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

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.

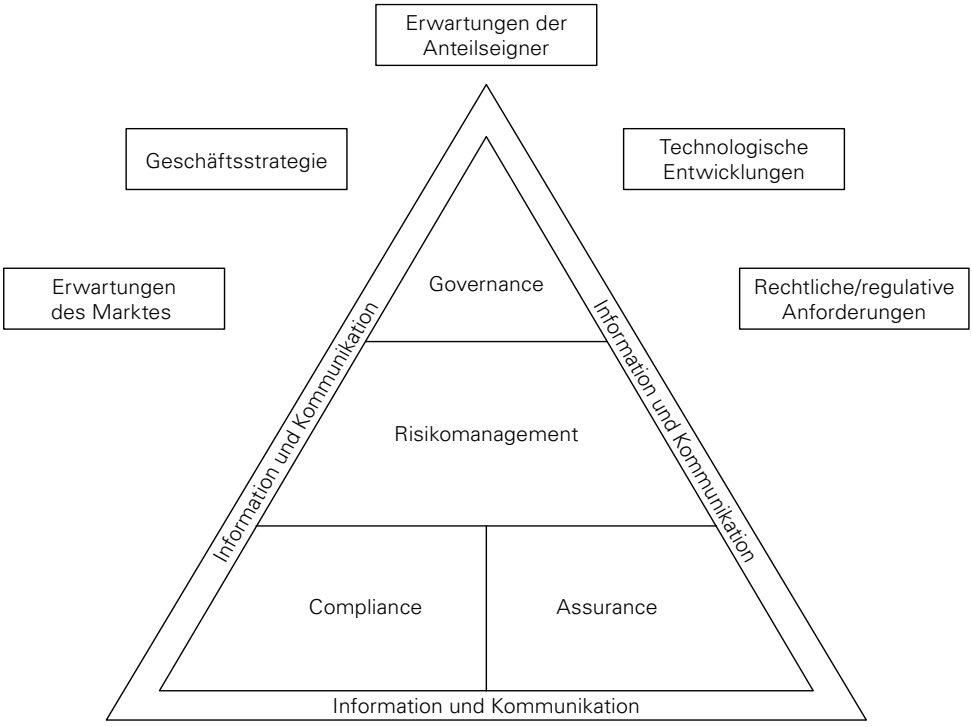

Abb. 1–1 *Treiber von Governance-Initiativen*

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.