

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

### Kontrollfragen und Aufgaben zu Kapitel 2

#### Lösung zu Frage 1

$$R = p_E * S_E$$

R: Risiko;  $p_E$ : Wahrscheinlichkeit, dass ein Schadensereignis mit dem Schaden  $S_E$  eintritt;  $S_E$ : Ausmass des Schadensereignisses (auch Tragweite oder Verlust).

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

#### Lösung zu Frage 2

Ein Risiko ist eine nach Häufigkeit (Eintrittserwartung) und Auswirkung bewertete Bedrohung eines zielorientierten Systems. Das Risiko betrachtet dabei stets die negative, unerwünschte und ungeplante Abweichung von Systemzielen und deren Folgen.

#### Lösung zu Frage 3

Impact-Kategorien:

- 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 regulatorischer Verpflichtungen (mit z.T. persönlicher Haftung leitender Personen);
- Beeinträchtigung der Gesundheit, Sicherheit und des Schutzes anderer Personen.

#### Lösung zu Frage 4

Die kardinale Berechnung und Bewertung des Risikos täuscht einerseits ein zu genaues Ergebnis vor und trägt andererseits der „Risiko-Wahrnehmung“ in einem Unternehmen zu wenig Rechnung. Um der Schadens- und Risiko-Wahrnehmung des Unternehmens gerecht zu werden, empfiehlt es sich stattdessen, die Bewertung mit vorgefertigten Ordinalskalen durchzuführen.

#### Lösung zu Frage 5

Die Risiko-Matrix (Abbildung 2.2) zeigt bei einem „katastrophalen Schaden“ eines „seltenen“ Ereignisses ein „katastrophales Risiko“. Dasselbe Risiko wird auch bei einem „sehr seltenen“ Ereignis ausgewiesen. Der gleichen 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 „oft“ vorkommen können. Deshalb ist die Bestimmung eines derartigen Risiko-Wertes „irrelevant“ (s. Risiko-Matrix, Abbildung 2.2).

#### Lösung zu Frage 6

Der Anwendungszweck des Risiko-Katalog ist für die darin enthaltenen Elemente massgebend.

Folgende Elemente sind meist enthalten:

- Risikoart,
- bedrohte Gegenstände resp. bedrohte Objekte,
- Bedrohungen.

Pro solchermaßen qualifiziertem Risiko enthält der Katalog:

- Einschätzung „Eintritts-Häufigkeit“ und „Verlusthöhe“,

- Risiko-Bewertung und allenfalls bereits vorhandenen Massnahmen.

Lösung zu Frage 7

Pro darzustellendem Risiko die „Häufigkeit“ sowie das „Schadensausmass“.