MUSTERLÖSUNG, H.P. KÖNIGS, SPRINGER VIEWEG „IT-RISIKOMANAGEMENT MIT SYSTEM“, 5. AUFLAGE

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 4

Lösung zu Frage 1

Das St. Galler Management-Modell unterscheidet die drei Kategorien von Unternehmensprozessen wie folgt:

Managementprozesse: Die Managementprozesse dienen der effektiven und effizienten Führung eines Unternehmens. Solche Managementprozesse sind beispielsweise der Strategieprozess, der Risikomanagement-Prozess, die Prozesse für das Qualitätsmanagement oder das Sicherheitsmanagement, die Planungs- und Budgetierungsprozesse sowie die Kontrollprozesse, wie sie beispielsweise durch CobiT* vorgegeben werden.

Geschäftsprozesse: Die Geschäftsprozesse dienen der eigentlichen Wertschöpfung des Unterbehmens.

Unterstützungsprozesse: Die Unterstützungsprozesse unterstützen vor allem die Geschäftsprozesses, aber wo nötig auch die Mangementprozesse. Typische Unterstützungsprozesse sind die IT-Prozesse oder die Prozesse zur Bereitstellung von Ressourcen, wie Personal oder Infrastruktur.

Lösung zu Frage 2

Unter „Corporate Governance“ wird das System verstanden, mit dem die Verantwortlichkeiten, die Kontrolle und die 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 (Management), 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.“

* Control Objectives for Information and Related Technology

Lösung zu Frage 3

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 Gefahren (Risiken) in angemessenem Masse wahrzunehmen und damit effektive Unternehmensziele zu bestimmen und zu erreichen.

Lösung zu Frage 4

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, Risiko-Messverfahren bei Basel II, Compliance zu den COSO-Standards beim Sarbanes-Oxley-Gesetz). Fehlentscheide aufgrund der Unterlassung eines angemessenen Risiko-Managements können persönliche Haftungsfolgen für Verwaltungsrats- und Geschäftsleitungs-Mitglieder nach sich ziehen. Das IT-Risiko-Management ist dann eminent wichtig, wenn zum einen IT-Risiken auf Grund der IT-Abhängigkeit grosse Gefährdungen des Unternehmens mit sich bringen und zum anderen, das Financial-Reporting des Unternehmens von der Funktionstüchtigkeit und der Integrität von IT-Systemen abhängt.

Lösung zu Frage 5

Der Verwaltungsrat hat für die notwendigen Strukturen, die Transparenz und Kontrolle (z.B. Einrichtung eines Audit-Komites) 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 6

Um die SOX-Anforderungen zu erfüllen, muss ein Unternehmen ein „Framework“ einrichten, mit dem Risiken bezüglich „Financial Reporting“ identifiziert und gemanagt werden können.

Die Bestimmungen müssen von bestimmten Firmen des öffentlichen Sektors und solchen, die an der amerikanischen Börse (US Securities Exchange Commission) registriert sind (auch Providers, an die Prozesse ausgelagert sind), strikt eingehalten werden.

Wirtschaftprüfer müssen nicht nur die Richtigkeit der im Finanzergebnis ausgewiesenen Zahlen überprüfen, sondern auch den unternehmensinternen Prozess und die Fehlerfreiheit der Systeme beurteilen, die zu diesen Zahlen geführt haben.

Der Zweck dieser Übung liegt beim Schutz der Anliegen der Anteileigener (Shareholder). Die Anforderungen sind in Section 404 von SOX festgelegt. Die 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). Zu den siebzehn siebzehn Kontroll-Grundsätzen

von COSO gehören auch vier wichtige Grundsätze zum Risiko-Assessment (z.B. „Die Organisation identifiziert die Risiken im Erreichen ihrer Ziele über die gesamte Organisationseinheit und analysiert die Risiken als Basis für deren Behandlung.“

Lösung zu Frage 7

Der Schutz der unternehmenseigenen Daten (im privaten Bereich,) fällt

a) in der Schweiz unter das Datenschutzgesetz (DSG) des Bundes (das für natürliche und juristische Personen gilt)

   sowie

   im Schweizerischen Strafgesetzbuch in Art. 162: 2. „Verletzung des Fabrikations- oder Geschäftsgeheimnisses: Wer ein Fabrikations- oder Geschäftsgeheimnis, das er infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte, verrät, wer den Verrat für sich oder einen andern ausnützt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.“

b) in Lichtenstein unter Datenschutzgesetz (DSG), das für natürliche und juristische Personen gilt

   sowie

   im „Lichtensteinischen Strafgesetzbuch“ (StGB) § 122 unter „Verletzung eines Geschäfts- oder Betriebsgeheimnisses“:

   1) Wer ein Geschäfts- oder Betriebsgeheimnis (Abs. 3) offenbart oder verwertet, das ihm bei seiner Tätigkeit in Durchführung einer durch Gesetz oder behördlichen Auftrag vorgeschriebenen Aufsicht, Überprüfung oder Erhebung anvertraut oder zugänglich geworden ist, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

   2) Wer die Tat begeht, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

   3) Unter Abs. 1 fällt nur ein Geschäfts- oder Betriebsgeheimnis, das der Täter kraft Gesetzes zu wahren verpflichtet ist und dessen Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse des von der Aufsicht, Überprüfung oder Erhebung Betroffenen zu verletzen.

   4) Der Täter ist nicht zu bestrafen, wenn die Offenbarung oder Verwertung nach Inhalt und Form durch ein öffentliches oder ein berechtigtes privates Interesse gerechtfertigt ist.

   5) Der Täter ist nur auf Verlangen des in seinem Interesse an der Geheimhaltung Verletzten (Abs. 3) zu verfolgen.

Lösung zu Frage 8

1 Dieses (Informationssicherheits-)Gesetz gilt für die nachstehenden Behörden (verpflichtete Behörden):

a. die Bundesversammlung;

b. den Bundesrat;

c. die eidgenössischen Gerichte

d. die Bundesanwaltschaft und die Aufsichtsbehörde der Bundesanwaltschaft;

e. die Schweizerische Nationalbank.

2 Es gilt für die nachstehenden Organisationen (verpflichtete Organisationen):

a. die Parlamentsdienste;

b. die Bundesverwaltung;

c. die Verwaltungen der eidgenössischen Gerichte;

d. die Armee;

e. Organisationen des öffentlichen und privaten Rechts, die im Rahmen der Erfüllung von Verwaltungsaufgaben im Sinne von Artikel 2 Absatz 4 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997

3 sicherheitsempfindliche Tätigkeiten ausüben;

f. kantonale Behörden und Stellen, die im Auftrag des Bundes und unter seiner Aufsicht sicherheitsempfindliche Tätigkeiten ausüben

Lösung zu Frage 9

In der Schweiz und in Lichtenstein bezieht sich das Datenschutzgesetz sowohl auf natürliche als auch auf juristische Personen.

Lösung zu Frage 10

In der 8. EU-Richtlinie, Euro-SOX genannt, wird die öffentliche Aufsicht, die externe Qualitätssicherung der Wirtschaftsprüfung, die Pflichten des Abschlussprüfers, die Anwendung internationaler Normen und die Unabhängigkeit des Prüfers behandelt. Der hauptsächliche Zweck von Euro-SOX ist die Transparenz und die Verlässlichkeit der Jahres-Abschlussprüfung zu verbessern, indem zusätzliche Kontrollen über Wirtschaftsprüfer und „Unternehmen von öffentlichem Interesse“ eingeführt werden. Damit soll die Funktion der Abschlussprüfungen in den Mitgliedstaaten der Europäischen Union (EU) gestärkt und harmonisiert werden.

Lösung zu Frage 11

Durch die in Basel II enthaltenen Bestimmungen soll eine **risikogerechtere** Eigenkapital-unterlegung von Markt-, Kredit- und operationellen-Risiken ermöglicht werden.

Mit Basel III sollen die Bankinstitute gezwungen werden, für Risikofälle zusätzliches und zwar nach vorgegebenen Regeln bezeichnetes Eigenkapital vorzuhalten, um den Risiken im vernetzten Finanzsystem infolge von Bank-Insolvenzen vorzubeugen.

Lösung zu Frage 12

Um einen sog. fortgeschrittenen (ambitionierten) Bemessungsansatz anwenden zu dürfen, müssen eine Reihe strenger qualitativer und quantitativer Mindestanforderungen (z.B. Verlustdatenbank mit Daten von drei Aufeinanderfolgenden Jahren) erfüllt werden, die gegenüber der nationalen Bankenaufsicht (D: BaFin; A: FMA, CH: FINMA) nachzuweisen sind. Mit den fortgeschrittenen (ambitionierten) Messansätzen soll das tatsächlich vorhandene Operationelle Risiko (zu dem auch das IT-Risiko gehört) adäquat gemessen werden können. In der Regel werden fortgeschrittene Bemessungsansätze lediglich von sehr grossen Banken eingesetzt (z.B. in der Schweiz durch CS und UBS).

Lösung zu Frage 13

Von Basel II sind auch die Kreditnehmer der Banken betroffen, da die Bonität resp. das Kreditrating des Kreditnehmers und damit die Höhe seiner Schuldzinsen aufgrund seiner Risiken zu beurteilen sind.