandteil sowohl des Risikomanagements als auch insbesondere der Prüfung selbst darstellt.

## IDW PS 340

Der IDW-Standard PS340 behandelt die Prüfung des nach Aktiengesetz einzurichtenden und laut Handelsgesetzbuch zu prüfenden Risikofrüherkennungssystems (§317 Abs.4 HGB i.V.m. §91 Abs.2 AG). Er benennt die Maßnahmen, die nach dem KonTraG Gegenstand der Prüfung sind, im Besonderen:

- \_\_\_\_\_ festgelegte Risikofelder,
- \_\_\_\_\_ Risikoerkennung und Risikoanalyse,
- \_\_\_\_\_ Risikokommunikation,
- \_\_\_\_\_ Zuordnung von Verantwortlichkeiten und Aufgaben,
- \_\_\_\_\_ Errichtung eines Überwachungssystems sowie
- \_\_\_\_\_ Dokumentation der getroffenen Maßnahmen.

Im Prinzip sind entsprechende Prüfungen lediglich bei Aktiengesellschaften verpflichtend durchzuführen, jedoch gilt auch hier – wie schon in anderem Zusammenhang mit dem KonTraG festgestellt –, dass eine Ausstrahlung auf andere Unternehmen und Rechtsformen zu erwarten ist.

Bezüglich der Dokumentation wird gefordert, dass sie zur Sicherstellung der dauerhaften personenunabhängigen Funktionsfähigkeit der getroffenen Maßnahmen und zum Nachweis der Erfüllung der Pflichten des Vorstandes einen angemessenen Nachweis über die getroffenen Maßnahmen und das institutionalisierte Überwachungssystem enthält. Eine fehlende oder unvollständige Dokumentation führt zu Zweifeln an der dauerhaften Funktionsfähigkeit des Risikomanagementsystems. Hierzu gibt es mittlerweile ein Gerichtsurteil, demzufolge einem Vorstand aufgrund Fehlens der Dokumentation des Risikomanagementsystems die Entlastung versagt wurde.

Der Abschlussprüfer hat darüber hinaus zu beurteilen, ob die getroffenen Maßnahmen geeignet sind, die

gesetzlichen Anforderungen zu erfüllen. Auch dieses steht im Einklang mit der 8. EU-Richtlinie.

## Standardisierung durch Tools

Die Vorteile des Einsatzes von Revisionstools für die Effizienz der Arbeit eines Revisors sind beträchtlich. Erfahrungen mit solchen Softwarewerkzeugen belegen, dass alle Phasen des Revisionsprozesses in den Bereichen IT-Sicherheit und Risikomanagement von hinreichend „intelligenten“ und technisch hochwertigen Tools unterstützt werden können. Dazu muss insbesondere der jeweilige Prüfstandard möglichst genau abgebildet sein, um nach dem Stand der Technik und des aktuellen Wissens hochqualifizierte Revisionsergebnisse liefern zu können.

Im Sinne der Richtlinie können solche Tools bereits von der internen Revision im Vorfeld eingesetzt werden, um die Einhaltung der Vorgaben (Compliance) festzustellen. Neben der eigentlichen Arbeit kann hierdurch auch die Akzeptanz von Berichten durch den Revisor deutlich positiver ausfallen.

Auch der externe Revisor kann sich auf Tools stützen, welche die Anforderungen der genannten Regularien (insbesondere der IDW-Prüfstandards) abbilden. Damit ist es möglich, die in der 8. EU-Richtlinie genannten Anforderungen nach Beherrschung des Risikomanagements durch den Prüfer wesentlich zu stützen und vor allem zu standardisieren, das heißt, Subjektivitäten in der Interpretation von Ordnungsmäßigkeitsanforderungen weitgehend einzuschränken.

## Fazit

Die 8. EU-Richtlinie bietet im Hinblick auf präzise Vorschriften zur Gestaltung von Risikomanagementsystemen der IT wenig Konkretes. Unternehmen und Prüfer müssen vor allem die vorhandenen Gesetze kennen, umsetzen und im Hinblick auf ihre Umsetzungsqualität prüfen. Hierbei reicht die deutsche Gesetzgebung aufgrund der Tendenzen zur Globalisierung im Zweifelsfall nicht aus, sondern sollte zumindest durch die Inhalte des SOX ergänzt werden. Als wesentliche Hilfen bei der Herstellung der Ordnungsmäßigkeit und ihrer Prüfung können die Standards des IDW angesehen werden. Der Einsatz geeigneter Tools unterstützt die Prüfer fachlich und trägt zudem zur Objektivierung der Prüfung bei. ■

*Prof. Dr. Reinhard Voßbein ist Geschäftsführer der UIMCert GmbH, Wuppertal ([www.uimcert.de](http://www.uimcert.de)).*

# Verantwortlich für die IT-Sicherheit...

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

## <kes>

- liefert Ihnen strategisches Know-how, damit Sie eine solide Grundlage zur Entscheidungsfindung haben
- berichtet über Trends und Neuentwicklungen
- gibt Hilfen zum Risikomanagement
- erläutert einschlägige Gesetze im Umfeld der IT und TK
- informiert über die wichtigsten Messen und Kongresse
- ermöglicht es Ihnen durch Anwenderberichte von den Erfahrungen anderer zu profitieren
- gibt mit Marktübersichten einen Überblick über ausgewählte Produkte und Dienstleistungen

Jetzt Probeheft anfordern!



## <kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter [www.kes.info](http://www.kes.info) nutzen. Hier finden Sie ohne Zugangsbeschränkung, das Thema der Woche und außerdem aktuelle Artikel zum Probelesen.

Abonnenten erhalten zusätzlich ein Passwort mit dem sie Zugriff auf alle aktuellen Artikel und auch auf das Online-Archiv erhalten.

## ABONNEMENT-BESTELLUNG

Ich abonniere die Zeitschrift <kes> ab Heft Nr. ....  
Als Dankeschön erhalte ich das erste Heft gratis.

Das Abonnement enthält ein Passwort zur Nutzung des Abo-Bereichs auf [www.kes.info](http://www.kes.info) mit allen aktuellen Beiträgen und dem <kes>-Archiv.

Ich kann das Abonnement bis 14 Tage nach Erhalt des ersten Exemplars formlos widerrufen.

Nach Ablauf der Widerrufsfrist wird das Abonnement zu den regulären Bedingungen gültig:

Jahresbezugspreis (6 Ausgaben) € 122,00 inkl. MwSt. und Versandkosten (Schweiz SFr 238,00 / restl. Ausland € 137,00).

Der Jahresbezugspreis wird jeweils für ein Jahr im Voraus berechnet. Eine Kündigung des Abos ist dennoch jederzeit zur nächsten nicht gelieferten Ausgabe möglich. Überbezahlte Abogebühren werden rückerstattet.

Ich bin einverstanden, dass die Deutsche Post AG eine eventuell geänderte Anschrift weitergibt.

## PROBEHEFT-ANFORDERUNG

Bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - Die Zeitschrift für Informations-Sicherheit zum Probelesen zu.

Datum

Zeichen

Unterschrift

**FAX an +49 6725 5994**

Lieferung bitte an

SecuMedia Verlags-GmbH

Abonnenten-Service

Postfach 12 34

55205 Ingelheim

Telefon Durchwahl