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

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 3

Lösung zu Frage 1

Bei der **Risiko-Analyse** wird die Wahrscheinlichkeit (resp. Häufigkeit) der Schadensereignisse analysiert und anhand dieser beiden Dimensionen das Risiko bestimmt. Die Risikobestimmung erfolgt mit für den Anwendungsfall geeigneten Methoden (z.B. Risikomatrix, Erwartungswert-, Value- at-Risk-Berechnungen.

Bei der **Impact-Analyse** wird lediglich das Schadenspotential bestimmt. Die Impact-Analyse ist dort sinnvoll, wo die Häufigkeiten eine untergeordnete Rolle spielen (z.B. bei grossen jedoch eher seltenen Schadensereignissen oder bei der Business-Continuity-Planung).

Bei der **Schwächen-Analyse** werden schwache Eigenschaften, Verletzlichkeiten oder für die im Bedrohungsumfeld fehlenden Massnahmen analysiert, aufgrund derer Schadensereignisse eintreten können. Bei der Schwächen- resp. Schwachstellen-Analyse werden anhand von vorab vorgefertigten Bedrohungslisten die bedrohten Objekte identifiziert.

Im Schwachstellen-Bewertungsprozess wird das zu analysierende Objekt auf das Vorhandensein notwendiger meist standardisierter Massnahmen zur Reduktion eines Risikos untersucht. Die Häufigkeit und Schwere von Ereignissen werden nicht berücksichtigt. Die Einschätzung einer Schwäche (Schwachstelle) wird aufgrund von allgemein möglichen Bedrohungen und Konsequenzen vorgenommen.

Für die Schwächen-Analyse (Schwachstellen-Analyse) können die gleichen Gruppierungen in Risiko-Arten wie bei der Risiko-Analyse verwendet werden.

Lösung zu Frage 2

Der Übergang von einer Bedrohung zu einem Schadenereignis kann durch ein Szenario beschrieben werden. Das Szenario ist somit sozusagen das Drehbuch nach dem ein Schadensereignis ablaufen könnte. Mit der Szenario-Analyse wird meist ein in die Zukunft prognostiziertes Ereignis mit Ursachen, Auswirkungen, Beeinflussungen und einem entsprechende Ablauf untermalt. Die Abläufe und kausalen Zusammenhänge werden meist durch Befragung von Experten und „Wenn-dann-Fragen“ herausgearbeitet. Die Szenarien ergeben Anhaltpunkte zur Einschätzung von Wahrscheinlichkeiten und Schäden sowie zur Berechnung statistischer Risikomasse, wie Erwartungswert, Value-at-Risk. Als meist von den Ursachen ausgehender Analyse gehört die Szenario-Analyse zu den Bottom-up-Analysen.

Lösung zu Frage 3

Hauptaufgaben:

- Kontext definieren,

- Risiko beurteilen in den Einzel-Schritten:
  - Risiko identifizieren,
  - Risiko analysieren und
  - Risiko bewerten
- Risiko bewältigen mit den Einzelschritten: Wahl einer Bewältigungsoption und Planung und Umsetzung der Bewältigungsmassnahmen.

Begleitende Nebenaufgaben:

- Risiko-Kommunikation und -Konsultation sowie
- Risiko-Überwachung und -Überprüfung.

Lösung zu Frage 4

Die **Begriffe „Bottom-up" und „Top-down"** werden in der Risikomanagement-Praxis unterschiedlich angewandt, z.B. für die Schwachstellen-Suche bei der Risikoidentifikation oder für das Vorgehen bei der Durchführung der Risiko-Analyse. Unter **„Bottom-up"** in der Risikoanalyse wird ein „induktives", von den Ursachen ausgehendes Vorgehen und unter **„Top-down"** ein „deduktives", von den Folgen ausgehendes Vorgehen verstanden. Diese Begriffe finden meist bei der Analyse des Gesamtrisikos aus Unternehmenssicht Anwendung, wobei beim Top-Down-Verfahren verschiedene Ergebniszahlen im Hinblick auf ihre Volatilität zur Ermittlung eines Gesamtrisikos untersucht werden; hingegen beim Bottom-up Verfahren die Risikokategorien, Geschäftsbereiche und Prozesse ursächlich erfasst, analysiert und die erfassten Einzelrisiken zu einem Gesamtrisiko aggregiert werden.

Im Rahmen der Unternehmensführung erfahren die Begriffe Top-down und Bottom-up eine oft unterschiedliche Verwendung (die sich manchmal auch in der Risikomanagement-Literatur wiederfindet), wobei beim Top-Down-Verfahren die obersten Führungskräfte die allgemeinen Geschäftsgrundsätze und Ziele formulieren aus denen dann die Teilplanungen und -aktivitäten für die einzelnen Unternehmensbereiche abgeleitet werden. Hingegen im Bottom-up-Verfahren die untergeordneten Unternehmensbereiche und Führungskräfte ihre Pläne und Aktivitäten an die übergeordneten Instanzen zur Konsolidierung und Erstellung der Gesamtplanung weiterreichen.

Lösung zu Frage 5

Unter dem Begriff „Risiko-Assessment" (Risiko-Beurteilung) werden alle Aufgaben der drei aufeinanderfolgenden Teilprozesse „Risiko-Identifikation", „Risiko-Analyse" und „Risiko-Bewertung" verstanden.

Als Ergebnis soll der Assessment-Prozess die Informationen darüber liefern, wo sich Risiken befinden, wie sie zu verstehen sind und wie mit ihnen aufgrund ihrer Höhe und Ausprägung hinsichtlich einer allfälligen Akzeptanz, umgegangen werden soll. Darüber hinaus soll das Risiko-Assessment den Input und die Entscheidungsgrundlagen für die risikogerechte Risiko-Behandlung liefern.

Lösung zu Frage 6

Die vier prinzipiellen Behandlungs-Optionen lauten:

- **Risiken vermeiden,** z.B. durch Aufgabe risikoreicher Aktivitäten
- **Risiken reduzieren,** durch Reduktion entweder der Eintritts-Wahrscheinlichkeit oder des Schadenausmasses
- **Risiken transferieren,** z.B. Überwälzung finanzieller Schäden auf Versicherungen
- **Risiken bewusst eingehen und tragen,** z.B. Tragen des Restrisikos, welches im Rahmen der betrieblichen Reserven und eines allfälligen Goodwill-Verlusts verkraftbar ist

Lösung zu Frage 7

Beispiele

Risiken vermeiden: Eine Bank meidet für die vertraulichen z.T. unter Bankgeheimnis stehenden Daten die Speicherung und Bearbeitung dieser Daten in einer „Public Cloud", da in der Cloud sowohl die Vertraulichkeit der Daten als auch die Compliance nicht sichergestellt werden kann.

Risiken reduzieren: Eine Bank reduziert die beim E-Banking vorgekommenen Betrugsattacken durch die Einführung eines Authentication-Verfahrens beruhend auf starker Kryptographie und „2-Faktor-Benutzerauthentisierung".

Risiken transferieren:

Ein Versicherungsunternehmen verfügt nicht über Räume und anderweitige Ressourcen, um die inzwischen anspruchsvolle Informatik risikoarm zu betreiben. Die Versicherung lagert deshalb den Betrieb ihrer Informatik an einen für solche Informatik-Leistungen prädestinierten Dienstleister aus.

Risiken bewusst eingehen und tragen:

Die Mitarbeiter eines staatlichen Verwaltungsbetriebs verfügen an ihrem Arbeitsplatz über den Zugriff auf das Internet und besitzen ein ihrer Person zugeteiltes E-Mail-Account. Trotz unterschriebener Geheimhaltungserklärung und häufigen Awareness-Aktionen kommt es in seltenen Fällen vor, dass als „vertraulich" klassifizierte Informationen an die Öffentlichkeit gelangen. Aufgrund der seltenen Vorkommnisse liegt jedoch das Risiko unterhalb der Akzeptanzschwelle und wird im Rahmen der Chancen-Abwägung der E-Mail- und Internet-Benutzung bewusst eingegangen und getragen. Doch bedarf das „bewusste" Eingehen eines Risikos oder „Restrisikos" auch der stetigen Aufsicht und Kontrolle.

Lösung zu Frage 8

„Überwachung und Überprüfung" behandeln zwei unterschiedliche Aspekte der Kontrolle. Dabei kümmert sich **die Überwachung (monitoring)** vorwiegend auf festgelegte Überwachungsaspekte, z.B. ob ein festgelegter Sicherheitsprozess überhaupt aussagekräftige Ergebnisse liefert und die Ergebnisse sich innerhalb vorgegebener Ziele und Limiten bewegen. Hingegen wird mit einer **Überprüfung (review)**, die entweder infolge eines

bestimmten Anlasses oder periodisch stattfindet, nicht nur die Funktionstüchtigkeit der Überwachung, sondern das gesamte Dispositiv und das Rahmenwerk des Managementsystem einschliesslich der gesetzten Ziele für die Sicherheit überprüft.

Sowohl die Überwachung als auch die Überprüfung dienen der Kontrolle in allen Schritten des Risikomanagement-Prozesses. Dabei muss berücksichtigt werden, dass die Akteure im Risikomanagement-Prozess ihre eigenen Handlungen nicht unbefangen selber kontrollieren können, sondern dass eine „Gewaltentrennung" bei Durchführung und Kontrolle oder wenigstens ein „Vieraugenprinzip" von Nöten ist.

Lösung zu Frage 9

„Kommunikation und Konsultation" behandelt generell die Kommunikation mit den Beteiligten und Betroffenen (z.B. Anspruchsgruppen), die wo möglichst bi-direktional erfolgen soll sowie die Konsultation zur Einholung von Rat, Hilfe und Expertise. Die Kommunikation soll dem Verständnis der Kommunikationspartner angepasst sein und sowohl deren Risiko-Wahrnehmung als auch deren Risikobewusstsein Rechnung tragen. Die Verständlichkeit kann mittels „stark strukturierten" Kommunikationsformen unterstützt werden. Wichtige Kommunikationsanforderungen und -voraussetzungen (z.B. für Normalbetrieb oder für Notfallsituationen)werden vorteilhaft in entsprechenden Kommunikationskonzepten ausgearbeitet und mit den Stakeholdern vereinbart. Dabei werden auch die verwendeten Begriffe und Definitionen bereits vor de Beginn des Risiko-Management-Prozesses festgelegt und kommuniziert.

Lösung zu Frage 10

a)

Der Risikomanagementprozess wird sinnvollerweise bei grösseren unternehmerischen Veränderungen gestartet, z.B. bei Fusionen, Reorganisationen, Personalabbau, Outsourcing-Vorhaben, Inbetriebnahme oder Veränderung von Produktions- und IT-Systemen.

b)

Der Risikomanagementprozess wird hand-in-hand mit anderen wichtigen periodischen Unternehmensprozessen, wie dem Strategieprozess oder dem Budgetprozess periodisch gestartet und durchgeführt.