

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.

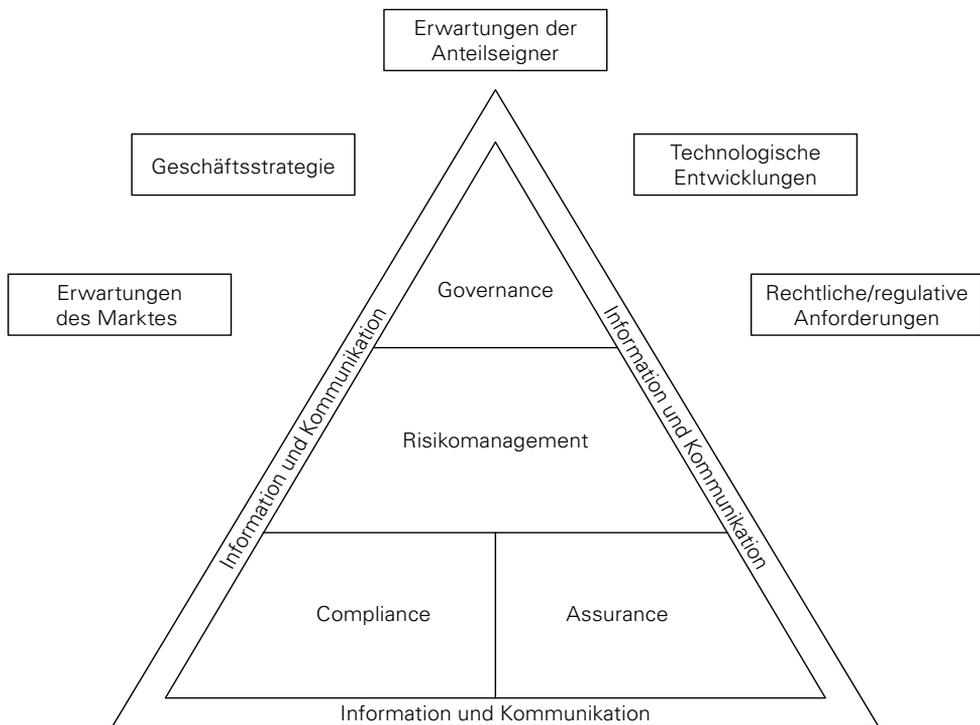


Abb. 1-1 Treiber von Governance-Initiativen

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.