

Praxiswissen COBIT



Markus Gaulke, Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC) und Project Management Professional (PMP), ist in Deutschland der führende Experte zum Thema COBIT und dessen Anwendung. Als das für COBIT zuständige Vorstandsmitglied im deutschen Chapter des internationalen IT-Berufsverbands »ISACA« hat er die COBIT-Zertifikate »COBIT Practitioner« für COBIT 4.1 und »IT-Governance & IT-Compliance Practitioner« für COBIT 5 ins Leben gerufen. Weiterhin entwickelte er zusammen mit der Hochschule Frankfurt School of Finance and Management die weiterführenden Zertifikate »IT-Governance-Manager« und »IT-Compliance-Manager«.

Markus Gaulke hat inzwischen weit über 1.000 Teilnehmer in COBIT und dessen Anwendung in unterschiedlichsten Veranstaltungsformaten geschult. Darüber hinaus hat er zur Anwendung von COBIT im Umfeld von IT-Governance, IT-Compliance und Risikomanagement zahlreiche Artikel und Fachbeiträge verfasst.

International war er als Mitautor an der deutschen Fassung von COBIT 4.0 sowie am internationalen ISACA-Standardwerk »Control Objectives for Basel II« beteiligt. Weiterhin hat er das Übersetzungsteam für die deutschen Versionen von COBIT 5 geleitet.

Beruflich ist er seit mehr als 16 Jahren bei der KPMG AG Wirtschaftsprüfungsgesellschaft in Frankfurt am Main für die IT-Prüfung und IT-Beratung von Unternehmen vor allem aus dem Finanzsektor zuständig. Die Praxisbeispiele in diesem Buch entstammen konkreten Beratungssituationen aus seiner Berufspraxis.

Markus Gaulke

Praxiswissen COBIT

**Grundlagen und praktische Anwendung
in der Unternehmens-IT**

2., aktualisierte und überarbeitete Auflage



dpunkt.verlag

Markus Gaulke
www.markus-gaulke.de

Lektorat: Vanessa Wittmer
Copy-Editing: Annette Schwarz, Ditzingen
Herstellung: Frank Heidt
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-86490-055-6

2., aktualisierte und überarbeitete Auflage 2014
Copyright © 2014 dpunkt.verlag GmbH
Wieblinger Weg 17
69123 Heidelberg

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

Vorwort

IT-Governance, IT-Risikomanagement, IT-Compliance, IT-Assurance und IT-Outsourcing sind wichtige Themen für das Management der Unternehmens-IT. Die aus diesen Themen erwachsenen Herausforderungen zu lösen, gelingt in der Praxis nur effizient, wenn ein ganzheitliches Verständnis für diese Themen vorhanden ist und die Aktivitäten in ein passendes Rahmenwerk eingebunden werden.

COBIT 5 stellt ein solches Rahmenwerk für die IT-Governance und das IT-Management dar. COBIT 5 ist ein umfassendes, integratives Rahmenwerk für eine effektive Governance und ein effektives Management der Unternehmens-IT und umfasst Methoden, Prinzipien, gute Praktiken und Leitfäden, die erforderlich sind, um eine optimale Wertschöpfung durch den IT-Einsatz im Unternehmen zu erreichen. Durch seine Konzentration auf sieben wichtige Umsetzungskomponenten (Enabler) für die IT-Governance und das IT-Management ist COBIT 5 unabhängig von Technologie und Branche. Dieses Enabler-Modell kann als Referenzmodell sowohl vom operativen IT-Management als auch vom Business Management gemeinsam verwendet werden.

COBIT strukturiert in diesem Zusammenhang alle Prozesse, die gewöhnlich in der IT-Funktion einer Organisation stattfinden, in einem Prozessmodell. Dieses berücksichtigt die Inhalte der weltweit am meisten eingesetzten Modelle, Praktiken und Standards im IT-Bereich, wie z. B. ITIL, COSO, ISO/IEC 38500, ISO/IEC 20000, ISO/IEC 9001, ISO/IEC 15504, PMBOOK, PRINCE2, CMMI und TOGAF. Dadurch stellt COBIT 5 ein umfassendes Prozessreferenzmodell für bewährte Verfahren der IT-Governance und des IT-Managements bereit.

COBIT 5 ist aber mehr als nur ein Referenzmodell für die Governance und das Management der Unternehmens-IT. COBIT 5 kann durch die integrierten Assessment-Modelle auch zum Benchmarking, zur Prozessbewertung und zur Gap-Analyse eingesetzt werden. Dabei richtet sich COBIT 5 nicht nur an IT-Fachleute, sondern stellt über die Ausrichtung an die Geschäftsprozesse auch den Geschäftsprozesseigentümern ein Rahmenwerk für das Management der Unternehmens-IT (Technologie-management) sowie der Geschäfts- und Bereichsleitung durch die vorhandenen Prozessmerkmale und -kennzahlen ein ganzheitliches Modell für die Governance, die Compliance und die Steuerung der Unternehmens-IT zur Verfügung.

COBIT wird weltweit von Tausenden von Unternehmen als Basis für ihre IT-Governance- und IT-Compliance-Aktivitäten herangezogen. Im deutschen Sprachraum ist die Akzeptanz von COBIT in den letzten Jahren deutlich gestiegen, im globalen Vergleich aber immer noch vergleichsweise niedrig. International hat sich COBIT als anerkanntes Rahmenwerk für die Governance und das interne Kontrollsystem in der Informationstechnologie etabliert. COBIT wurde sowohl von namhaften Unternehmen in das eigene interne Kontrollsystem integriert (u.a. Daimler, Philips) als auch von Behörden (u.a. amerikanisches Verteidigungsministerium, European Agricultural Guidance and Guarantee Fund) und anderen Institutionen (u.a. META-Group, Gartner) als Standard empfohlen. Die Aufsichtsbehörden einiger Länder haben COBIT sogar für verbindlich erklärt (u.a. Türkei, Kolumbien, Uruguay).

Das vorliegende Buch will den Lesern COBIT 5 und seine zahlreichen Elemente sowie die Grundzüge der dem Rahmenwerk zugrunde liegenden Konzepte erklären und vor allem Praxisbeispiele und Ideen für die Anwendung von COBIT 5 vorstellen. Durch die dargestellten Anwendungsbeispiele und Praxisbeiträge soll das Buch zum Gebrauch von COBIT animieren – denn letztendlich zeigt sich der Nutzen dieses IT-Management- und IT-Governance-Rahmenwerkes nur im konkreten Einsatz.

Das ISACA Germany Chapter e.V. hat zwei der ersten Bücher der COBIT-5-Produktfamilie (Rahmenwerk und Prozessreferenzmodell) ins Deutsche übersetzen lassen und im Oktober 2012 veröffentlicht. Auf dieser Übersetzung basieren auch die Ausführungen in diesem Buch. Alle Kernbegriffe werden zusätzlich in Englisch angegeben. Dies soll eine Anwendung der Fachbegriffe im internationalen Umfeld erleichtern. Insbesondere der Anhang mit den Übersichten aller COBIT-5-Prozesse sowie der COBIT-5-Zielkaskade in Deutsch und in Englisch hat sich in der Projektpraxis als hilfreich erwiesen.

COBIT 5 bietet in der aktuellen Version einen echten Mehrwert für die Unternehmensführung zur Steuerung der Unternehmens-IT. Ich hoffe, dass dieses Buch allen Lesern hilft, das hier behandelte Rahmenwerk COBIT 5 – auch im Kontext mit anderen Praktiken, Modellen und Standards – besser zu verstehen, um COBIT 5 erfolgreich im Sinne der Unternehmensziele einzusetzen.

Markus Gaulke

Königstein im Taunus, März 2014