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

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 15

Lösung zu Frage 1

Gründe aus Unternehmersicht für Outsourcing:

- Kostenreduktion (massive Kosteneinsparungen sind oft durch Verlagerung von IT-Dienstleistungen in Billiglohnländer möglich);
- Variabilisierung der Fixkosten durch Ausnutzung der Synergien des Outsourcers mit anderen Kunden und dadurch Möglichkeit eines mengenabhängigen Pricings;
- Verbesserung der Zuverlässigkeit und Innovation durch „kritische Masse“ des Outsourcers für neue technologische Trends und für Massnahmen zur Einhaltung aktueller Sicherheitsstandards;

Neue Kosten durch Outsourcing:

- Kosten und allfällige Schwierigkeiten bei Aufbau und Unterhalt eines „Demand Managements“ (z. B. durch Einsatz notwendiger Ansprechpartner auf der Auftraggeber-Seite);
- Transferkosten für die Eingliederung von IT-Technik und IT-Personal beim IT-Outsourcer;
- Erfüllung der IT-Sicherheits-Anforderungen und der neuen „Risiko-Kosten“, insbesondere bei der Auslagerung in Billiglohnländer.

Lösung zu Frage 2

Die Sicherheitsanliegen müssen möglichst früh in den Evaluationsprozess eingebracht werden und vollumfänglich bei den Vertragsverhandlungen berücksichtigt und bei der Vertragsunterzeichnung vereinbart werden. Nach Vertragsabschluss sind zusätzliche Sicherheitsanliegen, insbesondere, wenn sie dem Provider keinen Vorteil bringen, schwerlich umzusetzen.

Lösung zu Frage 3

Phase 1: Outsourcing-Strategie

Abklärung der Ziele, Absichten und Gründe für Outsourcing sowie Nutzen und Risiken.

Phase 2: Evaluation und Auswahl

Definition der Anforderungen und Suchen von Partnern, welche die Anforderungen erfüllen können.

Phase 3: Vertragsentwicklung

Strukturierung einer Partnerschaft mit definierten Service Levels und Zahlungs-Modellen; die Durchführung der Vertragsverhandlungen soll so schnell und sorgfältig wie möglich erfolgen.

Phase 4: Sourcing-Management

Betrieb des Outsourcings und Überwachung des Partnerschafts-Verhältnisses sowie effektive Reaktion bezüglich Veränderungen.

Lösung zu Frage 4

Ein IT-Sicherheitskonzept, das analog zu einem Risikomanagement-Prozess strukturiert wird, ist ein gutes Instrument, um Risiken und Massnahmen für Sourcing-Vorhaben in den einzelnen Sourcing Phasen systematisch zu analysieren und die Konsequenzen für Massnahmen abzusehen. (Das Erarbeiten und der Einsatz eines solchen IT-Sicherheitskonzepts ist im Buch beschrieben).

Lösung zu Frage 5

In der Evaluationsphase (Phase 2), d.h. der Phase, in der ein geeigneter Dienstleister gesucht wird, sollten wichtige Teile aus den Kapiteln 1 bis 4 des Sicherheitskonzept in den **„Request for Proposal" (RFP)** aufgenommen werden:

Kapitel	In RFP aufzunehmende Teile aus Sicherheitskonzept-Kapitel
1	Kontext, einschliesslich System- respektive Prozessbeschreibung;
2	Risiko-Identifikation;
3	Impact-Analyse, jedoch nicht die volle Risiko-Analyse, für die konkreten Fakten in dieser Phase noch nicht vorliegen;
4	Anforderungen an die Sicherheits-Massnahmen.

Lösung zu Frage 6

Sowohl aus der Sicht des auslagernden Unternehmens als auch des Dienstleister sollten folgende Themen der Informationssicherheit in die Vertragsausarbeitung einbezogen werden:

- Anforderungen an die Sicherheitsmassnahmen; diese sollten durch den Dienstleister und den Kunden im Kapitel 4 des endgültigen (betrieblichen) Sicherheitskonzepts gemeinsam definiert werden;
- Massnahmen-Beschreibung (Kapitel 5);

- Umsetzungs-Plan (Kapitel 6);
- Beschreibung der Umsetzung der Sicherheitsmassnahmen (Kapitel 6);
- Restrisiko-Betrachtung unter Beachtung der vereinbarten und umgesetzten Massnahmen; die Restrisiken können im Kapitel 3 des Sicherheitskonzepts zugefügt werden.

Lösung zu Frage 7

- Zum einen sollte auf der Auftraggeber-Seite wenigstens eine Person im Sinne eines Demand-Managements für die **Koordination und Überwachung mit entsprechendem Einsichtsrecht** definiert und eingerichtet sein.
- Zum anderen sollte im Vertrag das Revisionsrecht und Überprüfungsrecht eingeräumt sein; u.a. das Recht den Dienstleistungsbetrieb zu besuchen, Augenschein zu nehmen, Interviews durchzuführen, Einsicht in Dokumente und Konfigurationen zu nehmen und Sicherheitstests durchführen (z.B. Penetration Tests).

Lösung zu Frage 8

Um dem Wandel in der Risikolage gerecht zu werden, sollte der Outsourcing-Sicherheits-Prozess womöglich in einem PDCA-Zyklus betrieben werden. Eine periodische Kontrolle und die dadurch allenfalls notwendige Überarbeitung des Sicherheitskonzepts verhilft den PDCA-Zyklus zu schliessen. Für die Kontrolle ist in starkem Masse das unter Aufgabe 7 behandelte Revisionsrecht massgebend.

Auch der Betrieb des Sicherheitsmanagements im Rahmen eines ISMS mit zwangsläufigem Auditing unter Einbezug des Kunden, kann den Veränderungen der Risikolage angemessen Rechnung tragen.