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

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 7

Lösung zu Frage 1

Gemäss dem IT Governance Institut ist **IT-Governance** „die Verantwortlichkeit des Board of Directors* und des Executive Management†. Sie ist integraler Bestandteil der Corporate/Enterprise-Governance und besteht aus Führung, organisatorischen Strukturen und Prozessen, welche sicherstellen, dass die IT des Unternehmens die Unternehmens-Strategien und - Ziele aufrechterhält und ausbaut.“ [ITGI 2003a, S. 19].

Die **IT-Governance** betrifft vor allem zwei Verantwortlichkeiten:

- **Die IT muss Werte liefern** und das Geschäft ermöglichen sowie
- **IT-bezogenen Risiken** lindern (...) [ITGI 2005a, S. 167f].

Lösung zu Frage 2

- Sicherheitsanforderungen werden durch Unternehmens-Anforderungen getrieben
- Sicherheits-Lösungen sind auf die Unternehmens-Strategie zugeschnitten
- Investitionen in Informations-Sicherheit sind auf die Unternehmens-Strategie ausgerichtet und auf das Risiko-Profil abgestimmt
- Eine Auswahl an Standards über Sicherheits-Praktiken, z.B. Baseline Security gemäss „best practices“
- Priorisierte Anstrengungen auf denjenigen Bereichen zu-geteilt, wo sie am meisten bewirken und Geschäftsnutzen aufweisen
- Bewusste Risiko-Management-Prioritäten
- Mess-Prozess mit Feedback über die erzielten Fortschritte
- Unabhängige Kontrolle

* Verwaltungsrat in der Schweiz oder Aufsichtsrat in Deutschland

† Geschäftsleitung in der Schweiz und Vorstand in Deutschland

Lösung zu Frage 3

VR-Ebene:

- Einrichtung von „Ownership“ für Sicherheit und Kontinuität im Unternehmen.
- Einrichtung eines „Audit-Komitees“, welches seine Rolle betreffend Informations-Sicherheit und die Zusammenarbeit mit den Revisoren (Auditors) und dem Management klar versteht.
- Fordern, dass der Leiter IT-Sicherheit die Anliegen und den Fortschritt an das Audit-Komitee berichtet.
- Entwicklung von Krisen-Management-Praktiken, in welche das „Executive Management“ und das „Board of Directors“ von einer vereinbarten Eskalationsstufe an einbezogen werden.

GL-Ebene:

- Einrichtung einer Sicherheits-Funktion, welche das Management bei der Entwicklung von Policies und das Unternehmen bei deren Umsetzung unterstützt.
- Entwicklung von klaren Policies und detaillierten Richtlinien, unterstützt durch einen periodischen und erklärenden Kommunikations-Plan, mit dem alle Mitarbeiter erreicht werden können.
- Ständige Auswertung von „Vulnerabilities“ durch Überwachung von System-Schwachstellen (CERT), Intrusion- und Stress-Tests sowie Tests des Notfall-Plans.
- Einrichtung von robusten Geschäfts-Prozessen und Support-Infrastrukturen zur Vermeidung von Ausfällen, insbesondere aufgrund von „Single point of failures“.

Lösung zu Frage 4

- Gewaltentrennung durch unterschiedliche organisatorische Unterstellungen zwischen den die Informationssicherheit aus-führenden und den die Informationssicherheit kontrollierenden Instanzen.
- Benennung eines CISO mit einem direkten Berichtsweg zu den obersten Kontroll- und Führungsgremien. Der CISO sollte mit der notwendigen Bewegungsfreiheit und Unbefangenheit im Auftrag der obersten Kontroll- und Leitungsinstanzen die Informations-Sicherheit im Unternehmen durchsetzen und kontrollieren können.

Lösung zu Frage 5

Ein innerhalb der Linie einer IT-Organisation unterstellter CISO wird aufwendige unternehmensübergreifende Sicherheitsmassnahmen schwerlich durchsetzen können. Dieser Umstand lässt sich mit einer Principal/Agent-Situation zwischen dem für die

Unternehmens-Risiken verantwortlichen Top-Management und dem meist für kurzfristige Kosteneinsparungen belohnten Linien-Management erklären.

Lösung zu Frage 6

Während sich die **„IT-Governance“** vor allem auf die Umsetzung der geschäftlichen Anforderungen durch die Informationstechnologie bezieht, nimmt die **„Informations-sicherheits-Governance“** Bezug auf die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen, die sowohl in „Gefässen“ der Informationstechnologie (IT), als auch in nichttechnologischen „Erscheinungsformen“ existieren (z.B. Handnotizen auf Papier).

Lösung zu Frage 7

Der Governance Prozess besteht hauptsächlich aus den Teilprozessen (EDM):

- Beurteilen (Evaluate)
- Anweisen und Lenken (Direct)
- Überwachen (Monitor)

Dazu kommt der wichtige Teilprozess der Kommunikation (Communicate) mit den Anspruchsgruppen (s. ISO/IEC 27014:2013 und ISO/IEC 38500:2015).