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

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

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

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

Markus Gaulke

Praxiswissen COBIT

Grundlagen und praktische Anwendung in der Unternehmens-IT

2., aktualisierte und überarbeitete Auflage

dpunkt.verlag

Markus Gaulke
www.markus-gaulke.de

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

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

ISBN 978-3-86490-055-6

2., aktualisierte und überarbeitete Auflage 2014

Wieblinger Weg 17
69123 Heidelberg

5 4 3 2 1 0

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 (siehe 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.

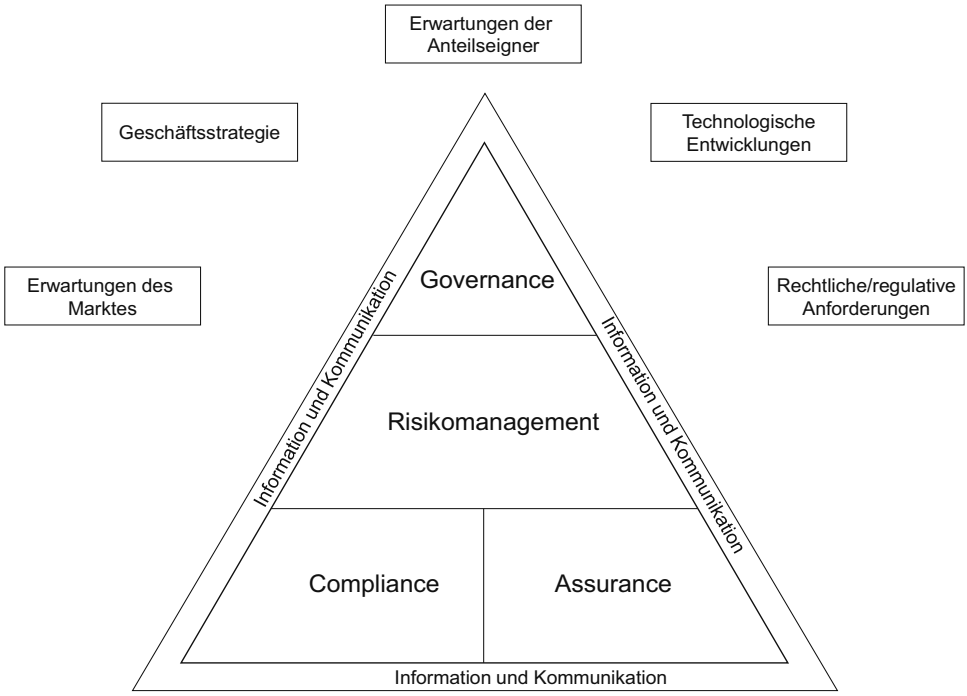

Abb. 1–1 *Treiber von Governance-Initiativen*

Die zunehmende Durchdringung von Unternehmen mit Informationstechnologie (IT) und die dadurch bedingte, steigende Abhängigkeit von der Verfügbarkeit und Verlässlichkeit der IT-Prozesse erfordern, die 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) haben in den letzten Jahren drei wichtige Rahmenwerke entwickelt: COBIT, Val IT und Risk IT. Das Rahmenwerk COBIT mit dem Fokus auf der Steuerung und dem Management von IT-Prozessen stellt dabei das Fundament da, auf dem Val IT mit dem Fokus auf die geschäftlichen Investitionen sowie Risk IT mit dem Fokus auf die IT-bezogenen Geschäftsrisiken aufbauen. 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, aber sie sind unter dem gemeinsamen Dach von COBIT 5 zusammengeführt worden und werden unter diesem Dach weiter entwickelt. COBIT 5 unterstützt die Unternehmensführung nachhaltig bei der Erreichung ihrer Ziele durch die Sicherstellung einer effektiven und innovativen Nutzung der Unternehmens-IT basierend auf einem ausgewogenen Verhältnis zwischen Unternehmensanforderungen und IT-Zielen. Die Anwendung von COBIT 5 trägt aber nicht nur zu einer höheren Zufriedenheit der Geschäftsanwender mit der IT bei, sondern auch zur Einhaltung der einschlägigen Gesetze, Bestimmungen, vertraglichen Vereinbarungen und internen Richtlinien. Mit COBIT 5 als Instrumentarium kann das Unternehmensmanagement die IT richtig im Sinne der Unternehmensziele aufstellen.

Das vorliegende Buch erklärt COBIT 5 und seine Elemente sowie die Anwendung von COBIT 5. Teil I führt in das Rahmenwerk und das Prozessmodell von COBIT 5 ein und weckt das Verständnis für die COBIT 5 zugrunde liegenden Konzepte.

In Teil II und III wird die Anwendung von COBIT 5 für die Umsetzung der unter dem Schlagwort GRC (Governance, Risikomanagement, Compliance) zusammengefassten aktuellen Herausforderungen für die Unternehmen erläutert und mithilfe von Beispielen illustriert. Mit IT-Outsourcing und dem weitgefassten Begriff der IT-Assurance werden weitere typische Anwendungsbereiche von COBIT 5 aufgezeigt und diskutiert. Zusätzlich berichten Praktiker aus unterschiedlichen Unternehmen über die Anwendung von COBIT in ihren Organisationen.

In Teil IV und V werden die von der berufsständischen Organisation ISACA angebotenen Zertifizierungen und Zertifikate dargestellt. Testfragen ermöglichen, das eigene COBIT-Wissen zu überprüfen und zu festigen. Als Vorbereitungsbuch für Teilnehmer an den deutschen Zertifikatsprüfungen des ISACA Germany Chapters (IT-Governance & IT-Compliance Practitioner) oder der APMG (COBIT Foundation) ist vor allem der erste Teil des Buches relevant; für Teilnehmer an den weiterführenden Zertifikatsstudiengängen (IT-Governance-Manager, IT-Compliance-Manager) ist der gesamte Inhalt dieses Buches maßgeblich.

Im Anhang werden die COBIT-5-Domänen und Prozesse sowie die COBIT-5-Prozesse und zugehörigen Prozesspraktiken tabellarisch sowohl in Deutsch als auch in Englisch dargestellt. Weiterhin ist dort auch die COBIT-5-Zielkaskade mit Unternehmenszielen und IT-bezogenen Zielen sowie den primär zugeordneten Prozessen tabellarisch abgebildet.