

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

Kontrollfragen und Aufgaben zu Kapitel 8

Lösung zu Frage 1

Die allgemeine Risiko- und Sicherheitspolitik gibt die für das Unternehmen gültigen Sicherheits- und Risiko-Ziele sowie die dazu wichtigsten Grundsätze wieder. Die Ziele und Grundsätze beziehen sich auf die Unternehmens-Mission und Unternehmens-Ziele und bringen wichtige Werte und Haltungen (ggf. auch ethische Grundsätze) zu Risiken und zur Sicherheit des Unternehmens zum Ausdruck. Diese Politik ist übergeordnet und langfristig angelegt und ist damit ein Führungs-Instrument des „Normativen Managements“. Folgerichtig wird auch der Verwaltungsrat massgeblich den Inhalt bestimmen und die Politik genehmigen.

Lösung zu Frage 2

Die IT-Sicherheits-Architektur resultiert aus der für das Unternehmen typischen System-Situation. Sie beinhaltet u.a. die auf die allgemeinen Systemanforderungen abgestimmten Sicherheits-Dienste und –Mechanismen und ist somit der Bauplan für die standardisierte IT-Sicherheits-Infrastruktur im Unternehmen.

Lösung zu Frage 3

Das Sicherheitskonzept eines IT-Systems (Objekt) definiert die Massnahmen zur Bewältigung der für das betreffende IT-System (Objekt) massgeblichen Risiken. Die Weisungen hingegen definieren Massnahmen und Verhaltensweisen genereller Natur und bewirken somit einen „Grundschutz“ im Unternehmen mit dem die generellen und allenfalls typischen Risiken bewältigt werden können. Zur Bewältigung der am System (Objekt) spezifischen Risiken sind jedoch oft andere Massnahmen angezeigt, die unter geringerem Aufwand den Zweck besser erfüllen können. Somit ist es im Ausnahmefall oft sinnvoll, die durch Weisungen vorgeschriebenen Massnahmen mittels einer alternativen Massnahmenbestimmung im Rahmen des Sicherheitskonzepts übersteuern zu können.