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

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 11

Lösung zu Frage 1

Der jährlich verbleibende Schaden mit Massnahme wird mit 0.5 x 10‘000 € = 5‘000 € erwartet, somit ist E_a = 95‘000 €

Netto-Verlustreduktion = E_a — T_a = 95‘000 € — 50‘000 € = 45‘000 €

ROSI = (E_a — T_a) / T_a = (95‘000 € — 50‘000 €) / 50‘000 € = 0.9

Lösung zu Frage 2

Der jährlich verbleibende Schaden mit Massnahme wird mit 1 x 10‘000 € = 10‘000 € erwartet, somit ist E_a = 40‘000 €.

Netto-Verlustreduktion = E_a — T_a = 40‘000 €— 40‘000 € = 0 € und ebenfalls ROSI = 0. Würde heissen, die neue Massnahme sei nicht rentabel.

Lösung zu Frage 3

Sollten die Massnahmen-Entscheide aufgrund von ROSI-Berechnungen gefällt werden, dann wäre die Einführung der Massnahme in Aufgabe 1 ein guter Entscheid und könnte als gute Investition gewertet werden. Das ROSI-Ergebnis aus Aufgabe 2 hingegen würde zum Entscheid der Nichteinführung der Massnahme führen, da die Investition in die Massnahme ja keinen Gewinn (Return) aufweist.

Für beide Fälle gilt es zu beachten:

1. Dass das solchermassen „berechnete“ Risiko lediglich auf Zahlen der unmittelbaren Vergangenheit beruht. Dabei gilt es zu bedenken, dass die Risiken, insbesondere der Informationssicherheit, mit „unsicheren“ Wahrscheinlichkeiten in der Zukunft eintreten können.
2. Den zwar seltenen aber möglicherweise sehr hohen Schäden wird durch die „erwarteten“ Schäden einer ROSI-Berechnung, im Sinne einer den Risiken entsprechenden statistischen Verteilungsfunktion, nicht Rechnung getragen.
3. Eine angeblich gute Investition gemäss Aufgabe 1 kann sich als trügerisch erweisen und darf erst recht nicht als Gewinn gewertet werden, da die Berechnungen und Annahmen aus Gründen, wie die oben erwähnten, hohen Unsicherheiten unterliegen.

Im Gegensatz zum ROSI-Verfahren werden **im COBIT®-5 -Rahmenwerk und den zugehörigen Anleitungen (Guides), vor allem in „COBIT® 5 for Information Security" und „COBIT® 5 for Risk"** die Investitionsentscheide im Rahmen eines integrierten Vorgehens unter Verwendung einer Balanced Scorecard aus der Warte der Zielerfüllung und der Erfüllung von Anforderungen und Erwartungen der Anspruchsgruppen (Stakeholder) behandelt. So behandelt COBIT® 5 die Relation von Risiken und Chancen sowie der Aufwand und der Nutzen von Sicherheitsmassnahmen auf der geschäftliche Ebene des Werterhalts und der Wertegenerierung des Unternehmens. Die Ausrichtung des Informationssicherheits-Managements am internen und externen Unternehmenskontext und den Anforderungen der Anspruchsgruppen im ISMS ISO/IEC 27001:2013 entspricht dabei einer strategischen Betrachtungsweise. Auch begegnet der COBIT®-5-Ansatz der Schwierigkeit von absoluten quantitativen Kostenberechnungen, indem die Bewertungen auf qualitativen Kennzahlen (z. B. Key-Risk-Indikatoren und Performance-Indikatoren) beruhen. Selbstverständlich muss bei der Bestimmung der Massnahmen auch beim COBIT®-5 Ansatz auf die Verhältnismässigkeit der Massnahmen gegenüber den Risiken geachtet werden, dafür können geeignete Ziele und Indikatoren herangezogen werden.

In der Philosophie des COBIT®-5- Ansatzes wäre beispielsweise folgendes Vorgehen möglich:

1. **Im Rahmen der „Kontextbetrachtung"** sollten die Anforderungen und Ziele der Governance festgestellt und Aussagen getroffen werden, inwiefern das Unternehmen bei Verletzung von Sicherheitszielen (z.B. Vertraulichkeit oder Verfügbarkeit) in der Erfüllung der Unternehmensziele (u.a. Wahrnehmung von Chancen) beeinträchtigt wird.

2. **Beurteilung der Risiken (Risiko Assessment);** dazu werden die Risiken und Chancen identifiziert, analysiert, und u.a. in entsprechenden Geschäftsbegriffen ausgewiesen, dabei kann die Analyse und Bewertung der Risiken mittels „Key-Risk-Indikatoren" erfolgen.

   Zur Beurteilung der Risiken sollten die Anforderungen und Ziele der Governance auf die Ziele der IT heruntergebrochen und mit geeigneten, womöglich vorlaufenden Indikatoren (Metriken) die Zieleinhaltung gemessen werden.

3. **Behandlung der Risiken (Risiko Reaktion);** bei der Massnahmenzuordnung muss u.a. gewährleistet werden, dass die IT-bezogenen Risiko-Fragen in einer kostensensiblen Weise und in einer geschäftsrelevanten Prioritätenfolge behandelt werden und dabei den Anforderungen und Zielen der Governance gerecht werden.

Lösung zu Frage 4:

Die Kennzahlen (Indikatoren) können alleinstehend oder im Zusammenhang mit einem Ziel angewandt werden. Für das Risiko-Assessment werden oft mehrere Indikatoren zur Anzeige der unterschiedlichen für das Risiko verantwortlichen Faktoren parallel eingesetzt. Für die Auswahl von Indikatoren im Risiko-Assessment gilt allgemein:

- Sensitivität: Indikatoren müssen repräsentativ und zuverlässig hinsichtlich dem anzuzeigenden Risiko sein
- Impact: Indikatoren müssen vorwiegend Risiken mit hohen Geschäfts-Impact aufzeigen
- Messaufwand: Bevorzugung von einfach zu benutzenden Indikatoren
- Zuverlässigkeit: Indikatoren müssen möglichst genau das Risiko und möglichst gute Vorhersagen und Ergebnisse wiedergeben

Beispiele alleinstehender Kennzahlen (Indikatoren):

- Anzahl von Produktionsausfällen, die eine bestimmte Dauer überschreiten;
- Anzahl Schwachstellen in Abhängigkeit von einer in einer ordinalen Skala definierten Ernsthaftigkeit;
- Prozentsatz von Benutzern, die sich nicht an die vorgegebene Passwort-Policy halten (z.B. Benutzung trivialer Passwörter);
- Anzahl von vermuteten und aktuellen Verletzungen von Zugriffsrechten;
- Anzahl erfolgter Informationssicherheitsvorfälle mit Schadenfolgen.

Beispiele von Indikatoren (Metriken), die den Grad einer Ziel-Erreichung angeben®:

- Ziel: Maximaler Schutz gegen bekannte und unbekannte Bedrohungen der Informationssicherheit.

  Indikator (Metrik): Anzahl von Informationssicherheitsrelevanten Vorfällen.

- Ziel: Genaue und vollständige Identifikation der Schwachstellen mit denjenigen Bedrohungen, durch welche die Schwachstellen der Assets ausgenutzt werden können.

  Indikator (Metrik): Anzahl Schwachstellen, die gemäss eingehender Untersuchung oder gemäss eingetretener Vorfälle, noch nicht mittels Massnahmen angemessen behoben sind.

- Ziel: Sicherheit der Informationen, der Anwendungen und der IT-Infrastruktur.

  Indikator (Metrik): Anzahl von Informationssicherheitsrelevanten Vorfällen, die finanzielle Verluste, Geschäftsunterbrechungen oder öffentliche Schwierigkeiten hervorrufen.