3. Auflage

Markus Gaulke

Praxiswissen COBIT

Grundlagen und praktische Anwendung in der Unternehmens-IT

Geeignet als Vorbereitung auf die ISACA-Prüfungen:

- COBIT Foundation
- IT-Governance & IT-Compliance Practitioner
- IT-Governance-Manager
- IT-Compliance-Manager
- CGEIT

ISACA Germany Chapter

dpunkt.verlag

Markus Gaulke, Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT) und Certified in Risk and Information Systems Control (CRISC), ist in Deutschland der führende Experte zum Thema COBIT und dessen Anwendung. Als das für Weiterbildung zuständige Vorstandsmitglied im deutschen Chapter des internationalen IT-Berufsverbands »ISACA« hat er die COBIT-bezogenen Zertifikatskurse »COBIT Practitioner« für COBIT 4.1 und »IT-Governance & IT-Compliance Practitioner« für COBIT 5 bzw. aktuell für COBIT 2019 ins Leben gerufen. Zudem hat er zusammen mit der Hochschule »Frankfurt School of Finance and Management« die weiterführenden dualen Zertifikatskurse »IT-Governance-Manager« und »IT-Compliance-Manager« entwickelt.

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

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

Beruflich ist er seit mehr als 20 Jahren bei der KPMG AG Wirtschaftsprüfungsgesellschaft in Frankfurt am Main für die IT-Prüfung und IT-Beratung von Unternehmen vor allem aus dem Finanzsektor zuständig. Die Praxisbeispiele in diesem Buch entstammen daher auch konkreten Beratungssituationen aus seiner Berufspraxis.

Markus Gaulke

Praxiswissen COBIT

Grundlagen und praktische Anwendung in der Unternehmens-IT

3., aktualisierte und überarbeitete Auflage

Edition ISACA Germany Chapter

ISACA® Germany Chapter

dpunkt.verlag

Markus Gaulke
www.markus-gaulke.de

Lektorat: Christa Preisendanz
Copy-Editing: Ursula Zimpfer, Herrenberg
Satz: Birgit Bäuerlein
Herstellung: Stefanie Weidner
Umschlaggestaltung: Helmut Kraus, *www.exclam.de*
Druck und Bindung: mediaprint solutions GmbH, 33100 Paderborn

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

Fachliche Beratung und Herausgabe von dpunkt.büchern in der Edition ISACA Germany Chapter:
Vorstand ISACA Germany Chapter – Vizepräsident für Publikationen
Prof. Dr. Matthias Goeken · *matthias.goeken@isaca.de*

ISBN:
Print 978-3-86490-699-2
PDF 978-3-96088-831-4
ePub 978-3-96088-832-1
mobi 978-3-96088-833-8

3., aktualisierte und überarbeitete Auflage 2020

Wieblinger Weg 17
69123 Heidelberg

Hinweis:
Dieses Buch wurde auf PEFC-zertifiziertem Papier aus nachhaltiger Waldwirtschaft gedruckt. Der Umwelt zuliebe verzichten wir zusätzlich auf die Einschweißfolie.

Schreiben Sie uns:
Falls Sie Anregungen, Wünsche und Kommentare haben, lassen Sie es uns wissen: *hallo@dpunkt.de*.

5 4 3 2 1 0

Geleitwort

Dass Markus Gaulke, ausgewiesener COBIT-Experte und Vorstandskollege im ISACA Germany Chapter, jetzt, im Herbst 2019, eine neue Auflage seines Buches »Praxiswissen COBIT« vorlegt, freut mich als Vizepräsident Publikationen ganz besonders.

Zum einen, weil damit recht bald nach der grundlegenden Überarbeitung des COBIT-Frameworks durch ISACA International eine leicht zugängliche und gut lesbare Aufarbeitung vorhanden ist, die sowohl Neulingen den Einstieg als auch COBIT-Kennern die Aktualisierung ihrer Kenntnisse erleichtert.

Das Framework wurde in vielen Belangen geändert und deutlich erweitert – insbesondere um solche Konzepte, die die unternehmensspezifische Anpassung und die Konfiguration vor dem Hintergrund verschiedener fachlicher Aufgabenstellungen unterstützen. Mit Blick darauf werden es sicherlich auch COBIT-Kenner schätzen, diese konzeptionellen Änderungen sich nicht eigenständig erarbeiten zu müssen. Insofern wird das Buch ein wichtiger Beitrag sein, das Wissen über das Framework sowie dessen jüngste Änderungen im deutschsprachigen Raum aktuell zu halten.

Zum anderen freut mich, dass Markus Gaulke sich entschieden hat, das Buch in der neuen ISACA-Buchreihe zu veröffentlichen. Der Vorstand hatte sich schon im letzten Jahr zusammen mit dem dpunkt.verlag entschlossen, neben der Zeitschrift IT-Governance und den Leitfäden der Fachgruppen eine Buchreihe ins Leben zu rufen, die umfangreichere Abhandlungen zu den verschiedenen Themen, die die Mitglieder unseres Berufsverbands bewegen, erlaubt. Es ist aus meiner Sicht besonders erfreulich, dass es nun gelungen ist, als ersten Band in dieser Buchreihe ein Buch herauszugeben, das das zentrale Rahmenwerk der ISACA in den Mittelpunkt stellt und so sicherlich zu dessen Verbreitung beiträgt.

Es behandelt neben dem Rahmenwerk an sich auch dessen Anwendung und zeigt, welche Schritte erforderlich sind, um in der Praxis von einer Einführung zu profitieren. Dass mit Blick auf die Zertifizierungen der ISACA auch Übungsfragen zur Überprüfung des erworbenen Wissens vorhanden sind, macht das Buch gewiss auch für Lernende wertvoll.

Ich wünsche dem Buch eine große Leserschaft und hoffe, dass es auf gute Resonanz bei den Mitgliedern des Germany Chapter sowie allen COBIT-Anwendern und -Interessierten stößt. Markus danke ich für sein Engagement und die beträchtliche Arbeit, die er geleistet hat, und dem dpunkt.verlag für die abermals gute Zusammenarbeit.

Prof. Dr. Matthias Goeken
Hochschule der Deutschen Bundesbank
Vizepräsident Publikationen

Vorwort

Auch zum Zeitpunkt dieser dritten Auflage sind IT-Governance, IT-Risikomanagement, IT-Compliance, IT-Assurance und IT-Outsourcing weiterhin wichtige Themen für das Management der Unternehmens-IT. Die Technologie und die Methodiken haben sich seit der ersten Auflage vor zehn Jahren weiterentwickelt. Themen wie agile Entwicklung, DevOps, Cloud, Cyber Security und Privacy gehören zum Grundwortschatz in der IT; die aus diesen Themen erwachsenen Herausforderungen zu lösen, gelingt in der Praxis aber nur effizient, wenn ein ganzheitliches Verständnis für diese Themen vorhanden ist und die Aktivitäten in ein passendes Rahmenwerk eingebunden werden.

COBIT stellt ein solches integratives Rahmenwerk für eine umfassende Governance und ein effektives Management der Unternehmens-IT dar. COBIT umfasst Methoden, Prinzipien, gute Praktiken und Leitfäden, die erforderlich sind, um eine optimale Wertschöpfung durch den Einsatz von Informationstechnologie im Unternehmen zu erreichen. COBIT strukturiert die wichtigsten Umsetzungskomponenten inkl. der Prozesse, die gewöhnlich in der IT-Funktion einer Organisation stattfinden, in einem zielorientierten Kernmodell. Dieses berücksichtigt die Inhalte der weltweit am meisten eingesetzten Praktiken und Standards im IT-Bereich, wie z. B. ITIL, COSO, ISO/IEC 20000, ISO/IEC 27001, ISO/IEC 38500, PMBOOK, CMMI und TOGAF. Dadurch stellt COBIT ein umfassendes Referenzmodell für bewährte Verfahren der IT-Governance und des IT-Managements bereit. Durch die Konzentration auf 40 universelle IT-Governance- und IT-Managementziele sowie sieben wichtige Umsetzungskomponenten ist COBIT unabhängig von Technologien und Branchen anwendbar.

COBIT ist aber mehr als nur ein Referenzmodell für die Governance und das Management der Unternehmens-IT. COBIT kann durch die integrierten Assessment-Modelle auch zur Prozessbewertung eingesetzt werden. Dabei richtet sich COBIT nicht nur an IT-Fachleute, sondern stellt über die Ausrichtung an die Unternehmens- und IT-bezogenen Ziele auch den Geschäftsprozesseigentümern ein Rahmenwerk für das Management der Unternehmens-IT (Technologiemanagement) sowie der Geschäfts- und Bereichsleitung ein ganzheitliches Modell für die Steuerung und Überwachung der Unternehmens-IT (IT-Governance) zur Verfügung.

International hat sich COBIT als anerkanntes Rahmenwerk für die Governance und das Management der Unternehmens-IT etabliert. COBIT wird weltweit von Tausenden von Unternehmen als Basis für Initiativen vor allem zur Verbesserung der IT-Governance und der IT-Compliance herangezogen. Behörden (u.a. amerikanisches Verteidigungsministerium, European Agricultural Guidance and Guarantee Fund) und andere Institutionen (u.a. META-Group, Gartner) empfehlen, COBIT einzusetzen. Die Aufsichtsbehörden einiger Länder haben COBIT sogar für verbindlich erklärt (u.a. Türkei, Kolumbien, Uruguay).

Auch im deutschen Sprachraum sind die Akzeptanz und die Anwendung von COBIT in den letzten Jahren deutlich gestiegen. Im Jahr 2010 bei der ersten Auflage dieses Buches, das sich auf COBIT 4.1 bezog, gab es nur wenige deutsche Unternehmen, die sich öffentlich zur Nutzung von COBIT bekannt haben. Mit dem Erscheinen von COBIT 5 im Jahr 2012 stieg die Akzeptanz und Nutzung von COBIT deutlich. Für die zweite Auflage konnte ich daher auch erstmals Autoren aus deutschen Unternehmen gewinnen, darüber zu berichten, wie diese COBIT einsetzen. Inzwischen wendet aus meiner Wahrnehmung die Mehrzahl der größeren deutschen Unternehmen, insbesondere im Finanzbereich, COBIT in irgendeiner Weise an. Daher sind in der hier vorliegenden, dritten Auflage dieses Buches auch wieder ganz neue Praxisbeiträge enthalten, diesmal ausschließlich von Unternehmen mittlerer Größe. Die Praxisbeispiele illustrieren die Anwendung von COBIT zur IT-Steuerung, für das IT-IKS, als umfassende GRC-Referenz, als Revisionswerkzeug sowie als Risiko-Rahmenwerk. Durch die im Buch beschriebenen Anwendungsszenarien und die externen Praxisbeiträge soll das Buch zum Gebrauch von COBIT animieren – denn letztendlich zeigt sich der Nutzen dieses IT-Management- und IT-Governance-Rahmenwerks nur im konkreten Einsatz.

Die Anwendung von COBIT strahlt also aus und liegt im Trend. Mit der Weiterentwicklung von COBIT 5 zu COBIT 2019 wurde von der ISACA auch bereits ein spezieller Umsetzungsleitfaden (Focus Area Guide) für kleine und mittlere Unternehmen mit weniger als 250 Mitarbeitern angekündigt, der diesen Trend unterstützen wird. Auch das Thema Agilität soll mit einem Umsetzungsleitfaden zum Thema DevOps aufgenommen werden. COBIT 2019 wird sich also über die hier behandelten Kernbücher hinaus weiterentwickeln. Die »Focus Area Guides« und andere wesentliche Weiterentwicklungen werde ich in Form von Beiträgen in der Zeitschrift »IT-Governance« darstellen.

Das vorliegende Buch bezieht sich auf COBIT 2019. Die Darstellungen sind aber weitestgehend auch für COBIT 5 anwendbar, weil COBIT 2019 vor allem eine nutzerorientierte Weiterentwicklung von COBIT 5 ist und das Kernmodell inhaltlich nur marginal verändert wurde. Viele Ausführungen gelten daher für beide COBIT-Versionen. Die deutschen Bezeichnungen in diesem Buch orientieren sich daher auch an der Übersetzung der beiden zentralen Bücher der COBIT-5-Produktfamilie (Rahmenwerk und Prozessreferenzmodell) durch das ISACA Germany Chapter. Zusätzlich werden die Veränderungen zwischen COBIT 5 und COBIT 2019 in Kapitel 16 zusammenfassend aufgezeigt.

Der Aufbau des Inhalts ermöglicht eine hohe Flexibilität beim Umgang mit diesem Buch. Der COBIT-Einsteiger sollte sich vor allem mit dem ersten Teil des Buches beschäftigen, in dem die Grundlagen von COBIT vermittelt werden. In den nachfolgenden Kapiteln können dann Interessenschwerpunkte vertieft werden. Der mit COBIT bereits vertraute Leser kann das Buch selektiv lesen und als Nachschlagewerk verwenden. Anhand der Testfragen kann der an einer Zertifizierung interessierte Leser auch gezielt seine Wissenslücken herausfinden und durch Bearbeiten der entsprechenden Themen schließen.

Ich hoffe, dass dieses Buch allen Lesern hilft, das aktuelle Rahmenwerk COBIT 2019 – auch im Kontext mit anderen Praktiken und Standards – besser zu verstehen, um COBIT erfolgreich im Sinne der Unternehmensziele einzusetzen.

Markus Gaulke
Königstein im Taunus, September 2019

Inhaltsübersicht

Inhaltsverzeichnis

Teil III
COBIT in der Praxis 329

1 Einleitung

Governance zusammen mit Risikomanagement, Compliance und Assurance haben sich auf den Prioritätenlisten vieler Unternehmen an die Spitze gesetzt. Diese Entwicklung wird maßgeblich von den Anforderungen der Anteilseigner und Aufsichtsgremien sowie der erhöhten Aufmerksamkeit des Gesetzgebers und der Aufsichtsbehörden sowie der Öffentlichkeit getrieben (vgl. Abb. 1–1). Der Trend zu einer verbesserten Governance in den Unternehmen wird durch eine Vielzahl von Initiativen sichtbar. Diese haben in der Regel das Ziel, die Kommunikation und Informationsflüsse zu verbessern, das Risikobewusstsein zu erhöhen und ein angemessenes internes Kontrollsystem aufzubauen und nachzuweisen.

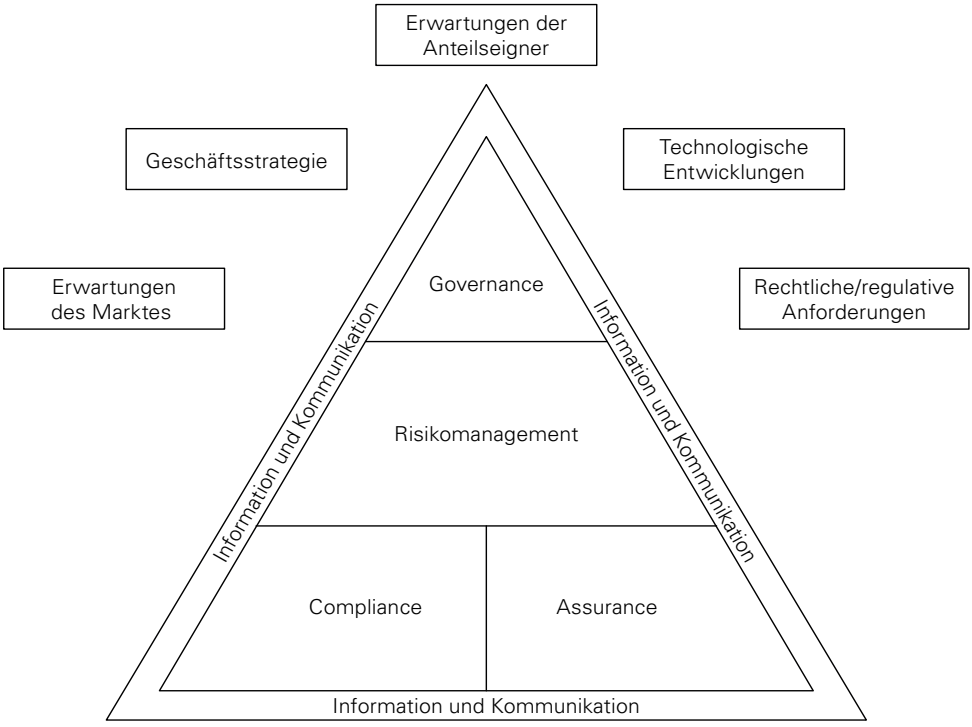

Abb. 1–1 *Treiber von Governance-Initiativen*

Die zunehmende Durchdringung von Unternehmen mit Informationstechnologie (IT) und die dadurch bedingte steigende Abhängigkeit von der Verfügbarkeit und Verlässlichkeit der IT-Prozesse und Daten erfordern, die Unternehmens-IT besser in die Governance-Prozesse und das interne Kontrollsystem des Unternehmens einzubeziehen und diese aus Unternehmenssicht zu steuern und zu überwachen. Corporate Governance der IT (kurz: IT-Governance) hat zum Ziel, dass die IT die Geschäftsziele des Unternehmens unterstützt, die IT-Investitionen auf die geschäftlichen Ziele hin optimiert und dass gleichzeitig die IT-Risiken beherrscht werden. IT-Governance ist damit ein wesentlicher Bestandteil eines ganzheitlichen Corporate-Governance-Ansatzes zur Steuerung und Überwachung eines Unternehmens.

Das IT Governance Institute (ITGI) als führende Institution für IT-Governance bzw. der Berufsverband Information Systems Audit and Control Association (ISACA) hatte neben COBIT als Rahmenwerk mit dem Fokus auf die Steuerung und das Management von IT-Prozessen noch zwei weitere Rahmenwerke entwickelt: das Rahmenwerk »Val IT« mit dem Fokus auf die geschäftlichen Investitionen sowie das Rahmenwerk »Risk IT« mit dem Fokus auf die IT-bezogenen Geschäftsrisiken. Die intelligente Anwendung dieser drei Rahmenwerke sollte Organisationen aller Art ermöglichen, ihre IT-Governance und ihre IT-Compliance zu verbessern sowie den optimalen Nutzen aus den IT-bezogenen Investitionen und aus den IT-Risikomanagement-Aktivitäten zu ziehen [ITGI 2009e].

Mit dem Erscheinen von COBIT 5 wurden diese drei Rahmenwerke nicht außer Kraft gesetzt, sondern die Inhalte sind unter dem gemeinsamen Dach von COBIT zusammengeführt worden und werden unter diesem Dach weiterentwickelt.

Das vorliegende Buch bezieht sich bereits auf die erste evolutionäre Weiterentwicklung von COBIT 5, die »COBIT 2019« genannt wird.

1.1 Aufbau des Buches

Der erste Teil des Buches führt in das neue Rahmenwerk von COBIT 2019 und das zentrale Modell mit allen seinen Elementen ein und erläutert die zugrunde liegenden Konzepte von COBIT. Neben den grundlegenden Prinzipien von Governance-Systemen und Governance-Rahmenwerken werden dazu die sieben im Kernmodell von COBIT dargestellten Komponenten (in COBIT 5: Enabler) ausführlich in allen ihren Dimensionen diskutiert. Das in COBIT 2019 neu hinzugekommene Prozessbefähigungsmodell wird ebenso dargestellt wie die mit COBIT eng verbundenen Praktiken, Standards und Rahmenwerke.

Im zweiten Teil werden vor allem Ansätze für die Anwendung von COBIT vorgestellt. Insgesamt werden elf Anwendungsszenarien ausführlich erläutert. Diese umfassen die vielfältigen Anwendungsmöglichkeiten von COBIT als Modell für die IT-Governance, die IT-Compliance, das IT-Risikomanagement, die IT-Assurance, das IT-Outsourcing, die Informationssicherheit sowie für die Identifikation von geschäftsrelevanten Prozessen und deren Überwachung.

Im dritten Teil berichten Praktiker aus deutschen Unternehmen, wie sie COBIT konkret einsetzen. In dieser Auflage sind neue Praxisbeiträge von unterschiedlichsten Unternehmen aufgenommen worden. Die Praxisbeispiele illustrieren die Anwendung von COBIT zur IT-Steuerung, für das IT-IKS, als umfassende GRC-Referenz, als Revisionswerkzeug sowie als Risiko-Rahmenwerk.

Der vierte Teil beschreibt die von der berufsständischen Organisation ISACA angebotenen COBIT-2019-bezogenen Zertifizierungsmöglichkeiten mit ihren Lehr- und Prüfungsinhalten sowie Testfragen für die Vorbereitung auf die Prüfungen »COBIT Foundation« und »IT-Governance & IT-Compliance Practitioner«.

Der Anhang enthält tabellarische Übersichten der Governance- und Managementziele sowie der Prozesse mit ihren Governance- und Managementpraktiken. Weiterhin wird die Zielkaskade von den Unternehmenszielen bis zu den primär zugeordneten Governance- und Managementzielen dargestellt. Die Übersichten sowie alle zentralen Begriffe im Buch sind in Deutsch und in Englisch aufgeführt, was sich in der Projektpraxis oftmals als hilfreich erwiesen hat.

Teil I

COBIT verstehen

2 Entwicklung und Bedeutung von COBIT

Dieses Kapitel stellt die Entwicklung des COBIT-Rahmenwerks und der komplementierenden Rahmenwerke Val IT und Risk IT sowie deren Integration in COBIT 5 und dessen Weiterentwicklung zu COBIT 2019 dar. Daneben wird die Rolle des internationalen Berufsverbandes ISACA und seiner Forschungseinrichtungen für COBIT beschrieben.

2.1 ISACA und das IT Governance Institute

Die Information Systems Audit and Control Association (ISACA) ist ein internationaler Berufsverband der IT-Revisoren, IT-Sicherheitsmanager und IT-Governance-Experten. Primäres Ziel des Verbandes ist die Entwicklung und Verbreitung von Berufsstandards und Arbeitstechniken sowie die Zertifizierung und Weiterbildung von Fachleuten, die sich mit der Kontrolle und der Sicherheit sowie dem Management und der Steuerung von Informationssystemen befassen.

Der Berufsverband ISACA wurde ursprünglich 1969 als Berufsverband der IT-Revisoren – EDP Auditors Association (EDPAA) – gegründet. 1976 wurde von der EDPAA eine Forschungseinrichtung, die »EDP Auditors Foundation« (EDPAF), gegründet, die größere Forschungsvorhaben aus der Mitgliederorganisation herausgelöst vornehmen sollte. Erst im Jahr 1994 erhielt der Verband seinen heutigen Namen: »Information Systems Audit and Control Association« (ISACA). Die Forschungseinrichtung wurde entsprechend in »Information Systems Audit and Control Foundation« (ISACF) umbenannt.

Im Jahr 1998 wurde von der ISACA zusätzlich das »IT Governance Institute« (ITGI) als Forschungseinrichtung auf dem Gebiet des Informationsmanagements gegründet. Damit erweiterte sich auch das thematische Spektrum des Berufsverbandes von der IT-Revision über das IT-Management bis hin zur IT-Governance. Im Jahr 2003 ging die ISACF im ITGI auf, sodass das ITGI der alleinige Herausgeber der Rahmenwerke COBIT 4.0 bzw. COBIT 4.1 und Val IT wurde.

Inzwischen trägt der Berufsverband ISACA seiner erreichten Anerkennung über die IT-Prüfung hinaus Rechnung und nutzt die neutrale Plattform des ITGI immer seltener. Bereits das Rahmenwerk Risk IT wurde im November 2009 wieder unter der

Herausgeberschaft der ISACA veröffentlicht. Für alle Veröffentlichungen von COBIT 5 und COBIT 2019 ist die ISACA der alleinige Herausgeber.

Dem Berufsverband ISACA gehörten zum Zeitpunkt der Entstehung dieses Buches weltweit über 150.000 Mitglieder an. Neben der zentralen Organisation in Rolling Meadows bei Chicago ist die ISACA dezentral in über 190 lokalen Chaptern organisiert. In Deutschland wird die ISACA durch den ISACA Germany Chapter e.V. vertreten. Das ISACA Germany Chapter war Ende 2018 mit knapp 3.000 Mitgliedern das siebtgrößte Chapter weltweit (vgl. Tab. 2–1).

Chapter	Internetadresse	Gründung	Anzahl Mitglieder
ISACA Germany Chapter	*www.isaca.de*	1986	2.968
ISACA Switzerland Chapter	*www.isaca.ch*	1988	1.567
ISACA Austria Chapter	*www.isaca.at*	1998	421

Tab. 2–1 *Übersicht der deutschsprachigen Chapter der ISACA (Stand: 31.12.2018)*

Die lokalen ISACA-Chapter bieten ergänzend zum zentralen Angebot der ISACA spezifische Fachinformationen, Weiterbildungs- und Qualifizierungsmaßnahmen sowie Veranstaltungen an, damit sich die Mitglieder ortsnah fortbilden und besser vernetzen können.

Neben COBIT haben auch die Berufszertifizierungen der ISACA weltweite Anerkennung gefunden. Die älteste Berufszertifizierung zum »Certified Information Systems Auditor« (CISA) trugen Mitte 2019 weltweit über 90.000 Personen, davon allein 2.074 Personen in Deutschland. Deutlich zugelegt hat auch die Anzahl der Inhaber der Berufszertifizierung zum »Certified Information Security Manager«. Diese Berufszertifizierung hatten in Deutschland Mitte 2019 fast 1.000 Personen erworben (vgl. Tab. 2–2).

Berufszertifizierung	Berufsbild	Initiierung	Anzahl zertifizierter Personen (weltweit)	Anzahl zertifizierter Personen (Deutschland)
Certified Information Systems Auditor (CISA)	IT-Revisor	1978	90.615	2.074
Certified Information Security Manager (CISM)	Informations-sicherheitsmanager	2003	36.449	979
Certified in the Governance of Enterprise IT (CGEIT)	IT-Governance-Beauftragter	2007	11.626	108
Certified in Risk and Information Systems Control (CRISC)	IT-Risiko- und Kontrollbeauftragter	2011	20.704	390

Tab. 2–2 *Übersicht der Berufszertifizierungen der ISACA (Stand: 31.07.2019)*

Weitere Informationen zu den vier Berufszertifizierungen erhalten Sie über die Internetseite der ISACA (*www.isaca.org*). Die lokalen Chapter bieten in der Regel Vorbereitungskurse für die Zertifizierungsprüfungen an. Das Seminarangebot des deutschen Chapter finden Sie unter *www.isaca.de*.

2.2 Entstehung und Entwicklung von COBIT

Das Akronym COBIT steht als Kurzwort für »Control Objectives for Information and Related Technology«. Die Wurzeln von COBIT liegen in der IT-Revision, inzwischen hat sich COBIT aber zu einem umfassenden IT-Governance- und Management-Rahmenwerk für Information und die sie verarbeitende Technologie entwickelt. Dieser Anspruch wird durch die aktuelle Version von COBIT noch deutlicher unterstützt: Explizites Ziel des Einsatzes der aktuellen Versionen von COBIT ist, einen optimalen Wertbeitrag aus Investitionen in Information und in die dazu benötigte Technologie zum Nutzen aller Anspruchsgruppen zu erhalten.

Die ursprüngliche Basis des Rahmenwerks COBIT war ein Standardwerk, in dem das Wissen und der Erfahrungsschatz des Berufsstandes der IT-Revisoren gebündelt war: »Control Objectives – Controls in an Information Systems Environment: Objectives, Guidelines und Audit Procedures«. Dieses Werk wurde bereits im Jahr 1976 erstmals von der EDPAF (später ISACF) herausgegeben und von dieser ständig weiterentwickelt. Im April 1992 erschien die vierte und letzte Ausgabe [EDPAF 1992], in der die allgemeinen IT-Kontrollen in Kontrollen

- des Managements (Management Controls),
- der IT-Systementwicklung, Beschaffung und Wartung (Information System Development, Acquisition, and Maintenance Controls) sowie
- des Betriebs (Information System Operations Controls)

gegliedert worden sind, was bereits im Wesentlichen der späteren Domänenstruktur von COBIT entsprach. Daneben gab es noch eine Darstellung der Anwendungskontrollen (Application Controls) sowie einen eigenen Abschnitt mit technologieorientierten Kontrollen (Technology Specific Controls). Dieser Abschnitt ist aufgrund seiner Technikorientierung nicht in das Rahmenwerk COBIT mit eingeflossen.

Die ISACA hat im Jahr 1993 begonnen, auf Basis der bestehenden Sammlung von Kontrollzielen und Kontrollen ein eigenständiges Rahmenwerk zu erarbeiten. Dazu wurde von der ISACA ein internationales Gremium eingesetzt (COBIT Steering Committee), das die erste Version von COBIT entwickeln sollte. An der Entwicklung des neuen Rahmenwerks waren auch die Free University of Amsterdam, die California Polytechnic University und die University of New South Wales beteiligt.

Die erste Version von COBIT wurde im April 1996 von der damaligen ISACA-Forschungseinrichtung ISACF (Information Systems Audit and Control Foundation) veröffentlicht. »COBIT 1« beinhaltete neben einem konzeptionellen Rahmen bereits ein Prozessmodell mit generell anwendbaren und international akzeptierten IT-pro-

zessbezogenen Anforderungen (Control Objectives). Das COBIT-Prozessmodell umfasste damals 32 Prozesse mit 271 detaillierten Anforderungen. Diese detaillierten Anforderungen sollten in einer Organisation beachtet und umgesetzt werden, um eine verlässliche Anwendung der Informationstechnologie zu gewährleisten. Die Idee dahinter: Erst wenn die Prozesse richtig organisiert sind, werden die Geschäftsprozesse die an sie gestellten Anforderungen erfüllen [ISACF 1996].

Zum Zeitpunkt der Veröffentlichung dieser ersten Version von COBIT waren die nächsten Schritte der Weiterentwicklung bereits klar definiert. Die Control Objectives sollten nochmals auf Basis weiterer Referenzmaterialien überarbeitet werden und vor allem sollten noch Richtlinien zur Selbsteinschätzung und Metriken für das Management entwickelt werden. Im April 1998 erschien die überarbeitete und erweiterte zweite Version mit 302 detaillierten Anforderungen (Control Objectives) in 34 Prozessen [ISACF 1998] sowie einem zusätzlichen »Implementation Tool Set«, bestehend aus einer Anleitung zur Implementation von COBIT und unterstützenden Materialien.

Das Rahmenwerk COBIT wurde anfangs hauptsächlich von der internen und externen Revision verwendet, da COBIT für das gesamte Spektrum der IT-Aktivitäten eines Unternehmens homogene Anforderungen (Control Objectives) als »Good Practices« beschrieb. Diese guten Praktiken konnten als Sollvorgaben zur Beurteilung der Ist-Situation verwendet werden. Weiterhin wurden detaillierte Prüfungshandlungen zu den COBIT-Prozessen in separaten »Audit Guidelines« beschrieben.

Um das Potenzial von COBIT in Richtung eines Rahmenwerks für das IT-Management und das Business Management besser zu unterstützen, hat die ISACA im Jahr 1998 die Forschungseinrichtung »IT Governance Institute« (ITGI) gegründet und die Entwicklung von COBIT dort angesiedelt.

Mit der dritten Auflage im Juli 2000 wurde COBIT vor allem um Aspekte des IT-Managements durch die sogenannten »Management Guidelines« erweitert. Diese umfassten ein Reifegradmodell (Maturity Model), kritische Erfolgsfaktoren (Critical Success Factors) sowie wesentliche Zielindikatoren (Key Goal Indicators) und Leistungsindikatoren (Key Performance Indicators). Damit wurden in COBIT Hinweise und Kriterien integriert, um dem Management zu ermöglichen, den Status und die Effektivität der eigenen IT-Prozesse im Vergleich mit den 34 COBIT-Prozessen und den 318 detaillierten Anforderungen (Control Objectives) beurteilen zu können. Das Management konnte auf dieser Basis einen Sollzustand definieren, die notwendigen Schritte zur Erreichung des gewünschten Sollzustandes festlegen und die Zielerreichung überwachen [ITGI 2000].

Nach Erscheinen der dritten Auflage haben die Unternehmen COBIT zunehmend sowohl als Leitfaden bei der Implementierung des internen Kontrollsystems in der Unternehmens-IT als auch für die Durchführung von Prozesszustandsbeurteilungen in Form von »Self Assessments« oder »Health Checks« angewandt.

Im Jahr 2004 starteten die Entwicklungsarbeiten an der nächsten Version von COBIT mit der Integration von diversen Forschungsprojekten, u.a. von der Antwerp

Management School und der University of Hawaii. Im Dezember 2005 kam die Version 4.0 heraus, die vor allem eine deutliche Verschlankung und Reduzierung der Control Objectives auf 215 bedeutete und auch explizit Aspekte der IT-Governance integrierte [ITGI 2005g]. In der Folge wurde COBIT 4.0 nochmals in einigen Details überarbeitet und zusammen mit ergänzenden Büchern – wie den »COBIT Control Practices« [ITGI 2007b], dem »IT Governance Implementation Guide: Using COBIT and Val IT« [ITGI 2007c] sowie dem »IT Assurance Guide: Using COBIT« [ITGI 2007d] – im Mai 2007 in der Version COBIT 4.1 veröffentlicht [ITGI 2007a].

Parallel mit der Ausarbeitung von COBIT 4.x begann die Entwicklung am Rahmenwerk Val IT, das im Jahr 2006 erstmals veröffentlicht wurde [ITGI 2006e]. Die zweite, besser mit COBIT integrierte Version Val IT 2.0 erschien im Jahr 2008 [ITGI 2008b]. Im Jahr 2008 startete auch die Entwicklung des ISACA-Rahmenwerks Risk IT. Dieses erschien erstmals im Entwurf im Mai 2009 und in der endgültigen Version im November 2009 [ISACA 2009a].

Im Jahr 2011 begann die ISACA mit der Weiterentwicklung von COBIT und rief eine entsprechende Task Force ins Leben. Ein Ziel dabei war die Integration der vorhandenen Inhalte aus verschiedenen ISACA-Rahmenwerken in ein Modell. Neben den bereits erwähnten Rahmenwerken Val IT und Risk IT wurden auch die Inhalte von ISACA-Veröffentlichungen wie dem IT Assurance Framework (ITAF) [ISACA 2008], dem Board Briefing on IT Governance [ITGI 2003] oder dem Business Model for Information Security (BMIS) [ISACA 2010a] integriert. Im April 2012 wurden die ersten drei Bücher der neu konzipierten COBIT-5-Produktfamilie veröffentlicht:

- das COBIT-5-Rahmenwerk »Business Framework« [ISACA 2012a],
- das Handbuch »COBIT 5: Enabling Processes« [ISACA 2012b] und
- der Umsetzungsleitfaden »COBIT 5 Implementation« [ISACA 2012c].

Das Business Framework diente als konzeptionelles Hauptwerk und umfasste vor allem eine Beschreibung der fünf Prinzipien, eine Einführung in die sieben Enabler sowie eine kurze Vorstellung des neuen Prozessmodells und des neuen Reifegradansatzes [Gaulke 2012]. COBIT 5 richtete sich dabei nicht nur an das IT-Management, sondern stellte über die Ausrichtung an die Geschäftsziele explizit auch ein Rahmenwerk für die Geschäftsbereichsleiter (Business Executives) zur Verfügung.

Das Prozessmodell wurde als separates Handbuch (COBIT 5: Enabling Processes) veröffentlicht und umfasste fünf Governance-Prozesse und 32 Managementprozesse, die jeweils einem von fünf Kernbereichen (domains) zugeordnet waren. Für jeden Prozess waren im COBIT-5-Prozessmodell zwischen drei und 14 normative Aussagen (Prozesspraktiken) formuliert. Die Idee dahinter: Werden die insgesamt 210 im COBIT-5-Prozessmodell enthaltenen Prozesspraktiken konsequent umgesetzt, kann damit eine umfassende Governance und ein gutes Management der IT-Prozesse im Sinne der Anforderungen der Anspruchsgruppen sichergestellt werden.

Der Umsetzungsleitfaden (COBIT 5 Implementation) gab Hilfestellungen für Initiativen zur Verbesserung der IT-Governance und enthielt neben einem siebenstufigen

Lebenszyklus zur Einrichtung einer nachhaltigen IT-Governance auch viele praxisrelevante Elemente aus Risk IT und Val IT.

Weitere COBIT-Handbücher und Umsetzungsleitfäden zur Vervollständigung der Produktfamilie erschienen sukzessive: Im Juli 2012 folgte beispielsweise der Leitfaden »COBIT 5 for Information Security« [ISACA 2012d], im Februar 2013 drei Bücher zum »Process Assessment Model« [ISACA 2013 a-c], im Juni 2013 der Leitfaden »COBIT 5 for Assurance« [ISACA 2013d] sowie im September 2013 »COBIT 5 for Risk« [ISACA 2013f] und im November dann »COBIT 5: Enabling Information« [ISACA 2013g].

Im November 2018 wurde schließlich eine Weiterentwicklung von COBIT 5 unter dem Namen COBIT 2019 veröffentlicht. Als übergeordnetes Rahmenwerk sollte COBIT an die ihrerseits weiterentwickelten Standards und Rahmenwerke angepasst werden, auf die COBIT referenziert. Weiterhin sollten auch technologische Trends wie die digitale Transformation und DevOps in COBIT 2019 berücksichtigt werden. Als erste Bücher erschienen die beiden zentralen Dokumente »COBIT 2019 Rahmenwerk: Einführung und Methoden« (COBIT 2019 Framework: Introduction and Methodology) und »COBIT 2019 Rahmenwerk: Governance- und Managementziele« (COBIT 2019 Framework: Governance and Management Objectives). Das letztgenannte Werk beschreibt das zentrale Modell (Core Model) und ersetzt mit 40 Governance- und Managementzielen das gegenüber COBIT 5 minimal erweiterte Prozessmodell. Zusätzlich sind nun im Kernmodell die mit COBIT 5 eingeführten Enabler als den Zielen zugeordnete Komponenten aufgeführt.

Bereits einen Monat später folgten der Designleitfaden (COBIT 2019 DESIGN GUIDE: Designing an Information and Technology Governance Solution) und der Implementierungsleitfaden (COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution). Der Designleitfaden enthält die Faktoren, die das Governance-System beeinflussen und unterstützt bei der Anwendung dieser Faktoren auf ein Unternehmen. Im Implementierungsleitfaden wurde der bewährte, siebenstufige Lebenszyklus zur Einrichtung einer nachhaltigen IT-Governance auf COBIT 2019 angepasst.

Angekündigt waren zum Zeitpunkt der Erstellung dieses Buches noch sogenannte »Focus Area Guides«. Diese eigenständigen Schwerpunktbereiche (Focus Areas) sollen das Rahmenwerk COBIT 2019 ergänzen und auf diese Weise an neue Entwicklungen und Themen anpassen. Beispielsweise kann dadurch das Kernmodell spezifisch für DevOps oder kleine und mittelständische Unternehmen angepasst werden oder für das Thema Informationssicherheit oder Risikomanagement erweitert werden.

2.3 COBIT-Produktfamilie

Die COBIT-2019-Produktfamilie basiert auf der COBIT-5-Produktfamilie, die konzeptionell überarbeitet wurde. In der COBIT-5-Produktfamilie war das Hauptwerk ein mit knapp 100 Seiten relativ kurzes Rahmenwerkdokument. Dieses Rahmenwerk wurde ergänzt durch Handbücher für die einzelnen Enabler (wie Prozesse oder Information) und Umsetzungsleitfäden für einzelne Anwendungsfelder (wie Sicherheit, Assurance oder Risiko).

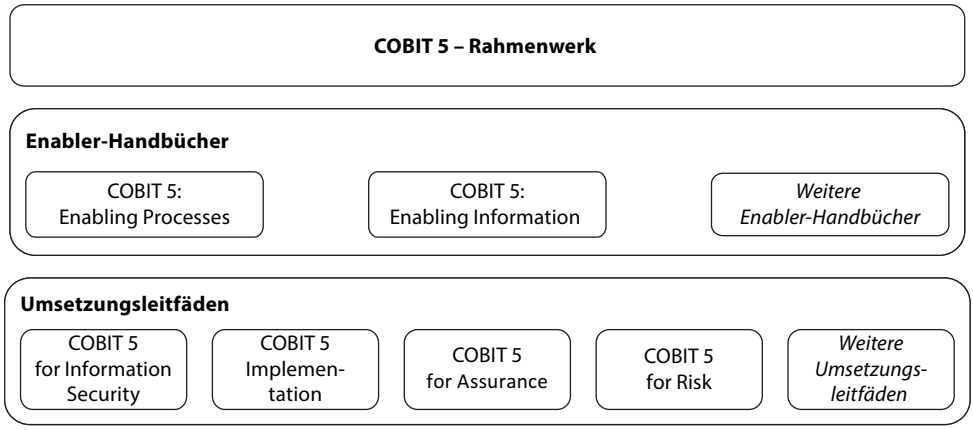

Abb. 2–1 *COBIT-5-Produktfamilie in Anlehnung an [ISACA 2012a]*

Abbildung 2–1 und Tabelle 2–3 geben einen Überblick über die COBIT-5-Produktfamilie.

COBIT-5-Bücher	Inhalte	Erscheinungsdatum
COBIT 5 Business Framework [ISACA 2012a]	Beschreibung des übergreifenden Rahmenwerks, insbesondere der fünf Kernprinzipien und der sieben Enabler	April 2012
COBIT 5: Enabling Processes [ISACA 2012b]	Beschreibung des Prozessmodells mit den 37 COBIT-Prozessen und seinen beschreibenden Elementen	April 2012
COBIT 5 Implementation [ISACA 2012c]	Beschreibung des siebenstufigen Lebenszyklus zur Einrichtung einer nachhaltigen IT-Governance	April 2012
COBIT 5 for Information Security [ISACA 2012d]	Leitfaden zur Anwendung von COBIT 5 für die Informationssicherheit	Juli 2012
COBIT Process Assessment Model (PAM): Using COBIT 5 [ISACA 2013a]	Beschreibung der Kriterien zur Beurteilung von Unternehmensprozessen nach COBIT 5	Februar 2013

→

COBIT-5-Bücher	Inhalte	Erscheinungsdatum
COBIT Self-Assessment Guide: Using COBIT 5 [ISACA 2013b]	Beschreibung einer vereinfachten Beurteilung von Unternehmensprozessen nach COBIT 5	Februar 2013
COBIT Assessor Guide: Using COBIT 5 [ISACA 2013c]	Beschreibung der Vorgehensweise zur Beurteilung von Unternehmensprozessen nach COBIT 5	Februar 2013
COBIT 5 for Assurance [ISACA 2013d]	Leitfaden zur Anwendung von COBIT 5 für Zwecke der Bestätigung (Assurance)	Juni 2013
COBIT 5 for Risk [ISACA 2013f]	Leitfaden zur Anwendung von COBIT 5 für das Management der Informationsrisiken	September 2013
COBIT 5: Enabling Information [ISACA 2013g]	Beschreibung des Enablers Information und eines Informationsmodells	November 2013

Tab. 2–3 *Übersicht der COBIT-5-Bücher*

Die COBIT-2019-Produktfamilie umfasst vier Kernbücher (vgl. Tab. 2–4). Dabei werden insbesondere alle Enabler in dem zweiten Rahmenwerk-Band ausführlich dargestellt. Des Weiteren wird mit dem Designleitfaden ein neues Buch zur Unterstützung der Anwendung von COBIT für die IT-Governance eingeführt.

COBIT-2019-Kernbücher	Inhalte	Erscheinungsdatum
COBIT 2019 Framework: Introduction and Methodology [ISACA 2018a]	Einführung in die wesentlichen Konzepte und Methoden von COBIT 2019	November 2018
COBIT 2019 Framework: Governance and Management Objectives [ISACA 2018b]	Beschreibung des Kernmodells, in dem die Prozessziele nunmehr im Vordergrund stehen, um diese mit den Unternehmenszielen besser abstimmen zu können.	November 2018
COBIT 2019 DESIGN GUIDE: Designing an Information and Technology Governance Solution [ISACA 2018c]	Beschreibung der Designfaktoren, um für die Unternehmen die passende Governance zu finden.	Dezember 2018
COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution [ISACA 2018d]	Beschreibung eines Implemetierungsansatzes für die kontinuierliche Verbesserung der Governance	Dezember 2018

Tab. 2–4 *Übersicht der COBIT-2019-Kernbücher*

Mit Veröffentlichung dieser vier Hauptwerke wurden für vier Schwerpunktbereiche (DevOps, SME, Risk und Security) bereits spezifische Ergänzungen zum Kernmodell von COBIT 2019 angekündigt. Diese sogenannten »Focus Area Guides« behandeln damit auch zwei Themen, die in der COBIT-5-Produktfamilie als Umsetzungsleitfäden veröffentlicht worden sind. Abbildung 2–2 stellt die COBIT-2019-Produktfamilie schematisch dar.

Abb. 2–2 *COBIT-2019-Produktfamilie*

Alle Dokumente der aktuellen COBIT-Produktfamilie stehen auf der Internetseite *www.isaca.org* zum Download als personalisierte PDF-Dateien zur Verfügung. Weiterhin bietet ISACA die Dokumente größtenteils auch als gedruckte Versionen zum Kauf an.

Neben diesen Büchern sind auf der Internetseite der ISACA noch eine Vielzahl von weiteren Publikationen der ISACA und des IT Governance Institute veröffentlicht, die spezielle Themen im Umfeld von IT-Governance und IT-Management aufgreifen. Diese referenzieren häufig auch COBIT und dessen Kernelemente, gehören im Sinne dieses Buches jedoch nicht zur engeren oder erweiterten COBIT-Produktfamilie und sind nicht Gegenstand dieses Buches.

3 Die sechs Prinzipien eines Governance-Systems

COBIT 2019 formuliert sechs Prinzipien, die der Ausgestaltung des Governance-Systems zur Steuerung der Unternehmens-IT zugrunde liegen sollten (vgl. Abb. 3–1). In diesem Kapitel werden die sechs Kernprinzipien von COBIT 2019 dargestellt. Sie lauten:

- Mehrwert für die Anspruchsgruppen bereitstellen (Provide Stakeholder Value)
- Ganzheitlicher Ansatz (Holistic Approach)
- Dynamisches Governance-System (Dynamic Governance System)
- Governance getrennt vom Management (Governance Distinct From Management)
- Zugeschnitten auf die Bedürfnisse des Unternehmens (Tailored to Enterprise Needs)
- End-to-End-Governance-System (End-to-End Governance System)

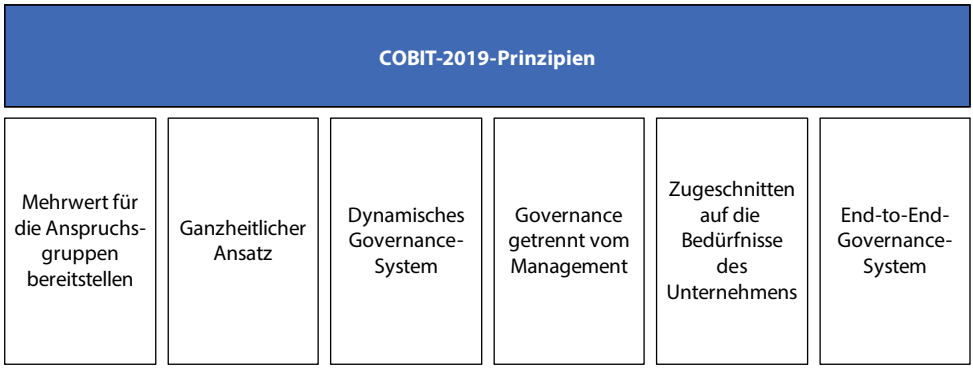

Abb. 3–1 *Prinzipien für Governance-Systeme [ISACA 2018a]*

Diese Prinzipien beschreiben die Kernanforderungen an ein Governance-System für die Unternehmens-IT und sind für das Verständnis von COBIT von herausragender Bedeutung.

3.1 Prinzip 1: Mehrwert für die Anspruchsgruppen bereitstellen

Dieses Prinzip zielt darauf ab, dass Informationsverarbeitung kein Selbstzweck ist, sondern sich am Geschäft (business) bzw. an den Anspruchsgruppen (stakeholder) orientieren muss. Diese machen die Vorgaben für die geschäftlich benötigte Informationsverarbeitung und stellen letztlich auch die (finanziellen) Mittel für die notwendige Technologie bereit. Unternehmen haben zum Ziel, für ihre Anspruchsgruppen maximalen Nutzen unter Beachtung der gegebenen Rahmenbedingungen zu erzeugen. Entsprechend muss das Ziel der IT-Governance sein, maximalen Nutzen aus der Anwendung von Informationstechnologie zu optimalen Ressourcenkosten und IT-Risiken zu realisieren.

Jedes Unternehmen benötigt eine Strategie und ein Governance-System, um die Bedürfnisse der internen und externen Anspruchsgruppen zu berücksichtigen. COBIT unterstützt die unterschiedlichen internen und externen Anspruchsgruppen, ihre Anforderungen an die Informationsverarbeitung umzusetzen, um aus der Nutzung der Unternehmens-IT den gewünschten Mehrwert zu generieren. Zudem stellt COBIT eine Beziehung zwischen den Anforderungen der Anspruchsgruppen und den Unternehmenszielen (Enterprise Goals) und den darauf ausgerichteten IT-bezogenen Zielen (Alignment Goals) her. Dadurch können die Ziele für die Governance und das Management der Unternehmens-IT (Governance and Management Objectives) besser priorisiert werden.

Als Instrument dafür stellt COBIT eine generische Zielkaskade (Goals Cascade) bereit, die an den jeweiligen Unternehmenskontext angepasst werden kann. Dabei können allgemeine Unternehmensziele über eine Zuordnungstabelle IT-bezogenen Zielen primär und sekundär zugeordnet werden und diese IT-bezogenen Ziele lassen sich dann über eine weitere Zuordnungstabelle den 40 Governance- und Managementzielen zuordnen. Diese Zuordnungstabellen basieren auf Forschungen der Management School der Universität Antwerpen und wurden im Rahmen der Entwicklung von COBIT 5 und COBIT 2019 nochmals von Experten des Berufsverbandes ISACA validiert. Abbildung 3–2 verdeutlicht die Idee der Zielkaskade.

Die COBIT-Zielkaskade ist der zentrale Mechanismus, mit dem Anforderungen von Anspruchsgruppen in konkrete, durchführbare und angepasste Unternehmensziele, daran ausgerichtete IT-bezogene Ziele und konkrete Governance- und Managementziele umgewandelt werden können. In Abschnitt 17.1 wird detailliert auf das Instrument der COBIT-Zielkaskade eingegangen.

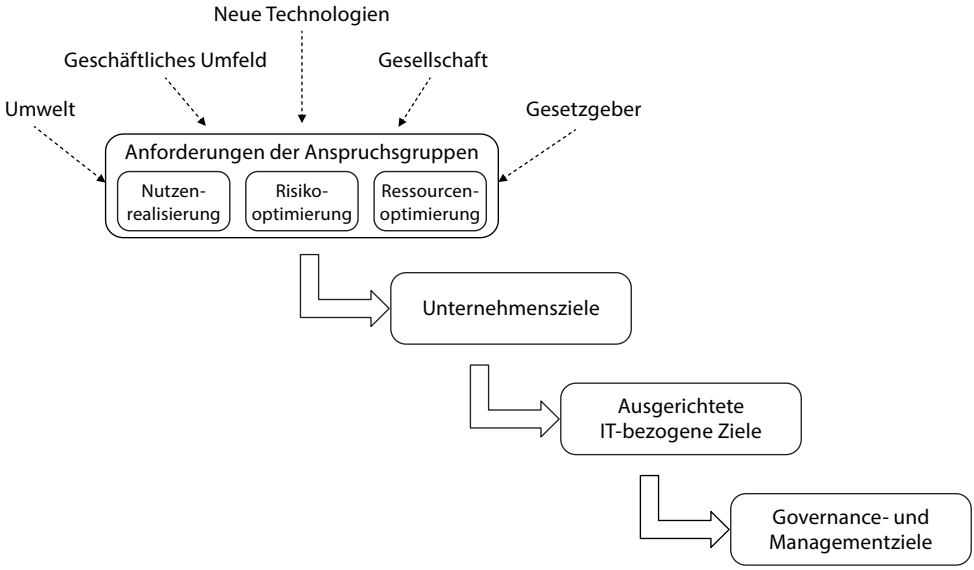

Abb. 3–2 *Mehrwert für die Anspruchsgruppen bereitstellen (in Anlehnung an [ISACA 2018a])*

3.2 Prinzip 2: Ganzheitlicher Ansatz

Ein Governance-System besteht aus einer Reihe von Komponenten, die unterschiedlichen Typs sein können, aber ganzheitlich zusammenwirken. Komponenten sind kritische Erfolgsfaktoren, die sowohl individuell als auch kollektiv Einfluss darauf haben, ob die ausgewählten Governance- und Managementziele erreicht werden. COBIT betrachtet in seinem Rahmenwerk vor allem sieben Komponenten (components):

- **Prinzipien, Richtlinien und Rahmenwerke (Principles, Policies and Frameworks)**
  Prinzipien, Richtlinien und Rahmenwerke sind das Vehikel zur Umsetzung des von der Unternehmensleitung erwünschten Verhaltens in die tägliche Praxis. Die Komponente »Prinzipien, Richtlinien und Rahmenwerke« umfasst die installierten Kommunikationsmittel, um die Vorgaben und Anweisungen der Governance-Organe und des Topmanagements zu vermitteln. Für die Komponente »Prinzipien, Richtlinien und Rahmenwerke« werden im COBIT-Rahmenwerk meist typische Richtlinien beschrieben, beispielsweise eine Beschaffungsrichtlinie (IT Procurement Policy) beim Lieferantenmanagement. Methodisch sollten sich diese Richtlinien an guten Praktiken wie Effektivität, Effizienz, Aktualität oder Eingängigkeit orientieren. Eine detaillierte Darstellung dieser Komponente erfolgt in Kapitel 6 dieses Buches.
- **Prozesse (Processes)**
  Prozesse beschreiben einen strukturierten Satz mit Praktiken und Aktivitäten zur Erreichung bestimmter Ziele und liefern einen Satz mit Ergebnissen, die zur Erreichung der allgemeinen IT-bezogenen Ziele beitragen. Die Komponente »Pro-

zesse« umfasst vor allem Prozesspraktiken mit dazugehörigen beispielhaften Metriken und dafür notwendige Aktivitäten. Die Prozesskomponente wird von anderen Komponenten mit Elementen wie Verantwortlichkeitsmatrizen und Informationselementen ergänzt. Eine detaillierte Darstellung dieser Komponente erfolgt in Kapitel 11 dieses Buches.

- **Organisationsstrukturen (Organisational Structures)**
  Organisationsstrukturen sind die wichtigsten Entitäten der Entscheidungsfindung im Unternehmen. Für die Komponente »Organisationsstrukturen« werden im COBIT-Rahmenwerk sowohl ein Rollenmodell beschrieben als auch gute Praktiken für Organisationsstrukturen wie Arbeitsprinzipien, ausgewogene Zusammensetzung der Mitglieder oder Umfang der Befugnisse. Eine detaillierte Darstellung dieser Komponente erfolgt in Kapitel 7 dieses Buches.
- **Kultur, Ethik und Verhalten (Culture, Ethics and Behaviour)**
  Kultur, Ethik und Verhalten der Mitarbeiter und des Unternehmens werden als Erfolgsfaktoren für Governance- und Managementaktivitäten häufig unterschätzt. Die Komponente »Kultur, Ethik und Verhalten« bezieht sich auf individuelles und kollektives Verhalten innerhalb eines Unternehmens. Das COBIT-Rahmenwerk führt für die Governance- und Managementziele jeweils wichtige kulturelle Elemente auf. Eine detaillierte Darstellung dieser Komponente erfolgt in Kapitel 8 dieses Buches.
- **Information (Information)**
  Informationen sind in jeder Organisation allgegenwärtig. Zu ihnen gehören sämtliche vom Unternehmen produzierten und verwendeten Informationen. Informationen sind für die Aufrechterhaltung des Betriebs der Organisation und dessen Steuerung unverzichtbar. Auf operativer Ebene sind Informationen häufig sogar das wichtigste Produkt des Unternehmens überhaupt. Für die Komponente »Information« werden im COBIT-Rahmenwerk sowohl die durch die Prozesspraktiken benötigten als auch die von den Prozesspraktiken erzeugten Informationselemente dargestellt. Die Ziele der Komponente »Information« können generisch durch die drei Dimensionen intrinsische Qualität, kontextabhängige Qualität sowie Sicherheit bzw. Zugangsmöglichkeiten beschrieben werden. Eine detaillierte Darstellung dieser Komponente erfolgt in Kapitel 12 dieses Buches.
- **Services, Infrastruktur und Anwendungen (Services, Infrastructure and Applications)**
  Services, Infrastruktur und Anwendungen umfassen die Infrastruktur, die Technologie und die Anwendungen, die innerhalb des Unternehmens die IT-Verarbeitung und IT-Services sicherstellen. Die Komponente »Services, Infrastruktur und Anwendungen« bezieht sich auf die Ressourcen, die bei der Bereitstellung von IT-Dienstleistungen genutzt werden. Im COBIT-Rahmenwerk werden für jedes Governance- und Managementziel typische unterstützende Services, Tools, Systeme, Plattformen und Anwendungen aufgeführt. Eine detaillierte Darstellung dieser Komponente erfolgt in Kapitel 9 dieses Buches.

- **Mitarbeiter, Fähigkeiten und Kompetenzen (People, Skills and Competencies)** Mitarbeiter, Fähigkeiten und Kompetenzen beziehen sich auf das Personal, das für die Durchführung aller Aktivitäten, das Treffen der richtigen Entscheidungen und die Umsetzung korrektiver Maßnahmen verantwortlich ist. Das COBIT-Rahmenwerk beschreibt wichtige Fähigkeiten der für jedes Governance- und Managementziel benötigten Mitarbeiter und entsprechende Referenzen zu gängigen Kompetenzrahmenwerken Eine detaillierte Darstellung dieser Komponente erfolgt in Kapitel 10 dieses Buches.

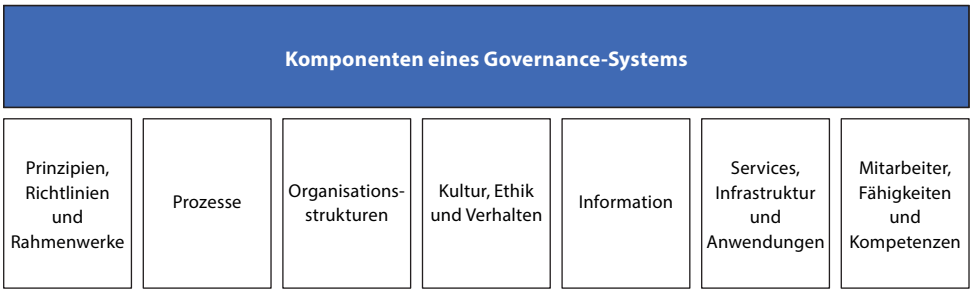

Abb. 3–3 *Ganzheitlicher Ansatz (in Anlehnung an [ISACA 2018a])*

Abbildung 3–3 zeigt das Governance-System bestehend aus den sieben Komponenten, die kritische Erfolgsfaktoren für die Erreichung der Governance- und Managementziele sind. Die Komponenten interagieren aber auch untereinander. Beispielsweise sind Prinzipien, Richtlinien und Rahmenwerke als Vehikel zur Kommunikation der Vorgaben und Anweisungen der Governance-Organe und des Managements bestimmender Ausgangspunkt für alle anderen Komponenten.

3.3 Prinzip 3: Dynamisches Governance-System

Ein Governance-System sollte dynamisch sein, sodass die Auswirkungen von Änderungen zum Beispiel an der Strategie, an der Bedrohungslage oder an der Technologie im Governance-System berücksichtigt werden. Die Designfaktoren repräsentieren typische Veränderungen, die ggf. im Governance-System zu beachten sind. Anhand von Designfaktoren sollte das Governance-System regelmäßig überprüft werden und Änderungen am System vorgenommen werden, wann immer dies erforderlich ist.

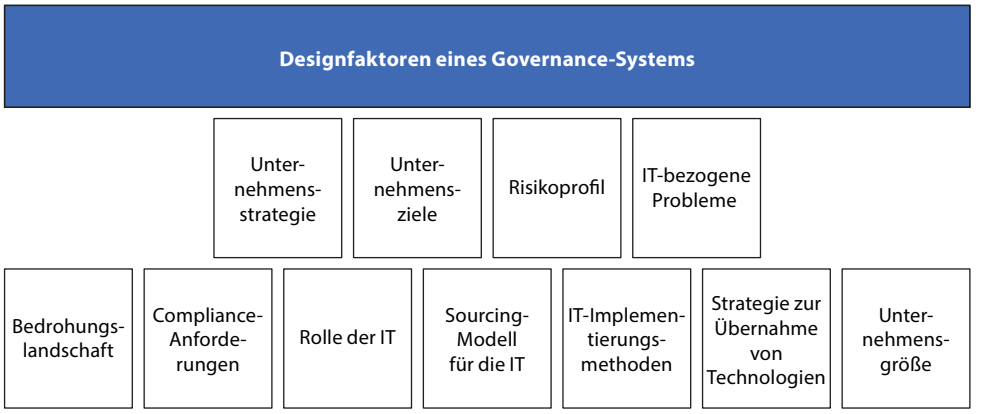

Abb. 3–4 *Dynamisches Governance-System (in Anlehnung an [ISACA 2018a])*

Die in Abbildung 3–4 dargestellten Designfaktoren sind im Designleitfaden beschrieben und in Bezug zu den Governance- und Managementzielen gesetzt worden. Eine detaillierte Darstellung dieser Komponente erfolgt in Abschnitt 17.2 dieses Buches.

3.4 Prinzip 4: Governance getrennt vom Management

COBIT unterscheidet deutlich zwischen Governance und Management der Unternehmens-IT. Diese beiden Disziplinen sind mit unterschiedlichen Arten von Aktivitäten verbunden, erfordern unterschiedliche Organisationsstrukturen und dienen unterschiedlichen Zwecken (vgl. Abb. 3–5). Um eine klare Zuordnung und Trennung von Verantwortlichkeiten zu erreichen, sind Governance und Management der Unternehmens-IT auch im Kernmodell von COBIT durch eigene Domänen getrennt.

Governance stellt sicher, dass die Anforderungen der Anspruchsgruppen, Rahmenbedingungen und Möglichkeiten evaluiert werden, um ausgewogene und vereinbarte Unternehmensziele zu bestimmen. Governance gibt die Richtung durch die Festlegung von Prioritäten und das Fällen von Entscheidungen vor und überwacht die Leistung und die Erreichung der vereinbarten Richtung und Zielvorgaben. Die Governance liegt in den meisten Unternehmen in der Zuständigkeit der Geschäftsleitung und des Aufsichtsorgans (Board of Directors).

Das Management plant, erstellt, betreibt und überwacht Aktivitäten – im Rahmen der von der Governance vorgegebenen Richtung –, um die Unternehmensziele zu erreichen. Das Management der Unternehmens-IT liegt meist in der Zuständigkeit der Ebene unterhalb der Geschäftsleitung (CEO).

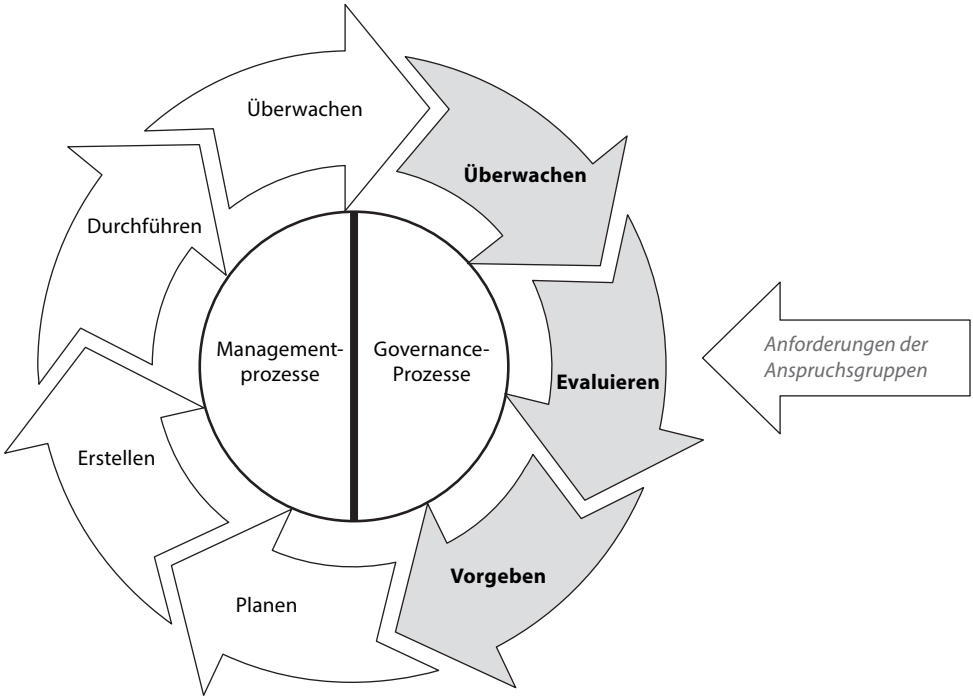

Abb. 3–5 *Unterscheiden zwischen Governance und Management*

Die Governance-Prozesse umfassen das Evaluieren der Anforderungen der unterschiedlichen Anspruchsgruppen, das Vorgeben der Richtung sowie das Überwachen der Zielerreichung. Die Prozesspraktiken zur Erreichung der Governance-Ziele in der Governance-Domäne von COBIT bilden jeweils genau diese drei Aufgaben der Governance ab. Das Management plant, erstellt, betreibt und überwacht Aktivitäten – im Rahmen der von der Governance vorgegebenen Richtung. Die vier Management-Domänen von COBIT bilden genau diese vier Aufgabengebiete ab.

3.5 Prinzip 5: Zugeschnitten auf die Bedürfnisse des Unternehmens

Ein Governance-System sollte auf die Bedürfnisse des Unternehmens zugeschnitten sein. COBIT 2019 benennt drei unterschiedliche Faktoren, die das Design der Governance beeinflussen (vgl. Abb. 3–6):

- **Auswahl und Priorisierung von Governance- und Managementzielen**
  Die 40 Governance- und Managementziele im COBIT-Kernmodell sind gleichwertig zueinander, d.h., es gibt erst einmal keine natürliche Rangfolge unter ihnen. Die besondere Unternehmenssituation, die sich in COBIT 2019 über die Designfaktoren abbilden lässt, kann diese Äquivalenz jedoch beeinflussen und bestimmte Governance- und Managementziele wichtiger erscheinen lassen als andere.

Ein bereits aus COBIT 5 bekannter Designfaktor zur Priorisierung von Governance- und Managementzielen ist die Zielkaskade. Über die Auswahl der relevanten Unternehmensziele aus der Unternehmenszielliste der Zielkaskade lassen sich die potenziell vorrangigen Governance- und Managementziele ableiten.

Beispiel: Für ein Unternehmen ist es wichtig, im Markt mit einem attraktiven Produktportfolio aufzutreten. Daher würde bei Anwendung der COBIT-Zielkaskade das Unternehmensziel »Portfolio wettbewerbsfähiger Produkte und Dienstleistungen« als sehr relevant eingestuft werden. Daraus folgt durch Anwendung der Zielkaskade, dass mit hoher Wahrscheinlichkeit das Governance- und Managementziel »Managed Portfolio« ein wichtiger Bestandteil des Governance-Systems dieses Unternehmens sein sollte.

In der Praxis bedeutet eine höhere Bedeutung, dass für diese Governance- und Managementziele höhere Zielfähigkeitsgrade angestrebt werden als für weniger wichtige Governance- und Managementziele.

- **Auswahl/Priorisierung von Komponenten**
  Komponenten sind erforderlich, um Governance- und Managementziele zu erreichen. Einige Designfaktoren können die Wichtigkeit einer oder mehrerer Komponenten beeinflussen oder spezifische Variationen erfordern.

  Beispiel: Kleine und mittlere Unternehmen benötigen möglicherweise nicht alle Rollen und Organisationsstrukturen, wie sie im COBIT-Kernmodell zur Komponente »Organisationsstrukturen« festgelegt sind. Diese Unternehmen können ein reduziertes Rollenmodell verwenden.

  Beispiel: Eine Bank ist in einem stark regulierten Umfeld tätig. Daher ist für dieses Unternehmen die Komponente »Prinzipien, Richtlinien und Rahmenwerke« besonders wichtig, da für Banken an dokumentierten Arbeitsergebnissen, Richtlinien und Verfahren besondere Anforderungen bestehen.

- **Anpassung des COBIT-Kernmodells**
  Einige Designfaktoren, wie die Bedrohungslandschaft oder die angestrebten IT-Implementierungsmethoden, erfordern kontextspezifische Anpassungen des COBIT-Kernmodells.

  Beispiel: Ein Unternehmen, das DevOps für die Entwicklung und den Betrieb von Lösungen einsetzt, benötigt beispielsweise für die Managementziele »Lösungsidentifizierung und -erstellung sind gemanagt« (BAI03) oder »Betrieb ist gemanagt« (DSS01) angepasste Komponenten, insbesondere für »Prozesse«, »Organisationsstrukturen« oder »Kultur, Ethik und Verhalten«. Solche Anpassungen sollen in von ISACA angekündigten Schwerpunktleitfaden näher beschrieben werden.

Abb. 3–6 *Parameter für den Zuschnitt auf die Bedürfnisse des Unternehmens*

Designfaktoren und Schwerpunkte (Fokus Area) dienen in COBIT 2019 als Parameter, um das Governance-System bzw. dessen Komponenten anzupassen. Daneben enthält COBIT 2019 auch eine Ablauffolge (Workflow), wie ein maßgeschneidertes Governance-System entworfen werden kann. In diesem »Governance System Design Workflow« werden die Designfaktoren in einer bestimmten Abfolge zur Festlegung des initialen Governance-Systems und zur weiteren Verfeinerung angeordnet. Eine detaillierte Darstellung der Designfaktoren und deren Anwendung erfolgt in Abschnitt 17.2 dieses Buches.

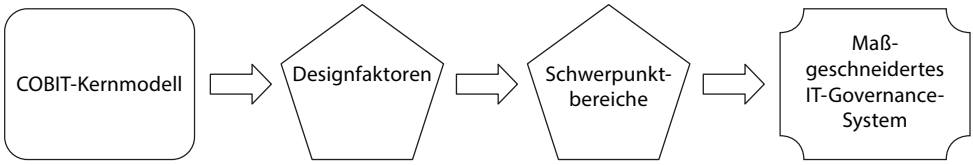

Abb. 3–7 *Maßgeschneidertes IT-Governance-System*

3.6 Prinzip 6: End-to-End-Governance-System

COBIT integriert die Governance der Unternehmens-IT in die unternehmensweite Governance und deckt alle Funktionen und Prozesse ab, die für das Steuern und Managen von Unternehmensinformationen und der zugehörigen Technologien erforderlich sind. Diese ganzheitliche und systemische Sicht auf die Governance der Unternehmens-IT basiert auf einem Governance-System, das aus drei Elementen besteht (vgl. Abb. 3–8):

- Governance-Komponenten
- Governance-Umfang
- Rollen, Aktivitäten und Beziehungen

Governance-Komponenten sind die für das Governance-System relevanten Ressourcen der Organisation (z. B. Rahmenwerke, Prinzipien, Strukturen, Prozesse und Praktiken). COBIT stellt bei der Governance und dem Management der Unternehmens-IT

auf eine Reihe von unternehmensweiten und durchgängigen Komponenten ab. Anspruchsgruppen müssen zur Unterstützung der Umsetzung ihrer Ziele Anforderungen an diese Komponenten definieren. Fehlende oder mangelhafte Komponenten beeinträchtigen die Fähigkeit des Unternehmens, die Governance- und Managementziele zu erreichen und damit die erwartete Wertschöpfung zu generieren.

Governance kann sich auf das gesamte Unternehmen, eine Entität oder auf einzelne Betriebsmittel beziehen. Der Umfang des Governance-Systems ist daher zu definieren. COBIT nimmt als Umfang das Unternehmen an sich an, aber theoretisch ist auch ein anderer Umfang möglich.

Das dritte Governance-Element besteht aus Rollen, Aktivitäten und Beziehungen und wie die Beteiligten innerhalb eines Governance-Systems miteinander interagieren. COBIT enthält daher ein erweitertes Rollenmodell, das sowohl die Verantwortlichkeiten von IT-Funktionen als auch von IT-relevanten Businessfunktionen abdeckt.

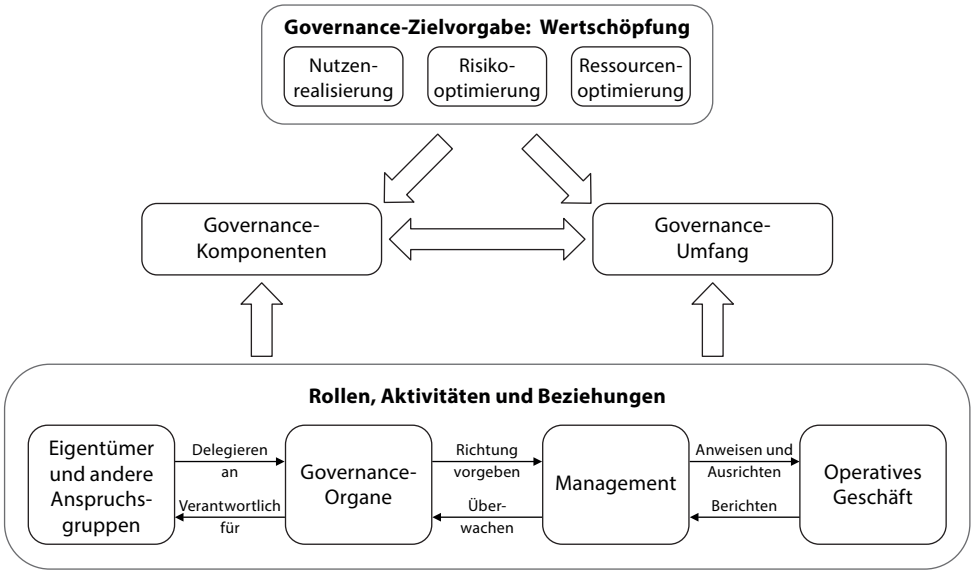

Abb. 3–8 *Abdecken des gesamten Unternehmens (in Anlehnung an [ISACA 2012a])*

COBIT betrachtet die Governance und das Management von Information und Technologie aus einer unternehmensweiten, durchgängigen Perspektive und unterstützt dabei, die Governance und das Management der Unternehmens-IT in das Governance-System des Unternehmens zu integrieren.

4 Prinzipien für Governance-Rahmenwerke

Neben den sechs Prinzipien eines Governance-Systems führt COBIT 2019 zusätzlich drei allgemeine Prinzipien für Governance-Rahmenwerke an (vgl. Abb. 4–1). Sie lauten:

- Basierend auf einem konzeptionellen Modell (Based on Conceptual Model)
- Offen und flexibel (Open and Flexible)
- An wichtigen Standards ausgerichtet (Aligned to Major Standards)

Diese Prinzipien sind Anforderungen an jedes Governance-Rahmenwerk, das in Organisationen angewendet wird.

4.1 Prinzip 1: Basierend auf einem konzeptionellen Modell

Dieses Prinzip stellt darauf ab, dass jedes Governance-Rahmenwerk auf einem konzeptionellen Modell basieren sollte, das die wesentlichen Komponenten und die Beziehungen zwischen diesen Komponenten beschreibt.

In COBIT 2019 wird diese Anforderung durch die Komponenten im Kernmodell erfüllt.

4.2 Prinzip 2: Offen und flexibel

Dieses Prinzip stellt darauf ab, dass jedes Governance-Rahmenwerk offen und flexibel sein sollte, um das Hinzufügen neuer Inhalte zu ermöglichen und neue Herausforderungen auf möglichst flexible Weise anzugehen.

In COBIT 2019 wird diese Anforderung durch die Designfaktoren und die Schwerpunktleitfäden erfüllt.

4.3 Prinzip 3: An wichtigen Standards ausgerichtet

Dieses Prinzip stellt darauf ab, dass jedes Governance-Rahmenwerk sich an wichtigen, relevanten Standards, Rahmenwerken und Regulierungen orientieren sollte.

In COBIT 2019 wird diese Anforderung durch die Verwendung von Referenzmaterialien im Kernmodell erfüllt. Das COBIT-Rahmenwerk integriert die Ideen von anderen IT-relevanten Standards (z.B. ISO-Standards) und Rahmenwerken (z.B. ITIL, TOGAF) und schafft damit die Grundlage für die effektive Integration gängiger Rahmenwerke, Standards und guter Praktiken. In Kapitel 15 wird detailliert auf die von COBIT referenzierten Standards, guten Praktiken und Rahmenwerke eingegangen.

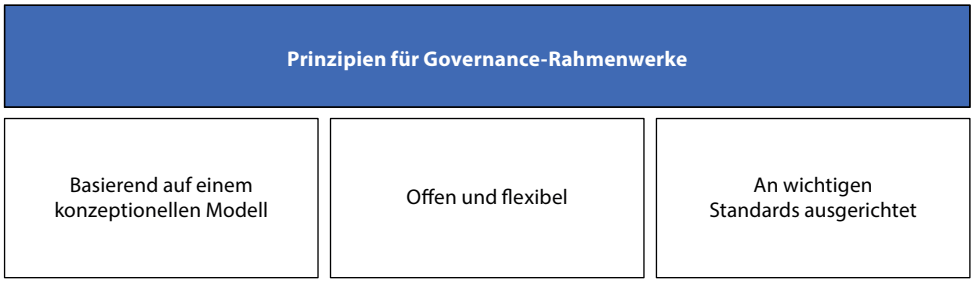

Abb. 4–1 *Prinzipien für Governance-Rahmenwerke (in Anlehnung an [ISACA 2018a])*