Eine Veröffentlichung des ISACA Germany Chapter e.V.

ISACA-Leitfaden

IT-Risikomanagement – leicht gemacht mit COBIT

ISACA®
Trust in, and value from, information systems
Germany Chapter

dpunkt.verlag

Herausgeber:
ISACA Germany Chapter e.V.
Im Birkenfeld 1a
65779 Kelkheim
E-Mail: webmaster@isaca.de
www.isaca.de

Redaktion: Dr. Paul Lokuciejewski
Verantwortliches Gremium: ISACA Germany Chapter
Fachgruppe: IT-Risikomanagement mit COBIT
Lektorat: Vanessa Wittmer
Copy-Editing: Annette Schwarz, Ditzingen
Satz & Herstellung: Frank Heidt
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck & Bindung: Wörmann PRODUCTION CONSULT, Heidelberg

ISACA-Leitfaden IT-Risikomanagement – leicht gemacht mit COBIT

Inhaltsverzeichnis

1 Vorwort

Risiken gibt es seit jeher. Im sechzehnten und siebzehnten Jahrhundert hat der Begriff durch die Seefahrt wesentlich an Bedeutung gewonnen. Ursprung waren die westlichen Forschungsreisen, die dazu dienten, die »neue Welt« zu erkunden. Die Seefahrernationen Spanien und Portugal prägten zu dieser Zeit das Wort »risco«, was so viel wie »Klippe« bedeutet. Sie bezeichneten damit eine Schifffahrt in unbekanntes, also nicht kartografiertes Gewässer. Man kann daher den Ursprung von »Risiken« von diesem räumlichen Phänomen ableiten.

Sehr schnell nahmen sich die Banken des Begriffes an, da dieser über Investitionsentscheidungsszenarien auf ein lukratives Geschäft mit unbekanntem Ausgang prognostizieren lässt. Versicherungen wiederum arbeiten mit dem Begriff »Risiko« im Kontext eines Ausfalls und der diesbezüglichen Eintrittswahrscheinlichkeit. Gleichwohl darf der Begriff nicht nur negativ gesehen werden, zumal »eine positive Einstellung zum Risiko die eigentliche Quelle ist, die in einer modernen Wirtschaft Wohlstand produziert« [1].

Der Begriff »Risiko« gewinnt auch in der heutigen Unternehmenswelt aufgrund der immer stärkeren Abhängigkeit von der Informationstechnologie (IT) an Bedeutung. Da sich nahezu alle optimierten Geschäftsprozesse auf Informationstechnologie stützen, rückt der sichere IT-Betrieb in den Fokus. Eine Kompromittierung der Informationssicherheitsgrundwerte Verfügbarkeit, Vertraulichkeit und Integrität und die damit einhergehende Eintrittswahrscheinlichkeit und Schadenshöhe schlägt unmittelbar auf IT-gestützte Prozesse durch. Der in diesem Zusammenhang genutzte Begriff des »Informationssicherheitsrisikos« findet sich in weit verbreiteten Werken, wie z. B. COBIT 4.1 (2007) oder der Norm ISO/IEC 27005 (2008) [2, 3].

Die Existenzabhängigkeit eines Unternehmens von der IT spiegelt sich ebenfalls verstärkt in den steigenden gesetzlichen und aufsichtsrechtlichen Anforderungen an das Management von IT-Risiken wider. Beispiele für solche gesetzlichen Regelungen sind »Basel II« mit der neuen Risikokategorie »operationelle Risiken« – zu der auch IT-Risiken zählen – oder die Konkretisierung des Kreditwesengesetzes durch die »Mindestanforderungen an das Risikomanagement« (MaRisk). Die Entwicklung der Anforderungen zeigt dabei auch, dass ein Wandel vom reaktiven zum proaktiven Risikomanagement stattfindet, da verstärkt ein Risikomanagementprozess mit Frühwarnsystemen gefordert wird [4].

2 Zusammenfassung

Der Begriff IT-Risiko leitet sich von der weit verbreiteten Definition des Risikos im Unternehmensumfeld ab [2, 3]:

Risiko ist das Potenzial, dass eine bestimmte Bedrohung eine Schwachstelle des organisationseigenen Wertes (Assets) oder einer Gruppe von Werten ausnutzt und dadurch einen Schaden in der Organisation verursacht.

Dabei wird das Risiko über die Kombination aus dem (negativen) Einfluss auf das Asset und der Eintrittswahrscheinlichkeit der Bedrohung bewertet. Basierend auf dieser Definition werden IT-Risiken wie folgt definiert [5]:

Ein IT-Risiko ist ein Geschäftsrisiko, das primär mit der Verwendung, dem Besitz, der Einbindung, dem Einfluss und der Adaptierung der IT innerhalb des Unternehmens verbunden ist.

Das IT-Risikomanagement wird in gängigen Normen, Standards und Best-Practice-Frameworks als ein zyklischer Prozess beschrieben, der mindestens die Phasen Identifizierung und Bewertung von IT-Risiken, deren Behandlung (Steuerung) über angemessene Maßnahmen sowie die Verfolgung (Tracking) der Umsetzung der Maßnahmen besteht (siehe Abbildung 1).

Für die Ausgestaltung und Durchführung dieses Prozesses gibt es aber sowohl in den regulatorischen Anforderungen (wie z. B. MaRisk) als auch in gängigen Standards und Best-Practice-Frameworks bisher nur unzureichende praxisorientierte Informationen. Dies hat z. B. zur Folge, dass die Vollständigkeit der im Rahmen der Risikoinventur identifizierten Schwachstellen nicht gewährleistet werden kann, so dass relevante IT-Risiken übersehen werden und im Fall ihres Eintritts das Unternehmen auf-

grund fehlender Maßnahmen zur Risikobehandlung einen Schaden erleidet.

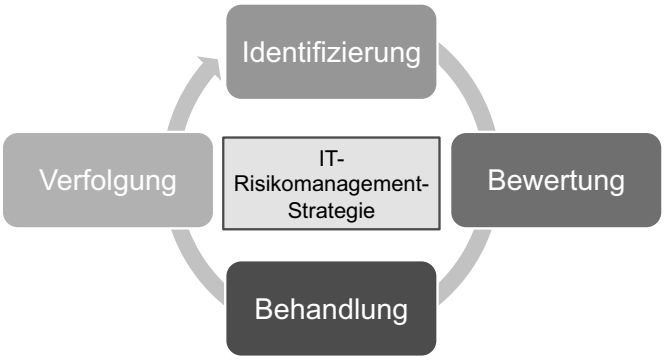


Abb. 1 *Der IT-Risikomanagementprozess [4]*

An dieser Stelle setzt die Arbeit der ISACA-Fachgruppe »IT-Risikomanagement mit COBIT« an. Da COBIT 4.1 [2] als IT-Framework alle relevanten Steuerungsbereiche abdeckt, wurden systematisch Informationen wie IT-Risiken oder deren Bezug zu Unternehmenszielen aus COBIT abgeleitet. Auf dieser Basis wurde der vorliegende Praxisleitfaden entwickelt, der als Ergänzung zu aufsichtsrechtlichen Regularien sowie gängigen Standards und Frameworks die notwendigen Informationen für die inhaltliche Ausgestaltung eines IT-Risikomanagements bietet.

Der Leitfaden besteht aus einer Liste von generischen Schwachstellen, die systematisch aus COBIT abgeleitet wurden. Die Schwachstellen können sowohl zur Überprüfung der Vollständigkeit des in einem Unternehmen bereits etablierten Risikoportfolios als auch bei dem Neuaufbau eines IT-Risikomanagements zur Definition von unternehmensspezifischen Risikoszenarien genutzt werden.

Der Leitfaden ist wie folgt strukturiert: Nach einem Abkürzungsverzeichnis in Kapitel 3 erläutert Kapitel 4 die Motivation und die Ziele der ISACA-Fachgruppe »IT-Risikomanagement mit COBIT«: die Erstellung eines Leitfadens, der eine Vielzahl wichtiger Praxisfragen zum Thema IT-Risikomanagement beantwortet. Ferner wird die Vorgehensweise der Fachgruppe, die zur Erstellung dieses Risikomanagement-Leitfadens auf Basis von COBIT gewählt wurde, beschrieben. Kapitel 5 stellt die daraus resultierenden Ergebnisse dar und zeigt, welche Bereiche aus COBIT für die Ableitung von Informationen für die einzelnen Phasen eines IT-Risikomanagements genutzt wurden. Kapitel 6 präsentiert ausgewählte Beispiele für die abgeleiteten Informationen aus COBIT, um dem Leser ein konkretes Bild für den praktischen Einsatz des Leitfadens zu vermitteln. Kapitel Vollständige Darstellung aller Schwachstellen, Indikatoren zur Risikobewertung und Risikobehandlungsmaßnahmen beinhaltet eine vollständige Darstellung aller Ergebnisse der Fachgruppe in Form eines generischen IT-Risikokatalogs, die eine Ausgestaltung de IT-Risikomanagements unterstützend begleiten können. Der Leitfaden schließt mit einer Danksagung sowie einem Abbildungs- und Quellenverzeichnis in den Kapiteln 8 bis 10 ab.

3 Abkürzungsverzeichnis

Abkürzung	Langform
AP	**A**rbeits**p**aket
AI	COBIT-Domäne »**A**cquire and **I**mplement«
CO	**C**ontrol Objective
COBIT	**C**ontrol **Ob**jectives for **I**T and related **T**echnology
DS	COBIT-Domäne »**D**eliver and **S**upport«
ISACA	The **I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation
ISMS	**I**nformations**s**icherheits-**M**anagement**s**ystem
ISO	**I**nternational **O**rganization for **S**tandardization
IT	**I**nformations**t**echnologie
IT-KGI	**IT K**ey **G**oal **I**ndicator
KGI	**K**ey **G**oal **I**ndicator
KPI	**K**ey **P**erformance **I**ndicator
MaRisk	**M**indest**a**nforderungen an das **Ris**i**k**omanagement
ME	COBIT-Domäne »**M**onitor and **E**valuate«
ONR	**Ö**sterreichisches **Nor**mungsinstitut
PO	COBIT-Domäne »**P**lan and **O**rganise«
RiskIT	The **Risk IT** Framework

4 Ziele und Vorgehensweise der Fachgruppe

Die Ausgangsbasis für die Arbeit der Fachgruppe war eine Zusammenstellung von Fragen, die sich in der Praxis bei der Ausgestaltung eines IT-Risikomanagements stellen und auf die Antworten gefunden werden sollten. Im Wesentlichen ergaben sich folgende Fragestellungen:

- Wie kann eine möglichst vollständige Liste von Risikofeldern (sog. Risikokatalog) definiert werden, damit im Rahmen einer regelmäßigen Risikoinventur keine wesentlichen Risiken übersehen werden?
- Welche Kennziffern können zur Messung von Schwachstellen verwendet werden, welche Kennziffern können die Implementierung eines Frühwarnsystems unterstützen?
- Wie können Auswirkungen von IT-Risiken insbesondere gegenüber dem IT-Management und dem Business dargestellt werden, um den Wertbeitrag des IT-Risikomanagements zu betonen?
- Wie können geeignete Maßnahmen zur Risikobehandlung identifiziert werden?

Daraus abgeleitet wurde das Ziel der Fachgruppe definiert: Erarbeitung von Hilfsmitteln für die obigen Praxisfragen, die der relevanten Zielgruppe – IT-Verantwortliche, Risikomanager, aber auch Linienverantwortliche – in Form eines praktischen Leitfadens zur Verfügung gestellt werden können. Hierzu hat die Fachgruppe eine Vorgehensweise entwickelt, die im Folgenden skizziert wird.

Zu Beginn der Arbeiten der Fachgruppe wurde eine Grobanalyse von COBIT durchgeführt, anhand derer bestimmt werden sollte, ob bzw. wie aus diesem Standard Informationen abgeleitet werden können, die zur Beantwortung der Fragestellungen und zur Erstellung des geplanten Leitfadens genutzt werden können. Parallel dazu wurden andere einschlägige Standards zum IT-Risikomanagement (wie ISO/IEC 27005, ONR 49000, Risk-IT etc.) analysiert, um herauszufinden, ob in diesen Antworten auf die genannten Fragestellungen enthalten sind, die eine Erarbeitung eines Leitfadens überflüssig machen.

Obwohl die analysierten Standards gute Ansätze für die methodische Ausgestaltung eines IT-Risikomanagements enthalten, liefern sie nur wenige Praxishilfen für die

Beantwortung der genannten Fragestellungen. Insbesondere waren in keinem der Standards umfassende Informationen zur Erstellung einer »vollständigen Risikoliste« enthalten.

Die Grobanalyse hat jedoch gezeigt, dass COBIT als umfassendes Framework für IT-Prozesse mit den enthaltenen Kontrollzielen (sog. Control Objectives, kurz COs) das größte Potenzial für die Ableitung einer solchen Risikoliste bietet, da es als Standard für IT-Governance alle relevanten IT-Steuerungsbereiche und IT-Normen abdeckt und implizit alle risikobehafteten Bereiche der IT adressiert. Darüber hinaus stellt COBIT auch für die weiteren Fragestellungen eine Vielzahl weiterer Informationen, wie z. B. Key Performance Indicators (KPIs) und Key Goal Indicators (KGIs), zur Messung von Aktivitäten, Prozessen und Zielen zur Verfügung, die für die Ausgestaltung eines IT-Risikomanagements sinnvoll sein können.

5 Ergebnisse der Fachgruppe

Aufgrund des Ergebnisses der Grobanalyse wurde eine systematische Detailanalyse von COBIT durchgeführt. Die Detailanalyse hat ergeben, dass mit den Informationen aus COBIT wertvolle Hinweise zur inhaltlichen Ausgestaltung eines IT-Risikomanagements erarbeitet werden können. Die Ausarbeitung dieser wesentlichen Ergebnisse wurde in Arbeitspaketen (APs) durchgeführt, die im Folgenden dargestellt werden:

- **AP 1: Ableitung der IT-Schwachstellen aus den Kontrollzielen**
  COBIT setzt voraus, dass IT-Prozesse aktiv gemanagt werden müssen, um die Geschäftsziele zu erreichen. Im Umkehrschluss heißt das, dass fehlende oder schlechte gemanagte IT-Prozesse die Geschäftsziele gefährden und somit eine Schwachstelle darstellen. Basierend auf dieser Annahme wurden alle Kontrollziele konsequent analysiert, und im Arbeitspaket 1 wurde eine Liste mit 215 Schwachstellen abgeleitet.
- **AP 2: Identifikation von Risikoindikatoren aus KPIs und KGIs**
  Je identifizierter Schwachstelle wurden die KGIs, KPIs und IT-KGIs des entsprechenden Prozesses analysiert, ob sie als Risikoindikator zur Früherkennung einer Veränderung des Risikos eingesetzt werden können. Geeignete Indikatoren wurden, wenn möglich, direkt einer Schwachstelle zugeordnet. Teilweise waren Indikatoren auf einem höheren Abstraktionsniveau als die Schwachstellen definiert – diese wurden den Schwachstellen indirekt auf Prozessebene zugeordnet. Diese im Leitfaden gesammelten Indikatoren können die Bewertung von Risiken, wie z. B. hinsichtlich ihrer Auswirkung, unterstützen.
- **AP 3: Ableitung von Risikobehandlungsmaßnahmen**
  Durch die inhaltliche Analyse der Anforderungen aus den Kontrollzielen sowie unter Einbeziehung der Stufen des Reifegrad-Modells von jedem COBIT-Prozess konnten die wichtigsten Maßnahmen für eine systematische Behandlung von identifizierten Schwachstellen extrahiert werden.
- **AP 4: Ableitung von Risikoauswirkungen auf IT- bzw. Geschäftsziele**
  Die Methodik der in COBIT hinterlegten Mapping-Tabellen zwischen IT-Prozessen und IT-Zielen sowie zwischen IT-Zielen und Geschäftszielen wurde genutzt, um die Auswirkungen von identifizierten IT-Risiken auf Geschäftsziele darstellen zu können. Dadurch bietet der Leitfaden eine transparente Darstellung für die Abhängigkeiten zwischen IT und Business.

6 Beispiele für die Ableitung von Informationen aus COBIT

Im Nachfolgenden werden die Ergebnisse dieser Arbeitspakete detailliert erläutert, und ihre praktische Verwendung zur Ausgestaltung eines IT-Risikomanagements wird durch praktische Beispiele illustriert. Eine vollständige Übersicht aller Ergebnisse ist in Kapitel 7 »Vollständige Darstellung aller Schwachstellen, Indikatoren zur Risikobewertung und Risikobehandlungsmaßnahmen« zu finden.

6.1 Ableitung der IT-Schwachstellen aus den Kontrollzielen (AP1)

Die Möglichkeit, aus COBIT Schwachstellen ableiten zu können, ergibt sich aus dem Aufbau bzw. den Kerneigenschaften von COBIT. Zwei dieser Eigenschaften sind:

- die Fokussierung auf das Geschäft (Business-focused) und
- die Orientierung an Prozessen (Process-oriented).

COBIT setzt voraus, dass Geschäftsziele nur angemessen erreicht werden können, wenn die Kontrollziele (Control Objectives) der entsprechenden IT-Prozesse ordentlich gemanagt werden. Dies bedeutet, dass nicht umgesetzte Kontrollziele Schwachstellen aus dem Bereich der IT darstellen, deren Ausnutzung durch eine Bedrohung potenziell negative Auswirkungen auf die Geschäftsziele zur Folge haben kann. Basierend auf dieser Methodik wurden 222 generische Schwachstellen aus den COs abgeleitet und in dem Leitfaden konsolidiert.

Tabelle 1 zeigt exemplarisch für jeweils ein CO aus einer der vier COBIT-Domänen eine abgeleitete Schwachstelle.

Im Folgenden wird am Prozess PO7 das weitere Vorgehen beispielhaft dargestellt.

Prozess	Schwachstelle Ableitung aus COs	Control Objective
PO7 – Manage die Humanressourcen	Fehlender oder unzureichender IT-Personaleinstellungsprozess, um Mitarbeiter einzustellen, die Fähigkeiten zur Unternehmenszielerreichung besitzen.	PO7.1
AI2 – Beschaffe und warte Anwendungssoftware	Fehlende oder unzureichende Konfigurations- und Implementierungsverfahren für zugekaufte Software, um diese an die eigenen Anforderungen anzupassen.	AI2.4
DS1 – Definiere und manage Service Levels	Fehlende oder unzureichende Reviews von SLAs, um sicherzustellen, dass Änderungen der Anforderungen bercksichtigt wurden und dass diese aktuell sind.	DS1.6
ME4 – Sorge für IT-Governance	Fehlendes oder unzureichendes Ressourcenmanagement für IT-Vermögenswerte, um sicherzustellen, dass die IT ausreichende, kompetente und fähige Ressourcen zur Umsetzung der strategischen Ziele hat.	ME4.4

Tab.1 *Abgeleitete Schwachstellen (aus [2])*

6.2 Identifikation von Risikoindikatoren aus KPIs und KGIs (AP2)

In einem zweiten Schritt wurden diesen Schwachstellen die entsprechenden Key Performance Indicators (KPIs), Key Goal Indicators (KPIs), und IT-KGIs zugeordnet. In der Regel konnten die KPIs direkt einem Control Objective und damit einer Schwachstelle zugeordnet werden, so dass eine direkte Bewertung des mit dieser Schwachstelle zusammenhängenden IT-Risikos durchgeführt werden kann. Für die Indikatoren KGIs und die IT-KGIs konnte diese 1:1-Beziehung nicht hergestellt werden, da diese Indikatoren auf einem höheren Abstraktionsniveau als die detaillierten Control Objectives angesiedelt sind, wie z. B. bei dem High-Level Control Objective PO7 (also auf Prozessebene). Diese Messkriterien können aber dennoch als komplementäre Hilfestellung bei der Bewertung einzelner Schwachstellen und Risikoauswirkungen hinzugezogen werden.

Anhand eines Beispiels für den Prozess PO7 wird diese Zuordnung in Tabelle 2 dargestellt.

6.3 Ableitung von Risikobehandlungsmaßnahmen (AP3)

Für die identifizierten und bewerteten IT-Risiken sind entsprechende Risikobehandlungsmaßnahmen zu definieren und umzusetzen. Die aus COBIT abgeleiteten Maßnahmen weisen grundsätzlich entweder einen proaktiven oder reaktiven Charakter auf. Die Organisation kann mit der Einleitung von Vorsorgemaßnahmen in Form der Umsetzung der Control Objectives entsprechend dem angestrebten Reifegrad bereits im Vorfeld potenziellen Risiken entgegenwirken.

Control Objective	Schwachstelle Ableitung aus COs	KPI	KGI	IT-KGI
PO7.1	Fehlender oder unzureichender IT-Personaleinstellungsprozess, um Mitarbeiter einzustellen, die Fähigkeiten zur Unternehmenszielerreichung besitzen	◗ % der IT-Stellen mit Stellenbeschreibungen und Qualifikationsanforderungen ◗ Durchschnittliche Anzahl der Tage, um offene IT-Rollen zu füllen	◗ % der IT-Mitarbeiter, die das Kompetenzprofil für die in der Strategie geforderten Rollen besitzen ◗ % der besetzten IT-Rollen ◗ % der durch ungeplante Abwesenheit verlorenen Arbeitstage ◗ % der IT-Mitarbeiter, die den jährlichen Schulungsplan absolvieren ◗ Ist-zu-Soll-Relation von internen und externen IT-Mitarbeitern ◗ % der IT-Mitarbeiter, die einer Überprüfung unterzogen wurden ◗ % der IT-Rollen, die eine qualifizierte Vertretung besitzen	◗ Grad der Zufriedenheit von Stakeholdern mit der Expertise und den Fertigkeiten von IT-Mitarbeitern ◗ % des zufriedenen IT-Personals (zusammengesetzte Messgröße) ◗ Fluktuation des IT-Personals
PO7.2		◗ ...		

Tab. 2 *Indikatoren zur Risikobewertung (abgeleitet aus [2])*

Auf der einen Seite wurden Risikobehandlungsmaßnahmen aus den Control Objectives erarbeitet. Auf der anderen Seite wurde das COBIT-Reifegrad-Modell verwendet, um weitere Maßnahmen abzuleiten, die über die Control Objectives hinausgehen. Somit ist es möglich, den identifizierten Risiken eine oder mehrere Aktivitäten zuzuweisen. In diesem Zusammenhang ist zu erwähnen, dass die Anzahl und Auswahl der Aktivitäten u.a. von folgenden wesentlichen Faktoren bestimmt werden:

- erforderlicher bzw. angestrebter Reifegrad
- festgestelltes Risikoprofil der Organisation der betrachteten Prozesse
- Bereitschaft und Akzeptanz für die Maßnahmenumsetzung durch die Stakeholder
- Überprüfung, ob die Maßnahme bereits durch andere Aktivitäten umgesetzt wurde, die eine äquivalente Risikobehandlung erzielen

Die abgeleiteten Risikobehandlungsmaßnahmen werden in Tabelle 3 für den Prozess PO7 exemplarisch dargestellt.

6.4 Ableitung von Risikoauswirkungen auf IT- bzw. Geschäftsziele (AP4)

Um festzustellen, welche Schwachstellen (und damit IT-Risiken) Einfluss auf welche Unternehmensziele haben, können die Mapping-Tabellen aus COBIT verwendet werden: Sie stellen zum einen die Beziehung zwischen den IT-Prozessen und den IT-Zielen, zum anderen die Beziehung zwischen IT-Zielen und Unternehmenszielen dar.

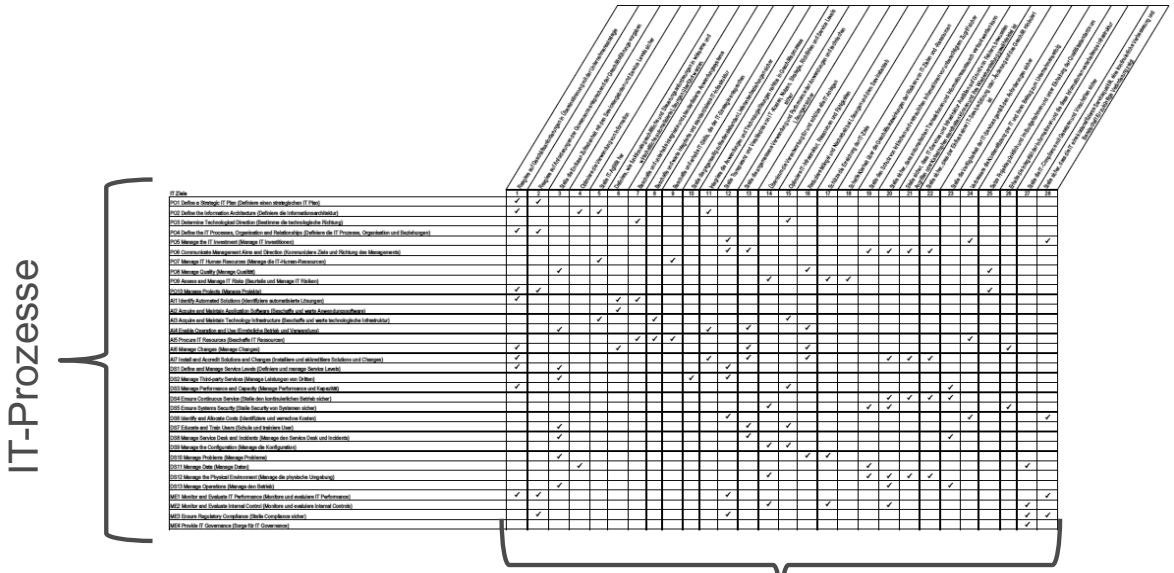
Risikobehandlungsmaßnahmen abgeleitet aus COs und Reifegradmodell
◗ Implementiere einen Personalrekrutierungsprozess, der sicherstellt, dass die Organisation über angemessenes IT-Personal mit den geforderten Fähigkeiten verfügt.
◗ Stelle durch laufende Überprüfung sicher, dass das Personal über die für die jeweiligen Aufgaben erforderliche fachliche Kompetenz und Erfahrung verfügt, und fördere diese durch Programme zur Qualifizierung und Zertifizierung.
◗ Definiere, monitore und überwache Rollen, Verantwortlichkeiten und den Vergütungsrahmen der Mitarbeiter entsprechend der Sensitivität der Position und der zugewiesenen Verantwortlichkeiten.
◗ Sorge für eine entsprechende Einweisung und laufende Schulung von Mitarbeitern, um Wissen und Fähigkeiten sowie das Bewusstsein für Internal Controls und Security aufrechtzuerhalten.
◗ Minimiere die Gefahr kritischer Abhängigkeiten von Schlüsselpersonen durch ausreichende Dokumentation, Vertretungsregelungen und Nachfolgeplanung.
◗ Führe Hintergrund-Checks für neue Mitarbeiter, Vertragspartner und Lieferanten in Abhängigkeit von der Sensitivität und/oder der Kritikalität der Funktion durch.
◗ Führe regelmäßig Beurteilungen der Mitarbeiter hinsichtlich Zielerreichung, Leistung und Verhalten durch.
◗ Stelle sicher, dass bei Mitarbeiterwechseln der Wissenstransfer erfolgt, Verantwortlichkeiten neu zugewiesen und Zugriffsrechte entfernt werden.

Tab. 3 *Ableitung von Risikobehandlungsmaßnahmen (aus [2])*

Diese Beziehung ist in Abbildung 2 dargestellt. Für eine identifizierte IT-Schwachstelle kann bestimmt werden, aus welchem IT-Prozess diese abgeleitet wurde und welche IT-Ziele von dieser Schwachstelle betroffen sind. Diese Beziehung ist im oberen Teil der Abbildung zu sehen. Weiterhin kann über die zweite Mapping-Tabelle aus der Abbildung bestimmt werden, welche IT-Ziele Auswirkung auf welche Unternehmensziele haben. Somit lässt sich über die IT-Ziele eine kausale Kette zwischen IT-Schwachstellen und Unternehmenszielen bilden.

Ein konkretes Beispiel für diese kausale Beziehung ist in Abbildung 3 für den Prozess PO7 illustriert. Das Control Objective PO7.1 »Personalrekrutierung und -bindung« hat beispielsweise Einfluss auf das IT-Ziel der Beschaffung und Erhaltung von IT-Skills. Laut der Mapping-Tabellen beeinflusst dieses Ziel unter anderem die Unternehmensziele der kostengünstigen Produktion wie auch der Geschäftsinnovation.

Anhand dieses Links zwischen Business und IT hat das entwickelte Framework ebenfalls einen praktischen Nutzen für das Management. Das Management definiert Unternehmensziele, die für das Unternehmen von großer Bedeutung sind. Über die Beziehung aus den Mapping-Tabellen lassen sich daraufhin relevante IT-Prozesse und



Unternehmensziele

	Unternehmensziele	IT Ziele						
1	Marktanteil erhöhen	25	28					
2	Erträge erhöhen	25	25					
3	Rendite	24						
4	Kapitalverwertung optimieren	14						
5	Geschäftsrisiken managen	2	14	17	18	19	20	21	22
6	Kunden- und Serviceorientierung erhöhen	3	23					
7	Kostengünstige Produkte und Services anbieten	5	24					
8	Verfügbarkeit von Services	10	16	22	23			
9	Agilität bei Reaktion auf sich ändernde Geschäftsanforderungen (time to market)	1	5	25				
10	Kostenoptimierung bei Serviceerbringung	7	8	10	24			
11	Automatisierung und Integration der Wertschöpfungskette	6	7	8	11			
12	Geschäftsprozess überarbeiten und verbessern	6	7	8	11			
13	Prozesskosten reduzieren	7	8	13	15	24		
14	Compliance mit Gesetzen und Regulativen	2	19	20	21	22	26	27
15	Transparenz	2	18					
16	Compliance mit internen Regelungen	2	13					
17	Betriebliche- und Mitarbeiterproduktivität steigern	7	8	11	13			
18	Produkt-/Geschäftsinovation	5	25	28				
19	Verlässliche und nützliche Informationen für strategische Entscheidungen erlangen	2	4	12	20	26		
20	Qualifizierte und motivierte MitarbeiterInnen einstellen und entwickeln	9						

Abb. 2 *Beziehung zwischen IT-Schwachstellen und Unternehmenszielen (abgeleitet aus [2])*

damit Risikofelder identifizieren, auf die sich die IT-Abteilung fokussieren sollte. Somit kann über dieses Vorgehen sichergestellt werden, dass die IT-Strategie und damit auch das IT-Risikomanagement adäquat von der Unternehmensstrategie abgeleitet werden.

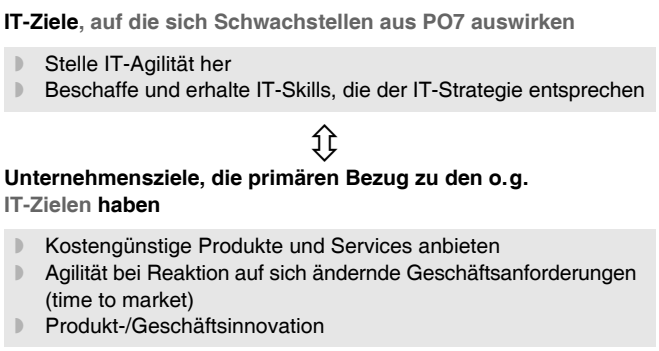


Abb. 3 *Einfluss des Prozesses PO7 auf die Unternehmensziele (abgeleitet aus [2])*

7 Vollständige Darstellung aller Schwachstellen, Indikatoren zur Risikobewertung und Risikobehandlungsmaßnahmen

Tabelle 4 stellt die vollständigen Ergebnisse aus der Arbeit der ISACA-Fachgruppe »IT-Risikomanagement mit COBIT« dar. Die Tabelle hat folgenden Aufbau:

- Gliederung der Control Objectives anhand der 34 COBIT-Prozesse aus den Domains »Plan and Organise (PO)«, »Acquire and Implement (AI)«, »Deliver and Support (DS)« und »Monitor and Evaluate (ME)«, dargestellt durch die grauen Zeilen
- Jeder Prozess beinhaltet in der ersten und zweiten Spalte die aus den Control Objectives (COs) abgeleiteten Schwachstellen sowie eine Referenz auf die entsprechenden COs.
- In der dritten bis fünften Spalte jedes Prozesses befinden sich die Indikatoren Key Performance Indicators (KPIs), Key Goal Indicators (KGIs) sowie die IT-KGIs zur Risikobewertung.
- Spalte sechs enthält die aus den COs und dem COBIT-Reifegrad-Modell abgeleiteten Risikobehandlungsmaßnahmen, um die Schwachstellen aus der ersten Spalte zu reduzieren.

Ein praktischer Nutzen für ein Unternehmen entsteht erst, wenn aus dem generischen IT-Risikokatalog ein unternehmensspezifischer IT-Risikokatalog abgeleitet werden kann und gleichzeitig eine Anleitung zur Reduktion der IT-Risiken zur Verfügung gestellt wird. Um eine effiziente Ableitung zu ermöglichen, wurden die Inhalte der nachfolgenden Tabelle durch die Fachgruppe zu Testzwecken in einen Software-Prototypen übertragen. Diese IT-gestützte Umsetzung dient als Proof of Concept. Der Software-Prototyp steht der Öffentlichkeit nicht zur Verfügung, kann jedoch durch den Leser selbst mit geringem Aufwand implementiert werden, indem die Inhalte der nachfolgenden Tabelle z. B. in ein Datenbanksystem übertragen werden.

PO1 – Definiere einen strategischen IT-Plan					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender Bezug zwischen IT-Investitionen/ -Projekten und Unternehmensstrategie, um Potenzial auszunutzen	PO1.1	◗ % von IT-Vorhaben/ -Projekten, die durch die Kerngeschäftsverantwortlichen getrieben werden ◗ Verzögerung zwischen der Aktualisierung von strategischen/taktischen Unternehmensplänen und der Aktualisierung von strategischen/taktischen IT-Plänen	◗ % der IT-Ziele des strategischen IT-Plans, die den strategischen Unternehmensplan unterstützen ◗ % von IT-Vorhaben des taktischen IT-Plans, die den taktischen Unternehmensplan unterstützen ◗ % von IT-Projekten im IT-Projektportfolio, die direkt auf den taktischen IT-Plan zurückverfolgt werden können	◗ Grad der Zustimmung von Kernprozesseignern der strategischen/ taktischen IT-Pläne ◗ Grad der Einhaltung mit Unternehmens- und Governance-Anforderungen ◗ Grad der Zufriedenheit des Kerngeschäfts mit dem derzeitigen Status (Anzahl, Umfang etc.) von Projekt- und Applikationsportfolio	◗ Schaffe ein Bewusstsein für die Notwendigkeit einer strategischen IT-Planung. ◗ Erarbeite eine Richtlinie zur Durchführung einer strukturierten strategischen IT-Planung. ◗ Arbeite mit den Fachabteilungen zur Sicherstellung IT-unterstützter Investitionen auf der Basis belastbarer, transparenter und nachvollziehbarer Business Cases unter Einbeziehung von Risikoaspekten zusammen. ◗ Stelle sicher, dass Verantwortlichkeiten für die Erreichung des Wertbeitrags und für die Kostenkontrolle klar festgelegt werden und ein Frühwarnsystem für alle Planabweichungen existiert. ◗ Unterrichte die Geschäftsführung über aktuelle und künftige technologische Möglichkeiten, welche die IT bietet, sowie über die durch das Unternehmen zu ergreifenden Maßnahmen. ◗ Integriere Geschäfts- und IT-Strategie durch Verbindung von Unternehmens- und IT-Zielen und analysiere Möglichkeiten und Grenzen der Potenzialausschöpfung. ◗ Identifiziere kritische Abhängigkeiten der Geschäftsstrategie von der IT. ◗ Bewerte die Performance der bestehenden Pläne und Informations-systeme, auf deren Beitrag zu Geschäftszielen sowie deren Funktionalität, Stabilität, Komplexität, Kosten, Stärken und Schwächen. ◗ Erstelle in Zusammenarbeit mit den relevanten Stakeholdern einen hinreichend detaillierten strategischen IT-Plan, der den Beitrag der IT zu den strategischen Zielen des Unternehmens und die damit verbundenen Kosten und Risiken aufzeigt.
Fehlende oder unzureichende Ableitung der IT-Strategie aus der Unternehmensstrategie, um Erfordernisse des Kerngeschäfts zu erfüllen	PO1.2	◗ Verzögerung zwischen der Aktualisierung von strategischen/taktischen Unternehmensplänen und der Aktualisierung von strategischen/taktischen IT-Plänen ◗ % von Meetings zur strategischen/taktischen IT-Planung mit aktiver Beteiligung von Mitgliedern aus Kernprozessen			

→

PO1 – Definiere einen strategischen IT-Plan					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Prozesse/Frühwarnsysteme, um die Performance bzw. Planabweichungen von Investitionen/Projekten zu messen	PO1.3				◗ Stelle sicher, dass der strategische IT-Planungsprozess vom Management überwacht und bei Bedarf aktualisiert wird. ◗ Leite aus dem strategischen IT-Plan ein Portfolio von taktischen IT-Plänen, die notwendigen IT-Vorhaben und Anforderungen an Ressourcen ab. ◗ Manage die taktischen Pläne und Initiativen aktiv durch die Analyse von Projekt- und Serviceportfolios.
Fehlender oder unzureichender strategischer IT-Plan, um aufzuzeigen, inwieweit die IT zu den strategischen Zielen des Unternehmens beiträgt und welche Kosten und Risiken damit verbunden sind	PO1.4	◗ Verzögerung zwischen der Aktualisierung von strategischen/taktischen Unternehmensplänen und der Aktualisierung von strategischen/taktischen IT-Plänen. ◗ % von Meetings zur strategischen/taktischen IT-Planung mit aktiver Beteiligung von Mitgliedern aus Kernprozessen			
Fehlende oder unzureichende taktische IT-Pläne, um die Festlegung von Projektplänen zu ermöglichen	PO1.5	◗ Verzögerung zwischen der Aktualisierung des strategischen zur derjenigen der taktischen IT-Pläne ◗ % von taktischen IT-Plänen, welche die vorgegebene Struktur bzw. die vorgegebenen Inhalte einhalten			
Fehlendes oder unzureichendes IT-Portfolio-Management zur Definition, Priorisierung und Steuerung von Projekten	PO1.6	◗ % von taktischen IT-Plänen, welche die vorgegebene Struktur bzw. die vorgegebenen Inhalte einhalten			

PO2 – Definiere die Informationsarchitektur					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes Informationsarchitekturmodell, um die optimale Errichtung, Verwendung und gemeinsame Benutzung von Informationen durch das Kerngeschäft zu erleichtern	PO2.1	◗ Beteiligungsgrad der User Community	◗ % der Datenklassen, die nicht dem Klassifikationsschema entsprechen ◗ % der Datenelemente, die nicht Teil des Modells für Unternehmensinformationen sind ◗ % der Applikationen, welche nicht den Informationsarchitekturen entsprechen	◗ % der zufriedenen User, welche das Modell für Unternehmensinformationen verwenden (z. B. »Ist das Data Dictionary benutzerfreundlich?«) ◗ % der redundanten/ doppelten Datenelemente	◗ Sorge für ein Bewusstsein und ausreichendes Fachwissen zur Entwicklung einer Informationsarchitektur. ◗ Entwickle und pflege ein Modell der Unternehmensinformation zur Unterstützung des Anwendungsentwicklungsprozesses. ◗ Führe ein unternehmensweites Data Dictionary, das die Datensyntaxregeln der Organisation enthält. ◗ Entwickle ein unternehmensweites Schema zur Klassifikation der Unternehmensdaten hinsichtlich ihrer Kritikalität und Sensitivität. ◗ Definiere und implementiere Verfahren zur Sicherstellung der Integrität und Konsistenz aller elektronischen Daten. ◗ Stelle sicher, dass die Einhaltung der Richtlinien, Standards und Werkzeuge auf allen Ebenen eingefordert wird.
Fehlendes oder unzureichendes unternehmensweites Data Dictionary und fehlende oder unzureichende Datensyntaxregeln, um das Entstehen inkompatibler Datenelemente zu verhindern	PO2.2	◗ % der Datenelemente, die keinen Eigentümer haben ◗ Häufigkeit der durchgeführten Aktivitäten zur Validierung von Daten			
Fehlendes oder unzureichendes Datenklassifikationsschema, um als Grundlage für die Anwendung von Controls, wie Zugriffskontrollen oder Verschlüsselung, zu dienen	PO2.3	◗ Häufigkeit der Updates des Modells für Unternehmensinformationen ◗ Häufigkeit der durchgeführten Aktivitäten zur Validierung von Daten			
Fehlendes oder unzureichendes Verfahren, um die Datenintegrität aller in elektronischer Form gespeicherten Daten sicherzustellen	PO2.4	◗ Häufigkeit der durchgeführten Aktivitäten zur Validierung von Daten			

PO3 – Bestimme die technologische Richtung					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Analyse von Technologien, um die technologische Ausrichtung planen zu können	PO3.1	◗ Häufigkeit der Treffen, welche im Rahmen des Technologieforums gehalten werden	◗ % der technischen Standards, die nicht eingehalten werden ◗ Anzahl der nach ihrer Funktion unterschiedlichen Technologieplattformen im gesamten Unternehmen	◗ Anzahl und Art der Abweichungen vom technologischen Infrastrukturplan	◗ Analysiere bestehende und künftige Technologien und plane, welche technologische Richtung für die Umsetzung der IT-Strategie und der Architektur angemessen ist. ◗ Erstelle und unterhalte einen technischen Infrastrukturplan, der mit den strategischen und taktischen IT-Plänen abgestimmt ist und die Geschäftsanforderungen widerspiegelt. ◗ Entwickle einen Prozess zur laufenden Überwachung von Trends und berücksichtige diese bei der Erstellung des technischen Infrastrukturplans. ◗ Etabliere ein Forum zur Festlegung von Technologierichtlinien, Standards und Methoden und zur Beratung zu Infrastrukturprodukten. ◗ Schaffe ein IT-Architekturgremium, das Vorgaben im Bereich der Architektur erstellt und Ratschläge für deren Anwendung sowie Einhaltung bereitstellt.
Fehlende oder unzureichende technische Infrastrukturplanung zur Abstimmung der technologischen Ausrichtung	PO3.2	◗ Häufigkeit der Reviews/ Aktualisierungen des technischen Infrastrukturplans			
Fehlender oder unzureichender Prozess, um aktuelle Trends der Branche (regulatorisch, Infrastruktur, Geschäftsfelder etc.) zu analysieren	PO3.3	◗ Häufigkeit der Treffen, welche im Rahmen des Technologieforums gehalten werden			
Fehlendes Technologieforum, um Richtlinien, Methoden und Standards zum Technologieeinsatz zu erstellen	PO3.4	◗ Häufigkeit der Treffen, welche im Rahmen des Technologieforums gehalten werden			
Fehlendes Gremium, um das Design der IT-Architektur zu bestimmen	PO3.5	◗ Häufigkeit der Treffen, welche im Rahmen des Architekturgremiums gehalten werden			

PO4 – Definieren IT-Prozesse, Organisation und Beziehungen					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes IT-Prozess-Framework, um den strategischen IT-Plan umzusetzen	PO4.1	◗ % der Rollen mit dokumentierten Stellenbeschreibungen und Befugnissen ◗ Anzahl der IT-Betriebsfunktionen/ -Prozesse, die mit den Unternehmensbetriebsstrukturen verknüpft sind	◗ Anzahl der aus Optik der Funktionstrennung widersprüchlichen Verantwortlichkeiten ◗ Anzahl der Eskalationen oder ungelösten Vorfälle aufgrund von mangelnder oder nicht ausreichend zugewiesener Verantwortung ◗ % der Stakeholder, die mit der Reaktionsfähigkeit (engl.: responsiveness) der IT zufrieden sind	◗ Zufriedenheit der Stakeholder (Befragungen) ◗ Anzahl der Vorhaben, die aufgrund der Trägheit der IT oder Nichtverfügbarkeit der entsprechenden Leistungen verzögert wurden ◗ Anzahl der Geschäftsprozesse, die nicht durch die IT-Organisation unterstützt werden, obwohl sie gemäß Strategie unterstützt sein sollten ◗ Anzahl der wesentlichen IT-Aktivitäten außerhalb der IT-Organisation, die nicht bewilligt sind oder die nicht den IT-Organisationsstandards unterstehen	◗ Definiere ein Framework der IT-Prozesse, um den strategischen IT-Plan umzusetzen. ◗ Etabliere einen IT-Strategieausschuss auf Ebene der Unternehmensleitung. ◗ Etabliere einen IT-Lenkungsausschuss zur Steuerung der Prioritäten, sowie der Überwachung von Projekten und Service Levels. ◗ Verankere die IT in der Gesamtorganisation unter Beachtung ihrer Bedeutung für das Unternehmen. ◗ Entwickle eine IT-Organisationsstruktur, die die Unternehmenserfordernisse widerspiegelt. ◗ Definiere und kommuniziere Rollen und Verantwortlichkeiten für alle Mitarbeiter der IT-Organisation und aktualisiere diese regelmäßig. ◗ Lege die Verantwortung für die IT-Qualitätssicherung fest. ◗ Verankere die unternehmensweite Verantwortung für IT-bezogene Risiken im Kerngeschäft, einschließlich spezifischer Verantwortung für Informationssicherheit, physische Sicherheit und Compliance auf angemessen hoher Ebene. ◗ Lege Verantwortlichkeiten für die Eigentümerschaft von Daten- und Informationssystemen fest. ◗ Lege Verfahren zur Überwachung der korrekten Ausführung von Rollen und Verantwortlichkeiten fest. ◗ Stelle eine ausreichende Funktionstrennung von Rollen und Verantwortlichkeiten bei kritischen Prozessen sicher. ◗ Stelle sicher, dass die IT-Organisation über ausreichende und qualifizierte Personalressourcen verfügt. ◗ Identifiziere Schlüsselpersonal in der IT. ◗ Definiere Policies und Verfahren für den Einsatz und die Steuerung externer Mitarbeiter. ◗ Sorge für eine Koordinations-, Kommunikations- und Verbindungsstruktur zwischen der IT-Organisation und den verschiedenen anderen Interessen innerhalb und außerhalb der IT.
Fehlender IT-Strategieausschuss, um die IT-Governance angemessen zu adressieren	PO4.2	◗ Häufigkeit der Meetings der Strategie- und Lenkungsausschüsse			
Fehlender IT-Lenkungsausschuss, um Projekte und Service Levels zu monitoren	PO4.3	◗ Häufigkeit der Meetings der Strategie- und Lenkungsausschüsse			
Fehlende oder unzureichende Platzierung der IT-Organisation, um diese in die Gesamtorganisation einzugliedern	PO4.4	◗ Anzahl der IT-Betriebsfunktionen/-Prozesse, die mit den Unternehmensbetriebsstrukturen verknüpft sind			
Fehlende oder unzureichende IT-Organisationsstruktur, um die Unternehmenserfordernisse widerzuspiegeln	PO4.5	◗ Anzahl der IT-Betriebsfunktionen/-Prozesse, die mit den Unternehmensbetriebsstrukturen verknüpft sind			
Fehlende oder unzureichende Definition von Rollen und Verantwortlichkeiten, um ausreichend Autorität für die Umsetzung dieser zu ermöglichen	PO4.6	◗ % der Rollen mit dokumentierten Stellenbeschreibungen und Befugnissen			
Fehlende oder unzureichende Zuweisung von Verantwortung, um eine unabhängige Qualitätssicherung zu gewährleisten	PO4.7	◗ % der Rollen mit dokumentierten Stellenbeschreibungen und Befugnissen			

PO5 – Manage IT-Investitionen					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes »Financial Management Framework«, um Budgetierung und Kosten-Nutzen-Analysen zu steuern	PO5.1	◗ % der Projekte mit vorab definiertem Nutzen ◗ % der bepreisten IT-Services ◗ Frequenz des Nutzenreportings ◗ % der Projekte, von denen eine Performance-Information (Kostenperformance, Planungsperformance und Risikoprofil) verfügbar ist	◗ Anzahl von Budgetabweichungen ◗ % der Budgetabweichung verglichen mit dem Gesamtbudget ◗ % der Reduktion der Stückkosten bei erbrachten IT-Services ◗ % der IT-Investitionen, die den vorab definierten Nutzen erbringen	◗ % der IT-Investitionen, die den vorab bestimmten Geschäftsnutzen erreichen oder übertreffen ◗ % der IT Value Driver abgebildet auf die Business Value Driver ◗ % der IT-Ausgaben im Verhältnis zu Business Value Driver (z. B.: Verkaufswachstum infolge erhöhter Konnektivität)	◗ Entwickle ein Framework für das Management der Portfolios für IT-Investitionen, Services und Anlagen als Basis für das IT-Budget und als Input für das Business. ◗ Implementiere einen Entscheidungsprozess zur optimalen Priorisierung und Steuerung der IT-Ressourcen. ◗ Implementiere einen Prozess zur Erstellung und laufenden Steuerung des IT-Budgets. ◗ Etabliere einen Kostenmanagement-Prozess zur laufenden Überwachung der aktuellen Kosten und des Budgets. ◗ Implementiere einen Prozess zur laufenden Überwachung des Business Case von IT-unterstützten Investitionsprogrammen.
Fehlender oder unzureichender Prozess zur Priorisierung von IT-Ressourcen-Verteilung (für Projekte, laufenden Betrieb etc.), um den IT-Wertbeitrag zu maximieren	PO5.2	◗ % der Projekte mit vorab definiertem Nutzen			
Fehlender oder unzureichender IT-Budgetierungsprozess, um die Kosten von Projekten und laufendem Betrieb zu planen	PO5.3	◗ % der bepreisten IT-Services			
Fehlender oder unzureichender Kostenmanagement-Prozess, um die aktuellen Kosten mit den Budgets zu vergleichen	PO5.4	◗ % der bepreisten IT-Services ◗ % der Projekte, von denen eine Performance-Information (Kostenperformance, Planungsperformance und Risikoprofil) verfügbar ist			
Fehlender oder unzureichender Prozess, um den von der IT erwarteten Beitrag zu überwachen	PO5.5	◗ % der Projekte mit einem nachträglichen Review ◗ Frequenz des Nutzenreportings			

PO6 – Kommuniziere Ziele und Richtung des Managements					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Festlegung von IT-Richtlinien und Control-Umfeld, um Nutzenerbringung und Risikomanagement zu unterstützen	PO6.1	◗ Frequenz von Reviews und Updates der Richtlinien ◗ Frequenz von Reviews und Updates des IT Control Frameworks	◗ % der Stakeholder, die die IT-Richtlinien verstehen ◗ % der Stakeholder, die das IT Control Framework verstehen ◗ % der Stakeholder, die Richtlinien nicht einhalten	◗ Anzahl der Fälle, wo vertrauliche Informationen kompromittiert wurden ◗ Anzahl der Unterbrechungen im Kerngeschäft aufgrund von IT-Service-Ausfällen ◗ Verständnis für Kosten, Nutzen, Strategie, Richtlinien und Service-Levels der IT	◗ Lege die Elemente des IT-Control-Umfelds (Wertbeitrag der IT, Risikobereitschaft, Integrität, ethische Werte, Kompetenz des Personals, Verantwortlichkeit) in Übereinstimmung mit der Philosophie und dem Arbeitsstil des Unternehmensmanagements fest. ◗ Entwickle und unterhalte ein Framework für das unternehmensweite IT-Risikomanagement und Internal Controls, das die rechtzeitige Erkennung von Unregelmäßigkeiten, die Begrenzung von Verlusten und die zeitnahe Wiederherstellung der Unternehmenswerte sicherstellt. ◗ Entwickle und unterhalte zur Unterstützung der IT-Strategie IT-Richtlinien zu den wichtigsten Themen wie Qualität, Sicherheit, Vertraulichkeit, Internal Controls und Schutz von geistigem Eigentum. ◗ Etabliere die IT-Richtlinien als integralen Bestandteil der Unternehmensabläufe. ◗ Stelle sicher, dass das Bewusstsein und Verständnis für Ziele und Ausrichtung des Unternehmens und der IT im gesamten Unternehmen kommuniziert werden. ◗ Achte darauf, dass das IT-Sicherheitsbewusstsein gestärkt und die Botschaft vermittelt wird, dass für IT-Sicherheit alle verantwortlich sind.
Fehlendes oder unzureichendes »Risk/Control Framework«, um Nutzen zu generieren und Ressourcen sowie Systeme zu schützen	PO6.2	◗ Frequenz von Reviews und Updates des IT Control Frameworks			
Fehlende oder unzureichende IT-Richtlinien, um die IT-Strategie zu unterstützen	PO6.3	◗ Frequenz von Reviews und Updates der Richtlinien			
Fehlende oder unzureichende Kommunikation der IT-Richtlinien, um diese den Mitarbeitern bekannt zu machen	PO6.4	◗ Zeitverzögerung zwischen Freigabe der Richtlinien und deren Kommunikation an User			
Fehlende oder unzureichende Kommunikation der Ziele und Ausrichtung sowohl des Unternehmens als auch der IT, um Bewusstsein und Verständnis für diese sowie Security Awareness zu schaffen	PO6.5				

PO7 – Manage die Humanressourcen					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender IT-Personaleinstellungsprozess, um Mitarbeiter einzustellen, die Fähigkeiten zur Unternehmens-zielerreichung besitzen	PO7.1	◗ % der IT-Stellen mit Stellenbeschreibungen und Qualifikationsanforderungen ◗ Durchschnittliche Anzahl der Tage, um offene IT-Rollen zu füllen	◗ % der IT-Mitarbeiter, die das Kompetenzprofil für die in der Strategie geforderten Rollen besitzen ◗ % der besetzten IT-Rollen ◗ % der durch ungeplante Abwesenheit verlorenen Arbeitstage ◗ % der IT-Mitarbeiter, die den jährlichen Schulungsplan absolvieren ◗ Ist-zu-Soll-Relation von internen und externen IT-Mitarbei-tern ◗ % der IT-Mitarbeiter, die einer Überprüfung unterzogen wurden ◗ % der IT-Rollen, die eine qualifizierte Vertretung besitzen	◗ Grad der Zufriedenheit von Stakeholdern mit der Expertise und Fertigkeiten von IT-Mitarbeitern ◗ % des zufriedenen IT-Personals (zusammengesetzte Messgröße) ◗ Fluktuation des IT-Personals	◗ Implementiere einen Personalrekrutierungsprozess, der sicherstellt, dass die Organisation über angemessenes IT-Personal mit den geforderten Fähigkeiten verfügt. ◗ Stelle durch laufende Überprüfung sicher, dass das Personal über die für die jeweiligen Aufgaben erforderliche fachliche Kompetenz und Erfahrung verfügt, und fördere diese durch Programme zur Qualifizierung und Zertifizierung. ◗ Definiere, monitore und überwache Rollen, Verantwortlichkeiten und den Vergütungsrahmen der Mitarbeiter entsprechend der Sensitivität der Position und der zugewiesenen Verantwortlichkeiten. ◗ Sorge für eine entsprechende Einweisung und laufende Schulung von Mitarbeitern, um Wissen und Fähigkeiten sowie das Bewusstsein für Internal Controls und Security aufrechtzuerhalten. ◗ Minimiere die Gefahr kritischer Abhängigkeiten von Schlüsselpersonen durch ausreichende Dokumentation, Vertretungsregelungen und Nachfolge-planung. ◗ Führe Hintergrund-Checks für neue Mitarbeiter, Vertragspartner und Lieferanten in Abhängigkeit von der Sensitivität und/oder der Kritikalität der Funktion durch. ◗ Führe regelmäßig Beurteilungen der Mitarbeiter hinsichtlich Zielerreichung, Leistung und Verhalten durch. ◗ Stelle sicher, dass bei Mitarbeiterwechseln der Wissenstransfer erfolgt, Verantwortlichkeiten neu zugewiesen und Zugriffsrechte entfernt werden.
Fehlendes oder unzureichendes IT-Aus- und Weiterbildungskonzept, um die Kompetenzen des Personals sicherzustellen	PO7.2	◗ % der IT-Mitarbeiter, die Entwicklungspläne abgeschlossen haben ◗ Durchschnittliche Anzahl der Schulungs- und Entwick-lungstage (inklusive Coaching) pro Person pro Jahr ◗ % des zertifizierten IT-Personals im Verhältnis zu den Erfordernissen der Stelle			
Fehlende oder unzureichende Definition und Überwachung von Rollen und Verantwortlichkeiten, um die Informationssicherheit und Compliance-Regeln sicherzustellen	PO7.3	◗ % der IT-Stellen mit Stellenbeschreibungen und Qualifikationsanforderungen			
Fehlende oder unzureichende Ausbildung bzw. Ausbildungs-planung, um Fähigkeiten auf einem angemessenen Niveau zu halten	PO7.4	◗ % der IT-Mitarbeiter, die Entwicklungspläne abgeschlossen haben ◗ Durchschnittliche Anzahl der Schulungs- und Entwicklungstage (inklusive Coaching) pro Person pro Jahr ◗ % des zertifizierten IT-Personals im Verhältnis zu den Erfordernissen der Stelle			

→

PO7 – Manage die Humanressourcen					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Wissensteilung, um die kritische Abhängigkeit von Einzelpersonen zu minimieren	PO7.5	◗ Rate der IT-Mitarbeiter-rotation ◗ Durchschnittliche Anzahl der Tage, um offene IT-Rollen zu füllen			
Fehlende oder unzureichende Hintergrund-Checks im IT-Recruiting-Prozess, um Personal zu überprüfen	PO7.6				
Fehlende oder unzureichende Leistungsbeurteilung von Mitarbeitern, um diese zu unterstützen	PO7.7	◗ % der IT-Mitarbeiter mit dokumentierten und validierten rechtzeitigen Reviews			
Fehlende oder unzureichende Prozesse, um den Jobwechsel von Mitarbeitern effizient durchzuführen (wie Wissenstransfer, Entfernung von Zugriffsrechten oder Zuweisung von Zugriffsrechten)	PO7.8				

PO8 – Manage Qualität					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes QMS, um Methoden und organisatorische Strukturen festzulegen	PO8.1	◗ % der IT-Mitarbeiter, die ein Training in Qualitätsbewusstsein/ -management erhalten	◗ % der Fehler, die vor der Inbetriebnahme erkannt wurden ◗ % Reduktion in der Anzahl der schwerwiegenden Störungen pro User und Monat ◗ % der durch eine QA überprüften und abgenommenen IT-Projekte, die den Qualitätsvorgaben und -zielen entsprechen ◗ % der regelmäßig durch eine QA formell überprüften IT-Prozesse, die den Qualitäts-vorgaben und -zielen entsprechen	◗ % der Stakeholder, die mit der IT-Qualität (gewichtet durch Bedeutung) zufrieden sind	◗ Entwickle und unterhalte ein Qualitätsmanagementsystem (QMS), das einen standardisierten, formalen und kontinuierlichen Ansatz zum Qualitätsmanagement bietet. ◗ Wende Standards, Methoden und Praktiken für die wesentlichen IT-Prozesse auf der Basis von Best Practices an. ◗ Etabliere in dem Lebenszyklus eines Endproduktes Standards für alle IT-Entwicklungen und Beschaffungen und berücksichtige Freigaben von wichtigen Milestones auf der Basis von vereinbarten Abnahmekriterien. ◗ Stelle sicher, dass das Qualitätsmanagement auf die Kundenanforderungen fokussiert ist. ◗ Gewährleiste, dass der Qualitätsplan die kontinuierliche Verbesserung fördert. ◗ Definiere, plane und implementiere Maßnahmen für die Einhaltung des QMS und stelle sicher, dass bei Abweichungen geeignete korrektive und präventive Maßnahmen getroffen werden.
Fehlende oder unzureichende Anwendung von Standards, Methoden und Praktiken des QMS, um die Organisation in der Erreichung der Ziele des QMS zu unterstützen	PO8.2	◗ % von Projekten, die QA-Review erhalten ◗ % der Prozesse, die QA-Review erhalten			
Fehlende oder unzureichende Anwendung von Standards in Beschaffung und Entwicklung, um einheitliche Ansätze z. B. zur Programmierung, Dateiformate, User-Interfaces oder Testpläne festzulegen	PO8.3	◗ % der IT-Mitarbeiter, die ein Training in Qualitätsbewusstsein/-management erhalten			
Fehlende oder unzureichende Fokussierung des Qualitäts-managements auf Kunden, um Kundenanforderungen effizient abzudecken	PO8.4	◗ % von IT-Prozessen und -Projekten mit aktiver Beteiligung der Stakeholder an der Qualitätssicherung ◗ % der Stakeholder, die sich an der Qualitätsüber-wachung beteiligen ◗ % von Projekten, die QA-Review erhalten			
Fehlende oder unzureichende Qualitätspläne, um eine kontinuierliche Verbesserung zu fördern	PO8.5	◗ % von Projekten, die QA-Review erhalten ◗ % der Prozesse, die QA-Review erhalten			
Fehlende oder unzureichende Messung der Qualität, um geeignete korrektive und präventive Maßnahmen treffen zu können	PO8.6	◗ % von Projekten, die QA-Review erhalten ◗ % der Prozesse, die QA-Review erhalten			

PO9 – Beurteile und manage IT-Risiken					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Integration des IT-Risiko-Managements in das unternehmensweite Risikomanagement, um eine abgestimmte Risikopolitik zu gewährleisten	PO9.1	◗ % des IT-Budgets, welches in Risikomanagement-Aktivitäten (Beurteilung und Begrenzung) investiert wurde ◗ Häufigkeit der Reviews des IT-Risikomanagement-Prozesses	◗ % von identifizierten kritischen IT-Ereignissen, die beurteilt wurden ◗ Anzahl der neu identifizierten IT-Risiken (im Vergleich zum vorhergehenden Durchlauf) ◗ Anzahl der signifikanten Störungen, die durch nicht vom Risikobeurteilungsprozess identifizierte Risiken verursacht wurden ◗ % von identifizierten kritischen IT-Risiken mit entwickeltem Maßnahmenplan	◗ % von kritischen IT-Zielen, die durch Risikobeurteilung abgedeckt sind ◗ % von IT-Risikobeurteilungen, die in den IT-Risikobeurteilungsansatz integriert sind	◗ Integriere die Frameworks für IT-Governance, IT-Risikomanagement und Controls in das unternehmensweite Modell für das Risikomanagement. ◗ Bestimme die internen und externen Rahmenbedingungen für jede Risikobewertung, die Ziele der Bewertung und die Kriterien, nach denen Risiken evaluiert werden. ◗ Identifiziere sämtliche Ereignisse (Bedrohungen oder Schwachstellen) mit einer potenziellen Auswirkung auf die Ziele oder den Betrieb des Unternehmens, bestimme die Art der Auswirkungen und überprüfe regelmäßig die Ergebnisse. ◗ Bewerte regelmäßig unter Anwendung qualitativer und quantitativer Methoden die Wahrscheinlichkeit und Auswirkungen aller identifizierten Risiken. ◗ Implementiere einen Prozess zur Entwicklung einer Risikostrategie (Festlegung von Sicherheitsmaßnahmen und Controls) als Reaktion auf identifizierte Risiken. ◗ Überwache die Umsetzung der Maßnahmen aus der Risikostrategie und berichte Planabweichungen an die Geschäftsführung.
Fehlende oder unzureichende Festlegung des Kontexts für die Einbettung des Risikobeurteilungs-Frameworks, um Risiken angemessen zu bewerten	PO9.2	◗ % von identifizierten IT-Ereignissen, die in Risikobeurteilungen genutzt werden			
Fehlende oder unzureichende Identifikation von Bedrohungen und Schwachstellen, um deren Auswirkungen auf Ziele und den Betrieb des Unternehmens zu bestimmen	PO9.3	◗ % des IT-Budgets, welches in Risikomanagement-Aktivitäten (Beurteilung und Begrenzung) investiert wurde ◗ % von identifizierten IT-Ereignissen, die in Risikobeurteilungen genutzt werden			
Fehlende oder unzureichende Bewertung von Risiken, um das Risikopotenzial angemessen zu beurteilen	PO9.4	◗ % des IT-Budgets, welches in Risikomanagement-Aktivitäten (Beurteilung und Begrenzung) investiert wurde ◗ % von identifizierten IT-Ereignissen, die in Risikobeurteilungen genutzt werden ◗ % von Risikobeurteilungen, die abgezeichnet wurden ◗ % der durchgeführten Risikoüberwachungsberichte in Relation zur vereinbarten Anzahl			
Fehlende oder unzureichende Risikobehandlungsmaßnahmen, um Risiken angemessen zu reduzieren	PO9.5	◗ % der Risikomanagement-Maßnahmenpläne, die für die Implementierung genehmigt sind			
Fehlende oder unzureichende Prozesse, um die Umsetzung des Risikobehandlungsplans zu überwachen.	PO9.6	◗ % der durchgeführten Risikoüberwachungsberichte in Relation zur vereinbarten Anzahl ◗ Häufigkeit der Reviews des IT-Risikomanagement-Prozesses			

PO10 – Manage Projekte					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes Programm-Management-Framework, um Projekte untereinander zu koordinieren und diese zur Unterstützung der Unternehmensziele einzusetzen	PO10.1	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen	◗ % von Projekten, die im Termin- und im Budgetrahmen liegen ◗ % der Projekte, die die Erwartungen der Stakeholder erfüllen	◗ % der Projekte, die die Erwartungen der Stakeholder erfüllen (zeitgerecht, im Budgetrahmen und die Anforderungen treffend – gewichtet nach Bedeutung)	◗ Manage und steuere das auf dem Portfolio der IT-gestützten Investitionsprogramme basierende Projektprogramm unter Berücksichtigung gegenseitiger Abhängigkeiten. ◗ Erstelle und unterhalte ein allgemeines Projektmanagement-Framework, das die anzuwendenden Methodologien für alle Projektphasen definiert. ◗ Etabliere einen generischen Projektmanagement-Ansatz zugeschnitten auf Projekte unterschiedlicher Größe, Komplexität und rechtlicher Rahmenbedingungen, der auch die Struktur zur Projektsteuerung in Form von Rollen, Verantwortlichkeiten und Zuständigkeiten definiert. ◗ Beteilige betroffene Stakeholder bei der Definition und Ausführung eines Projektes und sorge für ihr Commitment. ◗ Dokumentiere Art und Umfang eines Projekts, hole die Bestätigung der Stakeholder ein und lasse das Projekt vor Beginn durch die Programm- und Projektsponsoren formal freigeben. ◗ Stelle sicher, dass die Initialisierung wesentlicher Projektphasen basierend auf der Abnahme der Ergebnisse der vorhergehenden Phase formell verabschiedet und allen Stakeholdern kommuniziert wird. ◗ Erstelle einen die Unternehmens- und IT-Ressourcen umfassenden integrierten Projektplan unter Berücksichtigung von Abhängigkeiten und aktualisiere den Plan während der Projektlaufzeit unter Beachtung der Regularien zur Programm- und Projektsteuerung. ◗ Lege die Verantwortlichkeiten und Kompetenzen der Projektteam-Mitglieder fest und spezifiziere die Anforderungen an die einzusetzenden Projektmitarbeiter bzw. externen Vertragsnehmer sowie sonstigen benötigten Produkte oder Services. ◗ Identifiziere, dokumentiere und manage spezifische Projektrisiken.
Fehlendes oder unzureichendes Projektmanagement-Framework, um Projekte auf eine strukturierte Art und Weise durchzuführen	PO10.2	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen			
Fehlender oder unzureichender Projektmanagement-Ansatz, um Strukturen und Verantwortlichkeiten zur Projektsteuerung zu definieren	PO10.3	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen ◗ % der zertifizierten oder geschulten Projektmanager			
Keine oder unzureichende Beteiligung der Stakeholder, um diese bei der Festlegung und Ausführung von Projekten zu beteiligen	PO10.4	◗ % von Stakeholdern, die sich an den Projekten beteiligen (Anteil der Einbindung)			
Fehlende oder unzureichende Projektbeschreibungen, um unter den Stakeholdern ein gemeinsames Verständnis zu entwickeln	PO10.5	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen			
Fehlende oder unzureichende formelle Initiierung der einzelnen Projektphasen, um sicherzustellen, dass der Fortschritt des Projektes auf geforderten Ergebnistypen basiert	PO10.6	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen			

→

PO10 – Manage Projekte					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender integrierter (Unternehmens- und IT-Ressourcen umfassend) Projektplan, um eine strukturierte Steuerung der Projektumsetzung sicherzustellen	PO10.7	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen			◗ Erstelle einen Qualitätsmanagementplan als Teil des gesamten Projektplans, der formell geprüft und durch alle betroffenen Parteien abgenommen wird. ◗ Entwickle einen Change-Management-Prozess, der sicherstellt, dass wesentliche Änderungen insbesondere von Kosten, Zeitplanung, Umfang und Qualität des Projektes angemessen überprüft und freigegeben werden. ◗ Berücksichtige im Rahmen der Projektplanung, dass bei neuen oder geänderten Systemen Internal Controls und Sicherheitseigenschaften den festgelegten Anforderungen entsprechen. ◗ Messe und reporte die Projektperformance anhand wesentlicher Kriterien (z. B. Umfang, Zeitplan, Qualität, Kosten, Risiken) und erarbeite und überwache Verbesserungsmaßnahmen. ◗ Stelle sicher, dass am Ende jedes Projektes die Projekt-Stakeholder bestätigen, ob das Projekt die geplanten Ergebnisse und den geplanten Nutzen erbracht hat. Dokumentiere alle offenen Aktivitäten, die notwendig sind, um die geplanten Projektergebnisse und den Nutzen des Programms zu erzielen, und identifiziere und dokumentiere die Lessons Learned.
Fehlendes oder unzureichendes Projektressourcen-Management, um die Projektziele zu erreichen	PO10.8	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen ◗ % der zertifizierten oder geschulten Projektmanager			
Fehlendes oder unzureichendes Projekt-Risikomanagement, um mit dem Projekt in Verbindung stehende Risiken zu adressieren	PO10.9	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen ◗ % der zertifizierten oder geschulten Projektmanager			
Fehlende oder unzureichende Projektqualitätspläne, um durch deren Prüfung eine hohe Qualität des Projektes zu gewährleisten	PO10.10	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen			
Fehlendes oder unzureichendes Projekt-Change-Management, um nur autorisierte Änderungen im Projekt durchzuführen	PO10.11	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen			
Fehlende oder unzureichende Bestätigungsmethoden, um die Akkreditierung von neuen oder geänderten Systemen zu unterstützen	PO10.12	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen			
Fehlende oder unzureichende Messung, Berichterstattung und Monitoring der Projektperformance, um Abweichungen vom Projektplan zu identifizieren und Verbesserungsmaßnahmen treffen zu können	PO10.13	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen			
Fehlende oder unzureichende formelle Projektabschlüsse, um die Zielerreichung durch die Stakeholder zu bestätigen und Lessons Learned zu identifizieren	PO10.14	◗ % der Projekte, die Projektmanagement-Standards und -Praktiken folgen ◗ % der Projekte, für die Post-Implementation Reviews durchgeführt werden ◗ % von Stakeholdern, die sich an den Projekten beteiligen (Anteil der Einbindung)			

AI1 – Identifiziere automatische Lösungen					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Festlegung und Aktualisierung von funktionalen Geschäfts- und technischen Erfordernissen, um die vom IT-gestützten Investitionsprogramm erwarteten Ergebnisse zu erreichen	AI1.1		◗ % der Stakeholder, die mit der Genauigkeit der Machbarkeitsstudien zufrieden sind ◗ Relation des Nutzens umgesetzter IT-Projekte zum durch Machbarkeitsstudien vorher prognostizierten Nutzen ◗ % der Anwendungen im Portfolio, die nicht architekturkonform sind ◗ % der Machbarkeitsstudien, die Termin- und Budgetrahmen eingehalten haben	◗ Anzahl der Projekte, die den prognostizierten Nutzen aufgrund falscher Annahmen in der Machbarkeitsstudie nicht erreichen ◗ % der User, die mit der gelieferten Funktionalität zufrieden sind	◗ Spezifiziere und vereinbare die funktionalen und technischen Anforderungen zur Erreichung der mit dem IT-gestützten Investitionsprogramm erwarteten Ergebnisse. ◗ Identifiziere und analysiere im Rahmen der Anforderungsdefinition Risiken im Hinblick auf Gefährdungen der Datenintegrität, Sicherheit, Verfügbarkeit, des Datenschutzes und der Einhaltung von Gesetzen und Verordnungen. ◗ Führe eine Machbarkeitsstudie durch, die die Möglichkeit der Implementierung der Anforderungen sowie alternative Vorgehensweisen prüft, bewertet und eine Empfehlung an den Auftraggeber abgibt. ◗ Stelle sicher, dass der Auftraggeber die funktionalen und technischen Anforderungen sowie die Ergebnisse der Machbarkeitsstudie nach erfolgreicher Beendigung von Qualitätsreviews genehmigt und unterzeichnet.
Fehlende oder unzureichende Risikoanalyse im Anforderungsmanagement, um Gefährdungen der Datenintegrität, Sicherheit, Verfügbarkeit, Datenschutz und die Einhaltung von Gesetzen und Verordnungen zu adressieren	AI1.2				
Fehlende oder unzureichende Durchführung von Machbarkeitsstudien, um die Möglichkeit der Implementierung der Anforderungen zu prüfen und alternative Umsetzungsmöglichkeiten zu formulieren	AI1.3	◗ % der IT-Projekte im Jahresplan, für die Machbarkeitsstudien durchgeführt werden			
Fehlendes oder unzureichendes Freigabeverfahren durch Auftraggeber, um die Lösungsauswahl und den Beschaffungsansatz zu autorisieren	AI1.4	◗ % der vom Geschäftsprozesseigner abgezeichneten Machbarkeitsstudien			

AI2 – Beschaffe und warte Anwendungssoftware					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes Grobdesign innerhalb der Softwareentwicklung, um Unternehmenserfordernisse angemessen zu berücksichtigen	AI2.1	◗ % der Anwendungssoftware-projekte, für die ein angemessenes Review und eine Abnahme der Einhaltung von Entwicklungsstandards durchgeführt wird ◗ % der Anwendungssoftware-projekte, für die ein Qualitätssicherungsplan entwickelt und ausgeführt wird	◗ % der Entwicklungs-projekte, die innerhalb des vorgesehenen Termin- und Budget-rahmens bleiben ◗ % des Entwicklungs-aufwands, der für den Unterhalt vorhandener Anwendungen aufgebracht wird ◗ Anzahl der Probleme pro Anwendung in der Produktion, die sichtbare Stillstandzeit verursachen ◗ Anzahl berichteter Fehler pro Monat (pro Function Point)	◗ % der Projekte, die Unternehmensänderungen innerhalb des geforderten Zeitrahmens herbeiführen ◗ Anzahl der Projekte, bei denen der festgelegte Nutzen aufgrund schwachen Anwendungsdesigns oder schwacher Anwendungsentwicklung nicht erreicht wurde ◗ % der User, die mit der gelieferten Funktionalität zufrieden sind	◗ Überführe die Geschäftsanforderungen in eine grobe Designspezifikation für die Softwareentwicklung unter Berücksichtigung der technologischen Ausrichtung der Organisation sowie der Informationsarchitektur und lasse die Designspezifikation genehmigen. ◗ Erstelle ein detailliertes Design und technische Softwareanforderungen an die Anwendung, definiere Abnahmekriterien und lasse die Anforderungen abnehmen. ◗ Stelle sicher, dass Kontrollen aus Geschäftsprozessen in die Anwendung in angemessener Form implementiert werden, sodass die Verarbeitung richtig, vollständig, termingetreu, autorisiert und nachvollziehbar erfolgt. ◗ Behandle Anforderungen an die Sicherheit und Verfügbarkeit der Anwendung unter Berücksichtigung der identifizierten Risiken und in Übereinstimmung mit der Datenklassifikation, der Informationssicherheitsarchitektur sowie des Risikoprofils. ◗ Konfiguriere und implementiere erworbene Anwendungssoftware entsprechend den Geschäftsanforderungen. ◗ Stelle sicher, dass bei wesentlichen System-Upgrades, die signifikante Änderungen des Designs und/oder der Funktionalität beinhalten, analog zum Prozess für neu entwickelte Systeme verfahren wird. ◗ Stelle sicher, dass die Funktionalität entsprechend den Designspezifikationen, Entwicklungs- und Dokumentationsstandards und Qualitätsanforderungen entwickelt und im Falle erfolgreicher Reviews bestätigt wird. ◗ Entwickle einen Softwarequalitätssicherungsplan, stelle benötigte Ressourcen bereit und setze den Plan um.
Fehlendes oder unzureichendes detailliertes Design in der Softwareentwicklung, um Abdeckung mit den Anforderungen und dem Grobdesign sicherzustellen	AI2.2	◗ % der Anwendungssoftware-projekte, für die ein angemessenes Review und eine Abnahme der Einhaltung von Entwicklungsstandards durchgeführt wird ◗ % der Anwendungssoftware-projekte, für die ein Qualitätssicherungsplan entwickelt und ausgeführt wird			
Fehlende oder unzureichende Überleitung der Unternehmenskontrollen in die Anwendungskontrollen, um eine richtige, vollständige, zeitgerechte, autorisierte und nachvollziehbare Verarbeitung zu gewährleisten	AI2.3	◗ % der Anwendungssoftware-projekte, für die ein Qualitätssicherungsplan entwickelt und ausgeführt wird			
Fehlende oder unzureichende Umsetzung der Anforderungen an Sicherheit und Verfügbarkeit in den Anwendungen, um identifizierte Risiken angemessen zu berücksichtigen	AI2.4	◗ % der Anwendungssoftware-projekte, für die ein Qualitätssicherungsplan entwickelt und ausgeführt wird			
Fehlende oder unzureichende Konfigurations- und Implementierungsverfahren für zugekaufte Software, um diese an die eigenen Anforderungen anzupassen	AI2.5				

→

AI2 – Beschaffe und warte Anwendungssoftware					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Verfahren für wesentliche Upgrades bestehender Software, um diese in einer strukturierten und sicheren Weise zu aktualisieren	AI2.6	◗ % der Anwendungssoftware-projekte, für die ein angemessenes Review und eine Abnahme der Einhaltung von Entwicklungsstandards durchgeführt werden			◗ Stelle sicher, dass während Entwurf, Entwicklung und Implementierung der Status jeder Anforderung (einschließlich der abgelehnten Anforderungen) nachvollzogen werden kann und Änderungen von Anforderungen einem definierten Change-Management-Verfahren unterliegen. ◗ Entwickle eine Strategie und einen Plan für die Wartung von Anwendungssoftware.
Fehlende oder unzureichende Verfahren zur Entwicklung von Anwendungssoftware, um die Einhaltung der Vorgaben (Designspezifikationen, Entwicklungs- und Dokumentationsstandards, Qualitätsanforderungen und Autorisierung) sicherzustellen	AI2.7	◗ % der Anwendungssoftware-projekte, für die ein Qualitätssicherungsplan entwickelt und ausgeführt wird ◗ % der Anwendungssoftware-projekte, für die ein angemessenes Review und eine Abnahme der Einhaltung von Entwicklungsstandards durchgeführt werden ◗ Ø benötigte Zeit, um Funktionalität zu realisieren, basierend auf Messgrößen wie Function Points oder Lines of Code ◗ Ø benötigter Programmieraufwand zur Funktionalitätsrealisierung basierend auf Messgrößen wie Function Points oder Lines of Code			
Fehlende oder unzureichende Verfahren zu Software-Qualitätssicherung, um die in der Anforderungsdefinition und den Qualitätsrichtlinien und Verfahren der Organisation festgelegte Qualität zu erreichen	AI2.8	◗ % der Anwendungssoftware-projekte, für die ein Qualitätssicherungsplan entwickelt und ausgeführt wird			
Fehlender oder unzureichender Change-Management-Prozess in der Anwendungsentwicklung, um den Status von durchgeführten und abgelehnten Change Requests nachzuvollziehen	AI2.9				
Fehlende oder unzureichende Strategie und Planung für Wartung und Release von Anwendungssoftware, um Fehlerbehandlung und -behebung sowie Verbesserungen angemessen zu berücksichtigen	AI2.10				

AI3 – Beschaffe und warte technologische Infrastruktur					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender Beschaffungsplan für technologische Infrastruktur, um die bestehenden unternehmensweiten Anforderungen zu erfüllen	AI3.1	◗ Anzahl offener Beschaffungsanfragen	◗ % der Plattformen, die nicht mit der definierten IT-Architektur und den Technologiestandards abgestimmt sind ◗ Anzahl der nach ihrer Funktion verschiedenen Technologieplattformen im gesamten Unternehmen ◗ % der Infrastruktur-komponenten, bei denen der Beschaf-fungsprozess nicht eingehalten wurde ◗ Anzahl der nicht mehr oder bald nicht mehr unterstützten Infrastruk-turkomponenten	◗ Anzahl der von (bald) veralteter Infrastruktur unterstützten kritischen Geschäftsprozesse	◗ Entwickle eine Strategie und einen Plan für Wartung von Anwendungssoftware. ◗ Entwickle einen Plan für die Beschaffung, Implementierung und Wartung der technischen Infrastruktur, der die funktionalen und technischen Anforderungen erfüllt und im Einklang mit der unternehmensweiten technologischen Richtung steht. ◗ Implementiere im Rahmen der Konfiguration, Integration und Wartung von Hardware und Infrastruktursoftware Internal Controls sowie Maßnahmen zur Sicherheit und Prüfbarkeit. ◗ Entwickle eine Strategie und einen Plan für die Wartung der Infrastruktur und stelle sicher, dass Änderungen entsprechend des definierten Change-Management-Prozesses gesteuert ablaufen. ◗ Etabliere eine Entwicklungs- und Testumgebung, um die Überprüfung der Machbarkeit sowie Integrationstests von Infrastrukturkomponenten effizient und effektiv unterstützen zu können.
Fehlende oder unzureichende Maßnahmen zu internen Kontrollen, Sicherheit und Prüfbarkeit während der Konfiguration, Integration und Wartung von Hardware und Infrastruktursoftware, um Schutz und Verfügbarkeit von Infrastruk-turressourcen sicherzustellen	AI3.2	◗ Anzahl und Art der Notfalländerungen an Infrastrukturkomponenten			
Fehlende oder unzureichende Strategie und Planung für die Wartung der Infrastruktur, um Fehlerbehandlung und -behebung in einer strukturierten Weise durchzuführen	AI3.3	◗ Durchschnittliche Zeit zur Konfiguration von Infrastrukturkomponenten ◗ Anzahl und Art der Notfalländerungen an Infrastrukturkomponenten			
Fehlende oder unzureichende Entwicklungs- und Testumgebung, um in frühen Stadien Machbarkeits- und Integrationstests durchführen zu können	AI3.4	◗ Anzahl und Art der Notfalländerungen an Infrastrukturkomponenten			

AI4 – Ermögliche Betrieb und Verwendung					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Planung für operative Lösungen, um bei einer Einführung oder einem Upgrade eines automatisierten Systems oder neuer Infrastruktur alle technischen Aspekte, betrieblichen Möglichkeiten und erforderlichen Service-Levels zu identifizieren, zu dokumentieren und Verantwortungen zu definieren	AI4.1	◗ Zeitspanne zwischen Änderungen und Updates der Schulungs-, Verfahrens- und Dokumentations-unterlagen	◗ Anzahl der Zwischenfälle, die aufgrund mangelhafter Benutzer- und Betriebshandbücher sowie Schulungen verursacht worden sind ◗ Anzahl der vom Service Desk behandelten Schulungsanfragen ◗ % der Anwender/ Betreiamit den Schulungen und Dokumentationsunter-lagen zufrieden sind ◗ Verringerte Kosten für die Erstellung/Wartung der Benutzerdoku-mentation, Betriebs-verfahren und Schulungsunterlagen	◗ Anzahl der Applikationen, deren IT-Verfahren nahtlos in Geschäftspro-zesse integriert sind ◗ % der Geschäfts-prozesseigentümer, die mit den Anwender-schulungen und den Schulungsunterlagen zufrieden sind	◗ Entwickle einen Plan für die Einführung oder das Upgrade von Systemen, der alle technischen, betrieblichen und Nutzungsas-pekte umfasst. ◗ Stelle sicher, dass das notwendige Wissen für die Leistungserbringung und -qualität, Internal Controls und Administrations-prozesse der Anwendung an den verantwortlichen Fachbereich transferiert wird. ◗ Stelle sicher, dass dem Endbenutzer Wissen und Fertigkeiten zur effizienten Nutzung einer Anwendung vermittelt werden. ◗ Stelle sicher, dass das notwendige Wissen für den Betrieb und den technischen Support an die verantwortlichen Mitarbeiter transferiert wird.
Fehlender oder unzureichender Transfer von Wissen an das Fachbereichsmanagement, um diesem die Übernahme der Eigentümerschaft über die Anwendung und Daten sowie die Verantwortung für die Leistungs-erbringung und -qualität zu ermöglichen	AI4.2	◗ Stand der Schulungsteil-nahme der Anwender und Betreiber für jede Anwen-dung ◗ Anzahl der Applikationen mit angemessenen Anwender-schulungen und Schulungen des operativen Supports			
Fehlender oder unzureichender Transfer von Wissen an Endbenutzer, um ihnen die wirksame und wirtschaftliche Verwendung der Anwendung zur Unterstützung der Geschäfts-prozesse zu ermöglichen	AI4.3	◗ Stand der Schulungsteil-nahme der Anwender und Betreiber für jede Anwen-dung ◗ Verfügbarkeit, Vollständigkeit und Korrektheit der Anwender- und Betriebsdokumentation			
Fehlender oder unzureichender Transfer von Wissen an Betriebs- und Supportmitarbeiter, um ihnen die wirksame und wirtschaftliche Bereitstellung, Unterstützung und Wartung der Anwendung und der korrespondierenden Infrastruktur zu ermöglichen	AI4.4	◗ Verfügbarkeit, Vollständigkeit und Korrektheit der Anwender- und Betriebs-dokumentation ◗ Anzahl der Applikationen mit angemessenen Anwender-schulungen und Schulungen des operativen Supports			

AI5 – Beschaffe IT-Ressourcen					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Standards und Verfahren zur Beschaffung von IT-Ressourcen (Personal, Hardware, Software und Dienstleistungen), um die Erfüllung die Unternehmenserfordernisse sicherzustellen	AI5.1	◗ Zeitspanne zwischen einer Anfrage für die Beschaffung und der Unterzeichnung des Vertrages oder der Beschaffung ◗ Anzahl der termingetreu abgeschlossenen Beschafungsanfragen ◗ Anzahl der RFPs, die aufgrund der Lieferantenreaktionen zu verbessern waren ◗ Anzahl der auf RFP erhaltenen Antworten	◗ % der ursprünglichen Anforderungen, die durch die ausgewählte Lösung erfüllt werden ◗ % von Beschaffungen gemäß den feststehenden Beschaffungsrichtlinien und -verfahren ◗ Reduzierte Stückkosten der beschafften Güter oder Services	◗ Anzahl der Streitfälle im Zusammenhang mit Beschaffungsverträgen ◗ Reduzierte Beschaffungskosten ◗ % der wesentlichen Stakeholder, die mit den Lieferanten zufrieden sind	◗ Entwickle und führe Verfahren und Standards für die Beschaffung von IT-Infrastruktur, Hardware, Software sowie IT-Dienstleistungen in Einklang mit dem unternehmensweiten Einkaufsprozess und der Beschaffungsstrategie ein. ◗ Erarbeite ein Verfahren für den Abschluss, die Änderung oder Beendigung von Verträgen mit Lieferanten und stelle sicher, dass alle Verträge oder Änderungen rechtlich geprüft werden. ◗ Stelle sicher, dass die Lieferanten nach einem formalen und fairen Verfahren ausgewählt werden. ◗ Stelle sicher, dass die Interessen der Organisation bei vertraglichen Vereinbarungen über die Beschaffung von Software, IT-Infrastruktur, Entwicklungskapazitäten und IT-Services gewahrt sind (z. B. Eigentums- bzw. Lizenzrechte, Wartung, Gewährleistung, Service Level, Abnahmeverfahren, Schiedsgerichtsverfahren, Bedingungen für Upgrades, Hinterlegung des Quellcodes).
Fehlende oder unzureichende Verfahren zum Vertragsmanagement mit Lieferanten, um rechtliche, finanzielle, organisatorische Verantwortlichkeiten und Haftung abzudecken	AI5.2				
Fehlende oder unzureichende Verfahren zur Lieferantenauswahl, um eine optimale Eignung sicherzustellen	AI5.3	◗ Anzahl der Beschaffungsanfragen, welche durch die Liste bevorzugter Lieferanten erfüllt werden ◗ Anzahl der Lieferantenänderungen für die gleiche Art der beschafften Güter oder Services			
Fehlende oder unzureichende Verfahren zur Softwarebeschaffung, um entsprechende Rechte und Pflichten (wie z. B. Lizenzen definiert) zu berücksichtigen	AI5.4	◗ Anzahl der RFPs, die aufgrund der Lieferantenreaktionen zu verbessern waren ◗ Zeitspanne zwischen einer Anfrage für die Beschaffung und der Unterzeichnung des Vertrages oder der Beschaffung			

→

AI5 – Beschaffe IT-Ressourcen					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Verfahren zur Beschaffung von Entwicklungsressourcen, um entsprechende Rechte und Pflichten (wie z. B. Entwicklungsmethoden, Sprachen, Test- und Qualitätsmanagement-Prozesse) zu berücksichtigen	AI5.5	◗ Anzahl der RFPs, die aufgrund der Lieferantenreaktionen zu verbessern waren ◗ Zeitspanne zwischen einer Anfrage für die Beschaffung und der Unterzeichnung des Vertrages oder der Beschaffung			
Fehlende oder unzureichende Verfahren zur Beschaffung von Infrastruktur, Einrichtungen und entsprechenden Diensten, um entsprechende Rechte und Pflichten (wie z. B. Service Levels, Wartungsverfahren, Zugriffsschutz) zu berücksichtigen	AI5.6	◗ Anzahl der RFPs, die aufgrund der Lieferantenreaktionen zu verbessern waren ◗ Zeitspanne zwischen einer Anfrage für die Beschaffung und der Unterzeichnung des Vertrages oder der Beschaffung			

AI6 – Manage Changes					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender Change-Management-Prozess, um alle Anfragen für Changes (Anwendungen, Infrastruktur, etc.) zu behandeln	AI6.1	◗ % der Änderungen, die formale Änderungskontroll-prozesse befolgen ◗ Anzahl der unterschiedlichen Versionen jeder Geschäftsanwen-dungen oder Infrastruktur, die gewartet werden ◗ % der Änderungen, die aufgezeichnet und mit automatisierten Tools verfolgt werden ◗ Anzahl und Art der Patches an den Infrastrukturkompo-nenten	◗ Nacharbeit an Anwendungen, die durch mangelhafte Spezifikation der Änderungen entstanden ist ◗ Reduzierte Zeit und reduzierter Aufwand, um Änderungen durchführen zu können ◗ % der gesamten Änderungen, die Notfall-Changes sind ◗ % der nicht erfolgreichen Änderungen der Infrastruktur, die durch mangelhafte Spezifikation der Änderungen entstanden ist ◗ Anzahl der Änderungen, die nicht formal verfolgt oder berichtet werden oder nicht genehmigt sind	◗ Anzahl der Unterbrechungen oder Datenfehler, die durch mangelhafte Spezifikation oder unvollständige Beurteilung der Auswirkungen hervorgerufen ist	◗ Erarbeite ein formales Change-Management-Verfahren für die Behandlung von Changes an Anwen-dungen, Verfahren, Prozessen, System- oder Serviceparametern sowie an Basisplattformen. ◗ Stelle sicher, dass alle Anfragen für Changes in einer strukturierten Art und Weise auf deren Auswirkungen auf die operativen Systeme und deren Funktionalität hin beurteilt und deren Durchführungen genehmigt werden. ◗ Erstelle einen Prozess für die Definition, Aufnahme, Beurteilung und Genehmigung von Notfall-Changes, die nicht dem Standard-Change-Prozess unterliegen. ◗ Erstelle über den Status von Changes ein Nachverfolgungs- und Reportingsystem. ◗ Stelle sicher, dass nach der Durchführung von Changes die betreffende System- und Benutzerdokumentation sowie die Verfahrensbeschreibungen aktualisiert werden.
Fehlendes oder unzureichendes Verfahren zur Beurteilung (Kategorisierung, Priorisierung, Risikobewertung) von Change-Anfragen, um die Auswirkung aller Anfragen auf die operative Ebene zu beurteilen	AI6.2	◗ Verhältnis der akzeptierten zu abgelehnten Änderungsanfragen			
Fehlender oder unzureichender Prozess für Notfall-Changes, um kritische Änderungen außerhalb des regulären Change-Manage-ment-Prozesses durchzuführen	AI6.3	◗ Anzahl und Art der Notfalländerungen an Infrastrukturkomponenten			
Fehlender oder unzureichender Prozess zur Statusverfolgung und Berichterstattung von Änderungen, um Change Requester und Stakeholder über den Status der Änderung zu informieren	AI6.4	◗ % der Änderungen, die aufgezeichnet und mit automatisierten Tools verfolgt werden ◗ % der Änderungen, die formale Änderungskontroll-prozesse befolgen			
Fehlender oder unzureichender Change-Review-Prozess, um die entsprechende Aktualisierung von Dokumentationen und Verfahren nach einem Change sicherzustellen	AI6.5	◗ % der Änderungen, die aufgezeichnet und mit automatisierten Tools verfolgt werden ◗ % der Änderungen, die formale Änderungskontroll-prozesse befolgen			

AI7 – Installiere und akkreditiere Lösungen und Changes					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender Prozess zur Schulung von Betriebspersonal, um eine Einhaltung der Vorgaben bei Entwicklungs-, Implementierungs- und Änderungsprojekten sicherzustellen	AI7.1		◗ % der die Installation und Akkreditierungsprozess betreffenden Fehler, die während interner oder externer Audits gefunden wurden ◗ Nacharbeit nach Implementierung, die auf unzureichende Akzeptanztests zurückzuführen ist ◗ Service-Desk-Anrufe von Usern, die auf unzureichendes Training zurückzuführen sind ◗ Ausfallszeit der Anwendung oder Korrekturen an den Daten, die durch geeignete Tests hätten verhindert werden können	◗ % der Stakeholder, die mit der Dateninteg rität der neuen Systeme zufrieden sind ◗ % der Systeme, die bei der Messung des Nutzen im Post-Implementation Review den erwarteten Nutzen liefern	◗ Schule alle Mitarbeiter der betroffenen Abteilungen und das Betriebspersonal der IT gemäß den festgelegten Schulungs- und Implementierungsplänen. ◗ Erstelle basierend auf unternehmensweiten Standards einen Testplan, der die Rollen, Verantwortlichkeiten und Erfolgskriterien für die Testdurchführung beschreibt, und stelle sicher, dass der Plan genehmigt wird. ◗ Erstelle einen Implementierungsplan und hole das Einverständnis von den relevanten Parteien ein. ◗ Erstelle eine separate, sichere Testumgebung, die der künftigen Betriebsumgebung möglichst genau nachgebildet ist, und stelle sicher, dass die Testergebnisse dokumentiert werden. ◗ Stelle sicher, dass die System- und Datenmigration in die Entwicklungsmethoden des Unternehmens integriert sind. ◗ Stelle sicher, dass Changes entsprechend der definierten Testplanung vor der Übernahme in die Produktion unabhängig von der Entwicklung getestet werden. ◗ Stelle sicher, dass eine formale Evaluierung und Freigabe der Testergebnisse durch das Management der betroffenen User-Abteilung(en) und der IT als Teil der Abnahme oder abschließenden Qualitätssicherung verankert ist. ◗ Etabliere Verfahren zur Steuerung der Übergabe eines Systems von der Entwicklung, zum Test und in die Produktion, die vorsehen, dass vor Übernahme in die Produktion das Einverständnis aller Beteiligten eingeholt wird und dass ggfs. für einen definierten Zeitraum ein Parallelbetrieb stattfindet. ◗ Setze Verfahren zur zeitgerechten und korrekten Softwareverteilung oder Updates von freigegebenen Konfigurationseinstellungen ein. ◗ Automatisiere das Monitoring von Changes. ◗ Etabliere Verfahren zur Durchführung von Post-Implementation Reviews.
Fehlende oder unzureichende Testpläne zur Testvorbereitung, um Erfordernisse für Leistungs-, Stress-, Usability-, Pilot- und Sicherheitstests abzudecken	AI7.2	◗ % der Projekte mit einem dokumentierten und genehmigten Testplan ◗ Grad der Involvierung der Stakeholder in den Installations- und Akkreditierungsprozess			
Fehlende oder unzureichende Implementierungspläne, um einen angemessenen Release und Rollout inklusive eines ggf. notwendigen Fallbacks zu gewährleisten	AI7.3				
Fehlende oder unzureichende Testumgebung, um Changes produktionsnah zu testen	AI7.4	◗ % der Fehler, die während dem Qualitätssicherheitsreview der Installations- und Akkreditierungsfunktionen gefunden wurden			
Fehlende oder unzureichende Verfahren zur System- und Datenkonvertierung, um die Überführung von dem Alt- ins Neusystem sicherzustellen und die Konvertierung nachvollziehen zu können	AI7.5				
Fehlende oder unzureichende Tests von Changes in einer Testumgebung durch unabhängige Testgruppen, um die Korrektheit der Änderungen sicherzustellen	AI7.6	◗ % der Fehler, die während dem Qualitätssicherheitsreview der Installations- und Akkreditierungsfunktionen gefunden wurden ◗ Grad der Involvierung der Stakeholder in den Installations- und Akkreditierungsprozess			
Fehlender oder unzureichender finaler Akzeptanztest, um durch eine formale Evaluierung und Freigabe der Testergebnisse durch das Management der betroffenen User-Abteilung(en) und der IT die Korrektheit der Änderungen sowie die Einhaltung der Informationssicherheit sicherzustellen	AI7.7	◗ Grad der Involvierung der Stakeholder in den Installations- und Akkreditierungsprozess ◗ Anzahl der umgesetzten Änderungen ohne der erforderlichen Freigabe durch das Management			

→

AI7 – Installiere und akkreditiere Lösungen und Changes					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Verfahren zur Übergabe des Systems von der Entwicklung zum Test und dann in die Produktion, um im Einverständnis mit dem Systemeigner zu agieren und Altsysteme nicht verfrüht zu ersetzen	AI7.8	◗ Anzahl der umgesetzten Änderungen ohne der erforderlichen Freigabe durch das Management			
Fehlende oder unzureichende Verfahren zum Release von Software, um eine angemessene Paketerstellung, Verteilung, Statusverfolgung und Benachrichtigung der betroffenen Mitarbeiter zu gewährleisten	AI7.9	◗ Grad der Involvierung der Stakeholder in den Installations- und Akkreditierungsprozess ◗ Anzahl der umgesetzten Änderungen ohne der erforderlichen Freigabe durch das Management			
Fehlende oder unzureichende Steuerungsverfahren zur Verteilung und Updates von Configuration Items, um nur getestete und autorisierte Änderungen in die Produktion zu überführen	AI7.10				
Fehlende oder unzureichende Automatisierung des Systems für das Monitoring von Changes, um die Aufzeichnung und Verfolgung von Changes zu unterstützen	AI7.11				
Fehlende oder unzureichende Post-Implementation Reviews, um Änderungen nach Implementierung bezüglich Kostenwirksamkeit und vorgesehenem Nutzen zu bewerten	AI7.12	◗ Anzahl der durch den Post-Implementation Review gelernten Fakten			

DS1 – Definiere und manage Service Levels					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes »Service Level Management Framework«, um Service-Level-Prozesse, Organisation und Servicekatalog zu definieren	DS1.1	◗ Anzahl der formellen SLA Review Meetings mit den Geschäftsbereichen pro Jahr ◗ % der berichteten Service Levels	◗ Anzahl der erbrachten Services, die nicht im Katalog enthalten sind ◗ % der Services, die den Service Levels entsprechen ◗ % der gemessenen Service Levels	◗ % der Stakeholder, die zufrieden sind, dass die Dienstleistungserbringung die vereinbarten Service Levels erreichen ◗ % der Benutzer, die zufrieden sind, dass die Dienstleistungserbringung die vereinbarten Service Levels erreichen	◗ Schaffe ein Bewusstsein für die Notwendigkeit der Verwaltung von Service Levels. ◗ Definiere ein Framework für den Service-Level-Management-Prozess. ◗ Beschreibe in einem Servicekatalog die Service Level Agreements (SLAs), die Operating Level Agreements (OLAs) und Finanzierungsmittel. ◗ Definiere und vereinbare, basierend auf Kundenanforderungen und Fähigkeiten der IT, Service Level Agreements für alle entscheidenden IT-Services. ◗ Stelle sicher, dass Operating Level Agreements (OLAs) beschreiben, wie die Services technisch bereitgestellt werden, um die SLA(s) optimal zu unterstützen. ◗ Monitore kontinuierlich festgelegte Kriterien der Service Level Performance und berichte den Stakeholdern über die Erreichung der Service Levels. ◗ Etabliere ein regelmäßiges Review-Verfahren über Service Level Agreements und Underpinning Contracts mit internen und externen Leistungsanbietenden. ◗ Die zu erwartenden Service Levels sollen in der Phase der Definition von betrieblichen Anforderungen und Design der Anwendungen berücksichtigt werden. ◗ Definiere Kriterien für die Festlegung von Service Levels basierend auf der betrieblichen Kritikalität und Kriterien wie Verfügbarkeit, Verlässlichkeit, Performance, Wachstumskapazität, Anwenderunterstützung, Kontinuitätsplanung und Sicherheit.
Fehlende oder unzureichende Definition von Services, um Unternehmensanforderungen zu berücksichtigen	DS1.2	◗ Anzahl der formellen SLA Review Meetings mit den Geschäftsbereichen pro Jahr			
Fehlende oder unzureichende Definition von Service Level Agreements, um Kundenanforderungen und -verpflichtungen abzudecken.	DS1.3				
Fehlende oder unzureichende Spezifikation von OLAs, um die SLAs technisch zu unterstützen	DS1.4				
Fehlendes oder unzureichendes Monitoring und korrespondierender Berichterstattung von Services an Stakeholder, um Trends für Services zu identifizieren	DS1.5	◗ % der berichteten Service Levels ◗ % der automatisch berichteten Service Levels			
Fehlende oder unzureichende Reviews von SLAs, um sicherzustellen, dass Änderungen der Anforderungen berücksichtigt wurden und diese aktuell sind	DS1.6	◗ Anzahl der formellen SLA Review Meetings mit den Geschäftsbereichen pro Jahr ◗ Anzahl der verstrichenen Arbeitstage zwischen der Vereinbarung des Service Level Agreements mit dem Kunden und der Anpassung eines Service Levels			

DS2 – Manage Leistung von Dritten					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Identifikation und formelle Dokumentation aller Beziehungen mit Lieferanten, um erwartete Leistungen festzuhalten	DS2.1	◗ % der wichtigsten Lieferanten, die klar festgelegten Anforderungen und Service Levels unterliegen	◗ % der Hauptlieferanten, welche die klar definierten Anforderungen und Service Levels erfüllen ◗ Anzahl der formellen Streitfälle mit Lieferanten ◗ % der bemängelten Lieferantenrechnungen	◗ Anzahl der Anwenderbeschwerden hinsichtlich der vereinbarten Services ◗ % der Ankäufe, die einer konkurrenzbetonten Beschaffung unterstanden	◗ Identifiziere und dokumentiere alle Leistungen von Lieferanten und kategorisiere sie entsprechend Lieferantentyp, Bedeutung und Kritikalität. ◗ Definiere einen Prozess für das Beziehungsmanagement mit Lieferanten. ◗ Etabliere ein Risikomanagement für die Beziehung mit Lieferanten hinsichtlich Lieferfähigkeit, Vertragseinhaltung, Geheimhaltungsvereinbarungen und Konformität mit Sicherheitserfordernissen. ◗ Etabliere einen Prozess, um die Leistungserbringung zu überwachen, um sicherzustellen, dass der Lieferant die bestehenden Unternehmenserfordernisse erfüllt und weiterhin das Vertragswerk und die Service Level Agreements einhält. ◗ Definiere die erforderlichen KPIs und KGIs für die Beaufsichtigung der Leistungserbringung. ◗ Überprüfe regelmäßig die mit Drittparteien abgeschlossenen Verträge.
Fehlender oder unzureichender Prozess für das Lieferantenmanagement, um eine auf Transparenz basierende Verbindung zwischen Kunden und Lieferanten (z. B. durch SLAs) sicherzustellen	DS2.2	◗ % der wichtigsten Lieferanten, die klar festgelegten Anforderungen und Service Levels unterliegen ◗ Zufriedenheitsgrad der Geschäftsbereiche mit der Wirksamkeit der Kommunikation des Lieferanten ◗ Zufriedenheitsgrad des Lieferanten mit der Wirksamkeit der Kommunikation des Unternehmens ◗ % der wichtigsten Lieferanten, die gemonitort werden			
Fehlendes oder unzureichendes Lieferanten-Risikomanagement, um sicherzustellen, dass sich Verträge an Unternehmensstandards sowie rechtlichen, regulatorischen und vertraglichen Anforderungen orientieren	DS2.3	◗ % der wichtigsten Lieferanten, die klar festgelegten Anforderungen und Service Levels unterliegen			
Fehlender oder unzureichender Prozess für die Überwachung und Messung der Leistungserbringung durch die Lieferanten, um sicherzustellen, dass Lieferanten Unternehmenserfordernisse, Verträge und SLAs erfüllen und die Leistungen konkurrenzfähig sind	DS2.4	◗ % der wichtigsten Lieferanten, die gemonitort werden ◗ Zufriedenheitsgrad der Geschäftsbereiche mit der Wirksamkeit der Kommunikation des Lieferanten ◗ Anzahl der wesentlichen Ereignisse der Non-Compliance des Lieferanten			

DS3 – Manage Performance und Kapazität					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender Prozess für die Planung von Performance und Kapazität, um sicherzustellen, dass diese für den in den SLAs definierten Workload verfügbar sind	DS3.1	◗ % der Anlagen, die in Kapazitätenreviews enthalten sind ◗ % der Anlagen, die durch zentralisierte Tools überwacht werden	◗ Lastspitzen und Gesamtauslastungsrate ◗ % der Spitzenlast-zeiten, in denen die Zielauslastung übertroffen wird ◗ % der Antwortzeiten, die den SLAs nicht entsprechen ◗ Versagensrate von Transaktionen	◗ Anzahl der verlore-nen Stunden pro User und Monat aufgrund unzureichender Kapazitätsplanung ◗ Anzahl der kritischen Geschäftsprozesse, die nicht von einem definierten Service Availability Plan gedeckt werden	◗ Definiere einen Planungsprozess zur Überprüfung der Performance und Kapazität von IT-Ressourcen. ◗ Verwende geeignete Modellierungs-techniken für die derzeitige und künftige Performance, die Kapazität und den Durchsatz der IT-Ressourcen. ◗ Überprüfe die derzeitige Kapazität und Performance der IT-Ressourcen, um zu bestimmen, ob ausreichende Kapazität und Performance vorhanden ist, um die Leistungen entsprechend der Service Level Agreements zu erbringen. ◗ Minimiere das Risiko einer Service-unterbrechung aufgrund ungenügender Kapazität oder einer Performance-Verschlechterung mit regelmäßigen Vorhersagen. ◗ Stelle die benötigte Kapazität und Performance bereit unter Berücksichtigung von Aspekten wie normale Auslastung, Notfälle, Speicheranforderungen und Lebenszyklus von IT-Ressourcen. ◗ Das Management sollte sicherstellen, dass Kontinuitätspläne die Verfügbarkeit, Kapazität und Performance der einzelnen IT-Ressourcen angemessen berücksichtigen. ◗ Monitore laufend die Performance und Kapazität von IT-Ressourcen. ◗ Stelle die Performance- und Kapazitäts-anforderungen über den gesamten System-Lebenszyklus eines Services sicher und führe Trendanalysen durch. ◗ Stelle die erforderlichen Werkzeuge für die Messung der Systembenutzung, Performance und Kapazität. ◗ Definiere die Metriken für die Messung der IT-Performance und -Kapazität und stimme diese mit KGIs und KPIs für alle kritischen Geschäftsprozesse ab.
Fehlender oder unzureichender Prozess für die Überprüfung der vorhandenen Performance und Kapazität, um sicherzustellen, dass diese die in den SLAs definierten Leistungen erbringen können	DS3.2	◗ % der Anlagen, die in Kapazitätenreviews enthalten sind ◗ % der Anlagen, die durch zentralisierte Tools überwacht werden			
Fehlender oder unzureichender Prozess für Kapazitäts- und Performance-Prognosen, um das Risiko einer Serviceunterbrechung zu minimieren und überschüssige Kapazitäten zu ermitteln	DS3.3	◗ Häufigkeit von Performance- und Kapazitätsprognosen ◗ % der Anlagen, die in Kapazitätenreviews enthalten sind			
Fehlende oder unzureichende Berücksichtigung von Aspekten wie Auslastung, Notfälle, Speicheran-forderungen und Lebenszyklus von IT-Ressourcen, um die Verfügbar-keit von IT-Ressourcen sicherzu-stellen	DS3.4	◗ Häufigkeit von Performance- und Kapazitätsprognosen ◗ % der Anlagen, die durch zentralisierte Tools überwacht werden			
Fehlendes oder unzureichendes Monitoring der Performance und Kapazität von IT-Ressourcen, um IT-Leistung zu bewerten und die Verfügbarkeit im Rahmen des SLM zu berichten	DS3.5	◗ % der Anlagen, die in Kapazitätenreviews enthalten sind ◗ % der Anlagen, die durch zentralisierte Tools überwacht werden			

DS4 – Stelle den kontinuierlichen Betrieb sicher					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes Framework für IT-Kontinuität, um ein unternehmensweites Management der Geschäftskontinuität durch einen konsistenten Prozess zu unterstützen	DS4.1		◗ % der Verfügbarkeiten, die die SLAs erfüllen ◗ Anzahl von geschäftskritischen, auf IT angewiesenen Prozessen, die durch die IT-Notfallplanung nicht abgedeckt wurden ◗ % der Tests, die die Zielsetzungen bezüglich Wiederherstellung erreichen ◗ Häufigkeit der Service-unterbrechungen bei kritischen Systemen	◗ Anzahl der verlorenen Stunden pro User und Monat aufgrund von ungeplanten Ausfällen	◗ Entwickle ein Framework für IT-Kontinuität zur Unterstützung eines unternehmens-weiten Managements der Geschäftskonti-nuität. ◗ Lege die Organisationsstruktur für Kontinuitätsmanagement, Rollen, Aufgaben und Verantwortlichkeiten von internen und externen Dienstleistern, Strukturen für Dokumentation, Test und Ausführung der Wiederanlauf- und IT-Kontinuitätspläne fest. ◗ Entwickle basierend auf dem Framework IT-Kontinuitätspläne, die auf die Reduktion der Auswirkungen einer wesentlichen Unterbrechung auf die Schlüssel-Geschäftsfunktionen und -Prozesse ausgelegt sind. ◗ Lenke die Aufmerksamkeit auf die im IT-Kontinuitätsplan als am kritischsten definierte Elemente, um Ausfallsicherheit einzubauen und um Prioritäten für den Wiederanlauf festzulegen. ◗ Halte den IT-Kontinuitätsplan bei Durchführung von Changes aktuell. ◗ Teste den IT-Kontinuitätsplan regelmäßig, um sicherzustellen, dass alle IT-Systeme wirksam wiederhergestellt werden können, ◗ Stelle sicher, dass alle betroffenen Parteien regelmäßig Schulungen für die im Ereignis- oder Katastrophenfall anzuwendenden Verfahren sowie ihre Rollen und Verantwortlichkeiten erhalten. ◗ Plane die Aktionen für den Zeitraum, während die IT wiederhergestellt und die Services wieder aufgenommen werden.
Fehlende oder unzureichende IT-Kontinuitätspläne, um die Auswirkungen wesentlicher Unterbrechungen von Schlüssel-Geschäftsfunktionen und -Prozessen zu minimieren	DS4.2	◗ Schulungsstunden über die IT-Kontinuität pro Jahr und betroffenem IT-Mitarbeiter			
Fehlende oder unzureichende Fokussierung auf die in den IT-Kontinuitätsplänen als kritisch definierten Elementen, um Ausfallsicherheit wesentlicher IT-Ressourcen sicherzustellen und die Prioritäten für den Wiederanlauf festzulegen	DS4.3	◗ Schulungsstunden über die IT-Kontinuität pro Jahr und betroffenem IT-Mitarbeiter ◗ Häufigkeit von Reviews des IT-Kontinuitätsplans ◗ % der kritischen Infrastrukturkomponenten mit automatisierter Verfügbarkeitsüberwachung			
Fehlende oder unzureichende Unterstützung des IT-Managements bei der Steuerung von Changes, um sicherzustellen, dass der IT-Konti-nuitätsplan aktuell gehalten und Veränderungen der Verfahren und Verantwortlichkeiten klar und rechtzeitig kommuniziert werden	DS4.4	◗ Häufigkeit von Reviews des IT-Kontinuitätsplans ◗ Schulungsstunden über die IT-Kontinuität pro Jahr und betroffenem IT-Mitarbeiter			
Fehlende oder unzureichende Tests der IT-Kontinuitätspläne, um sicherzustellen, dass alle IT-Systeme wirksam wiederhergestellt werden können	DS4.5	◗ Zeitspanne zwischen den Tests von jeglichen Bestand-teilen des IT-Kontinuitätsplans			

→

DS4 – Stelle den kontinuierlichen Betrieb sicher					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Schulungen der in den IT-Kontinuitätsplänen beteiligten Mitarbeiter, um auf den Ereignis- und Katastrophenfall angemessen vorbereitet zu sein	DS4.6	◗ Schulungsstunden über die IT-Kontinuität pro Jahr und betroffenem IT-Mitarbeiter			◗ Lagere alle kritischen Backup-Medien, Dokumentationen und andere IT-Ressourcen, welche für den IT-Wiederanlauf und die Geschäftskontinuitätspläne notwendig sind, an einem entfernten Standort aus. ◗ Stelle die Kompatibilität von Hardware und Software sicher, um die archivierten Daten wiederherzustellen, periodisch zu testen und archivierte Daten aufzufrischen. ◗ Bestimme nach erfolgreichem Wiederanlauf der IT-Funktionen nach einem Unglück, ob das IT-Management Verfahren für die Beurteilung der Angemessenheit der Pläne und für deren dementsprechende Überarbeitung etabliert hat. ◗ Stelle eine Kommunikation des Managements über die Notwendigkeit der Planung für die Gewährleistung kontinuierlicher Services sicher. ◗ Nutze Good Practices der Systemverfügbarkeit und berücksichtige Benchmarking und die besten externen Praktiken. ◗ Stelle sicher, dass die Planungen für die Verfügbarkeit und für die Servicekontinuität abgestimmt sind. ◗ Stelle sicher, dass die Anforderungen für die Gewährleistung der Servicekontinuität durch die Anbieter und wesentliche Zulieferer gesichert werden. ◗ Stelle das Verständnis der Praktiken zur Eskalation durch die Beteiligten sicher. ◗ Messe die KGIs und KPIs für die Erreichung kontinuierlicher Services und nutze diese für die Planung der Servicekontinuität.
Fehlende oder unzureichende Verteilungsstrategie, um sicherzustellen, dass die IT-Kontinuitätspläne an geeignete Interessengruppen verteilt werden und bei Bedarf zur Verfügung stehen	DS4.7				
Fehlende oder unzureichende Definition von Maßnahmen (wie Aktivierung von Ausweichorten, Inbetriebnahme alternativer Verarbeitung, Kommunikation mit Kunden etc.), um eine angemessene Wiederherstellung des Normalbetriebs und einen Wiederanlauf von IT-Services zu sichern	DS4.8	◗ Schulungsstunden über die IT-Kontinuität pro Jahr und betroffenem IT-Mitarbeiter			
Fehlende oder unzureichende Auslagerung von Backup-Medien, Dokumentation und IT-Ressourcen an einen entfernten Ort, um die Durchführung der Maßnahmen für die Geschäftskontinuität und den IT-Wiederanlauf zu ermöglichen	DS4.9	◗ Schulungsstunden über die IT-Kontinuität pro Jahr und betroffenem IT-Mitarbeiter			
Fehlende oder unzureichende Review-Verfahren für die Beurteilung der Angemessenheit der Kontinuitätspläne nach einem tatsächlichen Notfall, um diese ggf. zu verbessern	DS4.10	◗ Häufigkeit von Reviews des IT-Kontinuitätsplans			

DS5 – Stelle Security von Systemen sicher					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes IT-Sicherheitsmanagement auf der höchsten organisatorischen Ebene, um die Aktivitäten zur IT-Sicherheit an den Unternehmensanforderungen auszurichten	DS5.1		◗ Anzahl und Art der vermuteten und wirklichen Zugangsverstöße ◗ Anzahl der Verstöße gegen die Funktionstrennung ◗ % der User, welche die Passwortstandards nicht einhalten ◗ Anzahl und Art von verhinderten bösartigen Codes	◗ Anzahl der Ereignisse mit Auswirkungen auf das Unternehmen ◗ Anzahl der Systeme, die den Sicherheitsanforderungen nicht entsprechen ◗ Dauer für die Bewilligung, Veränderung und Löschung von Zugangsberechtigungen	◗ Manage die IT-Sicherheit auf der höchstmöglichen organisatorischen Ebene und weise die Verantwortlichkeiten für die IT-Sicherheit eindeutig zu. ◗ Erstelle einen IT-Security-Plan für das Unternehmen und kommuniziere diesen an Stakeholder. ◗ Entwickle und implementiere ein Konzept für das Benutzer- und Berechtigungsmanagement. ◗ Stelle sicher, dass Antrag, Einrichtung, Ausstellung, Aufhebung, Änderung und Schließung von Benutzerkonten und zugehörige Benutzerberechtigungen durch die Benutzerkontenverwaltung behandelt werden. Ein Freigabeverfahren sollte darin enthalten sein, das den Daten- oder Systemeigner behandelt, der die Zugriffsberechtigungen bewilligt. Diese Verfahren sollten für sämtliche Benutzer, einschließlich Administratoren (privilegierte Benutzer), interne und externe Benutzer, für normale und für Notfalls-Changes Gültigkeit haben. ◗ Stelle sicher, dass die Umsetzungen der IT-Sicherheit getestet und proaktiv überwacht werden. ◗ Zertifiziere die IT-Sicherheit periodisch, um sicherzustellen, dass der genehmigte Sicherheitsgrad beibehalten wird. ◗ Etabliere eine Protokollierungs- und Monitoringfunktion für die frühzeitige Erkennung von ungewöhnlichen oder abnormalen Aktivitäten. ◗ Der Zugriff zur Protokollierungsinformation steht bezüglich Zugriffsrechten und Aufbewahrungsvorschriften in Einklang mit den Geschäftsanforderungen. ◗ Stelle sicher, dass die Charakteristika von möglichen Security Incidents klar definiert und kommuniziert werden, sodass Sicherheitsvorfälle korrekt durch den Incident oder Problem-Management-Prozess behandelt werden können.
Fehlender oder unzureichender Prozess, um den Informationsbedarf des Unternehmens in einen IT-Security-Plan zu überführen und daraus Sicherheitsrichtlinien, -verfahren und entsprechende Investitionen abzuleiten	DS5.2				
Fehlendes oder unzureichendes Identitätsmanagement, um alle Zugriffe eindeutig zu identifizieren und Benutzerberechtigungen für die Systeme und Daten an den Geschäftsbedürfnissen auszurichten	DS5.3	◗ Anzahl der Zugriffsberechtigungen, die autorisiert, widerrufen, gelöscht oder verändert wurden			
Fehlender oder unzureichender Prozess für das Management und Review von Benutzerkonten (u.a. inkl. Antrag, Einrichtung, Ausstellung, Änderung, Schließung), um die Angemessenheit der Benutzerkonten sicherzustellen	DS5.4	◗ Anzahl und Art von veralteten Benutzerkonten ◗ Anzahl der Zugriffsberechtigungen, die autorisiert, widerrufen, gelöscht oder verändert wurden			
Fehlendes oder unzureichendes Testen, Beobachten und Überwachen der IT-Sicherheit, um sicherzustellen, dass der genehmigte Sicherheitsgrad beibehalten wird	DS5.5	◗ Häufigkeit und Review der Art der Security Incidents, die überwacht werden sollen			
Fehlende oder unzureichende Definition von Security Incidents, um Sicherheitsvorfälle korrekt durch den Incident oder Problem-Management-Prozess zu behandeln	DS5.6	◗ Häufigkeit und Review der Art der Security Incidents, die überwacht werden sollen			

→

DS5 – Stelle Security von Systemen sicher					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender Schutz von Sicherheitseinrichtungen, um diese gegen Sabotage abzusichern	DS5.7	◗ % der kompromittierten und widerrufenen kryptografischen Schlüssel			◗ Stelle sicher, dass wichtige Sicherheitstechnologie gegen Sabotage abgesichert wird und dass Sicherheitsdokumentation nicht unnötigerweise veröffentlicht wird. ◗ Stelle sicher, dass technische Sicherheitsmaßnahmen und zugehörige Managementverfahren (z. B. Firewall, Sicherheits-Appliances, Netzwerksegmentierung und Intrusionserkennung) verwendet werden. ◗ Stelle sicher, dass sensitive Transaktionsdaten nur über einen vertrauenswürdigen Pfad oder ein Medium ausgetauscht werden, um die Authentizität des Inhalts, den Beweis der Aufgabe und des Empfangs und Nichtabstreitbarkeit der Quelle zu bieten. ◗ Sorge für ein angemessenes Sicherheitsbewusstsein im Unternehmen. ◗ Verwende Risikoanalysen als Grundlage der Sicherheitslösungen. ◗ Standardisiere die Anwenderidentifikation, Authentifizierung und Autorisierung. ◗ Führe die Sicherheitstests mithilfe standardisierter und formeller Prozesse durch, die zur Verbesserung der Sicherheit führen. ◗ Verknüpfe die IT-Sicherheit mit den betrieblichen Zielen. ◗ Plane und führe IT-Sicherheitsschulungen in den Fachbereichen durch und in der IT gemessen an betrieblichen Anforderungen und Risikoprofile. ◗ Definiere die KGIs und KPIs für das Sicherheitsmanagement als eine Grundlage für den kontinuierlichen Verbesserungsprozess. ◗ Beziehe die Anwender und Kunden vermehrt bei der Festlegung von Sicherheitsanforderungen und Sicherheitsfunktionen der Anwendungen in der Entwurfsphase. ◗ Etabliere formelle Verfahren und Werkzeuge für den Umgang mit Security Incidents. ◗ Führe periodische Sicherheitseinschätzungen des Prozesses durch. ◗ Kommuniziere angemessene Maßnahmen sofort und sorge für ihre Implementierung.
Fehlende oder unzureichende Verwaltung kryptografischer Schlüssel, um den Schutz der Schlüssel gegen Veränderung und unberechtigte Aufdeckung sicherzustellen	DS5.8	◗ % der kompromittierten und widerrufenen kryptografischen Schlüssel			
Fehlende oder unzureichende präventive, detektive und korrektive Maßnahmen (insb. Sicherheits-Patches und Virenschutz) in der gesamten Organisation, um den Schutz vor, die Erkennung und die Korrektur von bösartiger Software zu gewährleisten	DS5.9	◗ Häufigkeit und Review der Art der Security Incidents, die überwacht werden sollen			
Fehlende oder unzureichende Maßnahmen und Verfahren zur Netzwerksicherheit (wie z. B. Firewalls, Netzwerksegmentierung, IDS), um den Netzwerkzugriff zu bewilligen und den Informationsfluss zu steuern	DS5.10	◗ Häufigkeit und Review der Art der Security Incidents, die überwacht werden sollen ◗ Anzahl der nicht autorisierten IP-Adressen und Ports sowie der Typen des zurückgewiesenen Netzwerkverkehrs			
Fehlende oder unzureichende Schutzmaßnahmen beim Austausch sensitiver Daten, um die Authentizität des Inhalts und den Beweis der Aufgabe und des Empfangs zu bieten	DS5.11				

DS6 – Identifiziere und verrechne Kosten					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender Prozess zur Definition von Services, um Kosten innerhalb des Kostenmodells transparent auf IT-Services umzulegen und Service-Rechnungsgrößen zu bestimmen	DS6.1	◗ % der Kerngeschäftsverantwortlichen, die in die Bestimmung des Kostenmodells involviert waren ◗ % der Kosten, die automatisch/manuell verrechnet wurden	◗ % der Abweichung zwischen Budget, prognostizierten und aktuellen Kosten ◗ % der IT-Gesamtkosten, die nach dem vereinbarten Kostenmodell verrechnet wurden ◗ % der vom Fachbereich bestrittenen Kosten	◗ % der von der Geschäftsführung akzeptierten/ bezahlten IT-Service-Rechnungen ◗ Zeitliche Entwicklung der Stückkosten pro Service ◗ Zufriedenheit im Unternehmen (Umfrage) mit dem IT-Service-Kostenmodell	◗ Definiere die Aufgaben und die Verantwortlichkeiten für das Kostenmanagement für Informationsdienste. ◗ Identifiziere alle IT-Kosten und lege sie auf die IT-Services um, um ein transparentes Kostenmodell zu unterstützen. ◗ Verknüpfe IT-Services mit Geschäftsprozessen, sodass das Kerngeschäft die jeweiligen Servicerechnungsgrößen genau bestimmen kann. ◗ Zeichne die Ist-Kosten auf und weise diese entsprechend dem definierten Kostenmodell zu. ◗ Analysiere und berichte Abweichungen zwischen Plan- und Ist-Kosten entsprechend den unternehmensweiten Systemen zur Messung von Finanzzahlen. ◗ Lege basierend auf den definierten Services ein Kostenmodell fest, das direkte, indirekte und Gemeinkosten für Services berücksichtigt und das die Berechnung von Verrechnungssätzen je Service unterstützt. ◗ Mache die Verrechnung von Services für User nachvollziehbar, messbar und vorhersehbar. ◗ Überprüfe und benchmarke die Angemessenheit des Kostenverrechnungsmodells regelmäßig. ◗ Schaffe das notwendige Bewusstsein für die Identifikation und Zuordnung von Kosten. ◗ Verwende die Kosten für die Optimierung der Leistungen von IT-Ressourcen. ◗ Sorge dafür, dass das Management die KPIs und KGIs im Rahmen eines laufenden Verbesserungsprozesses überprüft.
Fehlendes oder unzureichendes IT-Rechnungswesen, um Abweichungen zwischen Plan- und Ist-Kosten festzustellen, zu analysieren und zu berichten	DS6.2	◗ % der Kosten, die automatisch/manuell verrechnet wurden			
Fehlendes oder unzureichendes Kostenmodell, das mit den unternehmerischen Kostenrechnungsverfahren übereinstimmt, um eine nachvollziehbare Kostenstruktur und angemessene Ressourcennutzung zu gewährleisten	DS6.3	◗ % der Kerngeschäftsverantwortlichen, die in die Bestimmung des Kostenmodells involviert waren			
Fehlende oder unzureichende Überprüfung des Kostenmodells, um die Angemessenheit und Sachlichkeit zu gewährleisten	DS6.4	◗ Häufigkeit der Überprüfung des Kostenverrechnungsmodells			

DS7 – Schule und trainiere User					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Identifikation von Schulungs- und Trainingsbedarf, um sicherzustellen, dass aktuelle und zukünftige Unternehmenserfordernisse beachtet werden	DS7.1	◗ Häufigkeit der Aktualisierungen des Schulungsplans ◗ Zeitspanne zwischen der Identifikation eines Schulungsbedarfs und dem Abhalten der Schulung	◗ Anzahl der Service Desk Calls für Schulungen oder zur Beantwortung von Fragen ◗ % der Zufriedenheit der Interessenvertreter mit den angebotenen Schulungen ◗ % der geschulten Mitarbeiter	◗ Gemessene Verbesserung der Mitarbeiterproduktivität als Ergebnis eines besseren Verständnisses der Systeme ◗ Erhöhte Benutzerzufriedenheit mit der Einführung von Services, Systemen oder neuen Technologien	◗ Definiere und implementiere ein umfassendes Ausbildungs- und Schulungsprogramm, das messbare Ergebnisse liefert. ◗ Institutionalisiere das Ausbildungs- und Schulungsprogramm und kommuniziere dieses an die Mitarbeiter und Manager. ◗ Identifiziere und dokumentiere den Schulungsbedarf. ◗ Entwickle und aktualisiere regelmäßig ein Curriculum für alle Zielgruppen von Mitarbeitern unter Berücksichtigung von: - derzeitige und künftige Unternehmenserfordernisse und -strategie, - unternehmensweite Werte (ethische Werte, Control, Sicherheitskultur etc.), - Einführung neuer IT-Infrastruktur und Software (Pakete und Anwendungen), - derzeitige Fertigkeiten, Kompetenzprofile, Bedarf an Zertifizierung sowie - Schulungsmethoden (z. B. Klassenraum, webbasierend), Größe der Zielgruppe, Erreichbarkeit und Zeitvorgaben. ◗ Identifiziere basierend auf dem festgestellten Schulungs- und Trainingsbedarf Zielgruppen und deren Mitglieder, wirksame Schulungsmethoden, Lehrkräfte, Trainer und Mentoren. ◗ Ernenne Trainer und organisiere zeitgerecht Schulungseinheiten. ◗ Beurteile die Vermittlung der Schulungs- und Trainingsinhalte nach dem Abschluss hinsichtlich Relevanz, Qualität, Wirksamkeit, Erfassen und Behalten des Wissens, Kosten und Nutzen. ◗ Verwende die Ergebnisse dieser Beurteilung als Input für die künftige Festlegung von Curricula und Trainingseinheiten. ◗ Nutze die Ausbildungen und Schulungen als entscheidende Komponenten der beruflichen Laufbahn der Mitarbeiter.
Fehlende oder unzureichende Abhaltung von Trainings und Schulungen, um den identifizierten Bedarf zu decken	DS7.2	◗ Häufigkeit der Aktualisierungen des Schulungsplans ◗ Zeitspanne zwischen der Identifikation eines Schulungsbedarfs und dem Abhalten der Schulung			
Fehlende oder unzureichende Evaluierung von Schulungen, um eine effektivere Schulung für folgende Trainingseinheiten zu ermöglichen	DS7.3	◗ Häufigkeit der Aktualisierungen des Schulungsplans			

DS8 – Manage den Service Desk und Incidents					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Einrichtung eines Service Desks, um eine Bearbeitung und Eskalation aller Anrufe, Incidents, Service- und Informationsanfragen gemäß den SLAs zu gewährleisten	DS8.1	◗ % der Ereignisse und Serviceanfragen, die reportet und mittels automatisierter Tools protokolliert wurden ◗ Anzahl der Schulungstage pro Service-Desk-Mitarbeiter pro Jahr ◗ Rückstand nicht gelöster Anfragen ◗ Anzahl der pro Service-Desk-Mitarbeiter pro Stunde bearbeiteten Anrufe	◗ % der direkten Lösungen basierend auf der Gesamtzahl der Anfragen ◗ % der erneut geöffneten Incidents ◗ Anteil der abgebrochenen Calls ◗ Durchschnittliche Dauer der Incidents nach Schweregrad ◗ Durchschnittliche Reaktionszeit auf Telefon und E-Mail-/Web-Anfragen	◗ Benutzerzufriedenheit mit dem Erst-Support (Service Desk oder Knowledge Base) ◗ % der innerhalb einer vereinbarten/akzeptablen Zeitspanne gelösten Incidents	◗ Sorge für ein umfassendes Verständnis über den Nutzen eines Incident-Management-Prozesses auf allen Ebenen des Unternehmens. ◗ Definiere und etabliere einen Incident-Management-Prozess. ◗ Stelle die erforderlichen Werkzeuge und Techniken wie eine zentrale Wissensdatenbank zur Verfügung. ◗ Richte eine Service-Desk-Funktion als Schnittstelle von Usern zur IT zur Aufnahme, Kommunikation, Weitergabe und Analyse aller Anrufe, gemeldeten Incidents, Service- und Informationsanfragen ein. ◗ Sorge dafür, dass basierend auf den vereinbarten Service Levels Verfahren für die Überwachung und die Eskalation umgesetzt werden, welche die Klassifikation und Priorisierung aller gemeldeten Vorfälle als Incident, Serviceanfrage oder Informationsanfrage erlauben. ◗ Messe die Zufriedenheit des Endbenutzers mit der Qualität des Service Desks und der IT-Services. ◗ Etabliere eine Funktion und ein System zur Aufzeichnung und Verfolgung von Anrufen, Incidents, Serviceanfragen und Informationsbedürfnissen, die von den Prozessen wie Incident-Management, Problem-Management, Change-Management, Kapazitäts- und Verfügbarkeitsmanagement genutzt werden kann. ◗ Klassifiziere Incidents entsprechend einer Geschäfts- und Servicepriorität und übergebe diese dem geeigneten Team zur Behandlung. ◗ Informiere die Kunden über den Status ihrer Anfragen.
Fehlendes oder unzureichendes System zur Aufzeichnung und Verfolgung von Anrufen, Incidents, Service- und Informationsanfragen, um Incidents gemäß ihrer Prioritäten zu klassifizieren, an das Problem Management weiterzugeben und die Kommunikation mit dem Kunden zu ermöglichen	DS8.2	◗ % der Ereignisse und Serviceanfragen, die reportet und mittels automatisierter Tools protokolliert wurden ◗ Anzahl der pro Service-Desk-Mitarbeiter pro Stunde bearbeiteten Anrufe			
Fehlende oder unzureichende Verfahren zur Eskalation von Incidents, um eine Überwachung des Incidents und Implementation von Workarounds gemäß den SLAs für den Nutzer zu gewährleisten	DS8.3	◗ Rückstand nicht gelöster Anfragen ◗ % der Ereignisse, die einen Vor-Ort-Support benötigen (Field Support, persönlicher Besuch)			
Fehlende oder unzureichende Verfahren zur Schließung von Incidents, um Incidents zeitnah zu erledigen und eine Bestätigung der Kundenakzeptanz einzuholen	DS8.4	◗ Rückstand nicht gelöster Anfragen			
Fehlende oder unzureichende Berichtserstellung, um eine geeignete Fehler- und Trendanalyse sowie eine stetige Verbesserung des Service zu ermöglichen	DS8.5	◗ Rückstand nicht gelöster Anfragen			

→

DS8 – Manage den Service Desk und Incidents					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
					◗ Erstelle Verfahren für den Service Desk, sodass nicht sofort lösbare Incidents angemessen, entsprechend den in den SLAs definierten Grenzen, eskaliert und, wo anwendbar, entsprechende Workarounds angeboten werden. ◗ Stelle sicher, dass die Eigentümerschaft von Incidents und deren Überwachung während des gesamten Lebenszyklus beim Service Desk verbleiben, unabhängig davon, welche Gruppe der IT an der Lösung arbeitet. ◗ Erstelle Verfahren für das zeitnahe Monitoring der Erledigung von Kundenanfragen. ◗ Sorge dafür, dass nach der Behebung eines Incidents der Service Desk die zugrunde liegende Ursache (falls bekannt) aufzeichnet und bestätigt, dass die getroffene Handlung vom Kunden akzeptiert wurde. ◗ Erstelle Berichte der Aktivitäten des Service Desks, um dem Management zu ermöglichen, die Leistungserbringung und Antwortzeiten zu messen und Trends oder wiederkehrende Probleme zu identifizieren, sodass der Service kontinuierlich verbessert werden kann. ◗ Definiere KPIs und KGIs für die Leistung der Benutzerunterstützung und nutze diese für eine kontinuierliche Verbesserung und den Vergleich mit anderen Unternehmen.

DS9 – Manage die Konfiguration					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes Repository aller relevanten Configuration Items, um nach einem vollzogenen Change die Änderungen durch eine Dokumentation nachzuvollziehen oder zur vorherigen Version zurückkehren zu können	DS9.1	◗ Durchschnittliche Zeitspanne (Verzögerung) zwischen Identifikation einer Abweichung und deren Richtigstellung ◗ Anzahl der Abweichungen in Bezug auf unvollständige oder fehlende Konfigurationsinformation	◗ Anzahl der festgestellten Abweichungen zwischen dem Konfigurations-Repository und der tatsächlichen Anlagenkonfiguration ◗ % der gekauften und im Repository nicht ausgewiesenen Lizenzen	◗ Anzahl der Business-Compliance-Probleme verursacht durch nicht korrekte Konfiguration von Anlagen	◗ Erstelle eine zentrale Sammlung (engl.: repository) aller relevanten Informationen über Configuration Items. Dieses Repository umfasst Hardware, Anwendungssoftware, Middleware, Parameter, Dokumentation, Verfahren und Werkzeuge. ◗ Bewahre eine Referenzversion der Configuration Items für jedes System und alle Services auf, um nach Changes wieder dazu zurückkehren zu können. ◗ Erstelle Verfahren für: - Identifikation von Configuration Items und deren Attribute, - Aufzeichnung neuer, modifizierter und gelöschter Configuration Items, - Identifikation und Wartung der Beziehungen zwischen Configuration Items im Configuration Repository, - Update bestehender Configuration Items im Konfigurations-Repository und - Verhinderung der Berücksichtigung nichtautorisierter Software. ◗ Überprüfe und verifiziere regelmäßig – wo notwendig unter Verwendung von entsprechenden Werkzeugen – den Status der Configuration Items, um die Integrität der derzeitigen und historischen Konfigurationsdaten zu bestätigen und mit der effektiven Situation zu vergleichen. ◗ Verwende automatisierte Hilfsmittel für die automatische Informationsweitergabe (engl.: push technology), um Standards durchzusetzen und die Stabilität zu verbessern. ◗ Setze die Regeln zur Begrenzung der Installation nicht freigegebener Software um. ◗ Sorge für eine vollständige Integration der in gegenseitiger Beziehung stehenden Prozesse. ◗ Überprüfe periodisch anhand der Policy für die Verwendung von Software die Existenz von privater oder nichtlizenzierter Software oder anderer Software, die gültigen Lizenzvereinbarungen widerspricht. ◗ Plane und führe eine Schulung der beteiligten Mitarbeiter durch. ◗ Korrigiere die Abweichungen und erstelle die diesbezüglichen Berichte.
Fehlende oder unzureichende Identifikation und Wartung von Configuration Items, um eine angemessene Autorisierung und Aufzeichnung aller Aktionen am Konfigurations-Repository zu ermöglichen	DS9.2	◗ Anzahl der Abweichungen in Bezug auf unvollständige oder fehlende Konfigurationsinformation			
Fehlendes oder unzureichendes Review der Integrität der Configuration Items, um Fehler und Abweichungen (insb. hinsichtlich der Lizenzvereinbarungen) zu berichten und zu korrigieren	DS9.3	◗ Anzahl der Abweichungen in Bezug auf unvollständige oder fehlende Konfigurationsinformation ◗ % der Configuration Items in Einklang mit den Service Levels für Performance, Sicherheit und Verfügbarkeit			

DS10 – Manage Probleme					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Prozesse zur Meldung und Klassifikation von Problemen, um diese dem Support-Personal zuweisen zu können	DS10.1	◗ Durchschnittliche Dauer zwischen der Erfassung eines Problems und der Identifizierung der zugrunde liegenden Ursache	◗ % der aufgezeichneten und nachverfolgten Probleme ◗ % der wiederkehrenden Probleme (innerhalb eines Zeitraums), geordnet nach deren Schwere ◗ % der Probleme, die innerhalb des geforderten Zeitraums gelöst werden ◗ Anzahl der offenen/ neuen/geschlossenen Probleme, geordnet nach deren Schwere ◗ Mittelwert und Standardabweichung der Zeitspanne zwischen Identifizierung und Lösung von Problemen ◗ Mittelwert und Standardabweichung der Zeitspanne zwischen Lösung und Schließen von Problemen	◗ Anzahl der wiederkehrenden Probleme mit Einfluss auf die Geschäftstätigkeit ◗ Anzahl der durch betriebliche Probleme hervorgerufenen Unterbrechungen der Geschäftstätigkeit	◗ Erstelle Prozesse zur Meldung und Klassifikation von Problemen, welche als Teil des Incident-Managements identifiziert wurden. ◗ Sorge dafür, dass eine Klassifizierung von Problemen nach Kategorie, Auswirkungen, Dringlichkeit und Priorität stattfindet. ◗ Sorge dafür, dass die identifizierten Probleme dem organisatorisch verantwortlichen Mitarbeiterkreis zugeordnet werden. ◗ Das Problem-Management-System sollte angemessene Prüfspuraufzeichnungen bieten, welche die Nachverfolgung, Analyse und Bestimmung der zugrunde liegenden Ursache (engl.: root cause) aller gemeldeten Probleme ermöglichen. ◗ Bei einem Problemlösungsverfahren sind folgende Informationen relevant: - alle verbundenen Konfigurationselemente - ungelöste Probleme und Ereignisse - bekannte und vermutete Fehler ◗ Während des gesamten Lösungsprozesses sollte das Problem-Management regelmäßig vom Change-Management Berichte über den Fortschritt in der Lösung von Problemen und Fehlern erhalten. ◗ Das Problem-Management sollte die andauernden Auswirkungen von Problemen und bekannten Fehlern (engl.: known errors) auf die User Services erhalten. ◗ Für den Fall, dass die Auswirkungen wesentlich werden, sollte das Problem-Management das Problem eskalieren, allenfalls an ein entsprechendes Gremium verweisen, um die Priorität der Änderungsanfrage (engl.: request for change = RFC) zu erhöhen oder um, falls notwendig, einen dringenden Change zu implementieren. ◗ Fortschritt der Problemlösung sollte gegen das SLA gemonitort werden. ◗ Setze ein Verfahren zum Abschluss von Problemaufzeichnungen entweder nach der Bestätigung einer erfolgreichen Beseitigung des bekannten Fehlers oder nach einer Übereinkunft mit dem Fachbereich, wie man das Problem alternativ lösen könnte, ein.
Fehlende oder unzureichende Verfahren zur Problemverfolgung und -lösung, um Problemursachen und -auswirkungen zu analysieren, zu berichten und gegebenenfalls zu eskalieren	DS10.2	◗ % der Probleme, für die eine Analyse der zugrunde liegenden Ursache gemacht wurde ◗ Durchschnittliche Dauer zwischen der Erfassung eines Problems und der Identifizierung der zugrunde liegenden Ursache ◗ Häufigkeit der Berichte oder Aktualisierungen über laufende Probleme, basierend auf der Schwere der Probleme			

→

DS10 – Manage Probleme					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes Verfahren für den Abschluss von Problemen, um deren Lösung zu dokumentieren und diese geregelt abzuschließen	DS10.3				◗ Um ein wirksames Management von Problemen und Incidents sicherzustellen, integriere die in Beziehung stehenden Prozesse Change-, Configuration- und Problem-Management. ◗ Verfolge, wie viel Aufwand in notfallartige Korrekturen anstelle von Maßnahmen zur Verbesserung des Kerngeschäfts gesteckt wird, und verbessere diese Prozesse, um Probleme zu minimieren. ◗ Der Problem-Management-Prozess soll auf allen Unternehmensebenen verstanden werden. Die Aufgaben und Kompetenzen sind klar definiert und zugewiesen. Methoden und Verfahren sind dokumentiert, kommuniziert und auf ihre Wirksamkeit hin gemessen. ◗ Die Mehrzahl der Probleme wird ermittelt, aufgezeichnet, in einem Bericht festgehalten und Lösungen sind initiiert. Know-how und Fachwissen werden gepflegt, aufrechterhalten und weiterentwickelt. ◗ Der Problem-Management-Prozess soll zu einem zukunftsweisenden und proaktiven Prozess entwickelt werden und einen Beitrag zur Realisierung der IT-Ziele leisten. ◗ Die Aufzeichnung, Berichterstattung über und Analyse von Problemen und deren Lösung sollten automatisch und unter vollständiger Integration in das Konfigurationsdaten-Management stattfinden. ◗ KPIs und KGIs sollen konsistent gemessen werden. ◗ Die meisten Systeme sollen mit automatischen Erkennungs- und Warnmechanismen ausgestattet, kontinuierlich verfolgt und bewertet werden. ◗ Der Problem-Management-Prozess soll in Hinblick auf eine kontinuierliche Verbesserung auf Grundlage der KPIs und KGIs analysiert und den betroffenen Stakeholdern darüber berichtet werden.
Fehlende oder unzureichende Integration von den in Beziehung stehenden Prozessen Change-, Configuration- und Problem-Management, um ein wirksames Management von Problemen und Incidents sicherzustellen und eine Fehlerminimierung zu erreichen	DS10.4	◗ Häufigkeit der Berichte oder Aktualisierungen über laufende Probleme, basierend auf der Schwere der Probleme			

DS11 – Manage Daten					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Datenmanagement-Prozesse, um eine effektive Distribution und Bearbeitung von Daten und Dokumenten, die am Kerngeschäft ausgerichtet sind, zu sichern	DS11.1		◗ % der erfolgreichen Wiederherstellung von Daten ◗ Anzahl von Vorfällen, wo sensitive Daten wiederhergestellt wurden, nachdem die Medien bereits entsorgt worden sind ◗ Anzahl von Betriebsunterbrechungen oder Vorfällen bezüglich Datenintegrität, die durch unzureichende Speicherkapazitäten hervorgerufen worden sind	◗ Vorkommnisse des Unvermögens der Wiederherstellung von Daten, die für Geschäftsprozesse kritisch sind ◗ Benutzerzufriedenheit mit der Verfügbarkeit von Daten ◗ Vorfälle der Nichteinhaltung von Gesetzen aufgrund von Fällen mit dem Speicherungsmanagement	◗ Erstelle Vorkehrungen, um sicherzustellen, dass vom Kerngeschäft erwartete Quelldokumente erhalten werden, alle vom Kerngeschäft erhaltenen Daten verarbeitet werden, der gesamte vom Kerngeschäft benötigte Output vorbereitet und abgeliefert wird und dass Anforderungen für den Wiederanlauf und die nochmalige Verarbeitung unterstützt werden. ◗ Definiere und setze Verfahren für die Datenspeicherung und -archivierung ein, sodass Daten im Zugriff sind und verwendbar bleiben. ◗ Die Verfahren sollten Anforderungen hinsichtlich Wiederauffindung, Kostengünstigkeit, kontinuierliche Integrität und Sicherheit berücksichtigen. ◗ Entwickle Speicherungs- und Aufbewahrungsvorkehrungen, um gesetzliche, regulatorische und Unternehmenserfordernisse für Dokumente, Daten, Archive, Programme, Berichte und (eingehende und ausgehende) Meldungen sowie die für deren Verschlüsselung und Authentifizierung verwendeten Daten einzuhalten. ◗ Definiere und setze Verfahren zum Unterhalt eines Inventars von lokal vorhandenen Datenträgern ein und stelle deren Verwendbarkeit und Integrität sicher. ◗ Verfahren sollten für ein zeitgerechtes Review und Abklärung aller gefundenen Differenzen sorgen. ◗ Definiere und setze Verfahren ein, die den Zugriff auf sensitive Informationen und Software von Geräten oder Datenträgern verhindern, wenn diese entsorgt oder einem anderen Zweck übertragen werden. Solche Verfahren sollten sicherstellen, dass als gelöscht markierte oder zur Entsorgung bestimmte Daten nicht wieder gewonnen werden können.
Fehlendes oder unzureichendes Verfahren für die Datenspeicherung und -archivierung, um Daten im Bedarfsfall abrufbar zu halten und bei ihrer Sicherung die gesetzlichen, regulatorischen und Unternehmensanforderungen einzuhalten	DS11.2	◗ Frequenz der Überprüfung von Sicherungsmedien ◗ Durchschnittliche Zeit für die Wiederherstellung von Daten			
Fehlendes oder unzureichendes Inventar von lokalen Datenträgern, um Daten effizient aufzufinden und für ein zeitgerechtes Review und Abklärung aller gefundenen Differenzen zu sorgen	DS11.3				
Fehlende oder unzureichende Verfahren zur Entsorgung von sensitiven Informationen und Software, um sicherzustellen, dass zur Entsorgung vorgesehene Daten nicht wiedergewonnen werden können	DS11.4				

→

DS11 – Manage Daten					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Backup-Verfahren und Recovery Tests, um die Geschäftsanforderungen und Anforderungen aus den Kontinuitätsplänen zur Wiederherstellung von Daten im Notfall zu ermöglichen	DS11.5	◗ Frequenz der Überprüfung von Sicherungsmedien ◗ Durchschnittliche Zeit für die Wiederherstellung von Daten			◗ Definiere und setze Verfahren für Sicherung und Wiederherstellung von Anwendungen, Daten und Dokumentation in Übereinstimmung mit den Geschäftsanforderungen und dem Kontinuitätsplan ein. ◗ Verifiziere die Einhaltung von Backup-Verfahren, die Fähigkeit sowie die notwendige Zeit für eine erfolgreiche und komplette Wiederherstellung. ◗ Teste Backup-Medien und den Wiederherstellungsprozess. ◗ Entwickle Vorkehrungen, um Sicherheitsanforderungen in Bezug auf Empfang, Verarbeitung, physische Speicherung und Ausgabe von Daten und sensitiven Meldungen zu identifizieren und umzusetzen. Dies umfasst physische Aufzeichnungen, Datenübermittlung und alle ausgelagerte Datenspeicherung. ◗ Die KGIs und KPIs werden mit den Kunden vereinbart, mit den Geschäftszielen verknüpft und durch ein klar definiertes Verfahren konsistent überwacht. ◗ Die Gelegenheiten für die Verbesserung werden fortlaufend erweitert. Die Schulungen für die Mitarbeiter des Datenmanagements sind institutionalisiert.
Fehlendes oder unzureichendes Datensicherheitsmanagement, um die Sicherheitsanforderungen an Empfang, Verarbeitung, physische Speicherung und Ausgabe von Daten zu gewährleisten	DS11.6				

DS12 – Manage die physische Umgebung					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Verfahren für die Auswahl von physischen Standorten für IT-Systeme, um Risiken von natürlichen und durch Menschen hervorgerufene Katastrophen zu identifizieren und die mit der Unternehmensstrategie verbundene Technologiestrategie zu unterstützen	DS12.1	◗ % des Personals, das in Maßnahmen bezüglich Safety, Sicherheit und der Einrichtungen geschult ist ◗ Anzahl von risikomindernden Überprüfungen, die im letzten Jahr durchgeführt worden sind	◗ Anzahl der durch Verletzungen oder Ausfälle der physischen Sicherheit hervorgerufenen Vorfälle ◗ Anzahl der Vorfälle mit autorisiertem Zugang zu Computereinrichtungen	◗ Stillstandzeit aufgrund von Vorfällen bezüglich der physischen Umgebung ◗ Anzahl der durch die physische Umgebung verursachten Verletzungen ◗ Durch Vorfälle bezüglich der physischen Umgebung entstandene Sicherheitsgefährdung	◗ Definiere und wähle die physischen Standorte für IT-Ausrüstungen aus, um die mit der Unternehmensstrategie verbundene Technologiestrategie zu unterstützen. ◗ Auswahl und Entwurf des Layouts eines Standortes sollten die Risiken von natürlichen und durch Menschen hervorgerufene Katastrophen einbeziehen und relevante Gesetze und Bestimmungen für Betriebsgesundheit und Safety berücksichtigen. ◗ Definiere und implementiere den Unternehmenserfordernissen entsprechende Maßnahmen zur physischen Sicherheit. ◗ Maßnahmen sollten unter anderem Layout und Perimeter des Sicherheitsbereichs, Sicherheitszonen, Standort kritischer Ausrüstung sowie Versand- und Anlieferungszonen umfassen. ◗ Halte insbesondere ein unauffälliges Profil bezüglich der Präsenz des kritischen IT-Betriebs. ◗ Verantwortlichkeiten für die Überwachung und Verfahren für Berichterstattung und Lösung von Incidents der physischen Sicherheit müssen aufgestellt werden. ◗ Entwickle und implementiere Verfahren für die dem Unternehmensbedarf inklusive Notfällen entsprechende Erteilung, Einschränkung und Zurücknahme von Zutritt zu Gelände, Gebäuden und Arbeitsbereichen. ◗ Der Zugang zu Gelände, Gebäuden und Arbeitsbereichen sollte begründet, genehmigt, protokolliert und überwacht werden. Dies gilt für alle Personen, die das Gelände betreten, inklusive Personal, temporäres Personal, Kunden, Lieferanten, Besucher oder andere Drittparteien. ◗ Entwickle und implementiere Maßnahmen zum Schutz gegen Umweltfaktoren. ◗ Spezielle Ausrüstung und Geräte zur Überwachung und Steuerung der Umwelt sollten installiert sein.
Fehlende oder unzureichende physische Schutzmaßnahmen, um den Sicherheitsbedarf u.a. durch die Definition von Sicherheitsbereichen, Versand- und Anlieferungszonen, Verantwortlichkeiten und Verfahren zur Berichterstattung zu decken	DS12.2	◗ % des Personals, das in Maßnahmen bezüglich Safety, Sicherheit und der Einrichtungen geschult ist ◗ Anzahl von risikomindernden Überprüfungen, die im letzten Jahr durchgeführt worden sind ◗ Frequenz von physischen Risikobewertungen und -überprüfungen			
Fehlende oder unzureichende Verfahren für den Zutritt und dessen Überwachung, um den Unternehmensbedarf inkl. der Notfallpläne zu decken und den Zutritt zu protokollieren	DS12.3				
Fehlende oder unzureichende Verfahren zur Überwachung und Steuerung der Umwelt, um sich gegen Umwelteinflüsse zu schützen	DS12.4	◗ Anzahl von risikomindernden Überprüfungen, die im letzten Jahr durchgeführt worden sind ◗ Frequenz von physischen Risikobewertungen und -überprüfungen			

→

DS12 – Manage die physische Umgebung					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes Management von physischen Einrichtungen, um Gesetzen und Unternehmenserfordernissen zu entsprechen	DS12.5	◗ Anzahl von risikomindernden Überprüfungen, die im letzten Jahr durchgeführt worden sind ◗ Frequenz von physischen Risikobewertungen und -überprüfungen			◗ Manage Einrichtungen, inklusive Strom- und Kommunikationsausrüstung entsprechend Gesetzen und Bestimmungen, technischen und Unternehmenserfordernissen, Spezifikationen von Anbietern und Gesundheits- und Safety-Richtlinien. ◗ Die für die Einrichtungen definierten Strategien und Standards sollen an den Verfügbarkeitszielen der IT-Dienste ausgerichtet und in die Business-Continuity-Planung und das Krisenmanagement integriert werden. ◗ Schule das in den Einrichtungen tätige Personal vollständig für Notsituationen ebenso wie für Gesundheits- und Safety-Praktiken. ◗ Standardisierte Kontrollmechanismen sollen eingesetzt werden, um den Zugang zu Einrichtungen zu beschränken sowie die Einflussfaktoren auf Umgebung und Safety zu adressieren. ◗ Das Management soll die Wirksamkeit der Sicherheitsmaßnahmen und die Einhaltung etablierter Standards überwachen. ◗ Das Management soll KPIs und KGIs zur Messung der Verwaltung der IT-Umgebung etablieren und die Einrichtungen kontinuierlich optimieren. ◗ Sämtliche Einrichtungen sollen inventarisiert und gemäß dem laufenden Risikomanagement-Prozess des Unternehmens klassifiziert werden.

DS13 – Manage den Betrieb					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende operative, standardisierte Verfahren für den IT-Betrieb, um einen kontinuierlichen Betrieb (inkl. Schichtübergaben) sicherzustellen	DS13.1	◗ Anzahl der Schulungstage pro Betriebsmitarbeiter pro Jahr ◗ Häufigkeit der Aktualisierung von Betriebsverfahren	◗ Anzahl der Stillstände und Verzögerungen, die durch Abweichung von Betriebsverfahren verursacht wurden ◗ % der geplanten Arbeiten und Anfragen, die nicht zeitgerecht fertiggestellt wurden ◗ Anzahl der Stillstände und Verzögerungen, die durch mangelhafte Verfahren verursacht wurden	◗ Anzahl der betriebsbedingten Incidents mit Einfluss auf Service Levels ◗ Anzahl der Stunden ungeplanter Betriebsunterbrechungen aufgrund betriebsbedingter Störungen	◗ Definiere, implementiere und unterhalte standardisierte Verfahren für den IT-Betrieb und stelle sicher, dass das Betriebspersonal mit allen für sie relevanten Betriebsaufgaben vertraut ist. ◗ Operative Verfahren sollten Schichtübergaben (formale Übergaben von Aktivitäten, Statusaktualisierungen, operative Probleme, Eskalationsverfahren und Berichte über derzeitige Verantwortungen) abdecken, um einen kontinuierlichen Betrieb sicherzustellen. ◗ Organisiere und plane Jobs, Prozesse und Aufgaben in der wirtschaftlichsten Reihenfolge, maximiere den Durchsatz und die Verwendung, um die Unternehmenserfordernisse zu erfüllen. ◗ Die erstmalige Planung sowie Änderungen dieser Pläne sollten autorisiert werden. ◗ Verfahren sollten vorhanden sein, um Abweichungen von normalen Jobplänen zu erkennen, abzuklären und freizugeben. ◗ Definiere und implementiere Verfahren zur Überwachung der IT-Infrastruktur und der damit in Zusammenhang stehenden Vorkommnisse. ◗ Stelle sicher, dass ausreichend chronologische Informationen in Betriebsprotokollen gespeichert sind, um Wiederherstellung, Review und die Untersuchung der zeitlichen Abfolge von Betriebs- und anderen Aktivitäten im Umfeld oder zur Unterstützung des Betriebs zu ermöglichen.
Fehlende oder unzureichende Verfahren zur Einplanung, Autorisierung, Änderung und Überwachung von Jobabläufen, um Unternehmenserfordernissen zu entsprechen und Abweichungen zu erkennen	DS13.2	◗ % der Arbeitspläne, die automatisiert sind			
Fehlende oder unzureichende Verfahren zur Überwachung von IT-Infrastrukturen, um auf Basis einer Protokollierung eine Überprüfung der zeitlichen Reihenfolge von Aktivitäten und deren Wiederherstellung zu ermöglichen	DS13.3				
Fehlende oder unzureichende Verfahren zum Umgang mit und Sicherheit von sensiblen Dokumenten und Ausgabegeräten, um physische Sicherheit zu etablieren	DS13.4				

→

DS13 – Manage den Betrieb					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende regelmäßige Wartung der Infrastruktur, um die Häufigkeit von Fehlern und deren Auswirkungen zu reduzieren	DS13.5	◗ % der Hardwareanlagen, die in präventive Wartungspläne aufgenommen wurden			◗ Etabliere geeignete physische Absicherungen, Verrechnungs- und Inventurpraktiken für sensitive IT-Anlagen wie Spezialformulare, verwertbare Einrichtungen, Spezialdrucker oder Security-Token. ◗ Definiere und implementiere Verfahren zur Sicherstellung einer zeitgerechten Wartung der Infrastruktur, um die Häufigkeit und Auswirkungen von Fehlern oder Leistungsabfall zu reduzieren. ◗ Die Ereignisse und Ergebnisse abgeschlossener Aufgaben sollen aufgezeichnet und eingeschränkt an das Management berichtet werden. ◗ Eine formelle Richtlinie zur Reduzierung der Anzahl unplanmäßiger Ereignisse soll entwickelt werden. ◗ Die Verantwortlichkeiten für den Betrieb und den Support sollen klar definiert und der Eigentümerschaft zugewiesen werden. ◗ Der Betrieb des IT-Supports soll wirksam, wirtschaftlich und ausreichend flexibel organisiert werden, um Service-Level-Bedürfnissen mit minimalem Produktivitätsverlust nachzukommen. ◗ Die operativen Verfahren des IT-Managements sollen standardisiert und innerhalb einer Wissensbasis dokumentiert sein sowie einer kontinuierlichen Verbesserung unterliegen. ◗ Sämtliche Probleme und Fehler sollen analysiert werden, um die Grundursache zu ermitteln. ◗ Regelmäßige Meetings mit Verantwortlichen des Change-Managements sollen eine zeitliche Eingliederung von Changes in die produktiven Ablaufpläne sicherstellen. ◗ In Kooperation mit den Lieferanten soll die Ausrüstung auf Alter und Anzeichen von Fehlfunktionen untersucht werden. ◗ Die Wartung sollte vorwiegend präventiv erfolgen. ◗ Die Mitarbeiter werden ausreichend und regelmäßig geschult.

ME1 – Monitore und evaluiere IT-Performance					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender unternehmensweiter Überwachungsansatz für IT-Prozesse und IT-Projekte, um den Beitrag der IT für das Portfoliomanagement und die Erbringung von Services zu überwachen	ME1.1	◗ Anzahl der Metriken (pro Prozess) ◗ Anzahl der identifizierten und in das Monitoring integrierten Ursache-Wirkungs-Zusammenhänge ◗ Anzahl von Problemen, die nicht durch den Messprozess identifiziert wurden	◗ Zufriedenheit der Stakeholder mit dem Bewertungsprozess ◗ % kritischer Prozesse, die überwacht werden ◗ Anzahl von Verbesserungsmaßnahmen, die durch Monitoring-Aktivitäten getrieben werden ◗ Anzahl der erreichten Performance-Ziele (erreichte Indikatoren)	◗ Anzahl der Änderung von Zielen für die Wirksamkeits- und Wirtschaftlichkeitsindikatoren der IT-Prozesse ◗ Zufriedenheit des Managements und des Governance-Gremiums mit der Performance-Berichterstattung ◗ Reduktion in der Anzahl von ungelösten Prozessunzulänglichkeiten	◗ Stelle sicher, dass das Management ein Framework und einen Ansatz für ein generelles Monitoring aufstellt. ◗ Das Framework soll den Scope, die Methoden und anzuwendenden Prozesse umfassen, die befolgt werden müssen, um den Beitrag der IT zu den Portfoliomanagement- und Programm-Management-Prozessen sowie jene Prozesse zu überwachen, die spezifisch sind für die Erbringung des Potenzials und der Services der IT. ◗ Das Framework sollte in das unternehmensweite System zum Performance-Monitoring integriert sein. ◗ Stelle sicher, dass das IT-Management in Zusammenarbeit mit dem Kerngeschäft ein ausgewogenes Maß an Vorgaben, Messgrößen, Zielen und Benchmarks für Performance definiert und dass diese auch durch Kerngeschäftsverantwortliche und andere relevante Stakeholder freigegeben werden. ◗ Messgrößen für Performance sollten die folgenden Punkte enthalten: - Beitrag zum Kerngeschäft, der auch, aber nicht nur finanzorientierte Zahlen enthält, - Performance im Vergleich zum strategischen Geschäfts- und IT-Plan, - Risiken aus Nichteinhaltung von Regulativen, - Zufriedenheit interner und externer User, - wesentliche IT-Prozesse inklusive Entwicklung und Service Delivery sowie - zukunftsorientierte Aktivitäten (z. B. neu entstehende Technologien, wiederverwendbare Infrastruktureinrichtungen, Fertigkeiten von Geschäftsbereichs- und IT-Personal). ◗ Prozesse sollten erstellt werden, um zeitnahe und richtige Daten zu sammeln und um über den Zielerreichungsgrad berichten zu können. ◗ Stelle sicher, dass der Monitoring-Prozess eine Methode einsetzt (z. B. Balanced Scorecard), die eine prägnante, umfassende Übersicht über die Performance der IT ermöglicht und die zum unternehmensweiten Monitoring-System passt.
Fehlende oder unzureichende Benchmarks und Verfahren zur Ermittlung von IST-Daten für die Themen Wertbeitrag, Performance, Risiken, Zufriedenheit, wesentliche IT-Prozesse und zukunftsorientierte Aktivitäten, um aktuelle Daten sammeln und über den Zielerreichungsgrad berichten zu können	ME1.2	◗ Erforderlicher Aufwand für die Sammlung der Messdaten ◗ Anzahl von Problemen, die nicht durch den Messprozess identifiziert wurden ◗ Zeitverzögerung zwischen dem Bericht der Abweichung und dem Beginn der Handlung			
Fehlende oder unzureichende Methode zur Überwachung (z. B. IT Balanced Scorecards), um einen prägnanten und umfassenden Überblick über die IT-Performance geben zu können	ME1.3	◗ Anzahl der Metriken (pro Prozess) ◗ Anzahl der identifizierten und in das Monitoring integrierten Ursache-Wirkungs-Zusammenhänge			
Fehlende oder unzureichende regelmäßige Analyse der Performance gegen Ziele, um Ursachen für die Abweichungen und Maßnahmen zur Behebung zu identifizieren	ME1.4	◗ Anzahl der Metriken (pro Prozess) ◗ Verzögerung in der Aktualisierung der Messung, um die wirklichen Performance-Ziele, -Messungen, -Zielwerte und -Benchmarks widerzuspiegeln ◗ Anzahl der identifizierten und in das Monitoring integrierten Ursache-Wirkungs-Zusammenhänge			
Fehlende oder unzureichende Berichte an die geschäftsführenden Gremien hinsichtlich identifizierter Ziele in Bezug auf die Performance, Service Levels und den Beitrag der IT, um den Fortschritt der Organisation aufzuzeigen und geeignete Maßnahmen bei Abweichungen zu identifizieren und zu beheben	ME1.5	◗ Zeitverzögerung zwischen dem Bericht der Abweichung und dem Beginn der Handlung ◗ Anzahl von Problemen, die nicht durch den Messprozess identifiziert wurden			

→

ME1 – Monitore und evaluiere IT-Performance					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Verbesserungsprozesse auf Basis des Monitorings, der Beurteilung und der Berichterstattung der Performance, um die Performance des Unternehmens kontinuierlich zu steigern	ME1.6	◗ Zeitverzögerung zwischen dem Bericht der Abweichung und dem Beginn der Handlung			◗ Vergleiche in regelmäßigen Abständen die Performance mit den Zielen, führe Ursachenanalysen (engl.: root cause analysis) durch und ergreife Maßnahmen, um die zugrunde liegenden Ursachen in Angriff zu nehmen. ◗ Erstelle Management-Berichte für den Review des Fortschritts der Organisation durch die Geschäftsführung hinsichtlich der identifizierten Ziele, speziell in Bezug auf die Performance des Unternehmensportfolios von IT-gestützten Investitionsprogrammen, auf die Service Levels individueller Programme und auf den Beitrag der IT zu dieser Performance. ◗ Statusberichte sollten das Ausmaß aufzeigen, wie geplante Ziele erreicht, Ergebnisse fertiggestellt, Performance-Ziele erreicht und Risiken vermindert wurden. ◗ Nach dem Review sollten sämtliche Abweichungen von der erwarteten Performance identifiziert, geeignete Management-Aktivitäten initiiert und darüber berichtet werden. ◗ Identifiziere und initiiere Verbesserungsmaßnahmen, welche basieren auf dem Monitoring, der Beurteilung und der Berichterstattung über die Performance. Dies umfasst die Nachverfolgung aller Überwachungen, Berichterstattung und Beurteilungen durch - Review, Verhandlung und Herbeiführung von Reaktionen des Managements, - Zuweisung von Verantwortlichkeiten für die Verbesserung und - Verfolgung der Ergebnisse der eingeleiteten Maßnahmen. ◗ Das Management soll standardisierte Überwachungsprozesse kommunizieren und institutionalisieren. ◗ Informations- und Ausbildungsprogramme für Monitoring werden umgesetzt. ◗ Das Management soll Toleranzgrenzen festlegen, innerhalb derer IT-Prozesse laufen müssen. ◗ Die Berichterstattung der Monitoring-Ergebnisse soll standardisiert werden. ◗ Ein Prozess zur kontinuierlichen Qualitätsverbesserung soll entwickelt werden, um die unternehmensweiten Standards und Richtlinien für Monitoring zu verbessern und um Best Practices der Industrie umzusetzen. ◗ Vom Kerngeschäft getriebene Metriken sollen verwendet werden, um die Performance zu messen.

ME2 – Monitore und evaluiere Internal Controls					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes laufendes Monitoring des IT-Control-Umfelds und des Control Frameworks, um die Umgebung und das Framework, z. B. mithilfe von Best Practices der Industrie, zu verbessern	ME2.1	◗ Zeitspanne zwischen dem Auftreten einer Schwäche der Internal Controls und deren Meldung	◗ Häufigkeit von Fehlern in Internal Controls ◗ Anzahl der von externen Qualifizierungs- und Zertifizierungsberichten identifizierten Schwachstellen ◗ Anzahl der Verbesserungsinitiativen für Controls ◗ Anzahl der Vorfälle aufgrund der Nichtbefolgung von Vorschriften oder Gesetzen ◗ Anzahl der zeitgerechten Handlungen auf Internal-Control-Ereignisse	◗ Grad der Zufriedenheit des Senior Managements mit der Berichterstattung des Internal Control Monitoring ◗ Anzahl der bedeutenden Verstöße gegen Internal Controls	◗ Monitore laufend das IT-Control-Umfeld und das Control Framework. ◗ Bewerte unter Anwendung von Best Practices der Industrie und Benchmarks, um die IT-Control-Umgebung und das Control Framework zu verbessern. ◗ Monitore die Wirksamkeit der Internal Controls über die IT durch einen übergeordneten Review und berichte darüber unter Einbezug von z. B. Einhaltung von Richtlinien und Normen, Informationssicherheit, Steuerung von Changes und in Service Level Agreements aufgeführte Controls. ◗ Zeichne Informationen für alle Ausnahmen von Controls auf und verwende diese für die Analyse der grundlegenden Ursachen und für Verbesserungsmaßnahmen. ◗ Das Management sollte entscheiden, welche Ausnahmen an die funktional verantwortliche Person kommuniziert werden und welche Ausnahmen eskaliert werden sollten. ◗ Das Management ist auch für die Information der betroffenen Parteien verantwortlich. ◗ Evaluiere durch ein ständiges Programm zur Selbsteinschätzung die Vollständigkeit und Wirksamkeit der Internal Control des Managements über die IT-Prozesse, -Richtlinien und -Verträge. ◗ Hole, wo notwendig, weitere Bestätigungen für die Vollständigkeit und Wirksamkeit der Internal Controls durch Reviews von Dritten ein. Solche Reviews können durch die Compliance-Funktion des Unternehmens auf Anfrage des Managements durch Internal Audit, durch extern beauftragte Prüfer, Berater oder Zertifizierungsstellen durchgeführt werden. ◗ Die Qualifikation der Personen, die diese Audits durchführen, muss sichergestellt sein, z. B. durch Zertifizierung als Certified Information Systems Auditor™ (CISA®).
Fehlendes oder unzureichendes übergeordnetes Review für das Monitoring der Wirksamkeit der Internal Controls über die IT, um über Einhaltung von Richtlinien oder Informationssicherheit berichten zu können	ME2.2	◗ Anzahl und Abdekkung der Internal Controls, die einem übergeordneten Review unterliegen			
Fehlende oder unzureichende Aufzeichnung von Informationen über Ausnahmen von Internal Controls, um Ursachenanalyse und Verbesserungsmaßnahmen zu ermöglichen und um ggf. eskalierende Maßnahmen einzuleiten	ME2.3	◗ Anzahl und Abdekkung der Internal Controls, die einem übergeordneten Review unterliegen			
Fehlende oder unzureichende ständige Selbstbeurteilung der Vollständigkeit und Wirksamkeit der Internal Controls über IT-Prozesse, -Richtlinien und -Verträge, um Abweichungen zu identifizieren	ME2.4	◗ Anzahl und Abdekkung der Control Self-Assessments			
Fehlende oder unzureichende Prüfung der Internal Controls durch Reviews von Dritten (z. B. Internal Audit, externe Prüfer), um die Vollständigkeit und Wirksamkeit der Internal Controls zu bestätigen	ME2.5	◗ Anzahl, Häufigkeit und Abdeckung der Internal-Compliance-Berichte ◗ Anzahl und Abdekkung der Internal Controls, die einem übergeordneten Review unterliegen			
Fehlende oder unzureichende Überprüfung des Status der Internal Controls von externen Dienstleistern, um sicherzustellen, dass diese rechtliche und regulatorische Anforderungen erfüllen	ME2.6	◗ Anzahl, Häufigkeit und Abdeckung der Internal-Compliance-Berichte			

→

ME2 – Monitore und evaluiere Internal Controls					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Auswertung der Berichte und Beurteilungen der Internal Controls, um Verbesserungen zu initiieren	ME2.7	◗ Anzahl, Häufigkeit und Abdeckung der Internal-Compliance-Berichte			◗ Bewerte den Status der Internal Controls von sämtlichen externen Dienstleistern. ◗ Bestätige, dass externe Dienstleister rechtliche und regulatorische Anforderungen sowie vertragliche Verpflichtungen einhalten. Dies kann durch ein Audit durch Dritte erfolgen oder durch ein Review der internen Audit-Funktion des Managements. ◗ Identifiziere auf Basis von Berichten und Beurteilungen von Controls Verbesserungsmaßnahmen und initiiere diese. Dies soll eine Nachbearbeitung aller Beurteilungen und Berichte durch: - Review, Verhandlung und Umsetzung von Reaktionen des Managements, - Zuweisung von Verantwortung für die Verbesserung (kann auch die Risikoakzeptanz umfassen) sowie - Verfolgung der Ergebnisse der vereinbarten Aktivitäten umfassen. ◗ Ein Prozess für Self-Assessments der Internal Controls soll mit Rollen für die verantwortlichen Business und IT-Manager definiert werden. ◗ Das Management soll ein Rahmenwerk zur Überwachung der IT Internal Controls implementieren und die Überwachung der Internal Controls institutionalisieren. ◗ Das Unternehmen soll für den Überwachungsprozess der Internal Controls Toleranzgrenzen etablieren und Werkzeuge zur Standardisierung von Bewertungen und zur automatischen Erkennung von Kontrollabweichungen implementieren. ◗ Das Management soll ein unternehmensweites, kontinuierliches Verbesserungsprogramm etablieren, welches Erfahrungsberichte und Industry Best Practices zur Überwachung von Internal Controls berücksichtigt. ◗ Die gemeinsame Nutzung des spezifischen Wissens der Informatikfunktion soll formell implementiert und Benchmarking gegen Industriestandards und Best Practices soll formalisiert werden.

ME3 – Stelle Compliance mit Vorgaben sicher					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlender oder unzureichender Prozess zur zeitnahen Identifikation von Anforderungen von Gesetzen, Regulatorien und Verträgen, um deren Auswirkung auf die IT einschätzen zu können	ME3.1	◗ Durchschnittliche Zeitspanne zwischen Identifikation externer Compliance-Themen und deren Lösung ◗ Durchschnittliche Zeitspanne zwischen der Veröffentlichung eines neuen Gesetzes oder einer neuen Vorschrift und der Einleitung eines Compliance-Reviews ◗ Schulungstage pro IT-Mitarbeiter pro Jahr in Bezug auf Compliance	◗ Anzahl der pro Jahr identifizierten, kritischen Non-Compliance-Fälle ◗ Häufigkeit der Compliance Reviews	◗ Kosten der IT-Non-Compliance, einschließlich Vergleichen und Strafen ◗ Anzahl der Non-Compliance-Fälle, die an die Geschäftsführung berichtet wurden oder die öffentliches Aufsehen und Reaktionen hervorgerufen haben	◗ Definiere und implementiere einen Prozess, um die zeitnahe Identifikation von lokalen und internationalen, durch Recht, Verträge, Richtlinien oder Regulative begründeten Anforderungen an Informationen, Informationserbringung (inklusive der Leistungen von Dritten) und die IT-Organisation, -Prozesse und -Infrastruktur sicherzustellen. ◗ Beachte Gesetze und Vorschriften des elektronischen Handelns, Datenfluss, Datenschutz, Internal Controls, Finanzberichterstattung, industriespezifische Vorschriften, geistiges Eigentum und Urheberrecht sowie Gesundheit und Arbeitnehmersicherheit. ◗ Reviewe und optimiere IT-Richtlinien, -Standards und -Verfahren, um sicherzustellen, dass rechtliche und regulatorische Anforderungen in wirtschaftlicher Weise abgedeckt sind. ◗ Evaluiere in wirtschaftlicher Weise, basierend auf der Governance-Übersicht und dem Betrieb der Internal Controls des Unternehmens- und IT-Managements, die Einhaltung von IT-Richtlinien, Standards und Verfahren, inklusive rechtlicher und regulativer Anforderungen. ◗ Definiere und implementiere Verfahren, um eine positive Bestätigung der Compliance zu erhalten und darüber zu berichten und, wo notwendig, über die rechtzeitige Einleitung von Verbesserungsmaßnahmen durch die verantwortlichen Prozesseigner zur Behandlung von Compliance-Lücken. ◗ Integriere die IT-Berichterstattung über den Fortschritt der Compliance und deren Status mit ähnlichen Ergebnissen anderer Unternehmensfunktionen. ◗ Integriere die IT-Berichterstattung bezüglich regulativer Anforderungen mit ähnlichen Ergebnissen anderer Unternehmensfunktionen. ◗ Definiere Richtlinien und entwickle Verfahren und Prozesse und kommuniziere diese in der Organisation.
Fehlende oder unzureichende Optimierung der IT-Richtlinien und -Verfahren, um sicherzustellen, dass Anforderungen in wirtschaftlicher Weise abgedeckt werden	ME3.2	◗ Durchschnittliche Zeitspanne zwischen Identifikation externer Compliance-Themen und deren Lösung ◗ Durchschnittliche Zeitspanne zwischen der Veröffentlichung eines neuen Gesetzes oder einer neuen Vorschrift und der Einleitung eines Compliance-Reviews			
Fehlende oder unzureichende Evaluierung der Einhaltung der IT-Richtlinien, Standards und der zu befolgenden Verfahren, um deren Compliance sicherzustellen	ME3.3	◗ Schulungstage pro IT-Mitarbeiter pro Jahr in Bezug auf Compliance			
Fehlende oder unzureichende Verfahren zur positiven Bestätigung der Compliance und der dazugehörigen Berichterstattung, um Verbesserungsmaßnahmen bei Compliance-Lücken treffen zu können	ME3.4	◗ Durchschnittliche Zeitspanne zwischen Identifikation externer Compliance-Themen und deren Lösung			

→

ME3 – Stelle Compliance mit Vorgaben sicher					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Integration der IT-Berichterstattung bezüglich Compliance mit ähnlichen Ergebnissen anderer Unternehmensfunktionen, um eine unternehmensweite Einhaltung der Compliance zu gewährleisten	ME3.5	◗ Durchschnittliche Zeitspanne zwischen Identifikation externer Compliance-Themen und deren Lösung			◗ Führe Schulungen in externen rechtlichen und regulatorischen Anforderungen mit Einfluss auf das Unternehmen durch. ◗ Stelle durch ein formelles Schulungsprogramm sicher, dass sich sämtliche Mitarbeiter ihrer Compliance-Verpflichtungen bewusst sind. ◗ Entwickle Prozesse und Mechanismen zur standardisierten Identifikation und Überwachung der Non-Compliance mit externen Anforderungen. ◗ Etabliere ein zentrales, unternehmensweites System zur Nachverfolgung, welches dem Management die Dokumentation des Workflows sowie die Messung und Verbesserung von Qualität und Wirksamkeit des Compliance-Überwachungsprozesses erlaubt. ◗ Etabliere einen Self-Assessment-Prozess in Zusammenhang mit externen Anforderungen.

ME4 – Sorge für IT-Governance					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlendes oder unzureichendes IT-Governance-Framework, um sicherzustellen, dass IT-Investitionen an der Unternehmensstrategie und den -zielen ausgerichtet sind und entsprechend diesen arbeiten	ME4.1	◗ % des Personals, das in Governance (z. B. Verhaltenskodex) geschult wurde ◗ Anzahl der Ethical Officers pro Abteilung ◗ % der Vorstandsmitglieder, die in IT-Governance geschult sind oder damit Erfahrung haben	◗ Häufigkeit der Berichterstattung der IT an den Vorstand (einschließlich deren Reife) ◗ Anzahl der Governance-Verstöße ◗ Häufigkeit von unabhängigen Reviews der IT-Compliance	◗ Häufigkeit, dass IT proaktiv auf der Tagesordnung einer Vorstandssitzung steht ◗ Häufigkeit der Vorstandsberichterstattung über die IT an Stakeholder (einschließlich Reifegrad) ◗ Anzahl wiederkehrender IT-Themen auf der Tagesordnung von Vorstandssitzungen	◗ Arbeite mit der Geschäftsleitung, um ein IT-Governance Framework festzulegen und einzurichten, das Führung, Prozesse, Rollen und Verantwortlichkeiten, Informationsbedarf und Organisationsstrukturen umfasst, um sicherzustellen, dass die IT-gestützten Investitionsprogramme des Unternehmens an den Unternehmensstrategien und -zielen ausgerichtet sind und entsprechend diesen arbeiten. ◗ Das Framework sollte eine klare Verbindung herstellen zwischen der Unternehmensstrategie, dem Portfolio von IT-gestützten Investitionsprogrammen, den individuellen Investitionsvorhaben und den Unternehmens- und IT-Projekten, die die Programme darstellen. ◗ Das Framework sollte unmissverständliche Zuständigkeiten und Praktiken unterstützen, um einen Zusammenbruch der Internal Controls und der Aufsicht zu vermeiden. ◗ Das Framework sollte mit der unternehmensweiten Control-Umgebung und allgemein akzeptierten Grundsätzen für Control konsistent sein. ◗ Ermögliche der Geschäftsführung, die strategischen IT-Belange wie die Rolle der IT, technologische Einblicke und Möglichkeiten zu verstehen. ◗ Stelle sicher, dass ein gemeinsames Verständnis zwischen dem Geschäftsbereich und der IT über den potenziellen Beitrag der IT zur Unternehmensstrategie besteht. ◗ Stelle sicher, dass ein klares Verständnis darüber besteht, dass nur Wertbeitrag durch IT erzielt wird, wenn durch IT gestützte Investitionen als ein Portfolio von Programmen gemanagt werden, das den vollen Umfang der Changes berücksichtigt, die das Unternehmen umzusetzen hat, um den Wertbeitrag für die Umsetzung der Strategie durch Potenziale der IT zu optimieren. ◗ Arbeite mit der Geschäftsleitung, um Governance-Gremien wie einen IT-Strategieausschuss festzulegen und zu implementieren, um strategische Vorgaben an das Management in Relation zur IT zu erstellen, womit sichergestellt wird, dass die Strategie und Ziele in die Unternehmenseinheiten und die IT-Funktionen heruntergebrochen sowie Zuversicht und Vertrauen zwischen dem Kerngeschäft und der IT aufgebaut werden.
Fehlende oder unzureichende strategische Ausrichtung zwischen der Unternehmens- und IT-Strategie (z. B. durch fehlende Governance-Gremien), um den Wertbeitrag der IT zu optimieren	ME4.2	◗ % des Personals, das in Governance (z. B. Verhaltenskodex) geschult wurde. ◗ Anzahl der Ethical Officers pro Abteilung ◗ Häufigkeit von IT-Governance als Tagesordnungspunkt in IT-Lenkungsausschuss/Strategie-Meetings ◗ % der Vorstandsmitglieder, die in IT-Governance geschult sind oder damit Erfahrung haben			

→

ME4 – Sorge für IT-Governance					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende IT-gestützte, standardisierte IT-Investitionsprogramme, um sicherzustellen, dass diese den höchstmöglichen Nutzen zur Unterstützung der Unternehmensstrategie und -ziele erbringen	ME4.3	◗ Häufigkeit von IT-Governance als Tagesordnungspunkt in IT-Lenkungsausschuss/Strategie-Meetings ◗ % der Vorstandsmitglieder, die in IT-Governance geschult sind oder damit Erfahrung haben ◗ Altersanalyse der vereinbarten Empfehlungen			◗ Ermögliche die Ausrichtung der IT am Kerngeschäft in strategischer und operativer Hinsicht durch die gemeinsame Verantwortung von Kerngeschäft und IT für das Treffen strategischer Entscheidungen und das Erzielen von Nutzen aus IT-gestützten Investitionen. ◗ Manage IT-gestützte Investitionsprogramme und andere Werte und Services der IT, um sicherzustellen, dass diese den höchstmöglichen Nutzen zur Unterstützung der Unternehmensstrategie und -ziele erbringen. ◗ Stelle sicher, dass der erwartete Unternehmenserfolg von IT-gestützten Investitionsprogrammen und der gesamte Umfang des Aufwands, der für die Erreichung dieses Erfolgs notwendig ist, verstanden werden. ◗ Stelle sicher, dass umfassende und konsistente Business Cases von Stakeholdern erstellt und freigegeben werden, dass Vermögenswerte und Investitionen über ihren gesamten wirtschaftlichen Lebenszyklus hinweg verwaltet werden und dass ein aktives Management der Realisierung des Nutzens vorhanden ist, wie z. B. der Wertbeitrag für neue Services, Steigerung der Wirtschaftlichkeit und verbesserte Reaktion auf Kundenanfragen. ◗ Stelle sicher, dass Technologieinvestitionen so weit wie möglich standardisiert sind, um erhöhte Kosten und Komplexität eines Wildwuchses technischer Lösungen zu verhindern. ◗ Optimiere die Investitionen in IT-Vermögenswerte, deren Verwendung und Belegung durch regelmäßige Beurteilungen, die sicherstellen, dass die IT ausreichende, kompetente und fähige Ressourcen hat, um die derzeitigen und künftigen strategischen Ziele umzusetzen und mit dem Unternehmensbedarf mitzuhalten. ◗ Das Management sollte klare, konsistente und durchgesetzte Humanressourcen- und Beschaffungsrichtlinien einsetzen, um sicherzustellen, dass Ressourcenanforderungen wirksam und entsprechend den Architekturrichtlinien und -standards erfüllt werden.
Fehlendes oder unzureichendes Ressourcenmanagement für IT-Vermögenswerte, um sicherzustellen, dass die IT ausreichende, kompetente und fähige Ressourcen zur Umsetzung der strategischen Ziele hat	ME4.4	◗ Häufigkeit von IT-Governance als Tagesordnungspunkt in IT-Lenkungsausschuss/Strategie-Meetings ◗ Altersanalyse der vereinbarten Empfehlungen			
Fehlendes oder unzureichendes IT-Risikomanagement, um sicherzustellen, dass die Risikobereitschaft des Unternehmens für IT-Risiken festgelegt ist sowie dass IT-bezogene Risiken regelmäßig beurteilt und berichtet werden, um auf ein Versagen der Internal Controls angemessen zu reagieren	ME4.5	◗ % des Personals, das in Governance (z. B. Verhaltenskodex) geschult wurde			

→

ME4 – Sorge für IT-Governance					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Messung der IT-Performance und Berichterstattung der Ergebnisse an die Geschäftsleitung, um geeignete Management-Maßnahmen bei Abweichungen von identifizierten Zielen zu initiieren	ME4.6	◗ Häufigkeit der Berichterstattung an den Vorstand über Erhebungen zur Stakeholder-Zufriedenheit			◗ Die IT-Infrastruktur sollte in periodischen Abständen beurteilt werden, um sicherzustellen, dass sie, wo immer möglich, standardisiert ist und dass eine Interoperabilität, wo gefordert, besteht. ◗ Arbeite mit der Geschäftsführung, um die Risikobereitschaft des Unternehmens für IT-Risiken festzulegen. Kommuniziere die IT-Risikobereitschaft im Unternehmen und vereinbare einen Plan zum IT-Risikomanagement. Bette die Verantwortlichkeiten für Risikomanagement in die Organisation ein, um sicherzustellen, dass das Unternehmen und die IT regelmäßig die IT-Risiken und deren Auswirkungen auf das Geschäft beurteilen und darüber berichten. ◗ Stelle sicher, dass das IT-Management drohende Risikogefährdungen behandelt und eine besondere Aufmerksamkeit auf das Versagen von IT-Controls und Schwachstellen in Internal Controls und die Beaufsichtigung legt sowie auf deren tatsächliche und potenzielle Auswirkungen auf die Geschäftstätigkeit. ◗ Die Haltung des Unternehmens bezüglich IT-Risiken sollte für alle Stakeholder transparent sein. ◗ Berichte dem Aufsichtsrat und der Geschäftsleitung rechtzeitig und genau über relevante Portfolios, Programme und die IT-Performance. ◗ Die Managementberichte sollten für den Review der Entwicklung des Unternehmens hinsichtlich der festgelegten Ziele durch die Geschäftsführung erstellt werden. ◗ Statusberichte sollten den Grad der Erreichung von Zielen, erstellte Ergebnisse, erreichte Performance-Zahlen und verminderte Risiken umfassen. ◗ Integriere die Berichterstattung mit ähnlichen Ergebnissen anderer Unternehmensfunktionen. ◗ Die Performance-Messung sollte durch die wichtigsten Stakeholder freigegeben werden.

→

ME4 – Sorge für IT-Governance					
Schwachstelle (vulnerability)		Indikatoren zur Risikobewertung			Risikobehandlungsmaßnahmen
Ableitung aus COs	Control Objectives	KPI	KGI	IT-KGI	Ableitung aus COs und Reifegradmodell
Fehlende oder unzureichende Verfahren, um dem Aufsichtsrat eine unabhängige Bestätigung der Compliance der IT mit ihren Richtlinien, Standards und allgemein anerkannten Praktiken zu geben	ME4.7				◗ Der Aufsichtsrat und die Geschäftsleitung sollten diese Performance-Berichte hinterfragen, und dem IT-Management sollte die Gelegenheit geboten werden, Abweichungen und Performance-Probleme zu erklären. ◗ Nach dem Review sollten geeignete Management-Maßnahmen initiiert und gesteuert werden. ◗ Stelle sicher, dass die Organisation eine kompetente und personell angemessen ausgestattete Funktion etabliert und betreibt und/oder sich externer Prüfungsleistungen bedient, um dem Aufsichtsrat über ein Audit Committee eine zeitgerechte, unabhängige Bestätigung der Compliance der IT mit ihren Richtlinien, Standards und Verfahren sowie mit allgemein anerkannten Praktiken zu liefern. ◗ Das Management soll Toleranzgrenzen festlegen, innerhalb denen die Prozesse zu betreiben sind. ◗ Auf allen Ebenen soll ein umfassendes Verständnis für IT-Governance-Sachverhalte entwickelt werden. ◗ IT-Prozesse und IT-Governance sollen ausgerichtet und integriert werden in die Geschäfts- bzw. die IT-Strategie.

Tab. 4 *Generischer IT-Risikokatalog auf Basis von COBIT (abgeleitet aus [2])*

8 Danksagung

Die erste Version des Leitfadens und Nachschlagewerks »IT-Risikomanagement – leicht gemacht mit COBIT« entstand durch die enge Zusammenarbeit zwischen ISACA und der Fachgruppe »IT-Risikomanagement mit COBIT«.

Unser besonderer Dank gilt den Autoren des Leitfadens und den Mitgliedern der Fachgruppe für das kontinuierliche Interesse am Thema sowie die zahlreichen Textbeiträge, die diesen umfassenden Leitfaden erst ermöglichten:

- Dr. Paul Lokuciejewski (PricewaterhouseCoopers AG)
- Werner Syndikus (tobaccoland Automaten GmbH & Co. KG)
- Karsten Wilop (PricewaterhouseCoopers AG)
- Heinz-Dieter Schmelling (WestLB AG)
- Mohammad Hamidi (T-Systems International GmbH)
- Martin Urban (Infosec-Coaching)
- Ralf Herter (BASF IT Services GmbH)

Für das Korrekturlesen, die Qualitätssicherung und die Bereitstellung von Vorlagen geht unser Dank an:

- Prof. Dr. Michael Klotz, Wissenschaftlicher Beirat des ISACA Germany Chapter
- Prof. Dr. Matthias Goeken, Wissenschaftlicher Beirat des ISACA Germany Chapter
- Andreas Teuscher, Vizepräsident Facharbeit und Arbeitskreise ISACA Germany Chapter e.V.
- dpunkt.verlag GmbH

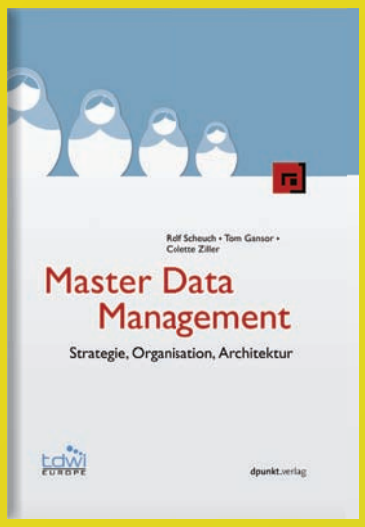
9 Quellenverzeichnis

1. A. Giddens: Entfesselte Welten, Edition Suhrkamp 2200, 1. Auflage 2001, ISBN 3-518-12200-2
2. IT Governance Institute: CobiT 4.1 (2007)
3. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC): Information technology – Security techniques – Information security risk management ISO/IEC 27005 (2008)
4. H. Seibold: Risikomanagement. Oldenbourg Verlag, München (2006)
5. ISACA: The Risk IT Framework (2009)

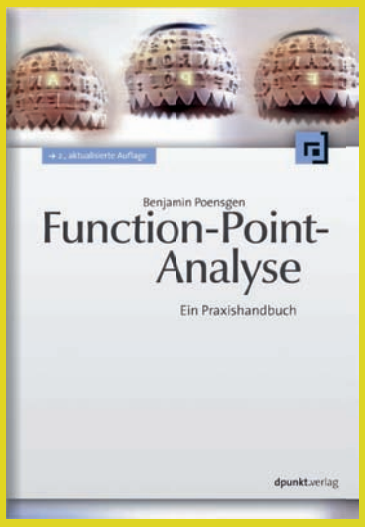
dpunkt.it & business

dpunkt.verlag

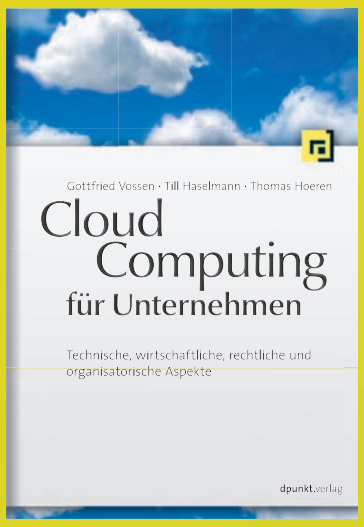
2013, 294 Seiten, Festeinband
€ 59,90 (D)
ISBN 978-3-89864-835-6



2012, 492 Seiten, Festeinband
€ 79,90 (D)
ISBN 978-3-89864-823-3



2012, 166 Seiten, Broschur
2., akt. Auflage
€ 36,90 (D)
ISBN 978-3-89864-762-5



2012, 254 Seiten, Festeinband
€ 36,90 (D)
ISBN 978-3-89864-808-0

2012, 322 Seiten, Broschur
€ 39,90 (D)
ISBN 978-3-89864-756-4

2012, 422 Seiten, Festeinband
2., überarb. u. erw. Auflage
€ 49,90 (D)
ISBN 978-3-89864-768-7

2012, 288 Seiten, Broschur
€ 29,90 (D)
ISBN 978-3-89864-793-9

2012, 318 Seiten, Broschur
€ 36,90 (D)
ISBN 978-3-89864-780-9

dpunkt.verlag GmbH · Ringstraße 19 B · 69115 Heidelberg
fon: 0 62 21 / 14 83 40 · fax: 0 62 21 / 14 83 99 · e-mail: bestellung@dpunkt.de

www.dpunkt.de

ISACA-Zertifizierungen – optimales Training durch unsere Vorbereitungskurse

ISACA bietet vier internationale Zertifizierungen an, mit unterschiedlichen fachlichen Schwerpunkten und für unterschiedliche Berufsgruppen und Tätigkeitsfelder.

Lassen Sie sich zertifizieren und demonstrieren Sie so Ihrem Arbeitgeber, Ihren Kollegen sowie Kunden Ihre Expertise in den Bereichen IT-Audit, Management der Informationssicherheit, IT-Risikomanagement und IT-Governance.

Die ideale Komponente zur optimalen Vorbereitung: Die Präsenzkurse des ISACA Germany Chapter:

- Kompakte Wissensvermittlung
- Erfahrungsaustausch mit anderen Examenskandidaten
- Examensinformation direkt durch den Anbieter
- Praktische Tipps von erfahrenen Referenten
- Praxistraining mit Originalfragen
- hohe Bestehensquote
- kostenlose Teilnahme am nächsten Kurs bei Nicht-Bestehen

Die nächsten Vorbereitungskurse finden im Okt./Nov. 2012 statt: CISA 4-tägig, CISM 2-tägig, CRISC und CGEIT auf Anfrage.

ISACA-Mitgliedern bieten wir die Kurse vergünstigt an.

Schauen Sie auf www.isaca.de vorbei oder kontaktieren Sie Doris Auf der Heyde unter doris.aufderheyde@isaca.de.

ISACA®

Trust in, and value from, information systems

Germany Chapter