Heft 35 | Juni 2022 | 16. Jahrgang | ISSN 1864-6557

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.



AUSZUG
AUS HEFT 35

COBIT® Focus Area: Information and Technology Risk

Markus Gaulke

ISACA Germany Chapter

dpunkt.verlag | it-governance.dpunkt.de | isaca.de

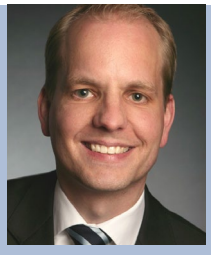
Liebe Leserinnen und Leser,

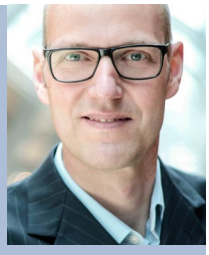
langsam starten wir in den Sommer dieses Jahres und wollen Ihnen mit der neuen Ausgabe unserer Zeitschrift die passende Lektüre für einen schönen Nachmittag in der Sonne mitgeben. Wenn in diesen Zeiten eines sicher ist, dann ist es die Tatsache, dass Planbarkeit und Sicherheit in den letzten Jahren deutlich abgenommen haben. Wir stellen uns alle für die Zukunft darauf ein, dass wir noch schneller als zuvor auf unbekannte Ereignisse reagieren und uns mit unserem Handeln anpassen müssen. Dies hat auch direkte Auswirkungen auf unseren konkreten beruflichen Bereich der IT, in dem es immer häufiger um Agilität, Transformation, aber auch um unterstützende Technologien, wie beispielsweise künstliche Intelligenz (KI) oder auch Blockchain-Technologien, gehen wird, um die zukünftigen Herausforderungen bestmöglich meistern zu können. Für IT-Expertinnen und -Experten, zu denen wir alle sicher gehören, wird dies insbesondere auch unter Governance- und Compliance-Aspekten eine große Herausforderung, da schneller Wandel und neue Technologien oftmals nicht Hand in Hand mit Governance- und Compliance-Anforderungen bzw. deren Erfüllung gehen. Damit uns dies gelingt, werden wir heute und in Zukunft dieses Spannungsfeld weiter beleuchten.


Martin Fröhlich


Matthias Goeken


Michael Klotz


Ingo Struckmeyer


Marc Weber

Der Artikel »Prozessfähigkeitsstufen (Capability Levels) verstehen und wirksam für die IT-Governance nutzen« von Urs Andelfinger beschreibt die Auswahl von COBIT-Prozessen zur Umsetzung der IT-Governance anhand unterschiedlicher Stufen der Prozessfähigkeit als Hilfsmittel hierfür. Die Autoren Christian Ewel und Kilian Trautmann beschäftigen sich mit dem Einsatz von Blockchain-Analytics-Technologien aus der Sicht von nach dem Kreditwesengesetz regulierten Instituten. Sie geben hierzu grundlegende Einblicke, Verfahren sowie ein konkretes Beispiel für eine reale Smart-Contract-Transaktion.

In unserer Praxis-Rubrik erläutern die Autoren Christina Leuchtweis und Thomas Thiele, welche Rolle heute und zukünftig der Einsatz künstlicher Intelligenz bei der Deutschen Bahn spielt und wie der dazugehörige strategische Ansatz sowie der operative Einsatz aussehen.

Im Abschnitt »IT-Prüfung« zeigt Niklas Stallmann einen konzeptionellen Ansatz für einen agilen Revisionsprozess auf, der zu einer weiteren Diskussion der Anwendbarkeit von agilen Methoden auf Prozessschritte bzw. Prozesse in der Internen Revision anregt. Des Weiteren stellt Martin Fröhlich in seinem Artikel den neuen Entwurf eines IDW-Prüfungsstandards zur Prüfung von KI-Systemen (IDW EPS 861) vor.

Markus Gaulke bringt uns mit der »COBIT® Focus Area: Information and Technology Risk« eine weitere ergänzende Veröffentlichung zum COBIT-Rahmenwerk in seinem Artikel in der Rubrik »Standards« näher und erläutert Inhalt und Relevanz dieses Themas. Das vorliegende Heft klingt mit einer Besprechung des Buches »IT-Compliance – Erfolgreiches Management regulatorischer Anforderungen« der Autoren Michael Rath und Rainer Sponholz aus.

Wir hoffen, Ihnen hiermit einige neue Denkanstöße mit auf den Weg geben zu können. Wie immer freuen wir uns auf Ihr konstruktives Feedback und möchten Sie ermuntern, gerne auch einen Artikel zu veröffentlichen.

Ihre Herausgeber

Heft 35 | 2022

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.

Inhalt

Fachthemen

3 **Prozessfähigkeitsstufen (Capability Levels) verstehen und wirksam für die IT-Governance nutzen**
Urs Andelfinger

7 **Der Einsatz von Blockchain Analytics bei KWG-Instituten**
Kilian Trautmann, Christian Ewelt

13 Praxisbericht
Heavy Metal meets AI
Strategische Transformation durch KI bei der Deutschen Bahn
Christina Leuchtweis, Thomas Thiele

Rubriken

17 IT-Prüfung
Agile Interne Revision – der agile Revisionsprozess als konzeptioneller Ansatz
Niklas Stallmann

21 IT-Prüfung
Entwurf eines Prüfungsstandards für die Prüfung von KI-Systemen
Martin Fröhlich

24 Standards
COBIT® Focus Area: Information and Technology Risk
Markus Gaulke

31 **Buchbesprechung**

32 **Inserenten**

32 **Vorschau**

32 **Impressum**

Standards

COBIT® Focus Area: Information and Technology Risk

Markus Gaulke

Das Rahmenwerk COBIT wird von ISACA kontinuierlich durch neue Veröffentlichungen erweitert. Nachdem im August 2020 die Erweiterung für den Schwerpunktbereich Informationssicherheit als Focus Area Guide [Gaulke 2020a] erschienen ist, wurde letztes Jahr auch der Leitfaden zum Schwerpunktthema IT-Risikomanagement bereitgestellt. Dieser Focus Area Guide: Information and Technology Risk [ISACA 2021] zeigt auf, wie das Rahmenwerk COBIT 2019 für einen speziellen Zweck – hier: I&T-Risikomanagement – erweitert werden kann. Dabei werden vor allem die COBIT-Komponenten aus einer I&T-Risikoperspektive ergänzt, um auf dieser Basis die I&T-Risikofähigkeiten im Unternehmen konzeptionell verankern, umsetzen und steuern zu können.

1 COBIT Focus Area: Information and Technology Risk

Im COBIT-Rahmenwerk waren grundlegende Anforderungen zum Thema Risikomanagement schon immer in den Governance- und Managementprozessen integriert. Aufgrund der zunehmenden Bedeutung des Themas Risikomanagement hat die ISACA das IT-Risikomanagement noch tiefgehender betrachtet. Im November 2009 wurde unter dem Namen »Risk IT« [ISACA 2009a] ein IT-Risikomanagement-Rahmenwerk mit einem dazugehörigen Umsetzungsleitfaden (The Risk IT Practitioner Guide [ISACA 2009b]) veröffentlicht. »Risk IT« stellte ein eigenständiges Rahmenwerk mit Leitlinien, einem Prozessmodell und Risikomanagementtechniken in Anlehnung an die einschlägigen Risikomanagement-Grundlagen COSO ERM und ISO 31000 dar.

Die Inhalte des Rahmenwerks »Risk IT« wurden mit Erscheinen von COBIT 5 im Jahr 2012 weitgehend in einen separaten COBIT 5-Umsetzungsleitfaden für das Risikomanagement integriert (COBIT 5 for Risk [ISACA 2013]). Der Umsetzungsleitfaden »COBIT 5 for Risk« ergänzte nicht nur die IT-relevanten Risikoaspekte für die einzelnen Komponenten (damals noch »Enabler« genannt) des COBIT 5-Prozessreferenzmodells, sondern stellte darüber hinaus gute Praktiken für das IT-Risikomanagement dar [Gaulke 2020b].

Mit Erscheinen von COBIT 2019 hat ISACA eine Aktualisierung des Rahmenwerks »Risk IT« angekündigt, das im Juni 2020 (Risk IT Framework 2nd edition [ISACA 2020a]) mit einem dazugehörigen Umsetzungsleitfaden (Risk IT Practitioner Guide [ISACA 2020b]) erschienen ist. Grundlegende

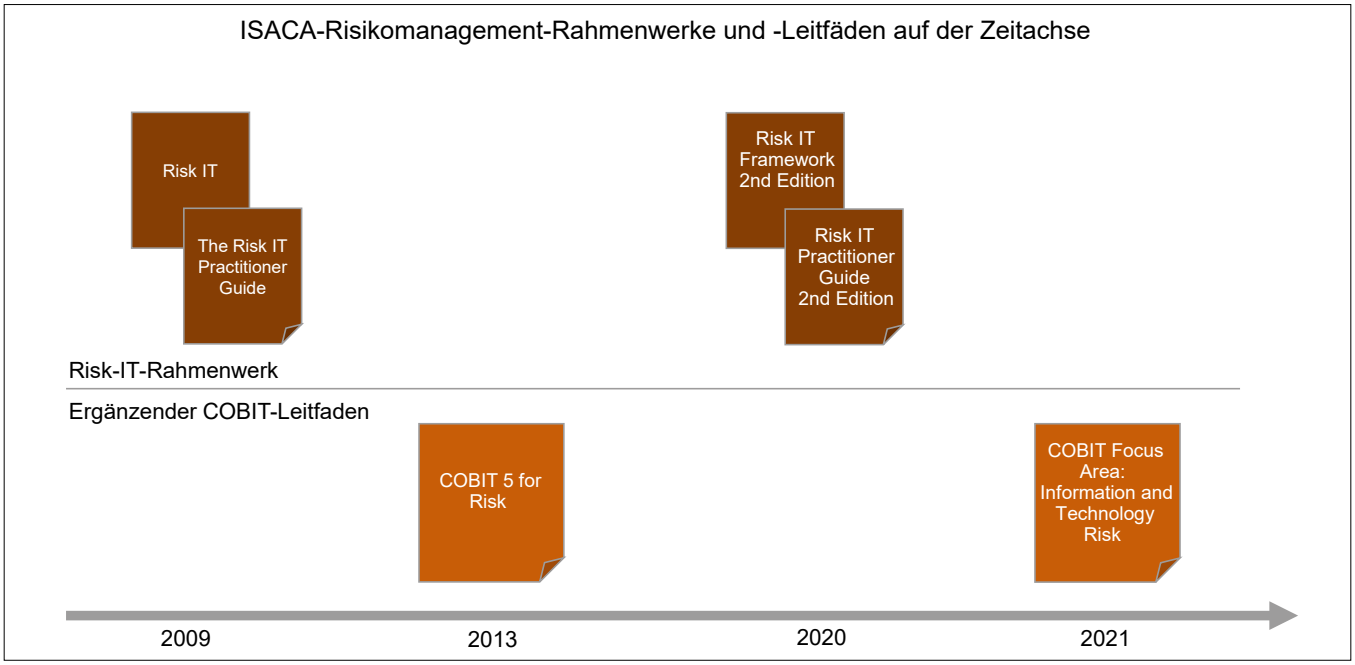


Abb. 1: Entwicklung der ISACA-Risikomanagement-Rahmenwerke und -Leitfäden

Risikomanagementprinzipien sowie Risikomanagementprozesse und -techniken sind dort konzeptionell und praxisnah dargestellt.

Im COBIT 2019-Kernmodell selbst ist das Thema Risikomanagement mit dem Governance-Ziel EDM03 (Risiko-Optimierung ist sichergestellt) und dem Managementziel APO12 (Risiko ist gemanagt) sichtbar abgebildet. Weiterhin finden sich gute Risikomanagementpraktiken auch in den Komponenten, beispielsweise der »Risikoausschuss« bei der Komponente »Organisationsstrukturen« oder die »Richtlinie zum Unternehmensrisiko« bei der Komponente »Richtlinien und Verfahren« [ISACA 2018a]. Diese bereits vorhandenen Risikomanagementaspekte im COBIT 2019-Rahmenwerk werden durch den Leitfaden »COBIT Focus Area: Information and Technology Risk« [ISACA 2021] erweitert. Der neue Leitfaden ist im Grunde genommen eine aktualisierte Version des Umsetzungsleitfadens »COBIT 5 for Risk« und ergänzt die Komponenten des COBIT 2019-Kernmodells, um sowohl die Einrichtung einer I&T-Risikomanagementfunktion als auch die Anwendung der COBIT-Prinzipien und Komponenten zur Steuerung von I&T-Risiken im Unternehmen zu unterstützen.

Der auch als »IRFA« (I&T Risk Focus Area) abgekürzte Leitfaden zum Schwerpunktthema I&T-Risikomanagement besteht aus vier Kapiteln:

- Kapitel 1 und 2 sind einführend und behandeln neben einigen Grundlagen zum Rahmenwerk COBIT 2019 vor allem Begrifflichkeiten und den Aufbau des Leitfadens.
- Kapitel 3 diskutiert die Verwendung der sieben COBIT-Komponenten für die Umsetzung des I&T-Risikomanagements.
- Kapitel 4 stellt detailliert dar, wie das COBIT 2019-Kernmodell in den Komponenten »Prozesse« und »Informationsflüsse und -elemente« für das I&T-Risikomanagement erweitert werden kann.

Ein umfangreicher Anhang ergänzt die Darstellungen um praxisnahe Informationen, wie Risikoszenarien, Risikoberichte und Vorlagen für Einträge ins Risikoregister.

2 Einführung

Im IRFA-Leitfaden erfolgt einleitend eine kurze Einführung in das COBIT 2019-Rahmenwerk, dessen grundlegende Konzepte und deren Bedeutung für das I&T-Risikomanagement. Ausgehend von der Geschäftsstrategie legen Unternehmen ihre Risikobereitschaft fest, d. h. das Risiko, das sie bereit sind, in Kauf zu nehmen, um die Unternehmensziele zu erreichen. Das Risikomanagement sorgt dafür, dass die Wahrscheinlichkeit des Eintretens eines Risikos, das ein akzeptables Maß überschreitet, sowie die Auswirkungen eines realisierten Risikos auf das Geschäft verringert werden.

I&T-Risiko wird dabei als Geschäftsrisiko definiert, das mit der Nutzung, dem Besitz, dem Betrieb, der Beteiligung, der Einflussnahme und der Einführung von Information und Technologie (I&T) zusammenhängt. I&T-Risiken sind all-

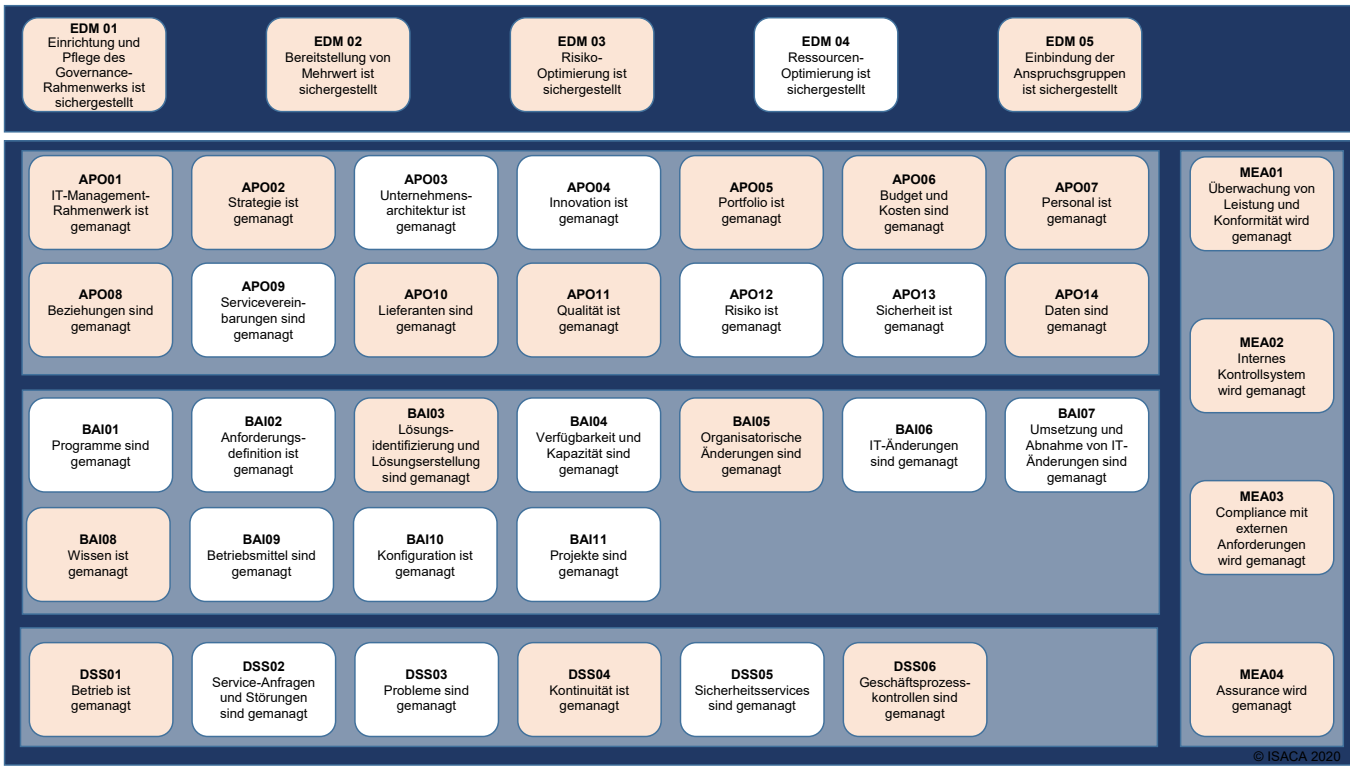


Abb. 2: I&T-risikorelevante Governance- und Managementziele im COBIT 2019-Kernmodell

gegenwärtig. Nahezu alle Aktivitäten, die ein Unternehmen zur Verfolgung seiner Ziele unternimmt, betreffen in hohem Maße die Aspekte Information und Technologie.

Im IRFA-Leitfaden werden von den 40 Governance- und Managementzielen des COBIT 2019-Kernmodells 23 behandelt, die als relevant für das I&T-Risiko angesehen werden.

3 I&T-Risikoaspekte der Komponenten

Das Management von I&T-Risiken betrifft alle Komponenten des COBIT 2019-Modells. Diese werden daher durch den IRFA-Leitfaden wie nachfolgend dargestellt erweitert.

3.1 Prozesse

Das COBIT 2019-Kernmodell adressiert das Thema Risikomanagement insbesondere im gleichnamigen Managementziel APO12 (Risiko ist gemanagt). Risikomanagement betrifft jedoch viele Prozesse in einem Unternehmen. Daher wurden weitere 23 Governance- und Managementziele ausgewählt und um risikorelevante Metriken und Aktivitäten erweitert.

In Abschnitt 4 werden die Erweiterungen des COBIT 2019-Kernmodells an einem Beispiel dargestellt.

3.2 Organisationsstrukturen

Als Organisationsstrukturen werden in COBIT die wichtigen Entitäten der Entscheidungsfindung im Unternehmen bezeichnet, also typischerweise Rollen und Gremien. Die für das I&T-Risikomanagement relevanten Organisationsstrukturen sind – mit Ausnahme der Gruppe der I&T-Risikomanager – bereits im Rollenmodell des COBIT 2019-Rahmenwerks vorhanden und stellen damit keine nennenswerte Erweiterung des Rahmenwerks dar. Die risikorelevanten Organisationsstrukturen werden im IRFA-Leitfaden aber hinsichtlich der Zusammensetzung, des Mandats, der Geschäftsordnung, der Verantwortlichkeiten und Zuständigkeiten, der Entscheidungs-, Delegations- und Eskalationsrechte sowie der Inputs und Outputs ausführlich beschrieben.

Tabelle 1 zeigt die für das I&T-Risikomanagement relevanten Rollen und Organisationsstrukturen im Überblick.

Die aufgeführten Rollen und Organisationsstrukturen waren auch bereits im Leitfaden »COBIT 5 for Risk« ausführlich beschrieben [ISACA 2013]. Neu ist die Rolle des »I&T-Risikomanagers«, der verantwortlich für die Entwicklung und Umsetzung des I&T-Risikomanagements zeichnet. Darüber hinaus werden im IRFA-Leitfaden neben den wesentlichen Rollen und Organisationsstrukturen auch unterstützende Rollen und Organisationsstrukturen aufgeführt, die nicht direkt in das I&T-Risikomanagement involviert sind, aber dennoch relevante Anspruchsgruppen darstellen. Als Beispiel sei hier der Einkauf genannt, also die Funktion, die Dritte beauftragt und die damit verbundenen Prozesse managt. Im Rahmen des I&T-Risikomanagements ist der Einkauf dann beim Management der I&T-Risiken bei Dritten involviert.

Rolle / Organisationsstruktur	Kurzbeschreibung
Risikoausschuss des Unternehmens	Gruppe von Führungskräften, die für die Zusammenarbeit und die Konsensfindung auf Unternehmensebene verantwortlich ist, die zur Unterstützung der Aktivitäten und Entscheidungen des unternehmensweiten Risikomanagements (ERM – Enterprise Risk Management) erforderlich sind. Der Risikoausschuss ist der zweiten Verteidigungslinie zuzurechnen. Zusätzlich kann ein IT-Risikorat eingerichtet werden, der sich eingehender mit IT-Risiken befasst und den Risikoausschuss berät. Die Mitglieder des Risikoausschusses werden in der Regel aus dem Vorstand ausgewählt und der CEO führt den Vorsitz des Ausschusses. Der Leiter der Internen Revision kann als Gast zu der Sitzung eingeladen werden.
Chief Risk Officer (CRO)	Oberste Führungskraft, die für sämtliche Aspekte des Risikomanagements im gesamten Unternehmen verantwortlich ist. Der CRO nimmt auch die Anweisungen des Risikoausschusses entgegen. Zusätzlich kann zur Überwachung der Risiken die Funktion eines I&T-Risikobeauftragten eingerichtet werden.
Interne Revision	Funktion, die für die Durchführung von internen Prüfungen verantwortlich ist und damit auch Berichte über das Risiko im Zusammenhang mit Kontrolllücken erstellt, die bei der Durchführung von Prüfungen festgestellt wurden. Die Interne Revision gilt als dritte Verteidigungslinie und ein Vertreter kann in den Risikoausschuss des Unternehmens eingeladen werden.
Compliance	Funktion, die für alle Richtlinien zur Einhaltung von externen Vorgaben verantwortlich ist. Compliance identifiziert Unternehmensrisiken im Zusammenhang mit aufsichtlichen und gesetzlichen Vorschriften sowie internen Richtlinien und Standards.
I&T-Risikomanager	Risikofachleute, die für die Identifizierung, Bewertung und Meldung von I&T-Risiken zuständig sind. Sie unterstützen die Verantwortlichen für I&T-Risiken.

Tab. 1: Übersicht der wichtigsten Rollen und Organisationsstrukturen für das I&T-Risikomanagement [ISACA 2021]

3.3 Informationsflüsse und -elemente

Im COBIT 2019-Kernmodell werden zu jeder Prozesspraktik als separate Komponente die Informationsflüsse und -elemente dargestellt. Soweit die Praktiken im COBIT 2019-Kernmodell um risikorelevante Aktivitäten erweitert werden, die Informationselemente benötigen oder erzeugen, werden diese ebenfalls im IRFA-Leitfaden beschrieben. In Abschnitt 4 stelle ich diese Erweiterungen des COBIT 2019-Kernmodells an einem Beispiel dar.

Darüber hinaus werden im Leitfaden zum Schwerpunktthema I&T-Risikomanagement die nachfolgenden sieben grundlegenden I&T-risikobezogenen Informationstypen ausführlich dargestellt:

- **I&T-Risikoprofil**
  Ein I&T-Risikoprofil ist eine Beschreibung des gesamten (identifizierten) I&T-Risikos, dem ein Unternehmen ausgesetzt ist, und stellt somit eine umfassende Sicht auf das I&T-Risiko dar. Ein I&T-Risikoprofil besteht aus dem Risikoregister, dem Maßnahmenplan, den eingetretenen Verlustereignissen, den Risikofaktoren sowie den Prüfungsfeststellungen.
- **I&T-Risikokommunikationsplan**
  Ein I&T-Risikokommunikationsplan legt die Häufigkeit der Berichterstattung, die Art der Informationen über I&T-Risiken und die Empfänger dieser Informationen fest.
- **I&T-Risikokarte**
  Auf einer Risikokarte werden gewöhnlich die wichtigsten Risiken in einem Diagramm in den Dimensionen Häufigkeit und Auswirkungen dargestellt. Die Risikokarte bietet einen intuitiven Überblick über die Risiken und die Bereiche mit Handlungsbedarf.
- **I&T-Risikobereitschaft oder -toleranz**
  Die Risikobereitschaft ist das I&T-Risiko, das ein Unternehmen bereit ist zu akzeptieren. Die Risikotoleranz ist die akzeptable Schwankungsbreite, die ein Unternehmen für ein bestimmtes Risiko zulässt.
- **Risikokapazität und tatsächliches Risiko**
  Die Risikokapazität ist die Höhe des Verlustes, den ein Unternehmen hinnehmen kann, ohne seinen Fortbestand zu gefährden. Die Risikokapazität stellt die Obergrenze für das tatsächliche Risiko dar.
- **Key Risk Indicators**
  Key Risk Indicators (KRI) sind Messgrößen, die zeigen, dass ein Unternehmen einem Risiko ausgesetzt ist oder mit hoher Wahrscheinlichkeit einem Risiko, das die festgelegte Risikobereitschaft oder -toleranz übersteigt, ausgesetzt sein wird.
- **Aufkommende I&T-Risikothemen und -faktoren**
  Aufkommende I&T-Risikothemen und -faktoren sind Informationen über bevorstehende oder wahrscheinliche Kombinationen von Wertentwicklung, Bedrohungssituation und Kontrolleffektivität, die ein nennenswertes I&T-Risiko in der Zukunft darstellen.

Im Vergleich zum Leitfaden »COBIT 5 for Risk« wurde die Anzahl der Informationstypen im neuen IRFA-Leitfaden deutlich reduziert. Auch wurde auf die tabellarische Darstellung der Lebenszyklusphasen, der Qualitätselemente, der guten Praktiken entlang der Qualitätsattribute sowie der Zusammenhänge mit anderen Komponenten verzichtet. Diese Informationen wurden in der Praxis wenig verwendet und die reduzierte Darstellung trägt deutlich zur besseren Lesbarkeit bei.

3.4 Mitarbeiter, Fähigkeiten und Kompetenzen

Für das Erreichen der Governance- und Managementziele müssen auch Mitarbeiter mit den erforderlichen Fähigkeiten zur Verfügung stehen. Im COBIT 2019-Kernmodell sind in den beiden zentralen, für das Risikomanagement relevanten Governance- und Managementzielen EDM03 und APO12 in der Komponente »Mitarbeiter, Fähigkeiten und Kompetenzen« bereits Fähigkeiten für das Risikomanagement aufgeführt, die notwendig sind, um die Governance- und Managementziele zu erreichen. Diese basieren auf dem »Skills Framework for the Information Age (SFIA®)« sowie dem »e-Competence Framework (e-CF)«.

Im Leitfaden zum Schwerpunktthema I&T-Risikomanagement werden darüber hinaus elf notwendige Fähigkeiten für das Risikomanagement näher betrachtet. Weiterhin werden für drei spezifische Rollen im Risikomanagement (Chief Risk Officer, Risk Manager, Risk Analyst) die notwendige Erfahrung, Ausbildung und Qualifikation sowie das relevante Wissen und die erforderlichen technischen und sozialen Fähigkeiten beschrieben. Für die Rolle des Risikomanagers, der für die Umsetzung und Überwachung der Risikostrategie verantwortlich ist, werden beispielsweise die in Tabelle 2 angegebenen Anforderungen pro Kategorie aufgeführt:

Anforderung	Beschreibung der Anforderung an den Risikomanager
Erfahrung	• Erfahrung im Management und in der Steuerung von Unternehmensrisiken und/oder -abläufen • Erfahrung in der Kommunikation von Risiken an die Geschäftsleitung und/oder den Vorstand
Ausbildung	• Hochschulabschluss in Managementinformationssystemen mit Erfahrung in den Bereichen I&T, Finanzen, Wirtschaft oder Ingenieurwesen
Geeignete Qualifikationen	• Certified Information Systems Auditor (CISA) • Certified Information Security Manager (CISM) • Certified in Risk and Systems Control (CRISC) • Certified Information Systems Security Professional (CISSP) • Certified Public Accountant (CPA)
Wissen	• Vertiefte Kenntnisse über das Unternehmen und die I&T-Systeme, die die Geschäftsfunktionen unterstützen, sowie Bewusstsein für die Kontextfaktoren, die diese beeinflussen • Solide Kenntnisse von Risikomethoden, allgemein verwendeten Risikostandards und bewährten Risikoverfahren
Technische Fähigkeiten	• Technische Kenntnisse über die I&T-Systeme zur Unterstützung der Geschäftsfunktionen
Verhaltensbezogene Fähigkeiten	• Führungsqualitäten • Kommunikation • Beeinflussung • Geduld • Eskalation

Tab. 2: Typische Anforderungen an die Fähigkeiten der Rolle »Risikomanager« [ISACA 2021]

Diese typischen Anforderungen eignen sich sowohl als Grundlage für die Erstellung von Stellenbeschreibungen für den Bereich I&T-Risikomanagement als auch zur Weiterentwicklung der Fähigkeiten in diesen Rollen.

3.5 Prinzipien, Richtlinien und Verfahrensanweisungen

Die Vorgaben für das Risikomanagement im Unternehmen werden durch Prinzipien, Richtlinien und Verfahrensanweisungen dokumentiert und kommuniziert.

Prinzipien

Prinzipien sind auf der obersten Ebene angesiedelt und sollten daher kurz und knapp sein. Der Schwerpunktleitfaden zum I&T-Risikomanagement referenziert auf die bereits im Rahmenwerk »Risk IT« [ISACA 2020a] dargestellten sechs allgemeinen Prinzipien des Risikomanagements:

- Verbindung zu den Zielen und der Mission des Unternehmens
- Ausrichtung am unternehmensweiten Risikomanagement
- Abwägung von Kosten und Nutzen
- Förderung einer ethischen und offenen Kommunikation
- Verankerung in der Unternehmenskultur (Tone at the top) und Verantwortlichkeit
- Verwendung eines konsistenten, auf die Strategie abgestimmten Ansatzes

Diese Prinzipien sind universell und eignen sich daher als Grundlage für die Erstellung von unternehmensspezifischen Prinzipien für das I&T-Risikomanagement.

Im Vergleich zum Leitfaden »COBIT 5 for Risk« wurden die Prinzipien nochmals geschärft und das Prinzip »Funktion als Teil der täglichen Aktivitäten« in das Prinzip »Verwendung eines konsistenten, auf die Strategie abgestimmten Ansatzes« integriert, da dieser Ansatz Teil der täglichen Aktivitäten werden sollte.

Richtlinien

Richtlinien bieten detailliertere Anleitungen, wie die Prinzipien in die Praxis umgesetzt werden können.

Das COBIT 2019-Kernmodell beschreibt typische Richtlinien in der Komponente »Richtlinien und Verfahren«. Im COBIT 2019-Kernmodell werden in den zentralen, für das Risikomanagement relevanten Governance- und Managementzielen EDM03 und APO12 mit der »Richtlinie zum Unternehmensrisiko« und der »Betrugsrisikorichtlinie« bereits zwei zentrale Richtlinien für das Risikomanagement aufgeführt. Der Leitfaden zum Schwerpunktthema I&T-Risikomanagement gibt weitere typische Richtlinien an, die einen Bezug zum I&T-Risikomanagement haben und mit der übergeordneten Risikorichtlinie abgestimmt sein sollten.

Auf die übergeordnete »Richtlinie zum Unternehmensrisiko« (Core Risk Policy) wird im IRFA-Leitfaden detailliert eingegangen und die typischen Inhalte einer solchen Richtlinie dargestellt. Dadurch kann der Leitfaden auch als Grundlage für die Erstellung von unternehmensspezifischen Richtlinien für das I&T-Risikomanagement genutzt werden.

3.6 Kultur, Ethik und Verhalten

Die COBIT-Komponente »Kultur, Ethik und Verhalten« unterstützt die Umsetzung gewünschter kultureller Elemente innerhalb der Organisation. Im COBIT 2019-Kernmodell sind in den zentralen, für das Risikomanagement relevanten Governance- und Managementzielen EDM03 und APO12 bereits zentrale kulturelle Elemente zur Förderung des Bewusstseins für das Risikomanagement aufgeführt. Zu den wünschenswerten Verhaltensweisen auf Ebene der Governance gehören beispielsweise: die Mitarbeiter zu ermutigen, Probleme oder negative Ergebnisse anzusprechen und I&T-Risiken transparent zu machen. Auf Managementebene werden bei APO12 folgende Verhaltensweisen als wünschenswert genannt:

- Ausrichtung der Richtlinien an der definierten Risikobereitschaft,
- Berichterstattung über Risikotrends an die Unternehmensleitung und die entsprechenden Gremien,
- Wertschätzung eines effektiven Risikomanagements sowie
- proaktive Überwachung der Risiken und deren Behandlung durch den Risikoaktionsplan.

Der Leitfaden zum Schwerpunktthema I&T-Risikomanagement beschreibt weitere konkrete wünschenswerte Verhaltensweisen auf drei Ebenen:

- Allgemeines unternehmensweites Verhalten,
- Verhalten der Risikoexperten und
- Verhalten des Managements.

Beispielsweise wird die im Governance-Ziel EDM03 aufgeführte positive Einstellung zur Ansprache von Problemen oder negativen Ergebnissen dem unternehmensweiten Verhalten zugeordnet. Die im COBIT 2019-Kernmodell beim Managementziel APO12 erwähnte Berichterstattung über Risikotrends an das Management oder die Wertschätzung eines effektiven Risikomanagements wird dem Verhalten des Managements zugeordnet.

Der IRFA-Leitfaden führt aber nicht nur deutlich mehr erwünschte Verhaltensweisen auf, sondern erläutert das erwünschte Verhalten auch weitergehend. Analog zum Leitfaden »COBIT 5 for Risk« wird zusätzlich in einem separaten Kapitel dargestellt, wie Management und Risikopraktiker das Verhalten beeinflussen können, und dies mit Beispielen illustriert.

3.7 Dienste, Infrastruktur und Anwendungen

Dienste, Infrastruktur und Anwendungen sind eine wichtige Unterstützung für die Erreichung der Governance- und Managementziele und unterstützen vor allem die Prozessdurchführung. Im COBIT 2019-Kernmodell werden in den zentralen, für das Risikomanagement relevanten Governance- und Managementzielen EDM03 und APO12 bereits typische Dienste und Anwendungen für das Risikomanagement aufgeführt, wie ein Risikomanagementsystem, Krisenmanagement-Services, GRC-Tools (Governance, Risiko und Compliance), Risikoanalyse-Werkzeuge oder Risk Intelligence Services.

Analog zum Leitfaden »COBIT 5 for Risk« wird diese Aufzählung im Leitfaden zum Schwerpunktthema I&T-Risikomanagement erweitert und jeder Dienst sowie jede Infrastrukturkomponente und Anwendung werden kurz erläutert.

Beispielsweise werden die bereits im Kernmodell nur erwähnten »Risk Intelligence Services« als Dienste beschrieben, die sowohl taktische als auch strategische Informationen über Bedrohungen, Schwachstellen und Vermögenswerte liefern, um Entscheidungen über Unternehmensrisiken zu unterstützen.

4 I&T-risikospezifische Erweiterung des COBIT 2019-Kernmodells

Das vierte Kapitel macht mit knapp 100 Seiten den Hauptteil des Leitfadens zum Schwerpunktthema I&T-Risikomanagement aus. In diesem vierten Kapitel werden die relevanten 23 Governance- und Managementziele um I&T-risikorelevante Elemente ergänzt. Dabei wird für jedes relevante Governance- und Managementziel die besondere Bedeutung für das I&T-Risikomanagement benannt. Beispielsweise sollte für das Managementziel APO10 »Lieferanten sind gemanagt« das I&T-Risiko in Bezug auf die Lieferanten des Unternehmens ermittelt und angemessen gesteuert werden.

Auf Ebene der Prozesse (Komponente A des Kernmodells) werden die Prozesspraktiken des COBIT 2019-Kernmodells um I&T-risikospezifische Metriken und Aktivitäten ergänzt. Beispielsweise sind beim Managementziel APO10 bei der Prozesspraktik APO10.01 »Identifizieren und Evaluieren der Lieferantenbeziehungen und -verträge« die nachfolgend dargestellten zwei I&T-risikospezifischen Aktivitäten inklusive ihres Fähigkeitsgrads ergänzt worden.

I&T-risikospezifische Aktivitäten zur Prozesspraktik APO10.01	Fähigkeitsgrad
Durchführung von Bewertungen der Informationsrisiken und Festlegung des Informationsrisikoprofils	3
Definition der Lieferantenbeziehung und der Anforderungen auf der Grundlage des Informationsrisikoprofils	3

Tab. 3: I&T-risikospezifische Aktivitäten zur Prozesspraktik APO10.01

Die Prozesspraktik APO10.01 wurde zudem um zwei I&T-risikospezifische Beispielmetriken ergänzt:

a. Prozentsatz der Anbieter, die sich einer formellen I&T-Risikobewertung unterzogen haben
b. Prozentsatz der beauftragten Lieferanten ohne I&T-Risikobewertung

Auf Ebene der Informationsflüsse und -elemente (Komponente C des Kernmodells) wurden die entsprechenden I&T-risikospezifischen Inputs und Outputs ergänzt. Im genannten Beispiel der Prozesspraktik APO10.01 wird der zu den neuen I&T-risikospezifischen Aktivitäten passende Output »Risikomanagementplan für Lieferanten« genannt.

Eine weitere I&T-risikospezifische Ergänzung erfolgte beim Managementziel APO10 bei der Prozesspraktik APO10.05 »Überwachen der Lieferantenleistung und -Compliance«. Dort wurde eine I&T-risikospezifische Aktivität inklusive ihres korrespondierenden Fähigkeitsgrads ergänzt.

I&T-risikospezifische Aktivitäten zur Prozesspraktik APO10.05	Fähigkeitsgrad
Sicherstellen, dass Risikoprobleme überwacht werden, um festzustellen, welche noch nicht behoben wurden oder bei welchen sich die geplante Behebung verzögert	3

Tab. 4: I&T-risikospezifische Aktivitäten zur Prozesspraktik APO10.05

Auf Ebene der Informationsflüsse und -elemente werden bei der Prozesspraktik APO10.05 dazu passend als I&T-risikospezifischer Input der »Bericht über Compliance-Verstöße von Lieferanten« und als Output der »Mängelbeseitigungsplan des Lieferanten« aufgeführt.

Die Ergänzungen fügen sich nahtlos in das COBIT 2019-Kernmodell ein und unterstützen die Integration von I&T-Risikomanagement in alle Prozesse. Insbesondere für Unternehmen aus regulierten Branchen sind diese Ergänzungen sogar als notwendig zu erachten – man denke beim Thema Lieferantenmanagement nur an die bankaufsichtlichen Anforderungen an die IT (BAIT) [BaFin 2021] zum sonstigen Fremdbezug von IT-Dienstleistungen.

5 Anhänge

Der IRFA-Leitfaden wird durch Anhänge abgerundet, in denen sich viele nützliche gute Praktiken für die Umsetzung finden, die teilweise aus anderen ISACA-Produkten übernommen wurden.

A I&T-Risikoszenarien
In Anhang A werden tabellarisch in 18 Risikoszenario-Kategorien beispielhaft generische und allgemeine I&T-Risikoszenarien aufgelistet. Diese Tabelle ist unverändert aus dem »Risk IT Practitioner Guide« [ISACA 2020b] übernommen worden.

B Mapping Risikoszenario-Kategorien zu COBITs Governance- und Managementzielen
In Anhang B werden die 18 Risikoszenario-Kategorien den 40 Governance- und Managementzielen des COBIT 2019-Kernmodells zugeordnet und deren Korrelation mit »hoch«, »mittel«, »niedrig« oder »nicht vorhanden« bewertet. Die Zuordnungstabelle ist aus dem »COBIT Design Guide« [ISACA 2018b] übernommen worden. Es wurde lediglich die numerische Skala (0 bis 4) auf eine Ordinalskala (nicht vorhanden (0) bis hoch (3+4)) umgeändert.

C Vorlage für Eintrag ins Risikoregister
In Anhang C befindet sich eine Vorlage für einen Risikoeintrag ins Risikoregister. Diese Vorlage wurde inhaltlich unverändert aus dem Anhang des Umsetzungsleitfadens »COBIT 5 for Risk« [ISACA 2013] übernommen.

D Beispiele für eine Berichterstattung über IT-Risiken
In Anhang D werden Beispiele für ein IT-Risikoindikator-Dashboard sowie für vier IT-Risikotrend-Diagramme aufgeführt. Das Dashboard referenziert konzeptionell auf das COBIT 2019-Kernmodell und zeigt drei Ebenen von Indikatoren an:

- Indikatoren für die geschäftlichen Auswirkungen (Ebene Unternehmensziele)
- Risikoindikatoren (Ebene IT-bezogene Ziele) und
- Kontrollindikatoren (Ebene COBIT-Managementpraktiken).

E Beispiele für Risikokarten
In Anhang E werden zwei Varianten einer Risikokarte dargestellt. Diese wurden unverändert aus dem »Risk IT Practitioner Guide« [ISACA 2020b] übernommen.

6 Zusammenfassung

Das Thema Risikomanagement ist insbesondere mit den beiden Governance- und Managementzielen EDM03 und APO12 im COBIT 2019-Rahmenwerk bereits grundsätzlich abgedeckt.

Der neue Leitfaden zum Schwerpunktthema I&T-Risikomanagement (COBIT Focus Area: Information and Technology Risk, IRFA) ergänzt vor allem die Prozesse im COBIT 2019-Kernmodell um Aspekte des I&T-Risikomanagements. Das Kernmodell von COBIT 2019 wird so themenspezifisch erweitert und kann damit als Referenz für die Governance und das Management der I&T-Risiken dienen. Mit den Fähigkeitsgraden für die I&T-risikospezifischen Aktivitäten sowie den I&T-risikospezifischen Metriken sind auch die COBIT-Elemente zur Beurteilung der Umsetzung des I&T-Risikomanagements im Unternehmen berücksichtigt worden. Für die anderen COBIT-Komponenten wurden weitgehend die relevanten Inhalte des Umsetzungsleitfadens »COBIT 5 for Risk« übernommen, aber an vielen Stellen deutlich entschlackt zugunsten einer besseren Lesbarkeit.

Mit diesem Leitfaden zum Schwerpunktthema I&T-Risikomanagement ist die für viele Unternehmen wünschenswerte Ergänzung des Kernmodells von COBIT 2019 für das I&T-Risikomanagement erfolgt. Zusammen mit den bereits veröffentlichten Risk-IT-Büchern gibt die ISACA allen, die sich mit dem Thema IT-Risikomanagement beschäftigen, einen strukturierten Ansatz für die Anwendung der COBIT-Prinzipien für die Steuerung und für das Management von I&T-Risiken an die Hand, der mit guten Praktiken unterlegt ist. Der Leitfaden zum Schwerpunktthema I&T-Risikomanagement erweitert das COBIT 2019-Rahmenwerk praxisnah und ermöglicht Risikospezialisten, das per Definition offene und flexible Rahmenwerk COBIT 2019 für ihre Zwecke optimal zu nutzen.

Literatur

[BaFin 2021] *Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin):* Bankaufsichtliche Anforderungen an die IT (BAIT), Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021.

[Gaulke 2020a] Gaulke, M.: COBIT Focus Area: Information Security. IT-Governance 14 (2020), 32, S. 25-30.

[Gaulke 2020b] Gaulke, M.: Praxiswissen COBIT: Grundlagen und praktische Anwendung in der Unternehmens-IT. 3., aktualisierte und überarbeitete Auflage, dpunkt.verlag, 2020.

[ISACA 2009a] *ISACA (Hrsg.):* The Risk IT Framework, 2009.

[ISACA 2009b] *ISACA (Hrsg.):* The Risk IT Practitioner Guide, 2009.

[ISACA 2013] *ISACA (Hrsg.):* COBIT® 5 for Risk, 2013.

[ISACA 2018a] *ISACA (Hrsg.):* COBIT® 2019 Framework: Governance and Management Objectives, 2018.

[ISACA 2018b] *ISACA (Hrsg.):* COBIT® 2019 Design Guide: Implementing and Optimizing an Information and Technology Governance Solution, 2018.

[ISACA 2020a] *ISACA (Hrsg.):* Risk IT Framework, 2nd edition, 2020.

[ISACA 2020b] *ISACA (Hrsg.):* Risk IT Practitioner Guide, 2nd edition, 2020.

[ISACA 2021] *ISACA (Hrsg.):* COBIT Focus Area: Information and Technology Risk, 2021.



Markus Gaulke

ist Senior Manager und Prokurist bei der KPMG AG Wirtschaftsprüfungsgesellschaft in Frankfurt. Dort berät er Finanzdienstleister vor allem im Umfeld der IT-Governance und IT-Compliance. Daneben ist er Vorstandsmitglied im deutschen Zweig des Berufsverbandes ISACA und Autor des Buches »Praxiswissen COBIT«.

Diplom-Betriebswirt Markus Gaulke
KPMG AG Wirtschaftsprüfungsgesellschaft
THE SQUAIRE/Am Flughafen
60549 Frankfurt am Main
mgaulke@kpmg.com
www.kpmg.de
www.markus-gaulke.de

Impressum

IT-Governance
Fachzeitschrift des Germany Chapter of »The Information Systems Audit and Control Association« e.V. (ISACA)

http://it-governance.dpunkt.de/

16. Jahrgang – Heft 35 – Juni 2022
ISSN: 1864-6557
© dpunkt.verlag GmbH
Wieblinger Weg 17, 69123 Heidelberg
Tel. 06221 1483-0, Fax 06221 1483-99
www.dpunkt.de

Vertrieb:
Evelin Wilbert
Tel. 06221 1483-40, wilbert@dpunkt.de

Redaktion:
Christa Preisendanz,
red-itgov@dpunkt.de

Anzeigen:
Julia Griebel
Tel. 06221 1483-50, anzeigen@dpunkt.de

Satz + Herstellung: Frank Heidt
Copy-Editing: Ursula Zimpfer, Herrenberg
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck: Wörmann PRODUCTION CONSULT, www.wp-consult.eu

Bezugsbedingungen (Stand 1.1.2022): Erscheinungsweise: 2 Ausgaben pro Jahr, Preis: €28,50 zzgl. Versandkosten (Inland: €3,50/Ausland: €7,80). GI-, OCG-, ASQF- und swissICT-Mitglieder erhalten eine Ermäßigung von 25%. Das Studenten-Abo kostet €18,00 zzgl. der Versandkosten (gegen Vorlage der Immatrikulationsbescheinigung). Das Einzelheft kostet €17,20 zzgl. Versandkosten.

Das Abonnement ist 8 Wochen vor Ablauf des Bezugszeitraums schriftlich kündbar.

Die Zeitschrift sowie alle in ihr enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Fotokopien für den persönlichen und sonstigen eigenen Gebrauch dürfen nur von einzelnen Beiträgen oder Teilen daraus als Einzelkopien hergestellt werden. Jede im Bereich eines gewerblichen Unternehmens hergestellte oder benützte Kopie dient gewerblichen Zwecken gemäß § 54 (2) UrhG und verpflichtet zur Gebührenzahlung an die VG WORT, Abteilung Wissenschaft, Goethestraße 49, 80336 München, von der die Zahlungsmodalitäten zu erfragen sind. Die Wiedergabe von Warenbezeichnungen in dieser Zeitschrift berechtigt auch ohne Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutzgesetzgebung als frei zu betrachten wären.

Vorschau* auf Heft 36 der »IT-Governance« (Dezember 2022)

Für Heft 36 der »IT-Governance« sind Fach- und Praxisbeiträge zu den Themen Prüfung digitaler Geschäftsmodelle, COBIT® for Small and Medium Enterprises using COBIT 2019 und Herausforderungen des Einsatzes von KI geplant sowie Artikel für die Rubriken »Zum Thema«, »Standards« und »IT-Prüfung« sowie Buchbesprechungen.

Wenn Sie zu einer der nächsten Ausgaben der »IT-Governance« einen Beitrag leisten möchten oder Anregungen haben, wenden Sie sich bitte an red-itgov@dpunkt.de.

Um sicherzugehen, dass Ihr Vorschlag bei entsprechender Eignung berücksichtigt werden kann, sollte dies bitte spätestens ca. 4 Monate vor Erscheinungstermin des jeweiligen Heftes erfolgen.

* Änderungen vorbehalten.

Inserentenverzeichnis

dpunkt.verlag GmbH, Heidelberg – 12, 20

ISACA Germany Chapter e.V., Berlin – Umschlaginnenseite vorne, Umschlagaußenseite hinten

IT-Compliance Implementation GmbH, Essen – 23

TLGG, Berlin – Umschlaginnenseite hinten

»IT-Governance« – Aims & Scope

»IT-Governance« adressiert die Herausforderungen des modernen IT-Managements und vermittelt aktuelles Wissen über wegweisende und beispielhafte Methoden, Konzepte und Erfolgsfaktoren der IT-Governance für Management, Berater, Auditoren und Wissenschaftler. Die Artikel umfassen Überblicksdarstellungen, Analysen, Forschungsergebnisse, Fallstudien, Success Stories und Tutorials. Sie sind praxisorientiert und reflektieren theoretische Konzepte sowie den aktuellen Stand der Forschung. Einen Schwerpunkt der Beiträge bilden einerseits Informationen rund um das Referenzmodell »Control Objectives for Information and related Technology« (COBIT), andererseits Ergebnisse, die in den ISACA-Arbeitskreisen erzielt werden.

Ein Serviceteil enthält außerdem Informationen zu Standards, IT-Prüfung und neuen Büchern aus dem Themenumfeld der IT-Governance.

»IT-Governance« ist die Fachzeitschrift des Germany Chapter der »Information Systems Audit and Control Association« e.V. (ISACA).

»IT-Governance« wird herausgegeben von
Dr. Martin Fröhlich
Prof. Dr. Matthias Goeken
Prof. Dr. Michael Klotz
Ingo Struckmeyer
(verantwortlicher Schriftleiter)
Marc Weber
(hrsg-itgov@dpunkt.de)