Klotz, Michael

Working Paper

IT-Compliance nach COBIT: Gegenüberstellung zwischen COBIT 4.0 und COBIT 5

SIMAT Arbeitspapiere, No. 06-14-025

Provided in Cooperation with:
Hochschule Stralsund, Stralsund Information Management Team (SIMAT)

Suggested Citation: Klotz, Michael (2014) : IT-Compliance nach COBIT: Gegenüberstellung zwischen COBIT 4.0 und COBIT 5, SIMAT Arbeitspapiere, No. 06-14-025, Fachhochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund, https://nbn-resolving.de/urn:nbn:de:0226-simat06140251

This Version is available at:
https://hdl.handle.net/10419/90163

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 06-14-025

IT-Compliance nach COBIT® – Gegenüberstellung zwischen COBIT® 4.0 und COBIT® 5

Prof. Dr. Michael Klotz

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team

Januar 2014

ISSN 1868-064X

Klotz, Michael: IT-Compliance nach COBIT – Gegenüberstellung zwischen COBIT 4.0 und COBIT 5. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2014 (SIMAT AP, 6 (2014), 25), ISSN 1868-064X

Download über URN vom Server der Deutschen Nationalbibliothek:
http://nbn-resolving.de/urn:nbn:de:0226-simat06140251

Impressum

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team
Zur Schwedenschanze 15
18435 Stralsund
www.fh-stralsund.de
www.simat.fh-stralsund.de

Herausgeber

Prof. Dr. Michael Klotz
Fachbereich Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@fh-stralsund.de

Autor

Prof. Dr. Michael Klotz lehrt und forscht am Fachbereich Wirtschaft der FH Stralsund auf den Gebieten der Unternehmensorganisation und des Informationsmanagements. Er ist u. a. Wissenschaftlicher Leiter des SIMAT, regionaler Ansprechpartner der gfo Gesellschaft für Organisation e.V., Mitglied des wissenschaftlichen Beirats und Academic Advocate der ISACA sowie Mitherausgeber der Zeitschrift „IT-Governance“.

IT-Compliance nach COBIT® – Gegenüberstellung von COBIT® 4.0 und COBIT 5®

Prof. Dr. Michael Klotz[1]

Zusammenfassung: IT-Compliance ist mittlerweile integraler Bestandteil des IT-Managements. Die Zielsetzung der nachweislichen Konformität mit Gesetzen und anderen rechtlichen Regularien, aber auch mit Normen, Standards und internen Richtlinien ist allgemein akzeptiert. Aufgabenumfang, Methoden und Techniken der IT-Compliance sind in Theorie und Praxis derzeit jedoch noch im Fluss begriffen. Eine Orientierung kann hier das IT-Governance-Framework "COBIT" (Control Objectives for Information and Related Technology) bieten. Mit der aktuellen fünften Version ("COBIT 5") wurden grundlegende Erweiterungen und Änderungen des Frameworks vorgenommen. Inwieweit sich dies auf das IT-Compliance-Verständnis und das Management von IT-Compliance ausgewirkt hat, wird in diesem Arbeitspapier untersucht. Hierzu werden die vierte und die fünfte Version von COBIT auf ihre compliance-relevanten Aussagen hin untersucht und vergleichend gegenübergestellt. Im Ergebnis weist COBIT 4.0 in seiner Struktur zahlreiche Inkonsistenzen auf und behandelt die Compliance-Thematik eher beiläufig. Zwar ist Compliance in den Unternehmens- bzw. IT-Zielen verankert, aber die Compliance betreffenden IT-Prozesse sind im Vergleich zu COBIT 5 begrenzt. So beinhalten in COBIT 5 insgesamt 26 von 37 Prozessen Compliance-Aufgaben, während dies in COBIT 4.0 lediglich für 4 bzw. 11 von 34 IT-Prozessen gilt.

Das Compliance-Verständnis von COBIT 5 umfasst sowohl die IT-Compliance als auch die IT-gestützte Corporate Compliance. Diese Unterscheidung wird bereits im Zielsystem im Rahmen der generischen Unternehmens- und der IT-Ziele abgebildet. Die für Compliance relevanten Regelwerke sind entweder externer Herkunft, wie im Falle von Gesetzen und behördlichen Vorgaben (auch Verträge werden dieser Gruppe zugeordnet), oder stammen aus dem Unternehmen selbst. Hierbei handelt es sich dann um Richtlinien, Verfahrensbeschreibungen, Hausstandards u. Ä. Durch die beträchtliche Erweiterung der Compliance-Thematik kann COBIT 5 – insbesondere das Framework-Dokument in Verbindung mit dem prozessorientierten Enabler-Handbuch – den mit IT-Compliance betrauten Funktionen und Personen als Orientierung und Hilfsmittel für die praktische Arbeit

[1] Prof. Dr. Michael Klotz, FH Stralsund, Fachbereich Wirtschaft, Zur Schwedenschanze 15, 18435 Stralsund, michael.klotz@fh-stralsund.de

dienen, beispielsweise bei der Definition von Compliance-Aufgaben, -Prozessen und -Verantwortlichkeiten oder bei der Einrichtung eines IT-Compliance-Managementsystems.

Gliederung

Schlüsselwörter: COBIT – Informationsmodell –IT-Compliance – IT-Management – IT-Prozesse – IT-Ziele – Prozessmodell – Unternehmensziele

JEL-Klassifikation: K12, K23, K32, K34, L15, L21, M14, M21, M42

Vorwort

Das vorliegende Arbeitspapier verbindet zwei wichtige Themen des IT-Managements: IT-Compliance und COBIT[2]. Zum einen stellt IT-Compliance ein mittlerweile sowohl in der Wissenschaft als auch in der Wirtschaft breit akzeptiertes Aufgabenfeld des IT-Managements dar. Dies lässt sich allein daran erkennen, dass im Akronym „GRC“ (bzw. der auf die Informationstechnologie bezogenen Variante „IT-GRC“) das „C“ für Compliance steht. Gleichwohl sind in Theorie und Praxis Aufgabenumfang und -abgrenzung sowie Methoden und Techniken der IT-Compliance noch im Fluss begriffen. Insofern ist es zum anderen von Interesse, das derzeit führende IT-Governance-Framework „COBIT“ (Control Objectives for Information and Related Technology) sowohl in seiner vierten als auch in seiner aktuellen fünften Version näher zu betrachten und dahingehend zu analysieren, wie das Framework die Compliance-Thematik in der IT adressiert. Hierbei wird auch immer auf die Diskussion in Wissenschaft und Fachwelt zurückgegriffen. Dennoch soll die Arbeit in erster Linie dem IT-Praktiker, der COBIT in seiner Arbeit verwendet, eine Hilfestellung und insbesondere einen schnellen Überblick über die compliance-relevanten Domänen und Prozesse von COBIT bieten.

Prof. Dr. Michael Klotz

[2] COBIT®, ISACA® und ITGI® sind eingetragene Warenzeichen der Information Systems Audit and Control Association (ISACA) und des IT Governance Institute (ITGI).

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AI	Acquire and Implement
APO	Align, Plan and Organise
AO	Abgabenordnung
BAI	Build, Acquire and Implement
BSC	Balanced Scorecard
CIO	Chief Information Officer
CMMI	Capability Maturity Model Integration
COBIT®	Control Objectives for Information and Related Technology
DS	Deliver and Support
DSB	Datenschutzbeauftragter
DSS	Deliver, Service and Support
EDM	Evaluate, Direct and Monitor
GRC	Governance – Risk – Compliance
HGB	Handelsgesetzbuch
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Informationstechnik / Informationstechnologie
ITGI	IT Governance Institute
ITIL®	Information Technology Infrastructure Library
KGI	Key Goal Indicator
KPI	Key Performance Indicator
ME	Monitor and Evaluate
MEA	Monitor, Evaluate and Assess
OLA	Operating-Level-Agreement
P	primär
PAM	Process Assessment Model
PBRM	Plan, Build, Run, Monitor
PMBOK	Project Management Body of Knowledge
PO	Plan and Organize
RACI	Responsible, Accountable, Consulted, Informed
S	sekundär
SIMAT	Stralsund Information Management Team
SLA	Service-Level-Agreement
TOGAF	The Open Group Architecture Framework
USA	United States of America

1 IT-Compliance nach COBIT 4.0

1.1 Überblick

Entstehung von COBIT

Das die Unternehmens-IT adressierende Framework „COBIT“ (Control Objectives for Information and Related Technology) wurde seit 1993 von dem in den USA ansässigen, international agierenden Prüfungsverband ISACA (Information Systems Audit and Control Association) entwickelt und erstmals im April 1996 veröffentlicht.[3,4] Die erste Version von COBIT legte – dem Namen entsprechend – den Schwerpunkt auf Anforderungen an die IT als so genannte Kontrollziele („Control Objectives“) und adressierte damit in erster Linie die Arbeit von Wirtschaftsprüfungsunternehmen. Durch die Verfolgung dieser Kontrollziele, ihre regelmäßige, systematische Überprüfung und die Umsetzung entsprechender Maßnahmen sollte in Unternehmen ein effizienter und effektiver Einsatz von IT-Ressourcen (d. h. von Anwendungen, Informationen, IT-Infrastruktur und Personal) für die Erreichung von Wettbewerbsvorteilen gewährleistet werden. An diesem Anspruch hat sich bis heute nichts geändert.

Entwicklung von COBIT

Im Verlauf der Jahre entwickelte sich COBIT zunehmend zu einem umfassenden Instrument für das IT-Management, mit dem die verschiedenen IT-Domänen und -Prozesse nicht nur nachgelagert geprüft, sondern proaktiv gestaltet werden können. Das zentrale COBIT-Framework wurde über die Versionen hinweg durch ergänzende Frameworks erweitert, zum einen durch das auf den Wertbeitrag von IT-Investitionen fokussierte Framework „Val IT“, zum anderen durch das IT-Risiko-Framework „Risk IT“.[5] Mittlerweile berücksichtigt COBIT auch wichtige Normen und Standards, z. B.

- die sog. „Information Technology Infrastructure Library”[6],
- The Open Group Architecture Framework (TOGAF),
- Project Management Body of Knowledge (PMBOK)

und verschiedene ISO/IEC-Normen, wie beispielsweise

- die ISO/IEC 20000 (für das IT-Servicemanagement),

---

[3] Dieser Abschnitt basiert auf *Klotz 2011*, S. 600-605.
[4] Nach *Gaulke 2010*, S. 8. Dort findet sich auf den S. 8-10 eine detaillierte Darstellung der Entwicklung von COBIT.
[5] Siehe *ITGI 2006* und *ISACA 2009*.
[6] Die zugehörige Abkürzung ITIL® ist ein eingetragenes Warenzeichen des Cabinet Office.

- die ISO/IEC 27005 (für das Risikomanagement im Rahmen eines Informationssicherheitsmanagementsystems) oder
- die ISO/IEC 38500 (für die IT-Governance).[7]

COBIT als Integrator

Aufgrund seiner übergeordneten Management- und Steuerungssicht kann das COBIT-Framework als Integrator dienen, wenn ein Unternehmen die gleichzeitige Nutzung dieser Normen und Standards aufeinander abstimmen will.[8] Aus dieser umfassenden Sichtweise folgte dann auch die Positionierung von COBIT als Framework für die IT-Governance.[9]

COBIT 4.0

COBIT 4.0 wurde Ende 2005 veröffentlicht, im Jahr darauf auch in deutscher Übersetzung.[10] Neben dem zentralen Dokument „COBIT 4.0“, welches das IT-Prozessmodell beinhaltet, gibt es zahlreiche weitere COBIT-Produkte, z. B. die grundlegende Darstellung „IT Governance für Geschäftsführer und Vorstände“, den prüfungsorientierten „IT Assurance Guide“ oder den die Umsetzung unterstützenden „IT Governance Implementation Guide“.[11] Im Folgenden konzentrieren sich die Ausführungen auf das COBIT 4.0-Dokument, in dem das IT-Governance-Modell und die IT-Prozesse beschrieben werden und das auch im Mittelpunkt der fachlichen Auseinandersetzung in Theorie und Praxis steht. Auf die sonstigen COBIT-Produkte wird lediglich am Rande Bezug genommen.

COBIT-Domänen

Kern von COBIT 4.0 ist das Domänen- und Prozessmodell, das aus insgesamt 34 IT-Prozessen in folgende vier Domänen besteht:

- Planung und Organisation (engl. Plan and Organize – PO);
- Beschaffung und Implementierung (engl. Acquire and Implement – AI);
- Betrieb und Unterstützung (engl. Deliver and Support – DS);
- Überwachung und Bewertung (engl. Monitor and Evaluate – ME).

---

7 Eine aktuelle Auflistung der Normen und Standards, die von COBIT integriert werden, findet sich in *ISACA 2012a*, S. 47.

8 Vgl. *ITGI 2005*, S. 197.

9 Gleichwohl richtet sich in Praxis und Wissenschaft der Fokus nach wie vor auf die Kontrollaspekte von COBIT, vgl. bspw. *Martens u. a. 2010*, *Sowa 2011*. *Böhm u. a.* sehen in der Herkunft aus dem Prüfungsbereich die Chance, dass COBIT in der Lage dazu sein kann, „konfligierende Anforderungen aus Geschäfts- und Compliance-Orientierung“ in einem zeitgemäßen IT-Management zu vereinen, *Böhm u. a. 2009*, S. 12f.

10 Mitte 2007 folgte die überarbeitete Version 4.1, die jedoch nicht mehr ins Deutsche übersetzt wurde. Zur besseren Nachvollziehbarkeit beziehen sich die weiteren Ausführungen auf die deutsche Version COBIT 4.0.

11 Siehe *ITGI 2003*, *ITGI 2007a* und *ITGI 2007b*.

Kontrollziele

Für jeden Prozess beinhaltet eine Prozessbeschreibung die von diesem IT-Prozess unterstützten Unternehmensziele und ein übergeordnetes Kontrollziel, das in 3 bis 15 detaillierte Kontrollziele in Form von normativen Aussagen untergliedert wird. Insgesamt enthalten die Prozessbeschreibungen 210 Kontrollziele, die unabhängig sowohl vom informations- und kommunikationstechnischen als auch vom geschäftlichen Umfeld (Branche, Unternehmensgröße, Organisationsstruktur etc.) sind.[12]

Compliance in COBIT 4.0

COBIT 4.0 berücksichtigt die Compliance-Thematik in verschiedener Hinsicht:

- Um die Unterstützung der Unternehmensziele durch die IT zu verdeutlichen, verwendet COBIT 4.0 ein Modell generischer Unternehmensziele, in dem zwei von zwanzig Unternehmenszielen – strukturiert nach der Systematik einer Balanced Scorecard (BSC) – die Compliance des Unternehmens adressieren. Zum einen ist dies das Ziel „Compliance mit Gesetzen und Regulativen“ (Ziel Nr. 14), zum anderen das Ziel „Compliance mit internen Regelungen“ (Ziel Nr. 16). Beide Ziele sind Bestandteil der internen BSC-Perspektive.[13]
- Weiterhin definiert COBIT 4.0 insgesamt 28 generische IT-Zielsetzungen, die durch die Ausführung der IT-Prozesse erreicht werden. Eine dieser Zielsetzungen ist das IT-Ziel „Stelle die IT-Compliance mit Gesetzen und Vorschriften sicher“ (Ziel Nr. 27). Dieses unterstützt – gemeinsam mit sechs weiteren IT-Zielsetzungen – die Erreichung des o. g. Unternehmensziels in Bezug auf Compliance mit Gesetzen und Regulativen.[14] Das compliance-bezogene IT-Ziel wiederum wird von vier IT-Prozessen unterstützt, drei ME-Prozessen und einem DS-Prozess.[15]

---

12 Vgl. *Gaulke 2010*, S. 11.

13 Vgl. *ITGI 2005*, S. 190.

14 Das Unternehmensziel in Bezug auf Compliance mit internen Regelungen wird jedoch nach der Kreuztabelle im Anhang I zu COBIT 4.0 nicht vom IT-Complianceziel unterstützt (siehe *ebd.*, S. 190), obwohl häufig interne Regelungen dazu dienen, externe Vorgaben umzusetzen. Dies ist ein erstes Beispiel für die häufig anzutreffende systematische Inkonsistenz von COBIT 4.0.

15 Nach *ebd.*, S. 191. Bei dem IT-Prozess der Domäne „Deliver and Support“ handelt es sich um den Prozess DS 11 (Manage Daten). Obwohl er dem IT-Complianceziel zugewiesen ist, ist in der zugehörigen Prozessbeschreibung das Informationskriterium „Compliance“ nicht entsprechend markiert, siehe *ebd.*, S. 157. Andererseits ist der Prozess ME 1 (Monitore und evaluiere IT-Performance) nicht dem IT-Complianceziel zugeordnet, obwohl dieser nach dem Informationskriterium „Compliance“ den Prozess immerhin sekundär unterstützt (siehe *ebd.*, S. 171) – noch eine Inkonsistenz von COBIT 4.0.

- Eine weitere Verankerung der Compliance-Thematik findet sich bei COBIT im Rahmen des IT-Risikomanagements. Mit der Positionierung von COBIT als Framework für die IT-Governance rückt auch das Risikomanagement als wichtiges Handlungsfeld des IT-Managements in den Vordergrund. Das Verständnis für Compliance-Erfordernisse wird hierbei als notwendig erachtet, um zu einem entsprechenden Bewusstsein für Compliance-Risiken und eine diesbezügliche Risikobereitschaft zu gelangen.[16] Eine diesbezügliche Unterstützungsfunktion wird einem „IT Strategy Committee“ zugeordnet, das der Unternehmensleitung bei der Steuerung und Überwachung der IT zur Seite steht.[17]
- Hinsichtlich der Verantwortlichkeit für Compliance richtet sich COBIT 4.0 explizit an interne und externe Stakeholder, die Compliance-Aufgaben wahrnehmen. Das Rollenmodell von COBIT sieht eine Rolle „Compliance, Audit, Risk und Security“ vor, in der diejenigen Stellen, Abteilungen oder Dienstleister zusammenfasst sind, denen eine Überwachungsfunktion, aber keine operative Verantwortung in der IT obliegt.[18] Aber auch die weiteren Rollen sind in unterschiedlichem Ausmaß an der Gewährleistung von Compliance beteiligt.
- Compliance stellt eines von sieben Informationskriterien („Information Criteria“) dar. Diese Informationskriterien stellen unternehmensspezifische Anforderungen dar, mit denen sich der Informationsbedarf definieren lässt. Aus der Zuordnung des Compliance-Informationskriteriums lassen sich insgesamt elf IT-Prozesse identifizieren, die für die Erreichung von Compliance relevant sind.
- Am umfangreichsten adressiert COBIT 4.0 das Compliance-Thema in einem seiner der 34 IT-Prozesse. So dient der Prozess ME 3 ("Stelle Compliance mit Vorgaben sicher") der COBIT-Domäne "Überwachung und Bewertung" speziell der Sicherstellung von (gesetzlicher und regulativer) Compliance.

---

16 Nach *ITGI 2005*, S. 7.
17 Nach *ITGI 2003*, S. 71f.
18 Im “IT Governance Implementation Guide“ stellen „Risk und Compliance“ eine eigene Stakeholdergruppe dar, deren Interessen im gesamten Einführungsprozess explizit zu berücksichtigen sind, siehe *ITGI 2007*a, S. 11.

1.2 Compliance als Informationskriterium

Compliance-Begriff

Informationen müssen zur Erreichung der Unternehmensziele bestimmten unternehmensspezifischen Anforderungen genügen, die in COBIT 4.0 als "Informationskriterien" (engl. information criteria) bezeichnet werden.[19] Eines der sieben aufgeführten Informationskriterien ist das Kriterium „Compliance“.[20] Aus der Beschreibung dieses Kriteriums ist das Complianceverständnis von COBIT 4.0 abzuleiten: Nach COBIT 4.0 umfasst Compliance die Einhaltung von Gesetzen, Regulativen und vertraglichen Vereinbarungen, die ein Geschäftsprozess zu berücksichtigen hat. Hierbei sind externe Vorschriften ebenso wie interne Richtlinien zu berücksichtigen.[21] Mit der Betonung der Geschäftsprozesse versteht COBIT IT-Compliance primär als Beitrag der IT zur Sicherstellung der Compliance von Geschäftsprozessen – mithin als IT-gestützte Compliance.[22]

Primäre/sekundäre Unterstützung

Die Erfüllung der Informationskriterien durch die IT-Prozesse wird in jeder Prozessbeschreibung als „primär“ (P) oder „sekundär“ (S) markiert bzw. bei mangelnder Relevanz entfällt eine Markierung. Hierdurch sind alle IT-Prozesse zu identifizieren, die einen mehr oder minder wichtigen Beitrag zur Erreichung von Compliance leisten. Im Ergebnis zeigt sich, dass Compliance von insgesamt elf IT-Prozessen über alle vier COBIT-Domänen hinweg adressiert wird.[23]

1.3 IT-Prozesse mit primärer oder sekundärer Complianceunterstützung

Dadurch, dass jeder IT-Prozess dahingehend charakterisiert wird, welche Informationskriterien als unternehmensspezifische Anforderungen er unterstützt, kann jeder compliance-relevante IT-Prozess identifiziert werden[24]. In

---

19 Nach *ITGI 2005*, S. 14.

20 Im Kern bestehen die Informationskriterien aus den informationsbezogenen Sicherheitsanforderungen der Vertraulichkeit, der Integrität und der Verfügbarkeit. Hinzu kommen die Kriterien Wirksamkeit, Wirtschaftlichkeit und Verlässlichkeit, vgl. *ebd*.

21 Nach *ebd*.; vgl. *Johannsen/Goeken 2010*, S. 61.

22 Zur Diskussion des Unterschieds zwischen IT-Compliance und IT-gestützter Compliance siehe *Klotz/Dorn 2008*, S. 9f.

23 Die Tatsache, dass die Erreichung des compliance-bezogenen IT-Ziels von nur vier IT-Prozessen unterstützt wird, durch das Informationskriterium „Compliance“ aber elf compliance-relevante IT-Prozesse identifiziert werden können, stellt eine weitere Inkonsistenz von COBIT 4.0 dar.

24 Es finden sich in verschiedenen, nicht in Tabelle 1 aufgeführten IT-Prozessen jedoch weitere Compliance-Bezüge, ohne dass dies explizit durch das Informationskriterium

der Prozessbeschreibung muss dann allerdings der jeweilige Compliance-Bezug durch Textstudium ermittelt werden. Tabelle 1 enthält das Ergebnis dieser Analyse für alle elf Prozesse, die für das Informationskriterium „Compliance“ relevant sind.

Tabelle 1
Compliance-Inhalte der COBIT 4.0 IT-Prozesse[25]

Notation	IT-Prozess	Compliance-Bezug
PO 6	Kommuniziere Ziele und Richtung des Managements	Im Rahmen dieses Prozesses sind Richtlinien zu erstellen, die die Nutzung der IT leiten. Hierzu ist eine IT-Kontrollumgebung einzurichten. Bestandteil dieser Richtlinien ist auch die Verpflichtung zu Compliance, die durch eine geeignete Überwachung, d. h. durch Kontrollen und Prüfungen im gesamten Unternehmen sicherzustellen ist.
PO 9	Beurteile und manage IT-Risiken	Die mangelnde Erfüllung externer Anforderungen (vor allem aus rechtlichen Vorgaben) wird als potenzielles IT-Risiko eingestuft, das es im Rahmen eines IT-Risikomanagements zu steuern gilt.
AI 4	Ermögliche Betrieb und Verwendung	Die Verantwortung für die fachliche Nutzung von Anwendungen liegt nach COBIT in der Fachabteilung bzw. beim Geschäftsprozesseigner. Diese Verantwortung richtet sich auch auf Compliance-Vorgaben, die der Geschäftsprozess einzuhalten hat und deren Einhaltung durch entsprechende Kontrollen sicherzustellen ist.
AI 5	Beschaffe IT-Ressourcen	In diesem Prozess sind alle diejenigen Aktivitäten compliance-relevant, die sich auf vertragliche Anforderungen richten. Dies sind vor allem die Entwicklung von IT-Beschaffungsrichtlinien, die Lieferantenauswahl, die Vertragsgestaltung und die Durchführung der Beschaffung. Hierbei stellt ein Vertragsmanagement die Compliance mit vertraglichen Vorgaben für die gesamte Unternehmens-IT nachweislich sicher.
DS 1	Definiere und manage Service Levels	Fragen der Compliance werden im Service-Level-Management dann relevant, wenn die zu vereinbarenden Service-Level-Agreements (SLAs) oder Operating-Level-Agreements (OLAs) Compliance-Anforderungen zu berücksichtigen haben. Die entsprechenden Festlegungen sind auch Gegenstand

„Compliance“ markiert wird. So soll beispielsweise auch der IT-Prozess PO 3 (Bestimme die technologische Richtung) technische und regulatorische Compliance sicherstellen, vgl. *ITGI 2005*, S. 41ff. Gleiches gilt für die Beschreibung der Prozesse im IT Assurance Guide, wo ebenfalls weitere Compliance-Bezüge aus Prüfungssicht hergestellt werden, für den genannten Prozess PO 3, siehe *ITGI 2007b*, S. 62ff.

[25] Entnommen aus *Klotz 2011*, S. 602f.

Notation	IT-Prozess	Compliance-Bezug
		der Überwachung, des Berichtswesens und etwaiger Reviews.
DS 2	Manage Leistungen von Dritten	Das Management von Drittleistungen umfasst explizit auch auf die Erfüllung von Compliance-Anforderungen durch den Lieferanten. Die Anzahl der diesbezüglichen Fälle von Non-Compliance ist ein Indikator der Leistungsmessung.
DS 5	Stelle Security von Systemen sicher	Im Rahmen der IT-Sicherheit ist die Compliance von IT-Sicherheitsrichtlinien und die Umsetzung zahlreicher compliance-relevanter Einzelfragen, wie Berechtigungskonzepte, Funktionstrennungen, Dokumentationsverpflichtungen oder Sicherheitszertifizierungen, relevant.
ME 1	Monitore und evaluiere IT-Performance	Die Leistungsüberwachung hat sich auch auf das Erreichen von Compliance zu beziehen. Hierfür sind geeignete Leistungsindikatoren zu bestimmen und in das Berichtssystem zu integieren.
ME 2	Monitore und evaluiere Internal Controls	Ziel dieses Prozesses ist es, eine Aussage darüber zu erhalten, ob bzw. inwieweit Gesetze und Vorschriften eingehalten werden. Hierzu soll sich das interne Kontrollsystem der IT an Richtlinien und Normen orientieren. Rechtliche, regulatorische und vertragliche Anforderungen müssen durch das IT-Kontrollsystem abgedeckt sein, wobei die Kontrollen auch externe Dienstleister zu berücksichtigen haben.
ME 3	Stelle Compliance mit Vorgaben sicher	Dies ist der zentrale IT-Prozess, durch den insbesondere die externe Compliance mit gesetzlichen und regulativen Vorgaben sichergestellt wird.
ME 4	Sorge für IT-Governance	Auch dieser Governance-Prozess zielt auf die Einhaltung von Gesetzen und Vorschriften. Konkret wird gefordert, dass durch eine interne oder externe Prüfung "die Compliance der IT mit ihren Richtlinien, Standards und Verfahren sowie mit allgemein anerkannten Praktiken"[26] bestätigt wird.

In Bezug auf den Grad der Unterstützung der Compliance-Anforderung durch den betreffenden IT-Prozess nimmt COBIT eine 2-stufige Differenzierung (primär, sekundär) vor. Den in der Tabelle 1 enthaltenen Prozessen wird – bis auf Prozess ME 3 – durchgängig eine sekundäre Bedeutung zugemessen.

[26] *ITGI 2005*, S. 185.

1.4 Der Prozess ME 3 zur Sicherstellung von Compliance

Compliance-Prozess ME 3

Der Prozess ME 3 "Stelle Compliance mit Vorgaben sicher" (engl. Ensure Regulatory Compliance) ist der dritte Prozess der Domäne "Überwachung und Bewertung".[27] Die Prozessbezeichnung stellt gleichzeitig das übergeordnete Kontrollziel dar. Dieses wird dann erreicht, wenn eine "positive Bestätigung der Einhaltung von Gesetzen und Vorschriften vorliegt".[28] Allerdings ist eine derartige Bestätigung allein für eine Messung der Zielerreichung nicht als ausreichend anzusehen. Vielmehr sollen für die Messung der Zielerreichung folgende Indikatoren Verwendung finden:

- Kosten von Non-Compliance, z. B. Straf- und Vergleichszahlungen;
- durchschnittliche Zeitdauer zwischen dem Auftreten externer Compliance-Probleme und deren Lösung;
- Häufigkeit von Compliance-Reviews.

Die Prozessbeschreibung enthält fünf Kontrollziele, die als normative Aussagen den Inhalt und den Umfang des Compliance-Managements in der IT nach COBIT 4.0 wiedergeben, vgl. Abbildung 1.

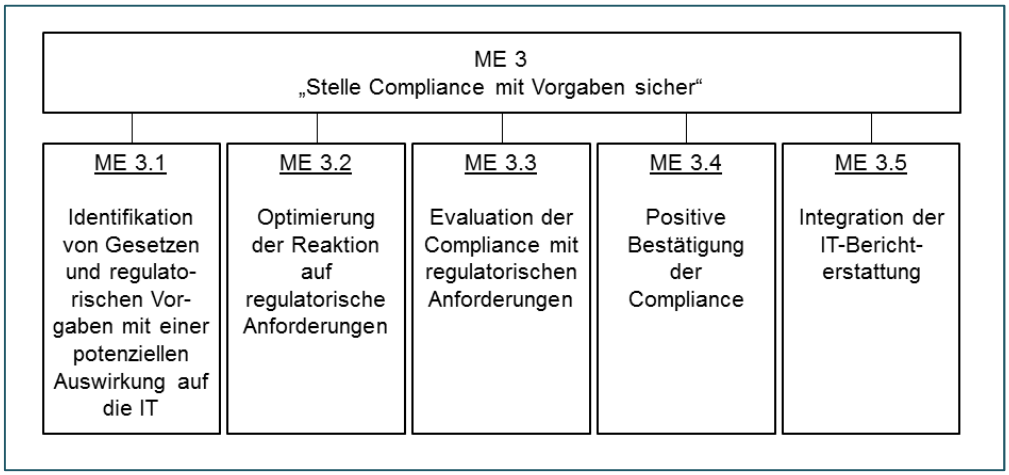

Abbildung 1
Kontrollziele des Prozesses ME 3 [29]

COBIT 4.0

Detaillierte Kontrollziele

Das Kontrollziel ME 3.1 beinhaltet eine Aussage zum Umfang der zu berücksichtigenden Compliance-Anforderungen. Diese ergeben sich aus rechtlichen und sonstigen regulatorischen Vorgaben (z. B. zu Datenschutz, Urheberrecht oder Regelungen zur Gesundheit und Arbeitnehmersicherheit)

---

[27] Im Folgenden nach *ITGI 2005*, S. 179ff.
[28] *Ebd.*, S. 179.
[29] Nach *Klotz 2011*, S. 603.

sowie aus Verträgen und Richtlinien. Um diesen Vorgaben in den verschiedenen IT-Aktivitäten zeitnah nachkommen und so Compliance sicherstellen zu können, ist ein entsprechender interner Prozess der Identifikation und der Umsetzung durch IT-Richtlinien, -Standards und -Verfahren erforderlich (ME 3.2). Die Einhaltung der Compliance-Anforderungen ist auf wirtschaftliche Weise kontinuierlich zu prüfen und zu beurteilen (ME 3.3). Ergebnisse sind adäquat zu berichten und gehen in die Leistungsdarstellung der IT-Funktion ein. Bei Feststellung von Compliance-Lücken sind Maßnahmen einzuleiten, vor allem in Bezug auf die Anpassung von IT-Richtlinien, -Standards und -Verfahren. Die Verantwortung hierfür wird den Prozesseignern (engl. process owner) zugeordnet (ME 3.4). Abschließend sind die Ergebnisse mit Ergebnissen anderer Unternehmensfunktionen abzustimmen und in die generelle Berichterstattung der Corporate Compliance zu integrieren (ME 3.5).[30]

Schlüsselaktivitäten

Die Beschreibung der einzelnen Control Objectives wird zu fünf Schlüsselaktivitäten verdichtet, die sowohl Teil des RACI-Modells als auch Grundlage der Erfolgsmessung sind:

- „Definiere einen Prozess zur Identifikation von Anforderungen aus Gesetzen, Verträge, Richtlinien und sonstigen Regulativen und führe diesen aus;
- Evaluiere Compliance der IT-Aktivitäten mit IT-Richtlinien, Standards und Verfahren;
- Berichte die eindeutige Zusicherung, dass die IT-Aktivitäten mit IT-Richtlinien, Standards und Verfahren übereinstimmen;
- Liefere Input zum Angleichen der mit IT-Richtlinien, Standards und Verfahren in Reaktion auf Compliance-Erfordernisse;
- Integriere die IT-Berichterstattung über regulative Anforderungen mit ähnlichem Output von anderen Bereichen“.[31]

Raci-Modell

Im dem dem Prozess zugehörigen RACI-Modell (R = responsible, A = accountable, C = consulted, I = informed) wird die Rechenschaftspflicht (A) in Bezug auf die Compliance der IT-Funktion dem Chief Information Officer (CIO) zugeordnet. Dagegen liegt die Durchführungsverantwortung (R) sowohl beim CIO als auch bei den Mitgliedern der Führungsebene

[30] Vgl. *ITGI 2005*, S. 180.
[31] *Ebd*.

unterhalb des CIO, d. h. bei den Leitungen für IT-Betrieb, -Entwicklung und -Administration, ebenso beim IT-Chefarchitekt sowie bei den compliance-affinen Stellen mit Kontroll- und Berichtsverantwortung (Corporate Compliance, Audit, Risiko und Sicherheit).

Indikatoren für Compliance

Jeder IT-Prozess hat zur Erfüllung der unternehmensspezifischen Anforderungen beizutragen, gemessen durch so genannte "Key Goal Indicators" (KGI). Diese Messung beinhaltet auch die Bestätigung der Compliance der unterstützten Geschäftsprozesse.[32] Generell wird zwischen Leistungs- und Zielindikatoren unterschieden. Der Leistungsindikator (Key Performance Indicator – KPI) misst das Erreichen der Aktivitätsziele, die beiden Zielindikatoren (Key Goal Indicator – KGI – und IT Key Goal Indicator) messen das Erreichen der Prozessziele bzw. der IT-Ziele. Tabelle 2 beinhaltet die verschiedenen Indikatoren.

Tabelle 2
Indikatoren des Prozesses ME 3 [33]

Key Performance Indicators	Key Goal Indicators	IT Key Goal Indicators
• Durchschnittliche Zeitspanne zwischen Identifizierung 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 oder die öffentliches Aufsehen und Reaktionen hervorgerufen haben

Maturitätsmodell

COBIT 4.0 beinhaltet als Grundlage einer Bewertung der Prozessreife ein Maturitätsmodell, das an das Reifegradmodell von CMMI (Capability Maturity Model Integration) angelehnt ist. Für ME 3 enthält Tabelle 3 die wesentlichen Merkmale des Maturitätsmodells.

---

[32] Nach *ITGI 2005*, S. 25.
[33] Nach *ebd.*, S. 181.

Tabelle 3
Maturitätsmodell des Prozesses ME 3 [34]

Stufe	Merkmal
0 (nicht existent)	• Bewusstsein für Compliance-Anforderungen ist nur gering ausgeprägt. • Prozess zur Einhaltung von Compliance-Anforderungen ist nicht vorhanden.
1 (initial)	• Bewusstsein für Compliance-Anforderungen ist vorhanden. • Informelle Prozesse zur Aufrechterhaltung von Compliance im Rahmen von Projekten oder als Folge von Audits werden befolgt.
2 (wiederholbar, aber intuitiv)	• Bewusstsein für externe Compliance-Anforderungen ist vorhanden und Notwendigkeit wird kommuniziert. • Bereichsspezifische Compliance-Verfahren sind definiert. • Wissen und Verantwortung von Einzelpersonen stehen im Vordergrund. • Compliance-Schulungen erfolgen informell.
3 (definiert)	• Richtlinien, Verfahren und Prozesse sind entwickelt, dokumentiert und kommuniziert, werden aber nicht durchgängig angewendet. • Eine Überwachung der Compliance erfolgt nur eingeschränkt. • Manche Compliance-Anforderungen werden nicht erfüllt. • Compliance-Schulungen werden für den Bereich der gesetzlichen und regulatorischen Vorgaben angeboten.
4 (gemanaged und messbar)	• Verständnis für Compliance und diesbezügliche Gefahren ist umfassend vorhanden. • Ein formelles Compliance-Schulungsprogramm existiert. • Sämtliche Mitarbeiter sind sich ihrer Compliance-Verpflichtung bewusst. • Standardisierte Compliance-Prozesse zur Überwachung von Non-Compliance sind etabliert. • Reviews des Umfeldes werden genutzt. • Ursachen von Non-Compliance werden identifiziert und nachhaltig beseitigt.

[34] In enger Anlehnung an *Klotz 2011*, S. 604f.

Stufe	Merkmal
5 (optimiert)	• Ein effektiver und effizienter Prozess zur Einhaltung externer Anforderungen ist vorhanden. • Eine zentrale Compliance-Funktion, die den Compliance-Prozess steuert, ist etabliert. • Wissen über externe Anforderung ist umfangreich vorhanden und wird intern kommuniziert. • Das Unternehmen ist in externe Plattformen integriert und kann auf externe Anforderungen Einfluss nehmen. • Der Compliance-Überwachungsprozess erfolgt systemgestützt. • Ein Self-Assessment in Bezug auf externe Anforderungen ist implementiert, sodass Non-Compliance nur selten auftritt. • Compliance-Schulungen müssen nur noch für neue Mitarbeiter oder bei wesentlichen Veränderungen durchgeführt werden.

1.5 Fazit zu COBIT 4.0

Externer Fokus

Grundlegend ist festzuhalten, dass COBIT 4.0 IT-Compliance in einem Umfang adressiert, der für das Publikationsjahr 2005 als durchaus umfangreich bezeichnet werden kann.[35] Das Compliance-Verständnis von COBIT 4.0 ist überwiegend das der IT-gestützten Compliance. Im Vordergrund steht hier die Frage, wie IT zur Compliance von Geschäftsprozessen beitragen kann. Dass sich Compliance-Anforderungen auch direkt an die IT richten, wird in diese Sichtweise integriert, wenn auch nur selten explizit, wie z. B. für den Datenschutz. Zudem fokussiert COBIT 4.0 die Compliance mit externen Regelwerken, also gesetzlichen, regulativen und vertraglichen Vorgaben. Das Begriffsverständnis bleibt jedoch zumindest teilweise unklar, insbesondere hinsichtlich des Umfanges von regulativen Vorgaben und der Bedeutung von Normen.

Inkonsistenzen im Zielsystem

Die begriffliche Unschärfe führt auf der Ebene der Unternehmens- und der IT-Ziele dazu, dass das Unternehmensziel der Compliance mit internen Regelungen nicht mit dem zentralen Compliance-Prozess ME 3 verbunden ist.

[35] Dass die „COBIT-Perspektiven“ mit IT-Compliance erst noch zu ergänzen seien, wie es *Bäumöl* für erforderlich zu halten scheint, ist insofern nicht ganz nachvollziehbar, vgl. *Baumöl 2012*, S. 11.

Ebenso unverständlich bleibt, warum in der Matrix aus IT-Zielen und IT-Prozessen das Compliance-Ziel, orientiert man sich am Informationskriterium „Compliance“, lediglich mit drei von elf IT-Prozessen verbunden wird – und zudem mit dem IT-Prozess DS 11 noch ein Prozess ohne „Compliance-Markierung“ aufgeführt wird.[36]

Inkonsistenzen beim Informationskriterium

Die Möglichkeit, über das Informationskriterium „Compliance“ compliancerelevante IT-Prozesse zu identifizieren, wurde als grundsätzlicher Vorteil eingestuft. Allerdings muss dies bei genauerer Analyse relativiert werden. Die P- oder S-Einstufung eines IT-Prozesses hinsichtlich seiner Unterstützung der Compliance-Anforderung muss von den Inhalten des Prozesses abhängen. Zur Erläuterung soll noch einmal der Prozess DS 11 (Manage Daten) herangezogen werden. Dieser unterstützt das IT-Ziel der Compliance mit Gesetzen und regulativen Vorgaben, ohne dass das Informationskriterium „Compliance“ markiert ist. Inhaltlich steht die hohe Relevanz aber außer Frage. In Kontrollziel DS 11.2 wird beispielsweise gefordert, dass die Datenspeicherung und -archivierung „gesetzliche, regulatorische und Unternehmenserfordernisse ... einzuhalten“[37] hat. Ein anderes Beispiel ist der Prozess AI 1 (Identifiziere automatische Lösungen). Das Kontrollziel AI 1.2 (Risikoanalyse-Bericht) umfasst die für Compliance zweifellos wichtige Forderung, mit Geschäftsprozessen verbundene Risiken zu identifizieren. Zu diesen Risiken zählen explizit auch die mangelnde Einhaltung von Gesetzen und Verordnungen.[38] Trotzdem ist das Informationskriterium „Compliance“ für diesen Prozess weder mit einem „P“ noch mit einem „S“ markiert. Weitere Beispiele lassen sich leicht finden.

Inkonsistenzen im RACI-Modell

Eine weitere kritische Analyse geht davon aus, dass bei vorliegender Compliance-Relevanz eines IT-Prozesses die Rolle „Compliance, Audit, Risk und Security“ im RACI-Modell eine A- oder R-Beteiligung aufweisen müsste. Auch hier sind jedoch Inkonsistenzen festzustellen. Dem Prozess PO 6 (Kommuniziere Ziele und Richtung des Managements) ist zwar eine S-Markierung für das Informationskriterium „Compliance“ zugeordnet, der Rolle „Compliance, Audit, Risk und Security“ wird aber durchgängig nur eine beratende Funktion (C-Beteiligung) eingeräumt.[39] Das Kontrollziel PO 6.3 fordert die Entwicklung von IT-Richtlinien. Diese sollten sich auch auf

---

[36] Vgl. *ITGI 2005*, S. 191.
[37] *Ebd.*, S. 158.
[38] Vgl. *ebd.*, S. 80.
[39] Vgl. *ebd.*, S. 57.

Compliance beziehen bzw. stellen als solche ein internes Regelwerk dar, durch das Compliance hinsichtlich externer Vorgaben gewährleistet werden kann. Insofern sind IT-Richtlinien vorstellbar, die von der Compliance-Rolle zu erstellen bzw. managen und/oder sogar gänzlich zu verantworten sind – und somit eine A- oder R-Beteiligung erfordern.

Managementsystem

Durch das Verständnis von Compliance als Informationskriterium lassen sich die compliance-relevanten IT-Prozesse in COBIT 4.0 leicht identifizieren. Zusammen mit dem zentralen Compliance-Prozess ME 3 "Stelle Compliance mit Vorgaben sicher" beinhaltet COBIT 4.0 ein Grundgerüst für ein IT-Compliance-Managementsystem mit Compliance-Zielsetzung, compliance-relevanten IT-Prozessen, einem generellen Compliance-Prozess in der IT, jeweils zugehörigen Verantwortlichkeiten sowie Ziel- und Leistungsindikatoren. Allerdings ist das Compliance-Thema über COBIT 4.0 verstreut, so dass der Nutzer die verschiedenen Aspekte und Teile selbst identifizieren und zusammenfügen muss.[40] Zudem führen die vielen Inkonsistenzen in der Systematik dazu, dass bei Nutzung von COBIT die Zusammenhänge der einzelnen Elemente hinterfragt und auf die individuelle Situation im Unternehmen angepasst werden müssen. Dies muss kein Nachteil sein, wird doch so eine unkritische Übertragung von COBIT verhindert. Allerdings bietet COBIT 4.0 damit auch nicht die leicht nutzbare Hilfestellung, die man von dem führenden Framework für die IT-Governance eigentlich erwartet.

[40] Anders als beispielsweise für das Thema der IT-Security, vgl. *ISACA 2007c,* gibt es auch keine gesonderte integrierende Darstellung zu IT-Compliance aus COBIT-Sicht.

2 IT-Compliance nach COBIT 5

2.1 Überblick über die generellen Änderungen

Neuerungen in COBIT 5

COBIT 5 wurde im Jahr 2012 veröffentlicht. Die wesentliche strukturelle Neuerung im Vergleich zur vorherigen Version besteht darin, dass COBIT 5 die beiden anderen ISACA-Frameworks „Val IT 2.0“ (aus dem Jahr 2008) und „Risk IT“ (aus dem Jahr 2009) integriert. Hierdurch ergeben sich zusätzliche Domänen, wobei sich eine Domäne nunmehr explizit auf die IT-Governance richtet, während die anderen vier Domänen das IT-Management adressieren. Die Differenzierung in Governance und Management der IT wird mit den unterschiedlichen Arten von Aktivitäten begründet, die jeweils unterschiedlichen Zwecken dienen und damit auch unterschiedliche Organisationsstrukturen erfordern.[41] Abbildung 2 zeigt die von COBIT 5 vorgenommene begriffliche Abgrenzung zwischen IT-Governance und IT-Management. Governance richtet sich vor allem auf die Zielvorgaben der unterschiedlichen Anspruchsgruppen, während das IT-Management den PBRM-Zyklus (Plan, Build, Run, Monitor) fokussiert.

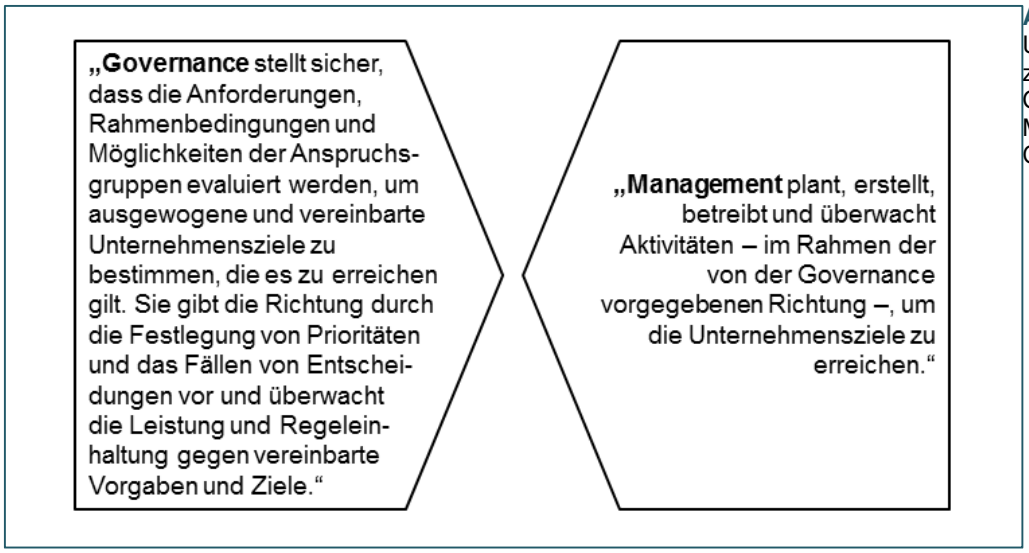

Abbildung 2 Unterscheidung zwischen Governance und Management nach COBIT 5 [42]

Aus der Unterscheidung zwischen IT-Governance und IT-Management ergibt sich eine neue Dokumentenstruktur, die kontinuierlich ergänzt wird. Durch die gestiegene Komplexität des Frameworks wird der grundsätzliche Ansatz von COBIT jetzt in einem eigenen Dokument beschrieben. Ent-

[41] Nach *ISACA 2012a*, S. 33.
[42] Nach *ebd.*

sprechend der erweiterten Governance-Perspektive trägt dieses Dokument den Titel: „COBIT® 5 – A Business Framework for the Governance and Management of Enterprise IT“.[43] Ebenfalls ein eigenes Dokument, „COBIT® 5 – Enabling Processes“, beinhaltet nunmehr die Beschreibung der IT-Domänen und -Prozesse.[44] Dieser Titel verweist darauf, dass die Prozesse einen der insgesamt sieben Enabler darstellen. Enabler sind nach COBIT 5 Erfolgsfaktoren, die das Erreichen der IT-Ziele ermöglichen. Die sieben Enabler-Kategorien sind:

- Prinzipien, Richtlinien und Rahmenwerke;
- Prozesse;
- Organisationsstrukturen Kultur, Ethik und Verhalten;
- Informationen;
- Services, Infrastruktur und Anwendungen;
- Mitarbeiter, Fähigkeiten und Kompetenzen.[45]

Enabler-Ansatz

Durch diese sieben Enabler kommt der ganzheitliche Ansatz von COBIT 5 zum Ausdruck.[46] Hierdurch wird klargestellt, dass eine erfolgreiche IT-Governance bzw. ein erfolgreiches IT-Management nicht nur von einem isolierten IT-Prozessmanagement abhängt. Für die Prozesse wird ihre Abhängigkeit von Organisationsstrukturen und Rollen, kulturellen und verhaltensbezogenen Aspekten, von Richtlinien und Verfahren und insbesondere von Informationen als notwendigem Input betont.[47] Dementsprechend wurde das Prozessmodell mittlerweile durch ein Informationsmodell ergänzt, das analog unter dem Titel „COBIT® 5 – Enabling Information“ veröffentlicht wurde. Weitere Enabling-Handbücher („Enabler Guides“) werden folgen.[48]

---

[43] Vgl. *ISACA 2012a*; die deutsche Übersetzung trägt den Titel“Rahmenwerk für Governance und Management der Unternehmens-IT“

[44] Vgl. *ISACA 2012b*.

[45] Nach *ISACA 2012a*, S. 29.

[46] Die „Ermöglichung eines ganzheitlichen Ansatzes“ ist wiederum als viertes Prinzip Teil der grundlegenden fünf von COBIT 5 postulierten Prinzipen für die Governance und das Management der Unternehmens-IT. Mit der Umsetzung der fünf Prinzipien soll ein Rahmen geschaffen werden, „mit dessen Hilfe die Investitionen in Informationen und Technologie und deren Nutzen zum Vorteil der Anspruchsgruppen optimiert werden können“ (*ebd.*, S. 16).

[47] Vgl. *ISACA 2012b*, S. 73.

[48] Vgl. *ISACA 2013d*, S. 9.

COBIT 5-Produktfamilie

Neben den Enabler- Handbüchern umfasst die COBIT 5-Produktfamilie ergänzende Umsetzungsleitfäden („Professional Guides“) zur Implementierung oder zu speziellen Anwendungsbereichen, die ebenfalls kontinuierlich ergänzt werden.[49] Eine auf Zusammenarbeit von IT-Professionals ausgerichtete Online-Plattform soll das COBIT-Angebot künftig abrunden. Somit umfasst die COBIT 5-Produktfamilie insgesamt vier Produktstränge, vgl. Abbildung 3.

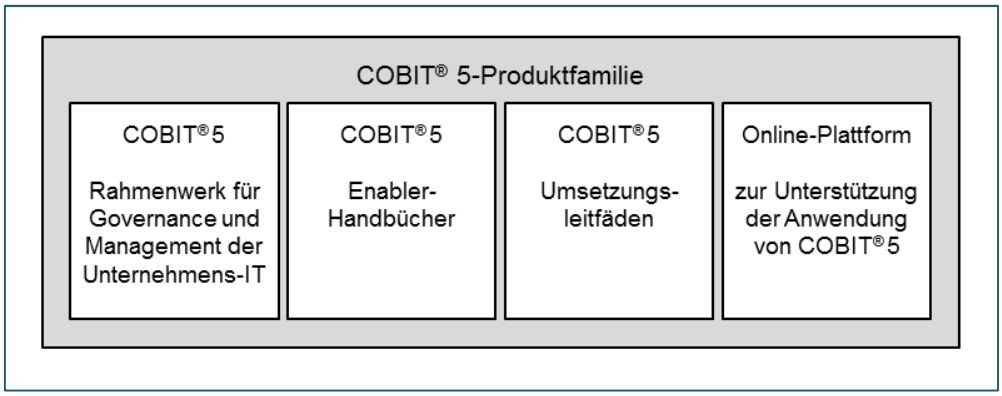

Abbildung 3
COBIT 5-Produktfamilie

Domänen

Aufgrund der Erweiterung besteht das Prozessmodell in COBIT 5 aus fünf Domänen mit insgesamt 37 Prozessen für IT-Governance und IT-Management, s. Tabelle 4.

Tabelle 4
COBIT 5 Domänen[50]

Domäne	Abk.	Bereich	Prozess-anzahl
Evaluieren, Vorgeben und Überwachen (engl. „Evaluate, Direct and Monitor”)	EDM	IT-Governance	5
Anpassen, Planen und Organisieren (engl. „Align, Plan and Organise“)	APO	IT-Management	13
Aufbauen, Beschaffen und Implementieren (engl. „Build, Acquire and Implement“	BAI	IT-Management	10
Bereitstellen, Betreiben und Unterstützen (engl. „Deliver, Service and Support“)	DSS	IT-Management	6
„Überwachen, Evaluieren und Beurteilen“ (engl. „Monitor, Evaluate and Assess“)	MEA	IT-Management	3

[49] So liegen bereits ein Prozessbewertungsmodell, vgl. *ISACA 2013a*, ein Selbstbewertungsleitfaden, vgl. *ISACA 2013b*, ein Leitfaden für die Informationssicherheit nach COBIT 5, vgl. *ISACA 2012c*, ein Leitfaden für das Risikomanagement nach COBIT 5, vgl. *ISACA 2013c*, und ein Leitfaden für die Prüfung der IT vor, vgl. *ISACA 2013e*.

[50] Vgl. *ISACA 2012b,* S. 26.

Prozess-beschreibung

Die grundlegenden Elemente der Prozessbeschreibungen bleiben in COBIT 5 erhalten bis auf das Maturitätsmodell, welches nicht mehr Bestandteil der Prozessbeschreibung ist.[51] Eine wesentliche systematische Verbesserung besteht darin, dass die Verantwortlichkeiten im RACI-Modell nunmehr direkt den insgesamt 210 Managementpraktiken[52] (dieser Begriff ersetzt den Begriff der Control Objectives) zugeordnet werden und nicht mehr – wie noch in COBIT 4.0 – den Aktivitäten. Die Aktivitäten selbst sind jetzt Teil der Managementpraktiken, was immens zur Klarheit des COBIT-Prozessmodells beiträgt.

2.2 Compliance-Verständnis von COBIT 5

Wegfall des Informationskriteriums „Compliance“

Eine für die Compliance-Thematik wesentliche Änderung in COBIT 5 ist der Wegfall der Informationskriterien. Hierdurch ist auch die Identifizierung der IT-Prozesse anhand des Informationskriteriums „Compliance“ als compliance-relevant nicht mehr möglich. COBIT 5 beinhaltet stattdessen Informationen wie bereits beschrieben als „Enabler“ (und als zu mangende Ressource). Damit entfällt in COBIT 5 auch die Sichtweise von Compliance als Informationskriterium. Nunmehr wird Compliance als „Ziel“ oder „Anforderung in Verbindung mit der Verwendung der Informationen“ und weniger als „eigentliche Qualität der Informationen“ gesehen.[53] Stattdessen wird „Compliance in dem Sinn, dass Informationen bestimmten Spezifikationen entsprechen müssen“, ... „je nach Anforderung von unterschiedlichen Qualitätszielen für Informationen abgedeckt.“[54]

Compliance-Definition in COBIT 5

Mit dem Wegfall des Informationskriteriums „Compliance“ entfällt auch die in COBIT 4.0 mit dem Kriterium verbundene Compliance-Definition. Dies hat zur Folge, dass sich in COBIT 5 keine zentrale Definition für Compliance bzw. IT-Compliance mehr findet. So enthält das Framework-Dokument nur noch eine allgemeine Compliance-Definition als „Einhaltung von

---

[51] Stattdessen verwendet COBIT 5 ein allgemeines, an der ISO/IEC 15504 orientiertes Prozessbefähigungsmodell. Nach dem Process Assessment Model (PAM) werden die den Prozessen zugeordneten grundlegenden Managementpraktiken (Base Practices) und ihre Arbeitsergebnisse (Inputs/Outputs als Work Products) als Leistungsindikatoren für die Prozessbeurteilung herangezogen; vgl. *ISACA 2013a*, S. 15; *Gaulke 2012*, S. 21.

[52] Diese wurden gebildet aus den 210 Control Objectives von COBIT 4.1, den 22 Management Practices von Val IT und den 9 Management Practices von Risk IT.

[53] *ISACA 2012a*, S. 65.

[54] *Ebd.*; als Beispiel bietet sich das Qualitätsziel „Verfügbarkeit“ an, das im Falle steuerlich relevanter Daten von verschiedenen Regelwerken (z. B. dem HGB oder der AO) adressiert wird.

Vorschriften“.[55] Bei der Beschreibung der Organisationsstrukturen erfolgt eine Detaillierung dahingehend, dass Compliance sich auf die Einhaltung von rechtlichen, behördlichen und vertraglichen Anforderungen richtet.[56] In der Beschreibung des Prozesses EDM01 (Sicherstellen der Einrichtung und Pflege des Governance-Rahmenwerks) richtet sich Compliance ebenfalls auf „ethische und professionelle Verhaltensrichtlinien“[57].

Bezug auf ISO/IEC 38500

Eine explizite Definition hielten die Autoren von COBIT 5 offenbar nicht für erforderlich. Selbst im Glossar ist der Begriff nicht enthalten. Allerdings ist dies durchaus nachvollziehbar, wird doch allein schon durch die beiden compliance-bezogenen Unternehmensziele und die entsprechenden IT-Ziele zum Ausdruck gebracht, dass sich Compliance auf die Konformität mit externen Gesetzen und Bestimmungen einerseits und mit internen Richtlinien andererseits richtet. Mit dem Bezug auf die ISO/IEC 38500 wird das dort enthaltene Conformance-Prinzip übernommen, insbesondere, was die Konformität mit rechtlichen und behördlichen Anforderungen und ihre Berücksichtigung in internen Richtlinien und Verfahren sowie in Verträgen mit Dritten anbelangt.[58] In der Summe entspricht das Compliance-Verständnis in COBIT 5 somit weiterhin demjenigen in COBIT 4.0. Eine Weiterentwicklung lässt sich in der im Rahmen des IT-Ziels vorgenommenen Differenzierung zwischen der IT-Compliance einerseits und der IT-Unterstützung der Compliance des Unternehmens andererseits – also der Unterscheidung zwischen IT-Compliance und IT-gestützter Compliance – sehen.

Mit dem Wegfall des Informationskriteriums “Compliance“ entfällt bei COBIT 5 ein systematischer „Quereinstieg“ in die Compliance-Thematik. Für eine diesbezügliche Analyse bleibt jetzt nur noch ein Top-down-Vorgehen, das bei den Unternehmenszielen beginnt, über ihre Unterstützung durch IT-Ziele seinen Fortgang nimmt und mittels der Verbindung von IT-Zielen und IT-Prozessen zu den compliance-relevanten IT-Prozessen und zugehörigen Managementpraktiken führt. Dieser Gang der Analyse soll im Folgenden nachvollzogen werden.

---

55 *ISACA 2012a*, S. 65.
56 *Ebd.*, S. 79.
57 *ISACA 2012b*, S. 33.
58 Vgl. *ISACA 2012a*, S. 61; vgl. *Klotz 2008*.

2.3 Compliance als Teil der Unternehmensziele

Compliance-bezogene Unternehmensziele

Unternehmensziele bzw. die Anforderungen von Stakeholdern werden von verschiedenen Treibern aus der Unternehmensumwelt beeinflusst, zu denen auch ein verändertes regulatives Umfeld zählt. Hierdurch findet Complinace Eingang in die Struktur der Unternehmensziele. COBIT 5 beinhaltet nur noch 17 generische Unternehmensziele (in COBIT 4.0 waren es noch 20), die weiterhin den einzelnen Ebenen einer Balanced Scorecard zugeordnet sind. Unverändert beziehen sich zwei Unternehmensziele auf Compliance:

- Unternehmensziel 4: Einhaltung externer Gesetze und Bestimmungen (Compliance);
- Unternehmensziel 15: Compliance mit internen Richtlinien.

Compliance-bezogene Unternehmensziele

Während allerdings bei COBIT 4.0 beide Ziele der internen BSC-Perspektive zugeordnet sind, ist dies jetzt nur noch der Fall für das Ziel der Compliance mit internen Richtlinien. Das Ziel der Einhaltung externer Gesetze und Bestimmungen (Compliance) als Unternehmensziel Nr. 4 ist dagegen nunmehr der Finanzperspektive zugeordnet.[59] Eine Erklärung hierfür findet sich in COBIT 5 nicht. Allerdings lässt sich die Zuordnung leicht mit den mit Non-Compliance verbundenen finanziellen Nachteilen für Unternehmen, die gegen gesetzliche und behördliche Vorgaben verstoßen, begründen. Dies entspricht auch der Sichtweise der potenziellen Non-Compliance als Risiko, das es zu minimieren gilt. Dementsprechend dienen die beiden Compliance-Ziele (ausschließlich) der Erfüllung der Governance-Vorgabe der Risikooptimierung.[60]

2.4 Compliance als Zielinhalt der IT-Ziele

Compliance-bezogene IT-Ziele

Auch die generischen IT-Ziele wurden in COBIT 5 von 28 auf 17 reduziert. Dennoch haben – während in COBIT 4.0 nur ein compliance-bezogenes IT-Ziel aufgeführt wurde – in COBIT 5 jetzt zwei der IT-Ziele Compliance als

---

[59] Vgl. *ISACA 2012a*, S. 21.

[60] Vgl. *ebd.* In COBIT 5 werden drei allgemeine Governance-Vorgaben als Anforderungen von Stakeholdern, die die Unternehmensziele beeinflussen, verwendet: Nutzenrealisierung, Risikooptimierung und Ressourcenoptimierung. Um einen Wertbeitrag für das Unternehmen bzw. die unterschiedlichen Stakeholder zu generieren, muss die Unternehmens-IT durch den IT-Einsatz Nutzen zu optimalen Ressourcenkosten und mit optimalem Risiko realisieren; nach *ebd.*, S. 19.

Zielinhalt. So richtet sich neben der extern orientierten Compliance ein IT-Ziel auch auf die Compliance mit internen Richtlinien:

- IT-Ziel 2: IT-Compliance und Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen;
- IT-Ziel 15: IT-Compliance mit internen Richtlinien.[61]

BSC-Perspektive

Die beiden IT-Ziele entsprechen inhaltlich den Unternehmenszielen, nur dass sie explizit auf die IT-Compliance abzielen, wobei auch die Corporate Compliance mittels IT unterstützt werden soll. Auch die Zuordnung zu den BSC-Perspektiven entspricht derjenigen der Unternehmensziele; die IT-Compliance und die Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen (IT-Ziel 2) ist der Finanzperspektive zugeordnet, die IT-Compliance mit internen Richtlinien (IT-Ziel 15) ist der internen Perspektive zugeordnet.

Zusammenhang Unternehmens-/ IT-Ziele

Für die Unterstützung der Unternehmensziele durch die IT-Ziele verwendet COBIT jetzt auch – genauso wie für den Zusammenhang zwischen IT-Zielen und IT-Prozessen – eine Unterscheidung nach primärer („wichtige Beziehung“) und sekundärer Unterstützung („weniger wichtige Beziehung“[62]), vgl. Tabelle 5.

Tabelle 5
Unterstützung der Unternehmensziele durch IT-Ziele[63]

IT-Ziele / **Unternehmensziele**	Nr. 2: IT-Compliance und Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen	Nr. 15: IT-Compliance mit internen Richtlinien
Nr. 4: Einhaltung externer Gesetze und Bestimmungen	P	S
Nr. 15: Compliance mit internen Richtlinien	P	P
P = primär, S = sekundär		

[61] Vgl. *ISACA 2012a*, S. 21.
[62] Vgl. *ebd.*, S. 51.
[63] Nach *ISACA 2012a*, S. 52.

Indikatoren

Für die Messung der Zielerreichung werden von COBIT 5 verschiedene Indikatoren (Metriken) angeboten. Diese sind jeweils bei den Prozessen verzeichnet, von denen die IT-Ziele primär unterstützt werden, wobei die Indikatoren nicht in Abhängigkeit von den Prozessen variieren. Für die IT-Compliance und die Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen (IT-Ziel 2) werden folgende Indikatoren genannt:

- „Kosten der IT-seitigen Nichteinhaltung (Non-Compliance), einschließlich Abfindungen und Geldbußen sowie Folgen von Reputationsverlust;
- Anzahl der IT-bezogenen Non-Compliance-Vorfälle, die der Geschäftsleitung gemeldet werden oder zu öffentlichen Diskussionen oder Unannehmlichkeiten führen;
- Anzahl der Non-Compliance-Vorfälle, die sich auf Vertragsvereinbarungen mit IT-Serviceanbietern beziehen;
- Abdeckung von Compliance-Beurteilungen.“[64]

Für die IT-Compliance mit internen Richtlinien (IT-Ziel 15) werden folgende Indikatoren angegeben:

- „Anzahl der Störungen in Verbindung mit der Nichteinhaltung (Non-Compliance) von Richtlinien;
- Anteil der Anspruchsgruppen, die Richtlinien verstehen;
- Anteil der Richtlinien, die durch effektive Standards und Arbeitspraktiken unterstützt werden;
- Häufigkeit, in der Richtlinien überprüft und aktualisiert werden.“[65]

2.5 Compliance-relevante IT-Prozesse in COBIT 5

Identifizierung

Die compliance-relevanten IT-Prozesse in COBIT 5 lassen sich durch die Zuordnung der IT-Prozesse zu den von ihnen unterstützten IT-Compliancezielen identifizieren. Von 37 IT-Prozessen unterstützen 20 die Erreichung von IT-Compliance und von Compliance mit externen Gesetzen und Bestimmungen. Hiervon leisten sieben Prozesse eine primäre, 13 Prozesse eine sekundäre Unterstützung, vgl. Tabelle 6. Wie ersichtlich wird die Compliance-Thematik von allen fünf Domänen adressiert. Deutlich werden die

[64] *ISACA 2012b*, S. 53.
[65] *Ebd.*

inhaltlichen Zusammenhänge zwischen IT-Compliance, IT-Risiko- und IT-Sicherheitsmanagement vor allem in der APO- und der DSS-Domäne.

Tabelle 6
IT-Ziel 2 unterstützende Prozesse[66]

IT-Ziel Nr. 2: IT-Compliance und Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen	
wird primär unterstützt durch ...	
1. APO01:	Managen des IT-Management-Rahmenwerks
2. APO12:	Managen von Risiken
3. APO13:	Managen der Sicherheit
4. BAI010:	Managen der Konfiguration
5. DSS05:	Managen von Sicherheitsservices
6. MEA02:	Überwachen, Evaluieren und Beurteilen des internen Kontrollsystems
7. MEA03:	Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen
wird sekundär unterstützt durch ...	
1. EDM01:	Sicherstellen der Einrichtung und Pflege des Governance-Rahmenwerks
2. EDM03:	Sicherstellen der Risiko-Optimierung
3. EDM05:	Sicherstellen der Transparenz gegenüber Anspruchsgruppen
4. APO07:	Managen des Personals
5. APO10:	Managen von Lieferanten
6. APO11:	Managen der Qualität
7. BAI02:	Managen der Definition von Anforderungen
8. BAI09:	Managen von Betriebsmitteln
9. DSS01:	Managen des Betriebs
10. DSS03:	Managen von Problemen
11. DSS04:	Managen der Kontinuität
12. DSS06:	Managen von Geschäftsprozesskontrollen
13. MEA01:	Überwachen, Evaluieren und Beurteilen von Leistung und Konformität

In Bezug auf die Compliance mit internen Richtlinien sind es sogar 24 IT-Prozesse, von denen vier Prozesse eine primäre, zwanzig Prozesse eine sekundäre Unterstützung leisten, vgl. Tabelle 7. Insgesamt unterstützen 26 von 37 IT-Prozessen das Erreichen der beiden IT-Complianceziele. Dabei stammen die Prozesse aus allen fünf Domänen, d. h. sowohl aus der Gover-

[66] Nach *ISACA 2012b*, S. 54f.

nance-Domäne EDM als auch den vier Management-Domänen. Am umfangreichsten fällt die Compliance-Unterstützung in Bezug auf beide IT-Complianceziele in den Domänen APO (Anpassen, Planen und Organisieren), DSS (Bereitstellen, Betreiben und Unterstützen) und MEA (Überwachen, Evaluieren und Beurteilen) aus.

Tabelle 7
IT-Ziel 15 unterstützende Prozesse[67]

IT-Ziel Nr. 15: IT-Compliance mit internen Richtlinien	
wird primär unterstützt durch ...	
1. EDM03:	Sicherstellen der Risiko-Optimierung
2. APO01:	Managen des IT-Management-Rahmenwerks
3. MEA01:	Überwachen, Evaluieren und Beurteilen von Leistung und Konformität
4. MEA02:	Überwachen, Evaluieren und Beurteilen des internen Kontrollsystems
wird sekundär unterstützt durch ...	
1. EDM01:	Sicherstellen der Einrichtung und Pflege des Governance-Rahmenwerks
2. EDM05:	Sicherstellen der Transparenz gegenüber Anspruchsgruppen
3. APO02:	Managen der Strategie
4. APO07:	Managen des Personals
5. APO08:	Managen von Beziehungen
6. APO09:	Managen von Servicevereinbarungen
7. APO10:	Managen von Lieferanten
8. APO11:	Managen der Qualität
9. APO12:	Managen von Risiken
10. BAI06:	Managen von Änderungen
11. BAI07:	Managen der Abnahme und Überführung von Änderungen
12. BAI09:	Managen von Betriebsmitteln
13. BAI010:	Managen der Konfiguration
14. DSS01:	Managen des Betriebs
15. DSS02:	Managen von Service-Anfragen und Störungen
16. DSS03:	Managen von Problemen
17. DSS04:	Managen der Kontinuität
18. DSS05:	Managen von Sicherheitsservices
19. DSS06:	Managen von Geschäftsprozesskontrollen
20. MEA03:	Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen

[67] Nach *ISACA 2012b*, S. 54f.

2.6 Compliance-Rollen und -Organisationsstrukturen

RACI – Bezug zu den Managementpraktiken

In Bezug auf das RACI-Rollenmodell verwendet COBIT 5 weiterhin die vier aus COBIT 4.0 bekannten Beteiligungsformen (R = responsible, A = accountable, C = consulted, I = informed). Das RACI-Diagramm verbindet aber nunmehr für jeden IT-Prozess die Organisationsstrukturen bzw. Rollen mit den einzelnen Managementpraktiken des betreffenden Prozesses (und nicht mehr wie noch in COBIT 4.0 mit wenigen Schlüsselaktivitäten). Damit ist es jetzt möglich, eine durchgängige Verantwortungs- und Beteiligungsstruktur für die zahlreichen Handlungsfelder der IT-Governance und des IT-Managements zu entwickeln – auch für IT-Compliance.

Compliance-Rollen

Ein weiterer Unterschied zur Vorgängerversion besteht darin, dass in COBIT 5 eine eigenständige Compliance-Rolle vorgesehen ist, die nicht mehr wie vorher in einer „Sammelrolle“ für „Compliance, Audit, Risk und Security“ aufgeht. Die Rolle „Compliance“ bezeichnet eine „Funktion im Unternehmen, die für die Sicherstellung der Einhaltung von rechtlichen, behördlichen und vertraglichen Anforderungen zuständig ist.“[68] Außerdem existiert zusätzlich die spezialisierte Compliance-Rolle des Datenschutzbeauftragten (DSB).[69] Dieser wird definiert als „Mitarbeiter, der für die Überwachung der Risiken und der Geschäftsauswirkungen von Datenschutzgesetzen zuständig ist, und die Implementierung von Richtlinien und Aktivitäten steuert und koordiniert, mit denen die Einhaltung der Datenschutzrichtlinien sichergestellt wird.“[70]

Umfang der Beteiligung der Compliance-Funktion

Bis auf vier IT-Prozesse[71], d. h. in insgesamt 33 von 37 Prozessen, ist die Compliance-Funktion ganz überwiegend an mehreren Governance- bzw. Managementpraktiken zumindest durch Information und Konsultation beteiligt. Dabei erstreckt sich die Beteiligung über alle COBIT-Domänen, s. Tabelle 8. Die Compliance-Funktion ist an insgesamt 142 von 210 Governance- bzw. Managementpraktiken beteiligt, was einer Beteiligungsquote in

---

68 *ISACA 2012a*, S. 79.

69 Im englischen Originaltext wird diese Funktion als „Privacy Officer“ bzw. „Data Protection Officer“ bezeichnet.

70 *Ebd.*

71 Dies sind die IT-Prozesse APO04 (Managen von Innovationen), APO07 (Managen des Personals), BAI04 (Managen von Verfügbarkeit und Kapazität) und BAI10 (Managen der Konfiguration). Bis auf APO04 muss dies verwundern, da APO07 und BAI10 das IT-Ziel der IT-Compliance mit internen Richtlinien sekundär unterstützen und BAI04 das IT-Ziel der IT-Compliance und der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen sogar primär unterstützt.

Höhe von 68 % entspricht. Dies ist als umfangreiche Beteiligung zu werten, insbesondere vor dem Hintergrund, dass in COBIT 4.0 das Informationskriterium „Compliance“ in lediglich elf IT-Prozessen unterstützt wurde. Die Verteilung der Zahlen verdeutlicht die überwiegend beratende Rolle der Compliance-Funktion. Durchführungsverantwortung bzw. Rechenschaftspflicht kommen der Compliance-Funktion nur in 11 bzw. 2 Governance- und Managementpraktiken zu. Am umfangreichsten fällt die Beteiligung in der EDM-Domäne – hier zu 100 % – und in der MEA-Domäne (88 %) aus, die die wesentlichen Prozesse und Managementpraktiken in Bezug auf IT-Compliance beinhaltet

Tabelle 8
Beteiligung der Compliance-Funktion an den Managementpraktiken[72]

Domäne	Governance-/ Managementpraktiken	Beteiligung Compliance-Funktion					
		R	A	C	I	Summe	Beteiligungsquote
EDM	15	0	0	13	2	15	100%
APO	72	3	0	39	5	47	65%
BAI	68	2	0	34	5	41	60%
DSS	38	0	0	20	4	24	63%
MEA	17	6	2	7	0	15	88%
Summe	210	11	2	113	16	142	68%

Umfang der Beteiligung des DSB

Die spezialisierte Rolle des Datenschutzbeauftragten ist immerhin noch an 23 von 37 IT-Prozessen beteiligt, wobei sich die Beteiligung ebenfalls über alle Domänen erstreckt, s. Tabelle 9. Auch dem DSB kommt überwiegend eine beratende Rolle zu. Seine höchste Beteiligungsquote, 88 %, liegt ebenfalls in der MEA-Domäne vor, wobei hier auch die relativ meisten Nennungen von Durchführungsverantwortung bzw. Rechenschaftspflicht zu finden sind. Fast ebenso umfangreich fällt die Beteiligung des DSB in der BAI-Domäne aus.[73]

---

[72] Eigene Berechnungen.

[73] In der umfangreichen Beteiligung der beiden Compliance-Rollen lässt sich die einzig ins Auge springende systematische Inkonsistenz von COBIT 5 identifizieren. So existieren durchaus Prozesse, die trotz einer relativ umfangreichen Beteiligung der Compliance-Rollen die betreffenden IT-Ziele formal nicht einmal sekundär unterstützen. Beispiele hierfür sind die Prozesse EDM02 und EDM04.

Domäne	Governance-/ Management-praktiken	Beteiligung Compliance-Funktion					
		R	A	C	I	Summe	Beteiligungsquote
EDM	15	0	0	2	6	8	53%
APO	72	4	0	11	4	19	26%
BAI	68	6	0	32	5	43	63%
DSS	38	0	0	6	3	9	24%
MEA	17	6	0	6	3	15	88%
Summe	210	16	0	57	21	94	45%

Tabelle 9
Beteiligung des Datenschutz-beauftragten an den Management-praktiken[74]

2.7 Compliance im Rahmen der MEA-Domäne

Die MEA-Domäne "Überwachen, Evaluieren und Beurteilen" gliedert sich in drei Prozesse, die sich in ihren Aufgaben der Überwachung, Evaluierung und Beurteilung auf jeweils unterschiedliche Objekte richten. MEA01 fokussiert das Erreichen von Leistungs- und Konformitätszielen, MEA02 befasst sich mit dem internen Kontrollsystem und MEA03 adressiert die Compliance mit externen Anforderungen. Alle drei Prozesse unterstützen eines der beiden oder beide IT-bezogene Complianceziele, vgl. Abbildung 4.

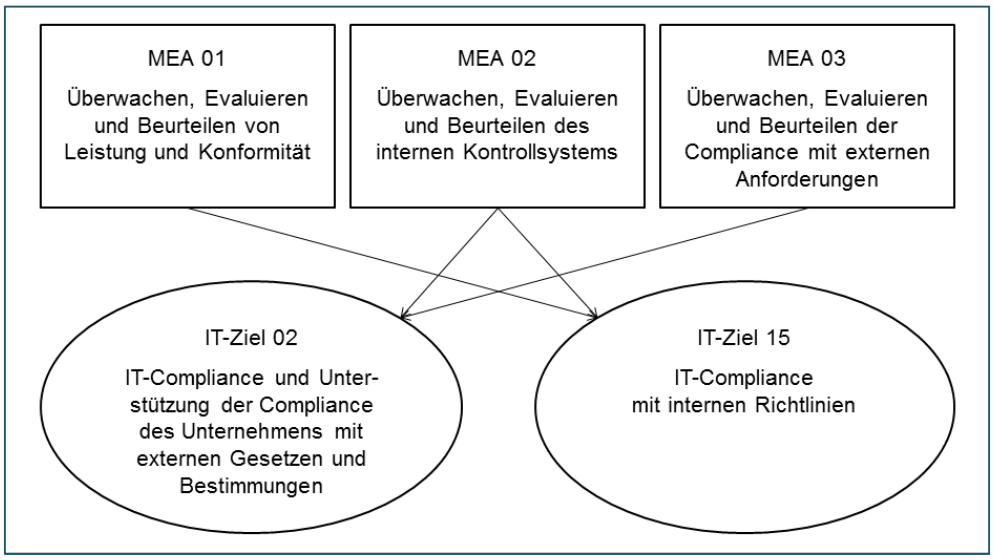

Abbildung 4
Von den MEA-Prozessen unterstützte IT-bezogene Complianceziele

[74] Eigene Berechnungen.

Die drei MEA-Prozesse sind in insgesamt 17 Managementpraktiken unterteilt, denen wiederum bis zu acht Aktivitäten zugeordnet sind. Die Untergliederung der Prozesse in Managementpraktiken zeigt Tabelle 10.

Tabelle 10
Managementpraktiken der MEA-Prozesse[75]

Nr.	MEA01 Überwachen, Evaluieren und Beurteilen von Leistung und Konformität	MEA02 Überwachen, Evaluieren und Beurteilen des internen Kontrollsystems	MEA03 Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen
.01	Einrichten eines Überwachungsansatzes	Überwachen interner Kontrollen	Identifizieren externer Compliance-Anforderungen
.02	Festlegen von Leistungs- und Konformitätszielen	Überprüfen der Effektivität von Geschäftsprozesskontrollen	Optimieren der Reaktion auf externe Anforderungen
.03	Erfassen und Verarbeiten von Leistungs- und Konformitätsdaten	Durchführen von Selbsteinschätzungen zu Kontrollen	Bestätigen der externen Compliance
.04	Analysieren und Berichten der Leistung	Identifizieren und Melden von Kontrollschwächen	Erhalten von Compliance-Bestätigungen
.05	Sicherstellen der Implementierung korrektiver Maßnahmen	Sicherstellen der Unabhängigkeit und Qualifikation der Prüfer	
.06		Planen von Prüfinitiativen	
.07		Festlegen des Umfangs von Prüfinitiativen	
.08		Umsetzen von Prüfinitiativen	

Vom Prozessnamen her stellt sich MEA03 (Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen) als der zentrale Compliance-Prozess von COBIT 5 dar. Allerdings werden in MEA01 die Ziele der Überwachung und damit auch die Complianceziele, in MEA02 die Kontrollumgebung und das interne Kontrollsystem und damit die Infrastruktur der Überwachung festgelegt. MEA03 basiert somit notwendig auf den in MEA01 und MEA02 getroffenen Festlegungen.

[75] Nach *ISACA 2012b*, S. 206, 210, 215.

MEA01

Der Prozesszweck von MEA01 „Überwachen, Evaluieren und Beurteilen von Leistung und Konformität“, besteht in der „Gewährleistung von Transparenz in Bezug auf Leistung und Konformität sowie Förderung der Zielerreichung“.[76] Die Prozessziele bestehen im Wesentlichen in der Festlegung von Zielen und Metriken, die sich eben auch auf Konformität (Compliance) beziehen. Diese IT-bezogenen Complianceziele und -metriken müssen in das Überwachungssystem des Unternehmens integriert und im Unternehmen kommuniziert sein, die Zielerreichung muss systematisch gemessen und entsprechende Berichte müssen zielgruppenadäquat und zeitgerecht zur Verfügung gestellt werden. Die Angemessenheit von Zielen, Metriken und Berichten ist regelmäßig zu bewerten, Anpassungen sind im Rahmen eines Änderungsmanagements vorzunehmen. Werden bei der Messung der Zielerreichung wesentliche Abweichungen festgestellt, so sind korrektive Maßnahmen zu ergreifen und bis zur Problemlösung zu verfolgen. Auch Status und Ergebnis der Maßnahmen sind kontinuierlich zu berichten.[77]

MEA02

Im Mittelpunkt von MEA02 „Überwachen, Evaluieren und Beurteilen des internen Kontrollsystems“ steht das interne Kontrollsystem (IKS). Der Prozess zielt vor allem darauf ab, die Angemessenheit und Effektivität des IKS für verschiedene Stakeholder nachzuweisen. Ein hierfür wesentliches Prozessziel besteht darin, dass interne Kontrollen eingerichtet und eventuelle Schwachstellen identifiziert und gemeldet werden.[78] In Bezug auf IT-Compliance stehen Compliance-Kontrollen und entsprechende Schwachstellen im Vordergrund. Diese sind im Rahmen des Kontrollsystems risikoorientiert zu konzipieren, zu implementieren und in ihrer Wirksamkeit zu evaluieren. Bei der Überwachung interner Kontrollen ist nicht nur die interne Sicht erforderlich, sondern es ist explizit darauf zu achten, „dass die Serviceanbieter den gesetzlichen, behördlichen und vertraglichen Anforderungen und Pflichten nachkommen“.[79]

MEA03

Durch den Prozess MEA03 "Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen" soll sichergestellt werden, dass das Unternehmen alle anwendbaren externen Anforderungen identifiziert und einhält. Das Erreichen dieser Zielsetzung wird durch vier spezielle Prozessmetriken gemessen:

---

[76] *ISACA 2012b*, S. 205.
[77] Vgl. *ebd.*, S. 205-207.
[78] Vgl. *ebd.*, S. 209-214.
[79] *Ebd.*, S. 211.

- „Durchschnittlich erforderliche Zeit zwischen der Identifizierung externer Compliance-Probleme und deren Lösung
- Häufigkeit von Compliance-Überprüfungen
- Anzahl der jährlich identifizierten, kritischen Non-Compliance-Ereignisse
- Anteil der Prozessverantwortlichen, die die Compliance durch Freizeichnung bestätigen“.[80]

MEA03 Managementpraktiken

Der Prozess selbst gliedert sich in vier Managementpraktiken, die den Inhalt und den Umfang des Managements der extern orientierten IT-Compliance wiedergeben.

- Compliance-Anforderungen resultieren nach MEA03.01 aus lokalen und internationalen „gesetzlichen, behördlichen und sonstigen externen vertraglichen Anforderungen …, die relevant für die Nutzung von IT-Ressourcen und die Verarbeitung von Informationen innerhalb der geschäftlichen und IT-bezogenen Abläufe des Unternehmens sind“.[81] Als spezielle Bereiche werden „Datenschutz, interne Kontrollen, Finanzberichtswesen, branchenspezifische Bestimmungen, geistiges Eigentum, Gesundheit und Sicherheit“[82] genannt. Damit die maßgeblichen Anforderungen abgestimmt gemanagt werden können, wird die Führung eines integrierten Registers empfohlen. Dieses stellt die Basis für die Analyse der Auswirkungen der Compliance-Anforderungen und die Festlegung erforderlicher Maßnahmen dar. Soweit erforderlich, ist auf externe Hilfe zurückzugreifen.
- MEA03.02 richtet sich auf die Anpassung an geänderte Compliance-Anforderungen. Um zeitnah auf neue oder geänderte Vorgaben reagieren und Compliance herstellen zu können, bedarf es eines internen Prozesses der Identifikation sowie der Umsetzung durch IT-Richtlinien, -Standards und -Verfahren, die regelmäßig zu bewerten und anzupassen sind. Wichtig ist die Kommunikation von Neuerungen und Änderungen in die betroffenen Stellen und Abteilungen des Unternehmens.
- Die Compliance der unternehmensintern verwendeten Richtlinien, Prinzipien, Standards, Verfahren und Methoden mit gesetzlichen, behördli-

[80] *ISACA 2012b*, S. 215.
[81] *Ebd.*, S. 216.
[82] *Ebd.*

chen und vertraglichen Anforderungen ist nach MEA03.03 regelmäßig durch interne und externe Überprüfungen zu überwachen und zu beurteilen. Die Überprüfung der Compliance hat sich sowohl auf Geschäfts- als auch auf IT-Prozesse, in denen die verschiedenen Regelwerke zum Einsatz gelangen, zu beziehen. Wurden Compliance-Lücken festgestellt, sind diese zu dokumentieren und zeitnah Maßnahmen mit dem Ziel der Anpassung der betroffenen Regelwerke, IT- oder Geschäftsprozesse einzuleiten.

- MEA03.04 richtet sich auf die Dokumentation der Compliance, die als Ergebnis aus internen und externen Überprüfungen resultiert. Eine wichtige Rolle spielen hierbei die Prozesseigner (engl. process owner), die die Compliance des von ihnen verantworteten Geschäfts- oder IT-Prozesses zu bestätigen haben. Gleiches gilt für IT-Dienstleister und Geschäftspartner. Die Ergebnisse – insbesondere zu Non-Compliance-Vorfällen und ihren Ursachen sowie zu ergriffenen Maßnahmen – sind in die generelle Berichterstattung des Unternehmens zu integrieren.

MEA03 RACI-Modell

Im RACI-Modell von COBIT wird dem Chief Information Officer (CIO) die Durchführungszuständigkeit (R) für alle vier Prozesspraktiken – allerdings nicht alleinig – zugeordnet. Für die Identifizierung der Compliance-Anforderungen sowie für die Reaktion auf externe Anforderungen sind die Führungskräfte des Unternehmens verantwortlich (A), für die Bestätigung der externen Compliance die Compliance-Funktion und für das Erhalten der Compliance-Bestätigungen die Audit-Funktion des Unternehmens. Darüber hinaus sind als Inputgeber und Informationsempfänger sämtliche IT-Führungskräfte (z. B. Information Security Manager, Business Continuity Manager, Leitung Entwicklung, Leitung IT-Operations), das Topmanagement des Unternehmens (Geschäftsleitung, Chief Executive Officer, Chief Financial Officer und Chief Operating Officer) sowie die Führungskräfte der Geschäftseinheiten beteiligt.[83]

2.8 Compliance im Rahmen des COBIT 5 Informationsmodells

Modell-zusammenhang

Der Zusammenhang zwischen dem COBIT 5 Prozess- und dem Informationsmodell ergibt sich hauptsächlich über die Prozessin- und -ouputs, die für gewöhnlich aus Informationsobjekten („information items“) i. S. einer

[83] Vgl. *ISACA 2012b*, S. 215.

Kombination aus Informationsinhalten und Informationsträgern bestehen. Insbesondere für die Zielerreichung kommt den Informationsobjekten eine wichtige Funktion zu, indem sie diese ermöglichen oder dokumentieren. Hierzu müssen die Informationsobjekte bestimmte Qualitätskriterien erfüllen, deren Erfüllung wiederum mittels der Zielmetriken bewertet werden kann. Tabelle 11 zeigt die Zusammenhänge für das IT-Ziel der externen Compliance exemplarisch auf.

Tabelle 11
Zuordnung von Informationsobjekten zu IT-Zielen[84]

Generische IT-Ziele	Informationsobjekte	Qualitätskriterien	Metriken
ITG02 IT-Compliance und Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen	• IT-bezogenes Register der Compliance-Anforderungen • Berichte über Compliance-Prüfungen	• Fehlerfreiheit • Vollständigkeit • Aktualität	Kosten der IT−seitigen Nichteinhaltung (Non-Compliance), einschließlich Abfindungen und Geldbußen sowie Folgen von Reputationsverlust
		• Fehlerfreiheit • Vollständigkeit • Aktualität • Klarheit • Interpretierbarkeit	Anzahl der IT-bezogenen Non-Compliance-Vorfälle, die der Geschäftsleitung gemeldet werden oder zu öffentlichen Diskussionen oder Unannehmlichkeiten führen
		• Fehlerfreiheit • Vollständigkeit • Aktualität • Klarheit • Interpretierbarkeit	Anzahl der Non-Compliance-Vorfälle, die sich auf Vertragsvereinbarungen mit IT-Serviceanbietern beziehen
		• Fehlerfreiheit • Vollständigkeit • Aktualität	Abdeckung von Compliance-Bewertungen

Compliance-bezogene Informationsobjekte

Regulatorische Compliance und Datenschutz werden als wesentliche Handlungsbereiche der Information Governance bzw. des Informationsmanagements angesehen. Das Informationsmodell empfiehlt bewährte Konzepte des Informationsmanagements, wie z. B. die Orientierung an den Informationsbedarfen der Stakeholder, die Betrachtung des Lebenszyklus eines In-

[84] Nach *ISACA 2013d*, S. 21.

formationsobjektes, die Beschreibung von Informationsobjekten durch insgesamt elf Merkmale oder das Management der Informationsqualität mithilfe von 15 Qualitätskriterien. Letztlich geht es darum, die Informationsobjekte als In- und Outputs der Prozesse effektiv und effizient zu managen. Als solche Informationsobjekte werden (weitgehend durchgängig über die verschiedenen COBIT 5-Dokumente) genannt:

- Abhilfemaßnahmen für Non-Compliance;
- Aktualisierte Richtlinien, Prinzipien, Verfahren und Standards;
- Compliance-Bestätigungen;
- Berichte zu Non-Compliance-Vorfällen und Ursachen;
- Berichte zur Compliance-Prüfung;
- Beurteilung der Berichtseffektivität;
- Ergebnisse aus der Überprüfung der Lieferanten-Compliance-Überwachung;
- Ergebnisse der Compliance-Prüfung;
- Ergebnisse installierter Lizenzprüfungen;
- Gesetzliche und behördliche Compliance-Anforderungen;
- Identifizierte Compliance-Lücken;
- Industriestandards und bewährte Verfahren;
- Kommunikation von geänderten Compliance-Anforderungen;
- Lizenzabweichungen;
- Meldungen von Non-Compliance-Vorfällen und Ursachen;
- Protokoll der erforderlichen Compliance-Maßnahmen;
- Regeln für die Validierung und Genehmigung von Pflichtberichten;
- Register der Compliance-Anforderungen;
- Versicherungsberichte.[85]

Wie diese einzelnen Informationsobjekte nun inhaltlich und formal auszugestalten sind, muss unternehmensspezifisch festgelegt werden. Hierbei sieht

[85] Vgl. *ISACA 2013d*, S. 68.

COBIT ein informationsbezogenes Rollenmodell vor, das grob zwischen Informationsproduzenten, -verwaltern und -konsumenten unterscheidet.[86] Eine Differenzierung in weitere Rollen ist in Abhängigkeit von relevanten Lebenszyklusphasen[87] vorzunehmen.

2.9 Fazit zu COBIT 5

COBIT 4.0 vs. COBIT 5

Die Compliance-Thematik ist in COBIT 5 deutlich umfangreicher, aber auch konsistenter enthalten als in COBIT 4.0, vgl. die Gegenüberstellung der wesentlichen Kenngrößen in Tabelle 12.

Tabelle 12 Vergleich von COBIT 4.0 und COBIT 5 in Bezug auf Compliance

Compliance-Bezug	COBIT 4.0	COBIT 5
Compliance-Definition	explizit als Informationskriterium	implizit in Zielen enthalten und durch Bezug auf ISO/IEC 38500
Compliance-Bezug der Unternehmensziele	2 compliance-bezogene Unternehmensziele: • Compliance mit Gesetzen und Regulativen (Nr. 14) • Compliance mit internen Regelungen (Nr. 16) Beide Ziele sind Bestandteil der internen BSC-Perspektive.	2 compliance-bezogene Unternehmensziele: • Einhaltung externer Gesetze und Bestimmungen (Compliance) (Nr. 4) • Compliance mit internen Richtlinien (Nr. 15) Ziel 4 ist Teil der Finanzperspektive der BSC, Ziel 15 ist Teil der internen BSC-Perspektive.
Compliance-Bezug der IT-Ziele	1 compliance-bezogenes IT-Ziel: • Stelle die IT-Compliance mit Gesetzen und Vorschriften sicher (Nr. 27) Zuordnung zu BSC-Perspektive nur indirekt über Zuordnung zu Unternehmensziel	2 compliance-bezogene IT-Ziele: • IT-Compliance und Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen (Nr. 2) • IT-Compliance mit internen Richtlinien (Nr. 15) Ziel 2 ist Teil der Finanzperspektive der BSC, Ziel 15 ist Teil der internen BSC-Perspektive.

[86] Vgl. *ISACA 2013d*, S. 28.
[87] Die Lebenszyklusphasen nach COBIT 5 sind Plan, Design, Build/Acquire, Use/Operate, Monitor und Dispose, vgl. *ebd*, S. 34.

Compliance-Bezug	COBIT 4.0	COBIT 5
Compliance-Bezug der IT-Ziele	1 compliance-bezogenes IT-Ziel: • Stelle die IT-Compliance mit Gesetzen und Vorschriften sicher (Nr. 27) Zuordnung zu BSC-Perspektive nur indirekt über Zuordnung zu Unternehmensziel	2 compliance-bezogene IT-Ziele: • IT-Compliance und Unterstützung der Compliance des Unternehmens mit externen Gesetzen und Bestimmungen (Nr. 2) • IT-Compliance mit internen Richtlinien (Nr. 15) Ziel 2 ist Teil der Finanzperspektive der BSC, Ziel 15 ist Teil der internen BSC-Perspektive.
Compliance-relevante IT-Prozesse	4 von 34 IT-Prozessen unterstützten das compliance-bezogene IT-Ziel 11 von 34 IT-Prozessen unterstützten das Informationskriterium „Compliance“	26 von 37 IT-Prozessen unterstützten die beiden compliance-bezogenen IT-Ziele (entfällt in COBIT 5)
Compliance-Rollen im RACI-Modell	1 Rolle: • Compliance, Audit, Risk und Security	2 Rollen: • Compliance • Datenschutzbeauftragter
Zentraler Compliance-Prozess	Prozess ME 3 (Stelle Compliance mit Vorgaben sicher) der COBIT 4.0-Domäne "Überwachung und Bewertung" mit • 5 Control Objectives • 5 Kernaktivitäten gemessen durch • 3 Key Performance Indicators • 2 Key Goal Indicators • 2 IT Key Goal Indicators	Prozess MEA03 (Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen) der COBIT 4.0-Domäne "Überwachen, Evaluieren und Beurteilen" mit • 4 Managementpraktiken • 18 Aktivitäten gemessen durch • 4 Metriken für das unterstützte IT-Ziel • 4 Metriken für zwei Prozessziele

Vergleich

Dies fängt mit den erweiterten compliance-bezogenen Zielen und ihrer korrekten Zuordnung zu den BSC-Ebenen an. Durch den Wegfall der Informationskriterien entfallen auch viele der systematischen Inkonsistenzen, die noch in COBIT 4.0 enthalten waren. Am deutlichsten fällt der Ausbau der Compliance-Thematik in COBIT 5 anhand der compliance-relevanten IT-

Prozesse ins Auge. Die Zahl 26 von 37 compliance-unterstützenden IT-Prozessen in COBIT 5 gegenüber 4 bzw. 11 von 34 IT-Prozessen in COBIT 4.0 spricht hier eine deutliche Sprache. Die externe Compliance bleibt in COBIT 5 ebenso wie in COBIT 4.0 Gegenstand desjenigen Prozesses, der den Compliance-Begriff in seiner Prozessbezeichnung beinhaltet und sich somit als zentraler Compliance-Prozess darstellt. In COBIT 5 fällt dieser Prozess insbesondere durch die größere Zahl der Managementpraktiken und ihre detaillierte Beschreibung umfangreicher aus als in COBIT 4.0. Einen gewissen Nachteil von COBIT 5 gegenüber COBIT 4.0 lässt sich im Wegfall des expliziten Reifegradmodells sehen. Dieses muss bei COBIT 5 individuell entwickelt werden, wobei in der COBIT 5-Produktfamilie das Process Assessment Model und das Informationsmodell hierbei eine Unterstützung bieten können.

Fazit

Compliance als IT-Compliance und IT-gestützte Corporate Compliance ist in COBIT 5 umfangreich ausgebaut. Damit kann COBIT 5 – insbesondere das Framework-Dokument in Verbindung mit dem prozessorientierten Enabler-Handbuch – den mit IT-Compliance betrauten Funktionen und Personen als Orientierung und Hilfsmittel für die praktische Arbeit dienen, beispielsweise bei der Definition von Compliance-Aufgaben, -Prozessen und -Verantwortlichkeiten oder bei der Einrichtung eines IT-Compliance-Managementsystems. Die ergänzenden COBIT-Produkte, hier vor allem die Enabler-Handbücher, werden den Nutzeffekt noch erhöhen. Wie am informationsorientierten Enabler-Handbuch zu sehen ist, müssen jedoch auch diese Produkte über die Zeit reifen, um einen eigenständigen Wertbeitrag zu liefern.

Quellenangaben

Böhm u. a. 2009: Böhm, Markus; Goeken, Matthias; Johannsen, Wolfgang: Compliance und Alignment: Vorgabenkonformität und Strategieabgleich als Erfolgsfaktoren für eine wettbewerbsfähige IT. In: Fröschle, H.-P. (Hg.): Wettbewerbsfaktor IT, HMD Praxis der Wirtschaftsinformatik, Heft 284, 49. Jg. 2012, S. 7-17.

Baumöl 2012: Baumöl, Ulrike: IT-Governance als Basis für ein wertorientiertes Informatikmanagement. In: Hofmann, J.; Knoll, M. (Hg.): Strategisches IT-Management, HMD Praxis der Wirtschaftsinformatik, Heft 284, 49. Jg. 2012, S. 6-14.

Gaulke 2010: Gaulke, Markus: Praxiswissen COBIT – Val IT – Risk IT: Grundlagen und praktische Anwendung für die IT-Governance, Heidelberg: dpunkt, 2010.

Gaulke 2012: Gaulke, Markus: COBIT 5 – die wesentlichen Veränderungen zu COBIT 4.1. In: IT-Governance, Heft 13, 6. Jg. 2012, S. 20-21.

ISACA 2009: Information Systems Audit and Control Association (ISACA): The Risk IT Framework – Principles, Process Details, Management Guidelines, Maturity Models, Rolling Meadows: ISACA 2009.

ISACA 2012a: Information Systems Audit and Control Association (ISACA): COBIT 5® – Rahmenwerk für Governance und Management der Unternehmens-IT, Rolling Meadows: ISACA 2012.

ISACA 2012b: Information Systems Audit and Control Association (ISACA): COBIT® 5 – Enabling Processes, Rolling Meadows: ISACA 2012.

ISACA 2012c: Information Systems Audit and Control Association (ISACA): COBIT® 5 for Information Security, Rolling Meadows: ISACA 2012.

ISACA 2013a: Information Systems Audit and Control Association (ISACA): Process Assessment Model (PAM): Using COBIT® 5, Rolling Meadows: ISACA 2013.

ISACA 2013b: Information Systems Audit and Control Association (ISACA): Self-assessment Guide: Using COBIT® 5, Rolling Meadows: ISACA 2013.

ISACA 2013c: Information Systems Audit and Control Association (ISACA): COBIT® 5 for Risk, Rolling Meadows: ISACA 2013.

ISACA 2013d: Information Systems Audit and Control Association (ISACA): COBIT® 5 – Enabling Information, Rolling Meadows: ISACA 2013.

ISACA 2013e: Information Systems Audit and Control Association (ISACA): COBIT® 5 for Assurance 5 for Assurance, Rolling Meadows: ISACA 2013.

ITGI 2005: IT Governance Institute (ITGI): COBIT 4.0, Deutsche Ausgabe, Rolling Meadows: ITGI 2005.

ITGI 2003: IT Governance Institute (ITGI): IT Governance für Geschäftsführer und Vorstände, zweite Ausgabe, Rolling Meadows: ITGI 2003; online verfügbar unter: http://www.isaca.org/German/Documents/Board-Briefing-on-IT-Governance-German.pdf (letzter Zugriff am 27.12.2013).

ITGI 2006: IT Governance Institute (ITGI): Enterprise Value: Governance of IT Investments – The Val IT Framework, Rolling Meadows: ITGI 2006.

ITGI 2007a: IT Governance Institute (ITGI): IT Governance Implementation Guide using COBIT® and Val IT™, 2nd. ed., Rolling Meadows: ITGI 2007.

ITGI 2007b: IT Governance Institute (ITGI): IT Assurance Guide using COBIT®, Rolling Meadows: ITGI 2007.

ITGI 2007c: IT Governance Institute (ITGI): COBIT® Security Baseline – An Information Security Survival Kit, Rolling Meadows: ITGI 2007.

Johannsen/Goeken 2010: Johannsen, Wolfgang; Goeken, Matthias: Referenzmodelle für IT-Governance – Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co, 2. Aufl. Heidelberg: dpunkt, 2010.

Klotz/Dorn 2008: Klotz, Michael; Dorn, Dietrich-W.: IT-Compliance - Begriff, Umfang und relevante Regelwerke, in: HMD Praxis der Wirtschaftsinformatik, 45. Jg. 2008, Heft 263, S.5-14.

Klotz 2008: Klotz, Michael: IT-Governance genormt – die neue ISO/IEC 38500. In: IT-Governance, 2. Jg. 2008, Nr. 4, S. 21-22.

Klotz 2011: Klotz, Michael: IT-Compliance. In: Ernst Tiemeyer (Hrsg.): Handbuch IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 4., überarb. u. erw. Aufl., München: Hanser, S. 585-639.

Klotz 2013: Klotz, Michael: IT-Compliance. In: Ernst Tiemeyer (Hg.): Handbuch IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 5. Auflage, München: Hanser 2013, S. 707-763.

Martens u.a. 2010: Martens, Benedikt; Teuteberg, Frank; Goss, Andreas: Performance Management der IT-Governance bei der Henkel AG & Co. KGaA. In: Rehrl, K.; Reich, S. (Hg.): Geoweb, HMD Praxis der Wirtschaftsinformatik 276, 47. Jg. 2010, S. 88-89.

Sowa 2011: Sowa, Alexandra: IT-Compliance in der Systementwicklung durch Einsatz von IT-Kontrollen. In: Reinheimer, S.; Winter, R. (Hg.): Führungsinformationssysteme für eine neue Manager-Generation, HMD Praxis der Wirtschaftsinformatik 282, 48. Jg. 2011, S. 83-92.

Das Stralsund Information Management Team (SIMAT)

Das von Prof. Dr. Michael Klotz geleitete „Stralsund Information Management Team“ (SIMAT) ist am Fachbereich Wirtschaft der FH Stralsund angesiedelt. Es bündelt akademische Lehre und Forschung, Weiterbildungsangebote und Projekte im Themenbereich des betrieblichen Informationsmanagements. Informationsmanagement richtet sich auf die effektive und effiziente Nutzung der informationellen Ressourcen eines Unternehmens. Diese Zielsetzung wird heute von verschiedenen spezialisierten Fachrichtungen in der Informatik, der Wirtschaftsinformatik und der Betriebswirtschaftslehre verfolgt. Das SIMAT arbeitet insofern interdisziplinär, wobei die inhaltlichen Schwerpunkte in Kompetenzzentren (Competence Center) fokussiert werden. Im Rahmen des RD&D-Ansatzes (Research, Development and Demonstration) dienen Labore, die mit aktuellen Tools des Informationsmanagements ausgestattet sind, sowohl der fachlichen Arbeit als auch zu Demonstrationszwecken. Eine intensive Kooperation mit ausgewiesenen Expertinnen und Experten sowie mit privatwirtschaftlichen Unternehmen und die Mitarbeit in anwendungsnahen Fachorganisationen gewährleisten eine praxis- und lösungsorientierte Vorgehensweise. Die Zusammenarbeit mit Lehrstühlen anderer Hochschulen, wissenschaftlichen Einrichtungen und eine umfangreiche Publikationstätigkeit stellen sicher, dass sich das SIMAT am State-of-the-Art des Informationsmanagements orientiert und diesen mitprägt. Auf diese Weise sind die Mitarbeiterinnen und Mitarbeiter des SIMAT in der Lage, anspruchsvolle Konzepte und Lösungen zu konzipieren und zu realisieren.

Das SIMAT versteht sich als Mittler zwischen akademischer Forschung und Lehre auf der einen, und der Wirtschaftspraxis auf der anderen Seite. Diese Transferaufgabe, verankert im Landeshochschulgesetz Mecklenburg-Vorpommerns, bildet den Schwerpunkt der Arbeit des SIMAT. Forschung und Lehre werden nicht als Selbstzweck begriffen, sondern führen zu handlungsrelevanten, innovativen Konzepten und Lösungen, die in die Unternehmenspraxis transferiert werden. Die berufliche Weiterbildung bildet hierbei ein wesentliches Element.

Die anwendungsnahe Forschung am SIMAT ist auf eine ökonomische Verwertung hin orientiert. Es sollen Innovationen entwickelt und in Kooperation mit anderen wissenschaftlichen Einrichtungen, Fach-Institutionen und Unternehmen in eine nachhaltige und profitable Praxis umgesetzt werden. Hierzu werden eigene F&E-Projekte auf dem Gebiet des Informationsmanagements und Innovationsprojekte mit Partnern durchgeführt. Zudem hat sich das SIMAT auf die betriebswirtschaftliche Begleitberatung bei IT-nahen Technologieprojekten spezialisiert. Studierenden und wissenschaftlichen Mitarbeiterinnen und Mitarbeitern wird die Möglichkeit eröffnet, an

der Lösung praktischer Problemstellungen zu arbeiten und sich so optimal auf das spätere Berufsleben vorzubereiten.

Die studentischen Mitarbeiterinnen und Mitarbeiter erhalten im SIMAT Einblick in die Arbeitsmethodik sowohl auf wissenschaftlichem als auch auf wirtschaftlichem Gebiet. Aus den Projekten des SIMAT entstehen zahlreiche Abschlussarbeiten, die den Studierenden der FH Stralsund offen stehen. Das SIMAT bietet zudem eine berufliche Perspektive für Studierende, die sich als wissenschaftliche Mitarbeiter in der anwendungsnahen Forschung qualifizieren wollen.

Das SIMAT beteiligt sich zudem an der Diskussion der wissenschaftlichen Gemeinschaft. Hierzu werden regelmäßig Arbeitspapiere veröffentlicht, die den Stand der Arbeit des SIMAT in die Öffentlichkeit tragen und zur Diskussion anregen sollen. Das SIMAT lädt zudem andere Wissenschaftler, aber auch Referenten aus der Praxis als Vortragende ein. Auf diese Weise lernen die SIMAT-Mitarbeiterinnen und -Mitarbeiter sowie andere interessierte Studierende aktuelle Forschungsergebnisse und praktische Fragestellungen aus erster Hand kennen. Erkenntnisse aus diesen Aktivitäten sowie aus den verschiedenen F&E-Projekten werden systematisch in die Lehre überführt, so dass alle Studierenden von der Forschungsarbeit des SIMAT profitieren können.

Zum Zwecke des ökonomischen Transfers verfolgt das SIMAT den RD&D-Ansatz (Research, Development and Demonstration). Hierzu werden Labore als Demonstrationsbereiche unterhalten. In den Laboren werden Produkte und Lösungen von Kooperationspartnern des SIMAT in den Bereichen des Informations-, Projekt- und Prozessmanagements betrieben. Auf dieser technischen Grundlage werden im Rahmen von Projekten durch das SIMAT-Team prototypische Lösungen erarbeitet.

Kontakt

FH Stralsund • SIMAT • Zur Schwedenschanze 15 • 18435 Stralsund
Ansprechpartner: Prof. Dr. Michael Klotz (Wissenschaftlicher Leiter)
☎ +49 (0)3831 45-6946
✉ michael.klotz@fh-stralsund.de
www.simat-stralsund.de

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance
01-09-002	02.2009	M. Klotz	Von der Informationsgesellschaft zum Informationsarbeiter
01-09-003	09.2009	L. Ramin M. Klotz	Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT
01-09-004	10.2009	S. Kubisch	Corporate Governance gemäß BilMoG und SOX
02-10-005	06.2010	M. Klotz	PMBOK-Compliance der Projektmanagement-Software Projektron BCS
02-10-006	07.2010	A. Woltering	Kontinuierliche Verbesserung von Desktop-Services mittels Benchmarking
02-10-007	09.2010	M. Klotz	Grundlagen der Projekt-Compliance
02-10-008	11.2010	I. Karminski	Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung
02-10-009	12.2010	D. Engel/ N. Zdrowomyslaw	Benchmarking-Studie Stralsund 2010
03-11-010	02.2011	E. Tiemeyer	Kennzahlengestütztes IT-Projektcontrolling – Projekt-Scorecards einführen und erfolgreich nutzen
03-11-011	05.2011	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke
03-11-012	06.2011	M. Klotz	Konzeption des persönlichen Informations-managements
03-11-013	08.2011	H. Auerbach/ N. Zdrowomyslaw	9. STeP-Kongress „Region gestalten! Gesundheitswirtschaft und Zukunftsmanagement“
03-11-014	08.2011	M. Klotz	Rollen der Information im Unternehmen
03-11-015	08.2011	Ahlfeldt	eGuides in kulturellen Einrichtungen – deutschsprachiger Museums-Apps
03-11-016	11.2011	S. J. Saatmann / I. Sulk / M. Klotz	Studie zu gewerblichen Strompreisen in Mecklenburg-Vorpommern – Strom als Wettbewerbsfaktor und Gegenstand der Standortvermarktung
04-12-017	02.2012	M. Klotz / I. Sulk / E. Wieck	GDPdU-Konformität von Projektmanagement-software – Exemplarische Konzeption und Umsetzung
04-12-018	07.2012	M. Horn-Vahlefeld	Projektdesign als organisatorischer Rahmen des Projektmanagements
04-12-019	08.2012	M. Klotz / J. Kriegel	ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in die IT-Prozesse nach ITIL
04-12-020	09.2012	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke, 2. Aufl.

AP	Datum	Autor	Titel
04-12-021	10.2012	I. Sulk / M. Klotz	Einsatz von eGuides auf der Marienburg in Malbork (Polen) – Erhebung und Analyse einer Best Practice
04-12-022	12.2012	Witty, M. / C. Kliebisch	Die Versicherungsbranche unter FATCA
05-13-023	01.2013	S. J. Saatmann	The price-link in the natural gas market – The development of the oil price-link and alternative price mechanisms
05-13-024	08.2013	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen
06-14-025	01.2014	M. Klotz	IT-Compliance nach COBIT® – Gegenüber-stellung von COBIT® 4.0 und COBIT® 5