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

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 2

Lösung zu Frage 1

$R = p_E \times S_E$

R: Risiko;

p_E: Wahrscheinlichkeit, dass ein Schadensereignis mit dem Schaden S_E eintritt;

S_E: Schadenshöhe des Schadensereignisses (Schadensausmass, Verlusthöhe)

Die Formel zeigt zwar rudimentär, dass das Risiko grösser wird, wenn entweder die Wahrscheinlichkeit (relative Häufigkeit) eines Schadensereignisses oder dessen Schadensausmass zunimmt. Doch gilt es zu bedenken, dass in der Realität mehrere Schadensereignisse in unterschiedlichen Zeitabständen mit meist unterschiedlichen Schadenshöhen zu berücksichtigen sind., wobei sowohl die „Schadenseintritte“ als auch die „Schadenshöhen“ statistisch verteilt eintreten, woraus sich eine kombinierte statistische Schadensverteilung ergibt. Die obige Formel nimmt jedoch keinen Bezug darauf, welche Kombination von Wahrscheinlichkeit und Schadenshöhe der statistischen Verteilung dem zu berechnenden Risiko zugrunde liegen soll.

Anm.: Im praktischen Umgang mit dieser Formel wird meist anstelle der Eintrittswahrscheinlichkeit p_E die Häufigkeit H_E des Schadeneintritts eingesetzt.

Lösung zu Frage 2

Risiko ist eine nach Wahrscheinlichkeit (Häufigkeit) und Konsequenz bewertete Bedrohung hinsichtlich der Abweichungen von erwarteten System-Zielen*. Das (Downside†-) Risiko betrachtet dabei stets die unerwünschten Abweichungen von den System-Zielen und deren Folgen.

Lösung zu Frage 3

* Unter **„System“** wird in diesem Zusammenhang ein allgemeines System verstanden, das beispielsweise ein ökonomisches, ein gesellschaftliches oder ein technisches System mit zielorientierten Werten sein kann.

† Die Risiko-Definition im «weiteren Sinne» betrachtet zusätzlich zum **«Downside-Risiko»** auch das **«Upside-Risiko»,** d.h. die erwünschten positiven Abweichungen von System-Zielen. An die Stelle von Bedrohungen treten dann die «Chancen».

$R_T = H_T$ x S

R_T: In der Zeitperiode T „erwarteter" Schaden (Risk Exposure);

HT: In der Zeitperiode T erwartete Anzahl der Ereigniseintritte (Rate of Occurence in T);

S: erwartete (durchschnittliche) Schadenshöhe der eintretenden Schadensereignisse (Single Loss Exposure).

Lösung zu Frage 4

Die oben angeführten „einfachen" Multiplikations-Formeln liefern bei grossen Schäden, die in der Regel eher selten, d.h. mit geringen und schlecht quantifizierbaren Wahrscheinlichkeiten (Häufigkeiten) im sog. Schwanz der Verteilung vorkommen, ein für das Unternehmen zu geringes und damit allenfalls „tragbares Risiko".

Vorsicht ist mit den einfachen Multiplikations-Formeln auch geboten, wenn grobe Schätzwerte für Häufigkeit und Schadenshöhe in die Formel eingesetzt werden. Eine mit solchen Werten vorgenommene Multiplikation erweckt zwar den Eindruck eines genauen rechnerischen Ergebnisses; ein genaues Ergebnis ist aber bei geringen Eintrittswahrscheinlichkeiten (-Häufigkeiten) überhaupt nicht möglich.

Lösung zu Frage 5

Zur Einstufung der Schäden können die zu betrachtenden Schadensarten wie folgt in sog. Impact-Kategorien eingeteilt werden:

- Direkter finanzieller Verlust (Barwert der Ersatzkosten + Opportunitäts-Kosten);
- Schädigung der geschäftlichen und wirtschaftlichen Interessen;
- Beeinträchtigung der Geschäfts- und Management-Vorgänge;
- Verlust an Reputation und Goodwill;
- Nichteinhaltung gesetzlicher und regulativer Verpflichtungen (mit z.T. persönlicher Haftung leitender Personen);
- Beeinträchtigung der Gesundheit, Sicherheit und des Schutzes anderer Personen.

Lösung zu Frage 6

Die kardinale Einschätzung und Berechnung (quantitative Analyse) des Risikos täuscht oft ein genaues Ergebnis vor. Auch trägt das rechnerische Ergebnis der tatsächlichen Wahrscheinlichkeitsverteilung sowie der „Risiko-Wahrnehmung" im Unternehmen bezüglich der Häufigkeiten und der Schadenshöhen oft ungenügend Rechnung. Um der Schadens- und Risiko-Wahrnehmung des Unternehmens besser gerecht zu werden, können stattdessen die Einstufungen und Bewertungen mit vorgefertigten Ordinalskalen (qualitativ) durchgeführt. Den Ordinalskalen (z.B. sehr gross, gross, mittel, klein) können sodann die für das

Unternehmen oder die zu analysierenden Objekte spezifischen meist monetären Werte zugeordnet werden. Die anhand solcher Skalen durchgeführten Analysen werden als „semi-quantitativ“ bezeichnet.

Lösung zu Frage 7

Die Risiko-Matrix (Abbildung 2.5 zeigt bei einem „katastrophalen Schaden“ eines seltenen Ereignisses ein „katastrophales Risiko“. Dasselbe Risiko wird auch bei einem „sehr seltenen“ Ereignis ausgewiesen. Der gleiche Risikowert bei verschiedenen Häufigkeiten ist darin begründet, dass das Risiko in beiden Fällen, unabhängig von der Häufigkeit, als „katastrophal“ wahrgenommen wird.

Ein „katastrophaler Schaden“ wird in demselben Unternehmen nicht „sehr oft“ vorkommen können. Deshalb ist die Bestimmung eines derartigen Risiko-Wertes eines mit grosser Häufigkeit eintretenden katastrophalen Schadens „irrelevant“ (s. Risiko-Matrix, Abbildung 2.5).

Lösung zu Frage 8

Die in einem Risiko-Katalog (Risiko-Register) enthaltenen Elemente sind durch den Anwendungszweck bestimmt:

Folgende Elemente sind meist enthalten:

- Risikoart oder Risikobezeichnung,
- bedrohte Gegenstände (Assets) resp. die bedrohten Objekte,
- Bedrohungen;
- Identifizierte Schwachstellen, die durch die angegebenen Bedrohungen ausgenutzt werden können und für das Zustandekommen der Risiken mitverantwortlich sind und Anhaltpunkte für den Einsatz von Massnahmen bieten.

Für jedes derart „identifizierte“ Risiko enthält der Katalog:

- die Resultate der Risiko-Analyse mit den Einschätzungen der Eintritts-Häufigkeit sowie der Schadenshöhe,
- die Resultate der Risikobewertung und der allenfalls bereits vorhandenen Massnahmen.

Lösung zu Frage 9

Das Risikoportfolio ist eine übersichtliche Zusammenstellung der Risiken meist in einer zweidimensionalen graphischen Darstellung mit den beiden Dimensionen Wahrscheinlichkeit (resp. Häufigkeit) und Schadensausmass. Diese Darstellung eignet sich zur Visualisierung der Risikohöhen und der Wirkungen von Massnahmen sowie allenfalls zum Aufzeigen von Risikoeinflüssen und -abhängigkeiten.

Lösung zu Frage 10

Mit der Akzeptanzlinie kann im Risikoportfolio visualisiert werden, welche Risiken unterhalb dieser Linie ohne besondere Massnahmen durch das Unternehmens-Management akzeptiert werden.

Lösung zu Frage 11

Pro darzustellendem Risiko die „Wahrscheinlichkeit“ (Häufigkeit) sowie das „Schadensausmass“.

Lösung zu Frage 12

Ordinate: Erwarteter Höchstschaden (VaR)

Abszisse: Erwartungswert

Lösung zu Frage 13

Die unerwarteten Verluste werden mit dem Value at Risk (VaR) zum Ausdruck gebracht, wobei sich die „unerwarteten Verluste“ aus dem Value at Risk abzüglich der „erwarteten Verluste“ (resultierend aus dem Erwartungswert) ergeben.

Das Risikomass VaR (V; α; T), ist wie folgt definiert:

> Der **„Value at Risk“** ist der maximal erwartete Verlust (Schaden) V, der unter üblichen Bedingungen innerhalb einer bestimmten Zeit-Periode T mit einer bestimmten Wahrscheinlichkeit α, dem sog. Konfidenz-Niveau, nicht überschritten wird.

Die katastrophalen Verluste befinden sich im sog. Schwanz der Verteilungsdichtefunktion jenseits des Value at Risk. Ein stochastisches Risiko-Mass zur Messung solcher katastrophalen Verluste ist beispielsweise der „Conditional Value at Risk“.

Lösung zu Frage 14

Die IT-Risiken gehören in die Kategorie der „Operationellen Risiken“.