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

## KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 9

**Lösung zu Frage 1**

Im Standard ISO/IEC 27001:2013 werden die Teilprozesse für das Risiko-Assessment und die Risiko-Behandlung im Kapitel 6 beschrieben, wobei die Beschreibung des Risiko-Assessments im Abschnitt 6.1.2 und die Beschreibung für die Risiko-Behandlung im Abschnitt 6.1.3 erfolgt.

**Lösung zu Frage 2**

**Das Kapitel 6** enthält die Vorgaben für die Entwicklung der Prozesse im Unternehmen zur Durchführung eines Informationssicherheits-Risikomanagements und erwartet neben den Prozess-Definitionen eine erste Ausführung der Teilprozesse „Risiko-Assessment“ und „Risiko-Behandlung“ mit aktuellen Fakten und einem durch den Risiko-Owner genehmigten Behandlungsplan unter gleichzeitiger Akzeptanz der voraussichtlichen Restrisiken.

**Das Kapitel 8** enthält die Vorgaben für das im Rahmen eines PDCA-Zyklus in geplanten Intervallen durchzuführenden Risiko-Management-Prozessen mit den Teilprozessen „Risiko-Assessment“ und „Risiko-Behandlung“ sowie die Umsetzung des jeweils erstellten Informationssicherheits-Risiken-Behandlungsplan (s. Abschn. 9.3.1).

**Lösung zu Frage 3**

Ist das Referenzdokument zur Auswahl von Massnahmen im Rahmen eines ISMS nach ISO/IEC 27001:2013. Die im Standard ISO/IEC 27002:2013in den Kapiteln 5 bis 18 aufgeführten Massnahmenziele und Massnahmen sind dem Standard ISO/IEC 27001:2013 als normativer Anhang (Annex A) angefügt.

Darüber hinaus bietet der Standard eine Anleitung bei der Umsetzung von allgemein akzeptierten Massnahmen zum Erreichen und Aufrechterhalten eines zielorientierten Informationssicherheitsniveaus im Unternehmen.

**Lösung zu Frage 4**

**Zu ISO/IEC 200000**

**ISO/IEC 20000–1:2011 (second edition): Service management – Part 1: Service management system requirements**

Der Teil 1 enthält die Muss-Anforderungen eines „Service-Management-Systems“ (SMS) zur Erlangung einer Zertifizierung durch ein sog. „Registered Certification Body“. Bei einer Zertifizierung wird gegen den normativen Teil ISO/IEC 20000-1:2011 geprüft. Ein erworbenes Zertifikat muss alle drei Jahre erneuert werden. Der Wert aus der Befolgung des Standards soll sowohl dem Kunden als auch dem Service-Provider zugutekommen. Der Standard zielt in seinen Anforderungen und Prozessen auf eine Integration der Planung und Implementierung sowie des Betriebs, der Überwachung und Überprüfung und der fortlaufenden Verbesserung des IT Service Management Systems (IT-SMS) ab. Dabei muss der PDCA-Zyklus berücksichtigt werden.

**Im Standard ISO/IEC 20000 werden die folgenden Anforderungen und Prozesse definiert:**

**[4] Service Management System (SMS) general requirements**

**[5] Design and Transition of new or changed Services**

- Planung und Implementierung des Service Managements
- Planen und Implementieren neuer oder geänderter Services

**[6] Service Delivery Processes**

- Service Level Management
- Capacity Management
- Availability und Service Continuity Management
- Information Security Management
- Service Reporting
- Finanzplanung und Kostenrechnung für IT-Services

**[7] Relationship Processes**

- Business Relationship Management
- Supplier Management

**[8] Resolution Processes**

- Incident Management and Service Request Management
- Problem Management

**[9] Control Processes**

- Configuration Management
- Change Management
- Release and Deployment Management

**ISO/IEC 20000–2:2012: Service management – Part 2 Guidance on the application of service management systems** (in ISO/IEC 20000:2005 wurde dieser Teil als "Code of Practice" bezeichnet)

Dieser 2. Teil zeigt anhand von Empfehlungen, wie die Anforderungen aus Teil 1 sinnvoll umgesetzt werden können.

**ISO/IEC 20000–3:2012: Service management – Part 3: Guidance on scope definition and applicability of ISO/IEC 20000–1.**

Dieser 3. Teil enthält hilfreiche Erläuterungen zu den Themen:

- Gültigkeitsbereich von Zertifizierungen;
- Anwendbarkeit des ISO/IEC 20000-Standards;
- Nachweis der Konformität.

Eine Reihe weiterer zum Standard gehörenden „Technischer Reports“ geben zusätzliche Hilfestellung bei der Umsetzung der Standard-Reihe.

**Zu ITIL®**

ITIL bietet „Best practice“ als De-facto-Standard für IT-Serviceprozesse und zeigt auf, was getan werden sollte, um Kunden mit adäquaten IT-Services zu bedienen. ITIL ist vor allem eine gut strukturierte Sammlung von besten Praxiserfahrungen über das IT-Service Management; Einzel-Personen können ITIL-Qualifizierungen erhalten, eine Zertifizierung von Organisationen nach ITIL® ist jedoch nicht gegeben.

ITIL® unterstützt eine prozessorientierte Strukturierung von Betreiber-Organisationen für IT- und Telekommunikations-Dienste unter Einbezug der Benutzer. Gegenüber früheren Versionen wurde mit der Version V3 die frühere Strukturierung in „Service Support“ und „Service Delivery“ durch die Strukturierung mit einem „Service Lifecycle“ abgelöst. Dieser besteht aus den hauptsächlichen Phasen:

- „Service Strategy“,
- „Service Design“,
- „Service Transition“,
- „Service Operation“ und
- „Continual Service Improvement“.

Die einzelnen Prozesse (z.B. Service Portfolio Management oder Availability Management) sind in diesen Service-Lifcycle eingebettet. Diese Struktur wurde auch in der aktuellen Edition 2011 beibehalten. Den Sicherheits-aspekten wird durch Prozesse wie „Availability Management“, „IT Service Continuity Management“, „Information Security Management“, umfassend Rechnung getragen (z. B. eigene Prozesse für „Access

Management“ und „Incident Management“). Beim Prozess „Information Security Management“ wird auf ein ISMS gemäss ISO/IEC 27001 hingewiesen. Für das Risikomanagement beispielsweise im „IT Service Continuity Management“ wird das Framework „Management of Risk“ M_o_R) der OGC angeführt.

**Vergleich und gegenseitige Beziehung von ISO2000 und ITIL®**

Personen können zwar ITIL®-Qualifikationen erhalten, aber Organisationen können für das Einrichten von ITIL®-Prozessen kein Zertifikat erhalten, da sie ledigliche „beste Praxiserfahrungen“, aber keine zertifizierbaren Anforderungen (Requirements) enthalten; eine Zertifizierung von Organisationen für den anforderungsgerechten Betrieb eines IT-Service-Managements ist lediglich anhand des Standards ISO/IEC 20000 möglich. ITIL® (besonders in der Version 3 und der nachfolgenden 2011 Edition) ist stark nach ISO/IEC 20000 ausgerichtet. Damit bildet die Umsetzung von ITIL® in einer Organisation eine sehr gute Ausgangsbasis für Aufbau und Betrieb von Prozessen, die Anforderungen des Standards ISO/IEC 20000 entsprechen. Somit ist die Einführung von ITIL® in einem Unternehmen eine gute Vorbereitung für eine spätere ISO/IEC-20000-Zertifizierung.

**Lösung zu Frage 5**

**Informationskriterien in CobiT® 4.1**

**Effektivität:** Es werden die für die Geschäftsprozesse relevanten und wichtigen Informationen in zeitgerechter, aktueller, fehlerfreier, konsistenter und verwendbarer Form geliefert.

**Effizienz:** Die Bereitstellung der Informationen erfolgt mit einer optimalen Verwendung von Ressourcen.

**Vertraulichkeit:** Die Informationen sind ausschliesslich dem durch den Besitzer autorisierten Personenkreis zugänglich.

**Integrität (und Authentizität):** Die Informationen werden lediglich in der vorgesehenen Weise erzeugt, verändert oder ergänzt und sind somit weder fehlerhaft, unvollständig noch verfälscht.

**Verfügbarkeit:** Die Informationen stehen dem Benutzer resp. dem Geschäftsprozess in der erforderlichen Weise (in vereinbarter Darstellung und Zeit) zur Verfügung. Dies betrifft ebenfalls die Sicherstellung der notwendigen Ressourcen und deren Kapazitäten.

**Zuverlässigkeit (Verlässlichkeit)**: Bereitstellung der geeigneten Informationen zur Geschäftsausübung und zur Wahrnehmung der geforderten gesetzlichen, regulativen und treuhänderischen Verantwortlichkeiten. (Ziel nicht zu verwechseln mit der im Verfügbarkeits-Ziel enthaltenen System-Zuverlässigkeit).

**Compliance:** Der Umgang mit Informationen und deren Verarbeitung erfolgt im Einklang mit den rechtlichen, regulativen und vertraglichen Erfordernissen, denen die Geschäfts- und IT-Prozesse unterliegen.

**Lösung zu Frage 6**

| Enabler Zielkategorie in COBIT® 5 | Zielkriterien für den Enabler „Information“ in COBIT® 5 | Informations-kriterium in CobiT® 4.1 |
|---|---|---|
| Intrinsische Qualität | Objektivität (Objectivity) | Effektivität sowie Zuverlässigkeit |
| | Glaubwürdigkeit (Believability) | Effizienz sowie Zuverlässigkeit |
| | Reputation (Reputation) | |
| | Genauigkeit (Accuracy) | Integrität |
| Kontextbezogene und darstellerische Qualität | Vollständigkeit (Completeness) | |
| | Relevanz (Relevancy) | Effektivität |
| | Geeignete Informationsmenge (Appropriate amount) | |
| | Interpretierbarkeit (Interpretability) | |
| | Verständlichkeit (Understandability) | |
| | Einfache Handhabung (Ease of manipulation) | Effizienz |
| | Aktualität (Currency) | Keine Angaben |
| | Präzise Darstellung (Concise repräsentation) | |
| | Konsistente Darstellung (Consistent representation) | |
| Zugänglich-keit / Sicherheit | Verfügbarkeit/Rechtzeitigkeit (Availability/Timeliness) | Verfügbarkeit |
| | Eingeschränkter Zugriff (Restricted Access) | Vertraulichkeit |
| Alle | Abhängig von den Anforderungen alle Ziele (All goals depending on requirements) | Compliance |

(vgl. [Cobf12], S. 63, 82)

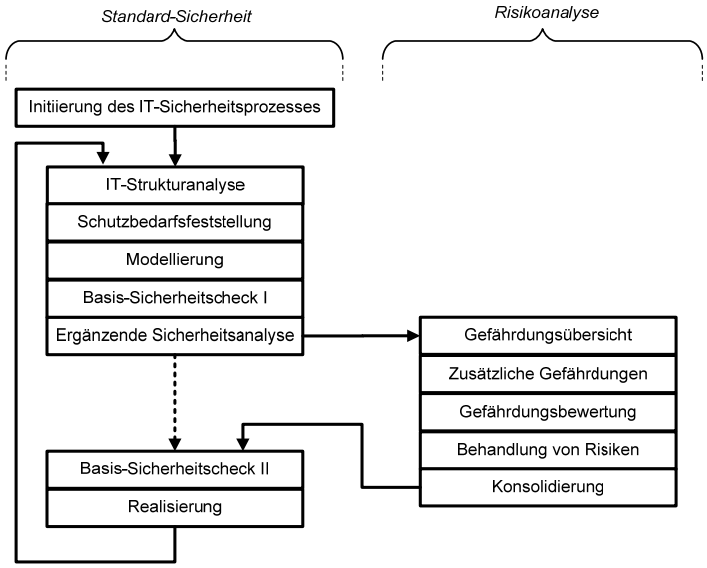
**Lösung zu Frage 7**

Die COBIT®-Prozesse und -Kontrollziele sind vor allem auf den IT-Governance-Bereich fokussiert. Der Bereich der Informationssicherheits-Governance wird im Rahmen von Informationstechnologien (IT) angesprochen. Ausserhalb der Informationstechnologie vorkommende Informations-Repräsentationen (z.B. handschriftliche Aufzeichnungen auf Papier) werden in den COBIT®-Rahmenwerken nicht explizit berücksichtigt.

**Lösung zu Frage 8**

Im BSI-Standard 100-3 wird die Risikobeurteilung (Risikoanalyse) gemäss untenstehender Figur in den Sicherheitsprozess integriert. Im Sicherheitsprozess findet bereits vorgängig zu einer Risikoanalyse eine Schutzbedarf-Feststellung statt, dies in den Stufen „normal“, „hoch“, und „sehr hoch“ hinsichtlich „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“. Die in der untenstehenden Abbildung gezeigte zusätzlich durchgeführte „Risikoanalyse“ berücksichtigt zum einen den vorgängig ermittelten Schutzbedarf sowie die für das jeweilige Zielobjekt relevanten „Gefährdungen“.

In der derzeit laufenden Überarbeitung des Standards Standard 100-3 sollen zur Risikobeurteilung die in den Gefährdungen implizit berücksichtigten Eintrittswahrscheinlichkeiten durch explizit eingeschätzte Eintrittswahrscheinlichkeiten (Eintrittshäufigkeiten) sowie explizit eingeschätzte Schadensauswirkungen herangezogen werden*.




BSI [Bsir08]

* Community Draft: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BSI_Standard_200-3.pdf?__blob=publicationFile&v=2, abgerufen am 2.5.2017

**Lösung zu Frage 9**

- Auswahl und Einführung von Standard-Regelwerken bedürfen vorgängiger
- Abklärungen der Anforderungen, Möglichkeiten, Ziele und Risiken;
- Gegenüberstellung von Aufwand und Nutzen vorteilhaft in der Form eines „Business Case“; Business Case soll die Grundlage für ein projektmässiges Einführen und die spätere Nutzen-Kontrolle darstellen.
- Einbindung „Top Management“ bei der projektmässigen Einführung als auch im weiteren Projektverlauf und späteren Betrieb mit entsprechenden Aktivitäten und Verpflichtungserklärungen.
- Durchführen Pilotprojekt in einem engen aber repräsentativen Anwendungsbereich erlaubt eine Lernphase zur Durchführung von Korrekturen bei der späteren Ausbreitung des Regelwerks auf das gesamte Unternehmen.

**Lösung zu Frage 10**

Die „Enabler“ sind Faktoren, die einzeln und im Verbund bewirken, dass die Forderungen und Ansprüche der Anspruchsgruppen (Stakeholder) an das Unternehmen erfüllt werden. So sorgen sie u. a. auch dafür, dass die Ziele in der Zielkaskade erfüllt werden. Anschaulich ausgedrückt, sind die Enablers die „Stellschrauben“, an denen gedreht wird, um die Ziele der an das Unternehmen gestellten Anforderungen der Anspruchsgruppen zu erfüllen.

COBIT® 5 unterscheidet die folgenden **Enabler Kategorien**:

1. Prinzipien, Policies und Rahmenwerke (Principles, Policies and Frameworks)
2. Prozesse (Processes)
3. Organisatorische Strukturen (Organisational Structures)
4. Kultur, Ethik und Verhalten (Culture, Ethics and Behaviour)
5. Informationen (Information)
6. Dienstleistungen, Infrastruktur und Anwendungen (Services, Infrastructure and Applications)
7. Mitarbeiter, Fähigkeiten und Kompetenzen (People, Skills and Competencies)

Jeder Enabler wirkt in den folgenden **vier Dimensionen**:

**Anspruchsgruppen**

Z. B. Parteien die an der Ausführung von Prozessen beteiligt sind oder Interesse an den Prozessergebnissen haben.

**Ziele**

Die Ziele können aufgrund ihres Einsatzbereiches in die folgenden Kategorienunterteilt werden:

- o Intrinsische Qualität,
- o Kontextbezogene und repräsentative Qualität und
- o Sicherheit und Zugänglichkeit;

**Lebenszyklus**

Jeder „Enabler“ hat einen Lebenszyklus mit den Phasen: Planen (Plan), Konzipieren(Design), Aufbauen/Beschaffen, (Build/Acquire), Benützen/Betreiben (Use/Operate), Überwachen Monitor), Beseitigen (Dispose).

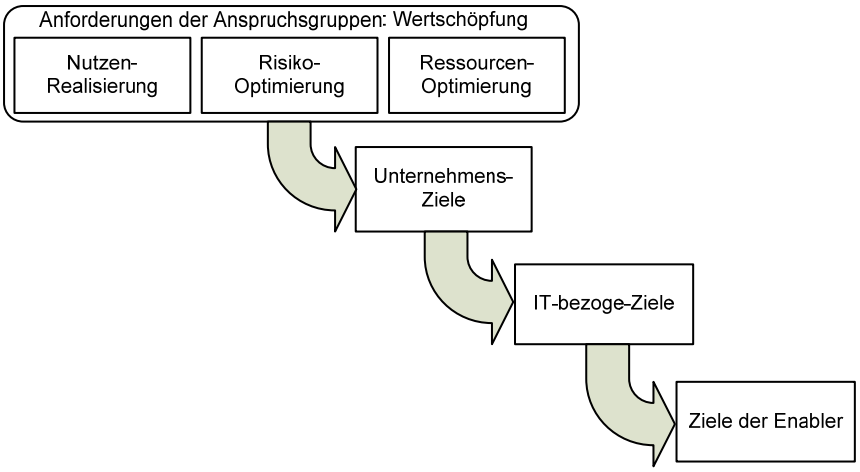
**Gute Praktiken**

Die Guten Praktiken helfen die Enabler umzusetzen und unterstützen die Erreichung der Enabler-Ziele.

**Lösung zu Frage 11**

**Ziele und Zielkaskade in COBIT® 5**

Die Integration von „Governance“ und „Management“ erfolgt einerseits über die Vernetzung der verschiedenen „Prozesspraktiken“ und „Enablers“ untereinander und andererseits über ein Zielsystem. Dieses Zielsystem wird mittels einer „Zielkaskade“ gebildet. Bei dieser Zielkaskade werden die Ziele, ausgehend von den „Anforderungen der Anspruchsgruppen an die Governance“ hinunter auf die Ebene der „Unternehmensziele“ und von dort auf die Ebene der „IT-bezogenen Ziele“ und von dieser Ebene letztlich auf die Ebene der sog. „Enabler-Ziele“ heruntergebrochen und umgesetzt. Die in die Enabler-Kategorie „Prozesse“ gehörenden 32 Prozesse haben auf den Ebenen dieser Zielkaskade entsprechende Ziele zu erfüllen.




So haben beispielsweise die in die Enabler-Kategorie „Prozesse“ gehörenden 32 Prozesse auf den einzelnen Ebenen dieser Zielkaskade entsprechende Ziele zu erfüllen.

**Generische Ziele in COBIT® 5**

COBIT 5 definiert sowohl auf der Ebene der „Unternehmensziele“ als auch auf der Ebene der „IT-bezogenen Ziele“ jeweils 17 generische Ziele sowie deren Beschreibungen zur Erfüllung von Anforderungen. Diese jeweils 17 generischen Ziele sind in die vier Perspektiven einer Balanced Scorecard eingeordnet, wobei die Ziele auf der Ebene der „Unternehmensziele“ hauptsächlich die für die Anspruchsgruppen zu erfüllenden Anforderungen hinsichtlich „Nutzen-Realisierung“, „Risiko-Optimierung“ und „Ressourcen Optimierung“ unterstützen sollen.