

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

Kontrollfragen und Aufgaben zu Kapitel 3

Lösung zu Frage 1

Bei der Risiko-Analyse wird die Wahrscheinlichkeit (resp. Häufigkeit) der Schadensereignisse sowie der Erwartungswert des Schadens analysiert und anhand dieser beiden Dimensionen das Risiko bestimmt.

Bei der Impact-Analyse wird lediglich das Schadenspotential bestimmt. Die Impact-Analyse ist dort sinnvoll, wo die Häufigkeiten eine untergeordnete Rolle spielen (z.B. für die grossen eher seltenen Schadensereignisse).

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 vorab anhand von 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 Konsequenzen vorgenommen.

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

Die Schwachstellen-Kataloge werden in ähnlicher Weise wie die Risiko-Kataloge angefertigt.

Lösung zu Frage 2

Hauptaufgaben:

- Kontextbestimmung
- Risiko-Identifikation
- Risiko-Einschätzung

- Risiko-Bewertung
- Risiko-Bewältigung mit Risiko-Strategien und Massnahmen-Umsetzung

Begleitende Aufgaben:

- Risiko-Kommunikation
- Risiko-Kontrolle und -Reporting
- Prozess-Initialisierung / -Wiederholung

Lösung zu Frage 3

1. Bildung von Risiko-Objekten und Abgrenzung des für die Risiko-Analyse relevanten Bereichs
2. Identifikation der für die Objekte massgeblichen Bedrohungen und Schwächen
3. Analyse der Bedrohungen auf die Objekte und Einschätzung der Häufigkeit H_E des Eintritts eines Schadens S_E
4. Einschätzung der vorraussichtlichen Schäden S_E
5. Bestimmung der Risiken eines Objekts

Lösung zu Frage 4

- Risiken vermeiden, z.B. durch Aufgabe risikoreicher Aktivitäten oder Verlagerung von Aktivitäten an Orte, wo das Risiko nicht auftritt.
- Risiken reduzieren, durch Reduktion entweder der Wahrscheinlichkeit oder des Schadensausmasses, z.B. durch Firewall oder Katastrophenorganisation. Reduziert werden die Risiken auch durch Diversifikation, z.B. durch regional voneinander getrennte Produktionsstätten oder Backup der Risiko-Objekte und Ressourcen.
- 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 ver-
kraftbar ist

Lösung zu Frage 5

Während allen Teilprozessen und Aktivitäten des Risiko-
Management-Prozesses ist es wichtig, den Prozess und auch die
Risiko-Situation bezüglich allfälliger Veränderungen zu überwa-
chen. Beim Reporting ist im Sinne einer neutralen Berichterstat-
tung die Unabhängigkeit gegenüber den Ausführenden durch
unabhängige Personen und/oder neutrale Aufzeichnungssysteme
erforderlich.

Lösung zu Frage 6

Ein gemeinsames Verständnis unter den Beteiligten eines Risiko-
Management-Prozesses ist von grosser Wichtigkeit. Sowohl die
direkt Beteiligten als auch die Betroffenen sind in jedem Teil-
Prozess auf einen entsprechenden Information-Austausch ange-
wiesen. Auch müssen unterschiedliche Fachpersonen und Exper-
ten ihre Informationen untereinander und den Entscheidungsträ-
gern austauschen. Deshalb empfiehlt es sich, stark strukturierte
Kommunikationsformen einzusetzen, z.B. Formulare oder formu-
largesteuerte Kommunikationssysteme. Die verwendeten Begriffe
und Definitionen müssen zum Beginn des Risiko-Management-
Prozesses festgelegt und kommuniziert werden.