

Wolfgang Goltsche

**COBIT kompakt
und verständlich**

Aus dem Bereich IT erfolgreich gestalten

Visual Basic .NET mit Methode

von Heinrich Rottmann

Warum ausgerechnet .NET?

von Heinrich Rottmann

Requirements Analysis realisieren

von Karl Scharbert

Management der Software-Entwicklung

von Carl Steinweg

Das neue PL/I

von Eberhard Sturm

Projektmanagement der SW-Entwicklung

von Werner Mellis

Profikurs ABAP®

von Patrick Theobald

SAP R/3® Kommunikation mit RFC und Visual Basic

von Patrick Theobald

Six Sigma in der SW-Entwicklung

von Thomas Michael Fehlmann

Profikurs Eclipse 3

von Gottfried Wolmeringer und Thorsten Klein

User Interface-orientierte Softwarearchitektur

von Paul Chlebek

Erfolgreiche Datenbankanwendung mit SQL3

von Jörg Fritze und Jürgen Marsch

Web-basierte Systemintegration

von Harry Marsh Sneed und Stephan Henry Sneed

Terminalserver mit Citrix Metaframe XP

von Thomas Joos

Exchange Server 2000

von Thomas Joos

Profikurs PHP-Nuke

von Jens Ferner

Unternehmensweites Datenmanagement

von Rolf Dippold, Andreas Meier, Walter Schneider und Klaus Schwinn

Netzarchitektur – Kompass für die Realisierung

von Thomas Spitz, Markus Blümle und Holger Wiedel

SIP – Die Technik

von Andreas Kanbach

IT-Sicherheit – Make or Buy

von Marco Kleiner, Lucas Müller und Mario Köhler

Mehr IT-Sicherheit durch Pen-Tests

von Enno Rey, Michael Thumann und Dominick Baier

IT-Risiko-Management mit System

von Hans-Peter Königs

IT-Sicherheit mit System

von Klaus-Rainer Müller

Der IT Security Manager

von Heinrich Kersten und Gerhard Klett

COBIT kompakt und verständlich

von Wolfgang Goltsche

Wolfgang Goltsche

COBIT kompakt und verständlich

**Der Standard zur IT Governance –
So gewinnen Sie Kontrolle über
Ihre IT – So steuern Sie Ihre IT und
erreichen Ihr Ziele**

Mit 92 Abbildungen



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.

Das in diesem Werk enthaltene Programm-Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor übernimmt infolgedessen keine Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne von Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage September 2006

Alle Rechte vorbehalten

© Friedr. Vieweg & Sohn Verlag | GWV Fachverlage GmbH, Wiesbaden 2006

Lektorat: Günter Schulz / Andrea Broßler

Der Vieweg-Verlag ist ein Unternehmen von Springer Science+Business Media.

www.vieweg.de



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Konzeption und Layout des Umschlags: Ulrike Weigel, www.CorporateDesignGroup.de

Umschlagbild: Nina Faber de.sign, Wiesbaden

Druck- und buchbinderische Verarbeitung: MercedesDruck, Berlin

Printed in Germany

ISBN-10 3-8348-0141-0

ISBN-13 978-3-8348-0141-8

Der Begriff der IT-Governance und der des IT Service Managements ist heute in aller Munde. Dies können Sie leicht feststellen, wenn Sie nur die einschlägigen Fachzeitschriften oder auch das Internet bemühen und nach diesen beiden Begriffen suchen. Dabei werden Sie höchstwahrscheinlich zwei Dinge feststellen: Erstens ist weder der Begriff der IT-Governance noch der Begriff des IT Service Managements einheitlich geklärt, und zweitens beziehen sich viele Autoren auf die beiden Begriffe COBIT und ITIL. COBIT steht für „Control Objectives for Information and related Technology“ ein vom IT-Governance Institute geprägter Ausdruck, und ITIL für „IT Infrastructure Library“, eine Abkürzung, die vom Office of Government Commerce geprägt wurde. Beide Begriffe werden in diesem Buch erläutert und in einen Kontext gestellt.

Dieses Buch soll in COBIT einführen und verwendet daher auch die Definitionen von COBIT. Im ersten Schritt wird erläutert, was bei COBIT unter Governance und speziell unter IT-Governance zu verstehen ist und was ihre Funktion darstellt. Es folgt danach eine allgemeine Einführung in COBIT und in die Grundlagen oder Quellen von COBIT. Eine komplette Auflistung der Prozesse mit jeweils einer kurzen Beschreibung runden das Bild ab. In diesem Rahmen wird auch auf die Kontrollziele von COBIT eingegangen.

Diese Einführung kann von allen IT-Interessierten, vom CIO bis zum Laien, genutzt werden, um sich ein Bild von COBIT zu machen und zu verstehen, worum es in diesem Modell geht.

Da viele der Abkürzungen feststehende oder allgemeine gebräuchliche Begriffe innerhalb der IT sind, wurde auf eine Übersetzung dieser Begriffe ins Deutsche verzichtet und die englische Originalabkürzung beibehalten. Diese werden aber im Glossar übersetzt, und es sollte mithin keine Schwierigkeiten bei der Verwendung der Begriffe geben.

Jeder einzelne Prozess wird im Überblick erläutert. Für eine Implementierung von COBIT sind weitergehende Informationen notwendig. Diese Ausarbeitung gibt Ihnen aber einen guten Überblick über die Gesamtheit von COBIT, und Sie haben dadurch die Möglichkeit, die Implementierungen zu bewerten, in

dem diese den Prozessen und den angeführten Kontrollen gegenübergestellt werden.

COBIT ist ein lebender Standard. Es ist daher möglich, dass sich bereits mehr Informationen finden lassen, als ich sie hier aufnehmen konnte. Bitte benutzen Sie für die Suche nach aktuellen Informationen die im Kapitel „COBIT Publikationen und Literaturverzeichnis“ aufgeführten Links und Literaturhinweise. Diese Ausarbeitung beruht auf der Version 4 von COBIT.

Auch wenn es sich empfiehlt, die ersten Kapitel zunächst zu lesen, müssen Sie diese Ausarbeitung nicht Kapitel für Kapitel durcharbeiten. Nach dem Lesen der ersten Kapitel können Sie das Werk auch als Nachschlagewerk benutzen.

Haben Sie Anregungen oder Fragen, Verbesserungen an dem Text? Bitte schreiben Sie mir. Jede Anregung ist willkommen.

Ich wünsche Ihnen viel Spaß und Freude beim Lesen, denn Sie werden einen umfassenden Standard für die IT-Governance kennen lernen, der in den nächsten Jahren immer bedeutender werden wird.

Ritterhude, im Juli 2006, Wolfgang Goltsche

Inhaltsverzeichnis

1	Einführung	1
1.1	IT-Governance – Eine Einführung.....	1
1.2	Modelle und Initiativen	7
1.2.1	COSO	8
1.2.2	ITIL.....	9
1.2.3	COBIT	11
1.2.4	Sonstige Frameworks.....	13
1.3	Qualität, Reifegradmodelle und Steuerungsinstrumente.....	13
1.3.1	Kontrollzyklus nach Deming.....	13
1.3.2	Normen	14
1.3.3	EFQM-Modell	15
1.3.4	Modellvergleich.....	16
1.3.5	CMM / Spice (ISO/IEC 15504)	17
1.3.6	Steuerungsinstrumente BSC & Co.....	21
2	Die Struktur von COBIT	25
2.1	Der Governance-Würfel	25
2.2	Die Dimension der COBIT-Prozesse	27
2.2.1	Planung und Organisation (PO)	28
2.2.2	Akquisition & Implementierung.....	30
2.2.3	Delivery & Support	31
2.2.4	Monitoring und Evaluierung	33
2.3	Ressourcen	34
2.4	Geschäftsanforderungen	35
2.5	Gesamtprozessübersicht.....	42

3

COBIT-Prozessbeschreibung	45
3.1 Die verwendete Prozessdarstellung.....	45
3.2 PO Planung und Organisation.....	51
3.2.1 PO1 Definieren eines strategischen Plans.....	51
3.2.2 PO2 Definieren der Informationsarchitektur.....	54
3.2.3 PO3 Festlegen der technischen Ausrichtung	57
3.2.4 PO4 Definieren der IT-Organisation und ihrer Beziehungen.....	60
3.2.5 PO5 IT-Investitionsmanagement	64
3.2.6 PO6 Kommunizieren der Management-Ziele und Strategien	67
3.2.7 PO7 Personalführungsmanagement.....	70
3.2.8 PO8 Qualitätsmanagement.....	73
3.2.9 PO9 Risikomanagement	76
3.2.10 PO10 Projektmanagement.....	79
3.3 AI Akquisition und Implementierung.....	83
3.3.1 AI1 Identifizierung automatisierter Lösungen	83
3.3.2 AI2 Erwerb und Pflege von Applikationssoftware	86
3.3.3 AI3 Erwerb und Pflege der technischen Infrastruktur.....	89
3.3.4 AI4 Befähigen des Betriebes	92
3.3.5 AI5 Zur Verfügung stellen von IT-Ressourcen.....	95
3.3.6 AI6 Change Management	98
3.3.7 AI7 Installieren und Abnehmen von Systemen und Änderungen.	101
3.4 DS Delivery und Support.....	104
3.4.1 DS1 Service Level Management	104
3.4.2 DS2 Lieferanten-Management (Third Party Services)	108
3.4.3 DS3 Performance und Kapazitätsmanagement	111
3.4.4 DS4 Continuity Management.....	114
3.4.5 DS5 Security Management.....	117
3.4.6 DS6 Kostenmanagement.....	120
3.4.7 DS7 Anwenderschulung und Training	123
3.4.8 DS8 Anwenderunterstützung	126

3.4.9	DS9 Konfigurationsmanagement.....	129
3.4.10	DS10 Problem Management.....	132
3.4.11	DS11 Data Management	135
3.4.12	DS12 Facility Management	138
3.4.13	DS13 Operationsmanagement.....	141
3.5	ME Monitoring und Überwachung (Monitoring and Evaluation).....	144
3.5.1	ME1 Überwachen und evaluieren der IT-Performance.....	144
3.5.2	ME2 Überwachung und Begutachtung der internen Kontrollen...	147
3.5.3	ME3 Sicherstellung der Einhaltung gesetzlicher Vorschriften.....	150
3.5.4	ME4 Sorgen für IT-Governance	153
4	IT-Governance-Implementierung	157
4.1	Einführung von COBIT	157
4.2	Methodisches Vorgehen.....	158
4.3	Verfügbare Tools	160
5	COBIT-Publikationen und Literaturverzeichnis	163
5.1	Struktur der Publikationen.....	163
5.1.1	Board Briefings	164
5.1.2	Framework und Control Objectives.....	164
5.1.3	Management Guidelines.....	164
5.1.4	IT Assurance Guide	166
5.1.5	IT Control Objectives for SOA	167
5.1.6	Implementation Guide.....	167
5.2	Weitere Publikationen	168
Glossar		169
Schlagwortverzeichnis.....		171