

Musterlösungen Vieweg-Buch „IT-Risiko-Management mit System“

Kontrollfragen und Aufgaben zu Kapitel 4

Lösung zu Frage 1

Unter „Corporate Governance“ wird das System verstanden, mit dem die Verantwortlichkeiten, Kontrolle und Transparenz an der Unternehmensspitze gewährleistet werden und die dazu notwendigen Strukturen, Verhalten und Verfahren geregelt sind.

Gemäss einer OECD-Definition von 1999 ist „Corporate Governance“ das System, mit welchem Geschäfts-Gesellschaften geführt und kontrolliert werden. Die „Corporate Governance“ - Struktur spezifiziert die Verteilung von Rechten und Verantwortlichkeiten unter den verschiedenen Mitgliedern in der Gesellschaft (Unternehmen), wie dem Verwaltungsrat (Board), der Geschäftsleitung (Manager), den Anteilseignern und anderen Anspruchsgruppen und drückt die Regeln und Verfahren aus, um Entscheidungen in Gesellschafts-Angelegenheiten zu fällen. Daneben stellt sie die Struktur zur Verfügung, um die Unternehmens-Ziele zu bestimmen sowie die Mittel, um diese Ziele zu erreichen und die Leistung zu überwachen.“

Lösung zu Frage 2

Das Risiko-Management unterstützt die Steuerung und Kontrolle der Aktionen in einem Unternehmen und hilft damit das Eintreten von übermässigen Verlusten für Anteilseigner und Anspruchsgruppen zu verhindern. In die Entscheidungsprozesse integriert hilft es zudem, die Chancen wie die Risiken in angemessener Masse wahrzunehmen und damit effektive Unternehmensziele zu bestimmen und zu erreichen.

Lösung zu Frage 3

In den Corporate-Governance Regelungen überbinden die Gesetzgeber und Regulatoren meist auch Anforderungen an ein Risiko-Management an die Unternehmen (z.B. Frühwarnsystem bei KonTraG, Basel II, COSO-Standards zur Compliance mit Sarbanes-Oxley). Fehlentscheide aufgrund der Unterlassung eines angemessenen Risiko-Managements können persönliche Haftungs-

folgen für Verwaltungsrats- und Geschäftsleitungs-Mitglieder nach sich ziehen. Das IT-Risiko-Management ist dann wichtig, wenn zum einen IT-Risiken auf Grund der IT-Abhängigkeit Unternehmensgefährdungen mit sich bringen und um anderen, wo das Financial-Reporting des Unternehmens von der Funktionsfähigkeit und Integrität von IT-Systemen abhängt. Welche Rollen kommen dem Verwaltungsrat (Aufsichtsrat) und dem CEO eines Unternehmens bezüglich Risiko-Management zu?

Der Verwaltungsrat hat für die notwendigen Strukturen, die Transparenz und Kontrolle (z.B. Einrichtung eines Audit-Komitees) zu sorgen. Der CEO ist der ultimative Risiko-Owner eines Unternehmens und ist im Auftrag des Verwaltungsrats für die Ausführung des Risiko-Managements verantwortlich und zur angemessenen Berichterstattung an den Verwaltungsrat verpflichtet.

Lösung zu Frage 4

Um die SOX-Anforderungen zu erfüllen, muss ein Unternehmen ein „Framework“ einrichten, mit dem Risiken bezüglich „Financial Reporting“ identifiziert und gemanaged werden können. Der Zweck dieser Übung liegt beim Schutz der Anliegen der Anteil-eigener. Die Anforderungen sind in Section 404 von SOX festgelegt. (Shareholder). Das amerikanische SEC (Security Exchange Commission) benützt zur Überprüfung von SOX den U.S. Audit Standard (AU319), in welchem die „COSO-Kontroll-Standards“ integriert sind (COSO = Committee of Sponsoring Organizations of the Treadway Commission).

Der COSO-Kontroll-Standard identifiziert fünf wichtige Komponenten für eine effektive Interne Kontrolle:

1. Kontroll-Umgebung
2. Risiko-Assessment
3. Kontroll-Aktivitäten
4. Information und Kommunikation
5. Überwachung

Die Umsetzung dieser für SOX wichtigen COSO-Kontroll-Komponenten führt zu folgenden Aktivitäten:

- Dokumentation der Schlüsselprozesse rund um das Financial Reporting

- Untersuchung aller Elemente der Schlüsselprozesse rund um das Financial Reporting, ob deren Risiken adäquat kontrolliert werden
- Behandlung / Bewältigung eines jeden höheren Risikos
- Ständige Überwachung (Monitoring) der Schlüsselprozesse rund um das Financial Reporting
- Schaffung einer Struktur und Umgebung, in der es möglich ist, allfällige Mängel unverzüglich an die verantwortlichen Führungs- und Kontrollstellen zu melden.

Ein entsprechend eingeführter Risiko-Management-Prozess erfüllt diese Aufgaben. Zusammenfassend kann festgehalten werden, dass ein IT-Risiko-Management als Teil eines Unternehmens-Risiko-Management-Prozesses die Einhaltung des SOX-Gesetzes und damit die Corporate Governance eines Unternehmens unterstützt.