IT-Governance

Ordnungsrahmen und Handlungsfelder für eine erfolgreiche Steuerung der Unternehmens-IT

DIE LESEPROBE

1 Grundlagen der IT-Governance

Ausblick

IT-Governance ist einerseits Teil der Corporate Governance und besteht – andererseits – aus einer Vielzahl an Handlungsfeldern, Zielen und Zwecken sowie inhaltlichen, strukturellen, personellen und instrumentellen Elementen. Diese gilt es zu einem konsistenten und ganzheitlichen Ordnungsrahmen für die IT zusammenzufügen. Aus diesem Grunde beginnen die Ausführungen mit der Darstellung des Governance-Begriffs und des Zusammenhangs zwischen Corporate Governance und IT-Governance. Ein klares Verständnis von IT-Governance wird als Voraussetzung für ihre Gestaltung angesehen. Daher werden verschiedene Ansätze der IT-Governance aus der Literatur ebenso wie das Verständnis von IT-Governance in Normen und Standards dargestellt. Insbesondere wird das Augenmerk auf die Unterscheidung von IT-Governance und IT-Management bzw. auf die Schnittstelle gelegt. Basierend hierauf werden das in diesem Buch zugrunde gelegte Begriffsverständnis und elf Prinzipien für IT-Governance entwickelt. Daraus lassen sich Handlungsfelder der IT-Governance, die in den weiteren Kapiteln diskutiert werden, ableiten. Für die betrachteten Handlungsfelder wird ein kurzer Ausblick gegeben.

1.1 Entwicklung der Corporate Governance

Herkunft des Governance-Begriffs

Das Wort »Governance« geht zurück auf das griechische Wort »*kybernétes*« (Steuermann) bzw. das lateinische Verb »gubernare« (steuern, herrschen) bzw. »gubernantia« (Steuerung, Leitung)« (nach [Klenk 2019], S. 153). In seiner aktuellen Verwendung wurde der Begriff »Governance« in den Sozialwissenschaften, insbesondere von der Politikwissenschaft, eingeführt. Obwohl er recht verbreitet ist und das Governance-Konzept einen häufig verwendeten Theorieansatz darstellt, hat sich bislang kein allgemein anerkanntes Verständnis herausgebildet – Governance ist vielmehr ein »anerkannt uneindeutiger Begriff« ([Bohne 2018], S. 123).

Good Governance

In der Politik bildet »Good Governance« einen »Sammelbegriff für Best Practices im Bereich des Regierungshandelns« [Klein 2018]. Der Begriff zielt u.a. auf einen effizienten öffentlichen Sektor, ein zuverlässiges Rechtssystem, eine der Öffentlichkeit rechenschaftspflichtige und transparente Verwaltung sowie weitere Aspekte wie z.B. die Unterbindung von Korruption ab (vgl. [Klein 2018]). Sie zeichnet sich also – und das gilt nicht nur für Governance in der Politik – durch Kriterien wie Legitimität, Nachvollziehbarkeit, Transparenz, Effizienz und Regelorientierung aus.

Governance-Forschung

Die Governance-Forschung richtet sich auf Handlungen (also Regieren, Steuern, Koordinieren etc.) von staatlichen, gesellschaftlichen und wirtschaftlichen Akteuren, die in Netzwerken interagieren (vgl. [Bohne 2018], S. 23 ff. u. S. 138 ff.). Im Vordergrund stehen nicht mehr singuläre Steuerungsaktivitäten staatlicher Akteure, sondern das abgestimmte Zusammenwirken verschiedener betroffener Akteure über mehrere Ebenen hinweg (z.B. national, international, transnational). Betrachtet wird dementsprechend der Prozess, durch den kontroverse oder unterschiedliche Interessen ausgeglichen und kooperatives Handeln initiiert werden kann. Hiermit angesprochene Aspekte wie Interessenausgleich, Konfliktmanagement und Koordination des Zusammenwirkens in Organisationen und Netzwerken sind sowohl für die »Corporate Governance« als auch für die »IT-Governance« von Bedeutung.

Corporate Governance

Der Begriff »Corporate Governance« entstammt der seit Anfang der 1990er-Jahre geführten angelsächsischen Diskussion um eine effektive Unternehmensleitung und -überwachung. Eine deutsche Übersetzung für »Corporate Governance« existiert nicht, sodass die Bezeichnung mittlerweile als eigenständiger Begriff Eingang in die hiesige Fachdiskussion und -literatur (siehe beispielsweise [Stiglbauer 2010], [Paetzmann 2012], [Hilb 2016], [Welge & Eulereich 2021]) gefunden hat. Adressiert werden letztlich Unternehmen aller Größenordnungen und Branchen, wobei sich die wissenschaftliche Betrachtung jedoch vor allem auf börsennotierte Publikumsgesellschaften bzw. kapitalmarktorientierte Unternehmen richtet (nach [Hilb 2016], S. 48). Mitunter wird der Begriff der Unternehmensverfassung als Übersetzung angeboten. Allerdings gehen Governance-Überlegungen deutlich über die teilweise gesetzlich vorgegebenen und damit eher starren konstitutiven Strukturregelungen einer Unternehmensverfassung hinaus und haben eine deutlich flexiblere Leitung und Überwachung des Unternehmens zum Ziel (vgl. [Stiglbauer 2010], S. 14 f.).

Skandale als Treiber

In die Öffentlichkeit gelangte die Governance-Thematik ab Mitte der 1990er-Jahre durch spektakuläre Bilanzfälschungen (beispielsweise der Firmen Enron und Worldcom in den USA, Flowtex in Deutschland)

bzw. Unternehmenskrisen (von Metallgesellschaft und Phillip Holzmann über Volkswagen bis hin zum aktuellen Fall von Wirecard). Missmanagement und Betrugsfälle werfen seitdem Fragen bezüglich der Effektivität von Steuerungs- und Planungssystemen, Kontroll- und Risikomanagementsystemen, Interner Revision und externer Prüfung auf. Hierbei gerät auch die Rolle der Verantwortungsträger in den Leitungsorganen in den Fokus – häufig in Verbindung mit ihnen gewährten, vermeintlich zu hohen Gehalts-, Prämien- oder Abfindungszahlungen.

G20/OECD-Grundsätze

In der internationalen Diskussion um Corporate Governance sind vor allem die Corporate-Governance-Grundsätze der OECD (Organisation for Economic Cooperation and Development) von nachhaltiger Wirkung gewesen. Diese von der OECD erstmals im Jahr 1999 aufgestellten Grundsätze waren in vielen Staaten ein Initiator für Reformen von Governance-Regularien. In der aktuellen Version von 2015 wurden die Grundsätze in die Kernstandards für solide Finanzsysteme des Finanzstabilitätsrats aufgenommen und von der G20, der Gruppe der wichtigsten Industrie- und Schwellenländer, gebilligt. Nach dem Verständnis von G20/OECD richtet sich Corporate Governance auf das »Geflecht der Beziehungen zwischen der Geschäftsführung eines Unternehmens, seinem Aufsichtsorgan (Board), seinen Aktionären und anderen Unternehmensbeteiligten (Stakeholdern)« sowie auf »den strukturellen Rahmen für die Festlegung der Unternehmensziele, die Identifizierung der Mittel und Wege zu ihrer Umsetzung und die Modalitäten der Erfolgskontrolle« ([OECD 2015], S. 9).

Deutscher Corporate Governance Kodex

Die Corporate-Governance-Grundsätze der OECD fanden in Deutschland im Rahmen des »Deutschen Corporate Governance Kodex« (DCGK) Berücksichtigung. Erstellt wurde der DCGK durch die 2001 einberufene »Regierungskommission Deutscher Corporate Governance Kodex«. Die erste Fassung des Kodex wurde 2002 vorgelegt. Seitdem finden jährliche Überprüfungen und ggf. Anpassungen statt. Ein grundlegendes Verständnis von Corporate Governance und die Zielsetzung des DCGK sind in seiner Präambel enthalten:

DCGK-Definition

> »Unter Corporate Governance wird der rechtliche und faktische Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens verstanden. Der Deutsche Corporate Governance Kodex (der ›Kodex‹) … enthält Grundsätze, Empfehlungen und Anregungen zur Leitung und Überwachung deutscher börsennotierter Gesellschaften, die national und international als Standards guter und verantwortungsvoller Unternehmensführung anerkannt sind. Er will das Vertrauen der Anleger, der Kunden, der Belegschaft und der Öffentlichkeit in die Leitung und Überwachung deutscher börsennotierter Gesellschaften fördern.« ([DCGK 2022], Präambel)

Bemerkenswert ist, dass in dieser im Vergleich zur OECD weiteren Fassung mit Belegschaft und Mitarbeitern sowie der Öffentlichkeit deutlich mehr Akteure in den Kreis der Stakeholder einbezogen werden – Corporate Governance also durchaus auch eine gesellschaftliche Perspektive einschließt (vgl. [Kreipl 2020], 37 ff.).

Entsprechenserklärung nach § 161 AktG

Der Kodex beschreibt in weiten Teilen geltende gesetzliche Regelungen. Er enthält zudem Empfehlungen und Anregungen. Folgen die betroffenen Unternehmen den Empfehlungen nicht, müssen sie ihre Abweichungen nach § 161 AktG offenlegen und begründen (Comply or Explain). Diese Darstellungen sind auf der Internetseite der Unternehmen zu publizieren. An dieser Stelle bzw. im Umfeld der Entsprechenserklärung finden sich Aussagen des Unternehmens zu seinem Verständnis von Corporate Governance (siehe die Beispiele in Tab. 1–1).

Tab. 1–1
Beispiele für Aussagen zur Corporate Governance

Unternehmen	Aussagen zur Corporate Governance
Deutsche Bank AG	»Wirkungsvolle Corporate Governance Strukturen, die höchsten internationalen Standards entsprechen, sind Teil unseres Selbstverständnisses. Durch diese stellen wir eine verantwortungsbewusste, auf nachhaltige Wertschöpfung ausgerichtete Leitung und Kontrolle der Bank sicher. Unsere Corporate Governance Strukturen beruhen auf vier wichtigen Säulen: Gute Beziehungen zu den Aktionären, eine effektive Zusammenarbeit von Vorstand und Aufsichtsrat, ein leistungsorientiertes Vergütungssystem für Führungskräfte und Mitarbeiter sowie eine transparente und frühzeitige Rechnungslegung.« [Deutsche Bank 2022]
Lufthansa AG	»Corporate Governance kommt bei Lufthansa zum Ausdruck durch eine verantwortungsbewusste und auf nachhaltige Wertschöpfung ausgerichtete Unternehmensleitung und -kontrolle, die hohen internationalen Standards entspricht. Sie ist von zentraler Bedeutung für erhöhte Transparenz gegenüber Aktionären und die kontinuierliche Steigerung des Vertrauens in die Unternehmensführung. Das deutsche Aktiengesetz und der Deutsche Corporate Governance Kodex sind dabei wesentliche Grundlagen.« [Lufthansa 2021]
Volkswagen AG	»Corporate Governance bezeichnet die verantwortungsvolle, transparente und auf langfristige Wertschöpfung ausgelegte Leitung und Überwachung von Unternehmen. Eine gute Corporate Governance bildet die Basis für nachhaltigen Erfolg und ist für uns zugleich eine wichtige Voraussetzung, um das Vertrauen unserer Stakeholder in unsere Arbeit zu stärken.« [VW 2021]

Definition des Cadbury Report

Neben den G20/OECD-Grundsätzen zur Corporate Governance finden zahlreiche nationale Reports in der Literatur Erwähnung. Der wohl am häufigsten zitierte Bericht ist der sogenannte »Cadbury Report«. Benannt ist er nach Sir Adrian Cadbury, dem Leiter einer Arbeitsgruppe, die sich mit der Verbesserung der Corporate Governance in der britischen Wirtschaft befasste. Die Ergebnisse der Arbeitsgruppe wurden 1992 als »Report of the Committee on the Financial Aspects of Corporate Gover-

nance« vorgelegt. In dem Bericht findet sich die knappe Definition von Corporate Governance, die seitdem häufig zitiert wird und in verschiedene Normen und Standards Eingang gefunden hat ([TC 1992], Ziff. 2.5):

> »Corporate governance is the system by which companies are directed and controlled.«

Diese Definition wurde 16 Jahre später, im Jahr 2008, von der Norm ISO/IEC 38500, die auf die Governance der Unternehmens-IT abzielt, übernommen. Im folgenden Abschnitt werden Definitionen und Konzepte von IT-Governance dargestellt und diskutiert, die zum Teil an das dargestellte Corporate-Governance-Verständnis anknüpfen.

1.2 Definitionen für IT-Governance

Aufkommen des Begriffs »IT-Governance«

Während der Begriff »IT-Governance« in der Literatur erst Mitte der 1990er-Jahre Eingang fand und erst nach 2005 im deutschsprachigen Raum an Bedeutung gewann, gab es bereits seit den 1970er-Jahren eine Reihe von Studien zu verwandten Konzepten und Fragestellungen, wie zum Beispiel der Kontrolle und Organisation von Informationssystemen (vgl. [Gregory et al. 2018], S. 1227; [Schwertsik 2013], S. 20). Insofern handelte es sich zwar um einen neuen Begriff – die betrachteten Fragestellungen waren allerdings nicht vollkommen neu.

Frühe Definition

Eine frühe Definition, die breite Beachtung fand, stammt vom IT Governance Institute (ITGI), einer Tochterorganisation der Information Systems Audit and Control Association (ISACA). Der in Bezug auf IT-Governance einflussreichste Wissenschaftler dürfte Peter Weill von der Sloan School of Management des Massachusetts Institute of Technology (MIT) sein. Er hat wesentliche Konzepte und Modelle der IT-Governance entwickelt und die Diskussion geprägt. In Europa sind es die Arbeiten von Wim Van Grembergen und Steven De Haes von der Universität Antwerpen, die großen Einfluss auf die Weiterentwicklung der IT-Governance haben. Tabelle 1–2 zeigt verschiedene einschlägige Definitionen im Überblick.[1]

1. Eine umfangreichere Betrachtung des Begriffs findet sich in [Gregory et al. 2018]. Im Anhang dieses Journalbeitrags stellen die Autoren eine Liste von 35 Definitionen von IT-Governance zusammen und arbeiten relevante »Dimensionen von IT-Governance« heraus.

Tab. 1–2 *Definitionen für IT-Governance*

Autor/ Institution	Jahr	Definition
ITGI	2001	»IT-Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.« ([ITGI 2001], S. 9)
Weill/ Woodham	2002	»We define IT governance as specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT.« ([Weill & Woodham 2002], S. 1)
Meyer/ Zarnekow/ Kolbe	2003	»Unter IT-Governance werden Grundsätze, Verfahren und Maßnahmen zusammengefasst, die sicherstellen, dass mit Hilfe der eingesetzten IT die Geschäftsziele abgedeckt, Ressourcen verantwortungsvoll eingesetzt und Risiken angemessen überwacht werden.« ([Meyer et al. 2003], S. 445)
Van Grembergen/ De Haes/ Guldentops	2004	IT-Governance is »the organisational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT«. ([Van Grembergen et al. 2004], S. 5)
ISO/IEC	2015	»The system by which the current and future use of IT is directed and controlled. […] Governance of IT is a component or a subset of organizational governance.« ([ISO/IEC 38500], S. 2)
De Haes/ Van Grembergen/ Joshi/ Huygh	2020	»Enterprise Governance of IT (EGIT) is an integral part of corporate governance for which, as such, the board is accountable. It involves the definition and implementation of processes, structures, and relational mechanisms that enable both business and IT stakeholders to execute their responsibilities in support of business/IT alignment, and the creation and protection of IT business value.« ([De Haes et al. 2020a], S. 3)

Wie zu erkennen ist, divergieren die Definitionen nach Umfang und Inhalten des als »IT-Governance« bezeichneten Themenfeldes (vgl. auch [Johannsen & Goeken 2011], S. 22).

ITGI

- Die Definition des ITGI stellt neben der Führungsverantwortung die Aufbau- und die Prozessorganisation in den Vordergrund. Diese bilden die Grundlage dafür, dass die IT die Ziele und Strategien des Unternehmens unterstützen und erweitern kann.

Weill/Woodham

- Die am von Peter Weill geleiteten Center for Information Systems Research (CISR) zugrunde gelegte Definition von IT-Governance fokussiert die Entscheidungs- und Verantwortungsstruktur in Bezug auf die Nutzung von IT. Die Definition und insbesondere das IT-Governance-Modell von Weill et al. werden in Abschnitt 1.3 näher betrachtet.

- In ihrer Diskussion des Schlagwortes »IT-Governance« weiten Meyer, Zarnekow und Kolbe die Sichtweise von strukturellen Überlegungen in Form von Verfahren auf Grundsätze und Maßnahmen aus, damit die IT das Erreichen der Unternehmensziele unterstützt. Weiterhin bringen sie die zu nutzenden IT-Ressourcen sowie eine Risikosicht ins Spiel. Der Umgang mit Risiken, die sich aus der IT-Unterstützung der Geschäftsprozesse ergeben, stellt einen »der Kernbereiche der IT-Governance« dar ([Meyer et al. 2003], S. 448). *Meyer, Zarnekow, Kolbe*
- In dieser, erstmals im Jahr 2002 veröffentlichten Definition von Van Grembergen werden das Aufsichtsorgan, die Unternehmensleitung und das IT-Management als die wesentlichen Akteure der IT-Governance explizit benannt. Deren Fokus soll die Formulierung und Implementierung einer IT-Strategie sein, die die Verzahnung von Geschäftsseite und IT sicherstellt. *Van Grembergen*
- Die Definition der ISO/IEC 38500:2015 stellt ebenso wie das ITGI heraus, dass IT-Governance einen (funktionsspezifischen) Teilbereich der Corporate Governance darstellt. Ausdrücklich wird in dieser Definition darauf hingewiesen, dass sich Steuerung und Überwachung sowohl auf die im Unternehmen aktuell eingesetzte als auch auf die künftig einzusetzende IT richten müssen. Das Modell nach ISO/IEC 38500 wird in Abschnitt 1.4 ausführlicher dargestellt. *ISO/IEC 38500*
- De Haes et al. sehen IT-Governance ebenfalls als Aufgabe der Unternehmensleitung und orientieren sich am Stakeholder-Konzept der Corporate Governance. Weiterhin wird hier wie in der Definition des ITGI die strategische Ausrichtung (»Alignment«) der IT am Business im Sinne der Unterstützung von Unternehmenszielen und -strategien und dem daraus folgenden Wertbeitrag der IT hervorgehoben. Eine Besonderheit dieser Definition ist, dass sie konkrete sogenannte »Governance-Mechanismen« benennt, die zur Ausgestaltung einer IT-Governance zum Einsatz kommen. Der EGIT-Ansatz von De Haes und Van Grembergen ist Gegenstand von Abschnitt 1.6. *De Haes et al.*

Nach der Darstellung von vier prominenten IT-Governance-Konzepten in den folgenden Unterkapiteln greifen wir die Definitionen zur Begründung des in diesem Buch vertretenen Verständnisses von IT-Governance wieder auf.

1.3 IT-Governance nach Weill et al.

Wie sich in der Definition oben bereits zeigte, stehen bei Weill und Woodham bzw. Ross Entscheidungsrechte und Rechenschaftspflichten im Mittelpunkt (»decision rights and accountability framework«). Einfach ausgedrückt: »Governance determines who makes the decisions« ([Weill & Ross 2004a], S. 8). Hieran anknüpfend grenzen sie IT-Governance und IT-Management voneinander ab: »IT governance is not about making specific IT decisions – management does that – but rather determines who systematically makes and contributes to those decisions« ([Weill & Ross 2004a], S. 2)

In ihrem Ansatz beschreiben sie, dass für eine effektive IT-Governance festgelegt werden muss, was in Bezug auf die IT geregelt werden soll. Darüber hinaus sind die Entscheidungsstrukturen und die Verantwortungsteilung zu definieren, d.h., wer trifft die Entscheidungen und wie wird diese getroffen sowie überwacht (siehe auch [Schwertsik 2013], S. 31 ff.; [Beetz 2014], S. 3 ff. u. S. 17 ff.).

Governance-Arrangement-Matrix

Dementsprechend ist in den Arbeiten von Weill et al. die sogenannte »Governance-Arrangement-Matrix«, die die genannten Aspekte kombiniert, von zentraler Bedeutung (Tab. 1–3):

»IT-Decisions« bzw. »Decision Domains«

- »IT-Decisions« bzw. »Decision Domains« sind Themenbereiche, die mit Blick auf die IT-Governance besondere Relevanz besitzen, beispielsweise die IT-Architektur oder IT-Investitionen. Sie beantworten die Frage, für welche Sachverhalte und Gegenstände Entscheidungen zu treffen sind.

»Archetypes«

- »Archetypes« sind Muster bzw. Ausprägungen der Verantwortungsteilung zwischen IT- und der Geschäftsseite. Sie beschreiben mögliche Zuordnungen von Entscheidungsrechten und Rechenschaftspflichten. Die jeweilige Ausprägung beantwortet somit die Frage, von wem eine bestimmte Entscheidung getroffen wird. Bei der Benennung der Archetypen orientieren sich Weill et al. anschaulich an Regierungsformen bzw. Formen des Staatsaufbaus.

Im Folgenden wird das Modell näher erläutert.

	IT Principles	IT Architecture	IT Infra-structure Strategies	Business Application Needs	IT Investment
Business Monarchy					
IT Monarchy			?		
Feudal					
Federal					
Duopoly					
Anarchy					
Don't Know					

Tab. 1–3 *Governance-Arrangement-Matrix ([Weill & Ross 2004a], S. 11)*

Archetypen

Die Ausprägungen der Archetypen ergeben sich daraus, welche Führungskräfte bzw. Bereiche in Entscheidungen einbezogen sind (Tab. 1–4). Sie sind jeweils nach dem Grad der Zentralität bzw. Dezentralität und der Frage, wie stark die Verantwortung bei den geschäftlichen Bereichen bzw. der IT-Einheit liegt, geordnet (absteigend).

Zentrale Modelle

Bei einer »Monarchy« werden Entscheidungen zentralisiert getroffen – entweder von den obersten Führungskräften oder der IT-Leitung. In der feudalen Ordnung werden die Entscheidungen hingegen von den Leitern der Business Units (BU), Geschäfts- oder Zentralbereiche dezentral und eigenverantwortlich getroffen, sodass hier die lokalen Bedarfe im Vordergrund stehen und unternehmensweite Synergien entsprechend von nachrangiger Bedeutung sind.

	Oberste Führungsebene (C-Level Executives)	Unternehmens-IT oder IT der Business Units	Führungskräfte der Business Units
Business Monarchy	✓		
IT Monarchy		✓	
Feudal			✓
Federal	✓	✓	✓
	✓		✓
IT Duopoly	✓	✓	
		✓	✓
Anarchy			

Tab. 1–4 *»Key Players« der IT-Governance-Archetypen ([Weill & Ross 2004a], S. 60)*

Dezentrale Modelle

Während bei den ersten drei Archetypen eine Partei allein entscheidet, ist ab dem föderalen Modell (»Federal«) ein abgestimmtes Zusammenwirken verschiedener betroffener Akteure über Ebenen hinweg gegeben. Entweder sind dies die obersten Führungskräfte zusammen mit den Leitern der Business Units, Geschäfts- oder Zentralbereichen; ggf. wird dabei die IT-Leitung einbezogen. Oder die Unternehmens-IT hat genau einen Counterpart (»IT Duopoly«). Ein Duopol unterscheidet sich also von einem föderalen Modell dadurch, dass in Letzterem immer sowohl die Fachseite als auch lokale Organisationseinheiten (BU/Fachbereiche) vertreten sind, während in einem Duopol entweder die eine oder die andere, nicht aber beide vertreten sind und immer auch IT-Fachleute einbezogen werden. Beim Duopol sitzen also Führungskräfte der IT immer »mit am Tisch«.

Vor allem im föderalen Modell ist das Ausbalancieren der Interessen der vielen beteiligten und formal gleichberechtigten BU/Fachbereiche eine wesentliche Herausforderung. Hier besteht die Gefahr, dass ein großer Fachbereich die anderen dominiert. Die Notwendigkeit, einen angemessenen Ausgleich herbeizuführen, ist in den dezentraleren Varianten in abgeschwächter Form ebenfalls gegeben. Gleichzeitig ermöglichen sie – vor allem im Vergleich mit dem föderalen Modell – die Identifizierung von Synergiepotenzialen. Insbesondere Duopole haben im Vergleich zu feudalen Modellen den Vorteil, dass die zentrale IT-Gruppe oft eine der wenigen Gruppen ist, die – mit Blick auf Technologienutzung – die Organisation als Ganzes sieht und nach Möglichkeiten für die gemeinsame Nutzung und Wiederverwendung von Ressourcen suchen kann (vgl. [Weill & Ross 2004a], S. 63).

Anarchie

Der Fall der Anarchie ist der Tendenz nach von der Abwesenheit einer Governance gekennzeichnet und wird daher im Folgenden nicht weiter betrachtet.

Das Nebeneinander verschiedener Entscheidungsstrukturen

Weill und Ross beschreiben konkrete Ausgestaltungen unter anderem anhand von Fallbeispielen aus Unternehmen, deren IT-Governance sie untersucht haben. Dabei zeigt sich eine gewisse Vielgestaltigkeit, zum Beispiel darin, dass im Falle einer IT-Monarchie in manchen Organisationen von vielen IT-Führungskräften gemeinsam entschieden wird (Führungskräfte der Unternehmens-IT und IT der Business Units bilden ein »IT Governance Committee«), in anderen hingegen nur wenige Führungskräfte involviert sind. Nichtsdestotrotz lässt sich für die verschiedenen Fälle jeweils ein dominierendes Muster identifizieren (vgl. [Weill & Ross 2004a], S. 58 ff.).

Die genannten Archetypen sind nicht für sämtliche die IT betreffenden Themen und Inhalte von Relevanz. Vielmehr sind lt. Weill und Ross fünf Entscheidungsdomänen – im Sinne von Entscheidungsberei-

chen der IT-Governance – besonders einschlägig und geeignet, die IT-Governance zu erfassen (vgl. [Weill & Ross 2004a], S. 27 ff.):

Entscheidungsdomänen der IT-Governance

- IT-Prinzipien sind Grundsatzentscheidungen bezüglich der strategischen Rolle der IT in der Organisation. Sie betreffen die Finanzierung der IT-Organisation sowie die Frage, wie die Prinzipien und Ziele der Geschäfts- bzw. Fachbereiche in IT-Ziele/Prinzipien umgesetzt werden.
- In der Entscheidungsdomäne »IT-Architektur« werden Anforderungen an die Integration und Standardisierung definiert. Dies beinhaltet Grundsatzentscheidungen bezüglich der Architektur, also Entscheidungen und Regeln, die die technologische Basis für die Standardisierung der realisierten IT-Services sowie andere technologische Fragen betreffen.
- IT-Infrastruktur bezieht sich auf gemeinsam genutzte (technische) IT-Services und definiert Verantwortlichkeiten für diese, d.h., welche IT-Services die Grundlage für die unternehmensweiten IT-Fähigkeiten bilden sollen, welche kritisch sind, welche selbst erstellt bzw. von extern bezogen werden und wer für sie verantwortlich ist.
- In der Entscheidungsdomäne »Business Application Needs« (Geschäftsanforderungen) werden die fachlichen Bedarfe und Anforderungen für eigenentwickelte oder fremdbezogene Anwendungssysteme spezifiziert. Vor dem Hintergrund der Unternehmensziele dient die vorzunehmende Priorisierung, also die Entscheidung darüber, welche Bedarfe wann adressiert werden sollen, der Definition funktionaler und nicht funktionaler Anforderungen an aktuelle oder zukünftige Anwendungssysteme. Dabei können auch Ausnahmen von Architekturrichtlinien beschlossen werden.
- Bei der letzten Domäne geht es um finanzielle Aspekte von IT-Investitionen. Diese betreffen den gesamten Entscheidungsprozess bei IT-Investitionen, also die Ermittlung, Priorisierung und die Auswahl der Schwerpunkte für IT-Investitionen, und beschreiben die Verfahren für die Beantragung, Priorisierung sowie Genehmigung von Projektvorschlägen etc. (vgl. [Weill & Ross 2004a]). Offensichtlich sind hier viele Schnittstellen zu den anderen Domänen zu beachten, da die finanziellen Aspekte auch die Priorisierung mit Blick auf Infrastruktur und Anwendungssysteme tangieren. Die Berührungspunkte und Schnittstellen von IT-Controlling (insbesondere Budgetierung) und Programm- bzw. Portfoliomanagement werden hier deutlich erkennbar.

Parallelität

Wie dargestellt können Governance-Arrangements von eher zentralen Ansätzen (vor allem Monarchien) bis hin zu eher dezentralen Ansätzen (vor allem feudale Formen) reichen, wobei föderale und einige Duopol-Formen zwischen diesen beiden Varianten liegen. Dabei wird in der Regel für die jeweiligen Entscheidungsdomänen eine jeweils unternehmensindividuelle Verteilung der Entscheidungsrechte vorgenommen. Innerhalb einer Organisation können dementsprechend gleichzeitig verschiedene Entscheidungsformen (Archetypen) parallel für unterschiedliche Domänen vorliegen (vgl. [Schwertsik 2013], S. 35).

Einbeziehung der Business Units

IT-Prinzipien, Geschäftsanforderungen und IT-Investitionen sind die geschäftsorientierten Entscheidungen, bei denen in den meisten Organisationen solche Archetypen gewählt werden, die eine Involvierung der Business Units/Fachbereiche oder der oberen Führungskräfte sicherstellen. Hingegen sind die eher technischen Entscheidungen (IT-Architektur und Infrastruktur) häufig in der Hand der IT (IT-Monarchie) bzw. die Beteiligung der IT ist sichergestellt (föderales Modell) (vgl. [Weill & Ross 2004a], S. 64 ff.).

»Governance on one page«

Weill und Ross bezeichnen die oben dargestellte »Governance-Arrangement-Matrix« auch als »one-page framework«, das die IT-Governance einer Organisation knapp und anschaulich darstellt (»Governance on one page«). Ihre Anwendung erfolgt, indem man für eine konkrete Organisation für jede Domäne die definierte oder faktisch gegebene (»gelebte«) Verantwortungsteilung oder -zuordnung gemäß den Archetypen markiert. Dies ermöglicht es zu spezifizieren, zu analysieren und zu kommunizieren, wo IT-Entscheidungen getroffen werden (vgl. [Weill & Ross 2004b]).

Empirische Erkenntnisse

In einer breit angelegten Untersuchung von fast 300 Unternehmen haben Weill et al. Muster identifiziert, die in besonders erfolgreichen Organisationen anzutreffen sind. Erfolg wird anhand von betriebswirtschaftlichen Kennzahlen gemessen. Es werden drei Performance-Strategien unterschieden:

Performance-Strategien

- **Profit**
  Gewinn-(Profit-)Orientierung, gemessen an der Eigenkapitalrendite (ROE), dem Return on Investment (ROI) und der Gewinnspanne in Prozent.
- **Asset Utilization**
  Effizienz der Nutzung aller Vermögensgegenstände, gemessen mit der Gesamtkapitalrentabilität (Return on Assets (ROA)).
- **Growth**
  Wachstum, gemessen an Umsatzsteigerungen (in Prozent), also Umsatzwachstum.

Besonders erfolgreiche Organisationen untersuchten sie daraufhin, welche Entscheidungsbereiche mit welchen Archetypen assoziiert sind. Die identifizierten Muster sind in Tabelle 1–5 dargestellt.

Erfolgreiche Kombinationen und Ausprägungen

	Leistung (»Performance«) durch		
	Gewinnorientierung (»Profit«)	**Nutzung von Anlagegütern (»Asset Utilization«)**	**Wachstumsorientierung (»Growth«)**
Strategische Zielsetzung	Wirtschaftlichkeit (Profitabilität) durch organisationsweite Integration und Fokus auf Kernkompetenzen	Effizienz durch Zusammenarbeit und Wiederverwendung	Unterstützung/Förderung von Innovationen in den Fachbereichen durch geringe Anzahl an Vorgaben
Wesentliche Metriken	ROI/ROE und Prozesskosten	ROA und Kosten pro IT-Einheit	Umsatz-/Ertragswachstum
Wesentliche IT-Governance-Mechanismen	■ Organisationsweite Managementmechanismen (z.B. Steuerungskomitee) ■ Architekturprozesse ■ Budgetierungsprozesse und Genehmigungsprozesse für Finanzmittel/Investitionen ■ Überwachung des Wertbeitrags der IT	■ Schnittstelle Business/IT wird aktiv gemanagt ■ Prozessteams mit IT-Mitarbeitern ■ SLA und Verrechnungssysteme ■ IT-Führungskräftegremium zur Entscheidungsfindung	■ Budgetbewilligung und Risikomanagement ■ Dezentrale Zuständigkeit ■ Portale und andere Informations- und Servicequellen
IT-Infrastruktur	Mehrere Ebenen zentraler Shared Services	Shared Services, die zentral koordiniert werden	Dezentral angepasste Services; Beschränkung auf wenige erforderliche Shared Services
Wesentliche IT-Prinzipien	Geringe Kosten durch standardisierte Geschäftsprozesse	Geringe Kosten pro IT-Einheit; Wiederverwendung von Standards und Services	Dezentrale Innovation mit Communities of Practice; Optionale Shared Services
Governance-Ansatz	Eher zentralisiert z.B. Monarchie und föderales System	Gemischt z.B. föderales System und Duopol	Eher dezentralisiert z.B. feudales System, Risikomanagement steht im Vordergrund

Tab. 1–5 *Erfolgreiche IT-Governance-Arrangements (»Governance Lessons from Top Performers«) (nach [Weill & Ross 2004b], S. 8; [Schwertsik 2013], S. 35)*

- Dabei finden sich bei Organisationen mit *Gewinn-/Profit-Orientierung* der Tendenz nach eher zentrale Archetypen, d.h., es stehen Effizienz durch Standardisierung, Synergien und Kosteneffizienz im Vordergrund, was eher durch zentralisierte Muster in Unternehmen und Betrieben umgesetzt werden kann.
- Organisationen, die *wachstumsorientiert* sind, erreichen dies durch lokale Optimierung und lokale Innovationen. Wachstum wird hier dadurch unterstützt, dass auf lokale Besonderheiten Rücksicht genommen werden kann, was mit dezentralen Governance-Archetypen einhergeht.

- Die Strategie in der Mitte (*Nutzung von Anlagegütern*) ist hingegen eine Mischung, die durch gemeinsame Koordination in Duopolen am besten realisiert werden kann.

Der Tendenz nach ist erkennbar, dass Zentralisierung Kontrolle, Effizienz und Zuverlässigkeit bei der Nutzung von IT-Ressourcen ermöglicht, während Flexibilität, Innovation und Reaktionsfähigkeit auf sich ändernde Anforderungen eher durch Dezentralisierung gefördert wird.

Dominanz der Struktursicht

Zwar beziehen Weill et al. auch das Business/IT-Alignment und Kommunikationsmechanismen in ihren Ansatz ein (vgl. [Weill & Ross, 2004a], S. 97 ff. sowie Abschnitt 2.6.2); im Wesentlichen dominiert jedoch die strukturorientierte Sicht auf die IT-Governance. Er ist gewiss einer der weitverbreitetsten Ansätze in diesem Bereich und insofern eine Pionierarbeit. Die anschauliche Darstellung der groben Muster, die die Zuordnung von Entscheidungsrechten und die Verantwortungsteilung deutlich machen, bietet einen guten Einstieg in die strukturelle Perspektive der IT-Governance und für die Beschreibung von organisationsspezifischen Ausgestaltungen in der Praxis.

Kritik

Gleichwohl bleiben einige der verwendeten Konzepte etwas vage (die Vielgestaltigkeit der Archetypen wurde oben bereits angesprochen). Darüber hinaus wird nicht deutlich, ob Weill et al. die Entscheidungsbereiche als so generisch ansehen, dass sie eher unveränderlich sind, oder ob sie davon ausgehen, dass sie mit der Veränderung von IT-Organisationen, Technologien und Konzepten sowie sich wandelnden Schwerpunktsetzungen in der IT anzupassen wären – beispielsweise ob gewisse Themen wie Cloud Computing, Cybersecurity und digitale Transformation ggf. die Neubegründung von Entscheidungsdomänen rechtfertigen (den Verfassern sind in dieser Hinsicht keine Weiterentwicklungen durch Weill et al. bekannt). Etwas zu kurz kommt bei Weill et al. die Betrachtung von Governance-Mechanismen, die sich nicht auf die Struktur im Sinne der Entscheidungsfindung und Verantwortungsteilung beziehen. In jüngeren Ansätzen – und entsprechend in den folgenden Abschnitten – werden diese mit Blick auf eine ganzheitliche Governance der Unternehmens-IT intensiver betrachtet und einbezogen.

1.4 IT-Governance nach der ISO/IEC 38500

ISO/IEC 38500 – die IT-Governance-Norm

Die erstmals im Juni 2008 publizierte Norm »ISO/IEC 38500:2008 Corporate governance of information technology« resultierte aus der australischen Norm »AS8015:2005 Corporate governance of information and communication technology«, die im sogenannten »Fast Track«-Verfahren übernommen worden war. Mittlerweile liegt die ISO/IEC 38500 in der zweiten Ausgabe vom 15. Februar 2015 vor und wird derzeit überarbeitet. Gegenüber der ersten Version trägt sie den veränderten Titel »Information technology – Governance of IT for the organization«.

Grundlegende Ausrichtung und Ziele

Die ISO/IEC 38500 zielt auf einen effektiven, effizienten und den Erwartungen der Stakeholder entsprechenden Einsatz der IT. Vor allem soll das Vertrauen der Stakeholder in die Governance der IT gestärkt werden. Für die Unternehmensleitung bietet die Norm eine Orientierung, wie sie ihrer Governance-Verantwortung für IT gerecht werden kann (nach [Klotz 2016b], S. 18). Die Norm versteht sich selbst als »principles-based advisory standard«. Demgemäß werden im Rahmen von sechs Prinzipien verschiedene Zielsetzungen guter IT-Governance (siehe Tab. 1–6) postuliert.

Tab. 1–6
Prinzipien der IT-Governance nach der ISO/IEC 38500:2015 (nach [Klotz 2016b], S. 19; vgl. [ISO/IEC 38500], S. 5 f.)

Nr.	Prinzip	Inhalt
1	**Verantwortlichkeit** (responsibility)	■ Kenntnis und Akzeptanz der Verantwortlichkeiten für IT-Nachfrage und -Angebot ■ Verteilung verantwortungsadäquater Befugnisse
2	**Strategie** (strategy)	■ Berücksichtigung der aktuellen und künftigen Potenziale der IT im Rahmen der strategischen Planung ■ Ausrichtung des IT-Einsatzes an der Unternehmensstrategie
3	**Beschaffung** (acquisition)	■ Transparenz und Fundierung von IT-Beschaffungen ■ Kurz- und langfristige Ausgewogenheit von Nutzen und Kosten, Chancen und Risiken von IT-Beschaffungen
4	**Performanz** (performance)	■ Verfügbarkeit von IT-Services entsprechend den aktuellen und künftigen Leistungs- und Qualitätsanforderungen der Geschäftsbereiche
5	**Konformität** (conformance)	■ Konformität der IT mit verpflichtenden gesetzlichen und regulatorischen Vorgaben ■ Definierte, implementierte und durchgesetzte Richtlinien und Verfahren
6	**Verhalten** (human behaviour)	■ IT-Richtlinien, -Verfahren und -Entscheidungen berücksichtigen Verhaltensweisen sowie aktuelle und künftige Bedürfnisse aller Personen, die in die IT-Nutzung involviert sind

Grundlegende Governance-Aufgaben

Die sechs Prinzipien werden durch drei grundlegende Governance-Aufgaben (Evaluate, Direct, Monitor), die von der Unternehmensleitung wahrzunehmen sind, ergänzt.

- **Evaluate**
  Die Bewertung des aktuellen und künftigen IT-Einsatzes richtet sich einerseits auf die Ergebnisse der Überwachung (Monitor), andererseits auf die seitens der Managementebene erstellten und eingereichten Planungen und Vorschläge sowie interne und/oder externe Liefervereinbarungen. Hierbei sind die Auswirkungen der verschiedenen internen und externen Einflussfaktoren zu berücksichtigen (z.B. technische und soziale Entwicklungen, regulatorische und geschäftliche Anforderungen).
- **Direct**
  Kern der Leitungsaufgabe ist die Festlegung von Strategien und Richtlinien zur IT-Nutzung. Zur Umsetzung der Strategien und Richtlinien hat die Unternehmensleitung entsprechende Verantwortlichkeiten an die Managementebene zu delegieren und den Prozess der Umsetzung zu steuern. Mittels der Strategien sind insbesondere die durch IT-Investitionen zu erreichenden Ziele festzulegen, während die Richtlinien eine korrekte Nutzung der IT durch die Mitarbeiter sicherstellen sollen. Für im Rahmen der Bewertung identifizierte Bedarfe ist durch die Leitungsorgane die Entwicklung entsprechender Vorschläge zu initiieren. Im Hinblick auf eine gute Governance-Kultur sind die Führungskräfte der Managementebene durch die Leitungsorgane zu transparenter Information sowie zum Einhalten aller Regelungen zur Steuerung der IT und der sechs Prinzipien der IT-Governance anzuhalten.
- **Monitor**
  Die Überwachungsaufgabe der Unternehmensleitung bezieht sich auf die Leistungsüberwachung der IT. Diese erfolgt auf der Basis entsprechender Rückmeldungen aus der Managementebene unter Nutzung geeigneter Messsysteme. Die Überwachung soll die Erreichung der Unternehmensziele, die Übereinstimmung mit den verfolgten Strategien und die Konformität mit Compliance-Verpflichtungen aus gesetzlichen, behördlichen und vertraglichen Vorgaben sowie unternehmensinternen Regelungen sicherstellen (nach [Klotz 2016b], S. 25 ff.; vgl. [ISO/IEC 38500], S. 7 f.).

Trennung von Governance und Management

Mit der Betonung von Governance-Aufgaben folgt die ISO/IEC 38500 der in den OECD-Grundsätzen beschriebenen, auf dem allgemeinen Konzept von Kontrolle und Gegenkontrolle beruhenden Trennung zwischen Governance und Management. Diese bildet in den OECD-Grundsätzen

ein durchgängiges Prinzip, das sich in der Unterscheidung zwischen der von der Unternehmensleitung ausgeübten Managementfunktion einerseits und der diesbezüglichen Steuerung und Überwachung durch Aufsichtsgremium und Eigentümer andererseits ausprägt. Für die IT führt dies zu einer expliziten Trennung der IT-Governance von Aufgaben des IT-Managements (siehe Abb. 1–1).

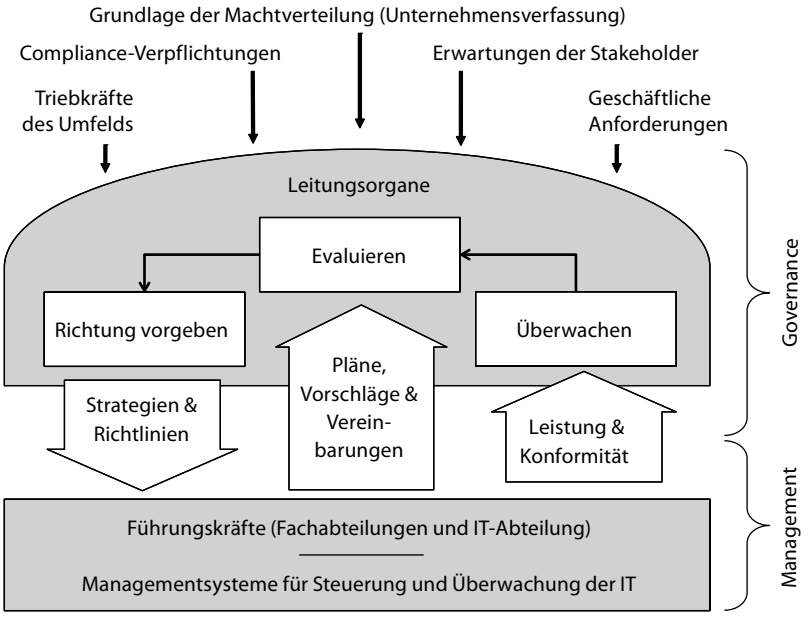


Abb. 1–1
IT-Governance nach ISO/IEC 38500:2015 (nach [Klotz 2016b]; vgl. [ISO/IEC 38500], S. 7)

Kombination von Aufgaben und Prinzipien

Die weitere Ausgestaltung der IT-Governance erfolgt in der ISO/IEC 38500 dadurch, dass die drei Governance-Aufgaben für jedes der sechs Prinzipien konkretisiert werden. So entstehen Leitlinien für die Unternehmensleitung, die ihre Verantwortung für IT-Governance umreißen. Die ISO/IEC 38500:2015 versteht diese Aussagen als Startpunkt für eine interne Diskussion darüber, wie die Governance-Verantwortung der Leitungsorgane unternehmensspezifisch auszugestalten ist (vgl. [ISO/IEC 38500], S. 8). So werden beispielsweise dem Strategieprinzip insgesamt sieben Leitlinien zugeordnet (vgl. Tab. 1–7).

Tab. 1–7 *Kombination aus Prinzip und Governance-Aufgaben am Beispiel von Prinzip 2*

Prinzip → **Governance-Aufgabe ↓**	**Strategie** (strategy) ■ Berücksichtigung der aktuellen und künftigen Potenziale der IT im Rahmen der strategischen Planung ■ Ausrichtung des IT-Einsatzes an der Unternehmensstrategie
Evaluieren	1. Entwicklungen sowohl der IT als auch der Geschäftsprozesse sollten bewertet werden, um die Unterstützung der künftigen Geschäftsanforderungen durch die IT sicherzustellen. 2. Im Rahmen der Prüfung von Plänen und Richtlinien sollten IT-Nutzung und -Maßnahmen bewertet werden, um die Ausrichtung an den Unternehmenszielen und die Erfüllung der Anforderungen wichtiger Stakeholder zu gewährleisten. Hierbei sollten auch bewährte Verfahren berücksichtigt werden. 3. Der IT-Einsatz sollte Gegenstand eines geeigneten Risikomanagements sein.
Richtung vorgeben	4. Die Erstellung und Verwendung von Strategien und Richtlinien sollte dahingehend gesteuert werden, dass das Unternehmen von den Entwicklungen der IT profitiert. 5. Vorschläge für innovativen IT-Einsatz sollten angeregt werden, damit das Unternehmen auf neue Chancen und Herausforderungen reagieren, neue Geschäftspotenziale erschließen oder Prozesse verbessern kann.
Überwachen	6. Der Fortschritt in der Umsetzung genehmigter IT-Vorschläge sollte überwacht werden, um sicherzustellen, dass die Ziele mit den geplanten Ressourcen in der vorgesehenen Zeit erreicht werden. 7. Der IT-Einsatz sollte überwacht werden, um sicherzustellen, dass der beabsichtigte Nutzen realisiert wird.

ISO/IEC 38500 und COBIT

Die drei von der ISO/IEC 38500 formulierten Governance-Aufgaben haben Eingang in das führende IT-Governance- und -Management-Framework »COBIT®« gefunden. Die COBIT-Version von 2012 (COBIT 5) führte die »Unterscheidung zwischen Governance und Management« als eines der grundlegenden Prinzipien für die Governance und das Management der Unternehmens-IT ein. Der wesentliche Beweggrund wurde darin gesehen, dass beide Disziplinen »mit unterschiedlichen Arten von Aktivitäten verbunden« sind, unterschiedliche Organisationsstrukturen erfordern und unterschiedlichen Zwecken dienen (vgl. [ISACA 2012a], S. 16). Im Prozessreferenzmodell von COBIT 5 wirkte sich die Anwendung des Prinzips in der Unterscheidung zwischen Governance- und Managementprozessen aus. Mit ausdrücklicher und erkennbarer Anlehnung an die Konzepte der ISO/IEC 38500 bestehen die Governance-Prozesse nach COBIT 5 »aus Praktiken und Aktivitäten, die darauf ausgelegt sind, strategische Optionen zu evaluieren, die IT-Richtung vorzugeben (die IT zu steuern) und Ergebnisse zu überwachen« ([ISACA 2012b], S. 25). Auch COBIT 5 verwendet für die Be-

nennung der Governance-Domäne bzw. der zugehörigen IT-Governance-Zielsetzungen die drei Begriffe »Evaluate, Direct, Monitor« (abgekürzt »EDM«). Die aktuelle COBIT-Version, COBIT 2019, führt diesen Ansatz fort. Auch hier fordert eines der Prinzipien für ein Governance-System eine klare Unterscheidung zwischen Governance- und Managementstrukturen und Aktivitäten (vgl. [ISACA 2020a], S. 17).

Normenreihe ISO/IEC 3850x

Die ISO/IEC 38500 steht am Anfang einer Normenreihe zu IT-Governance, die auch technische Spezifikationen und technische Reports umfasst. Die verschiedenen Dokumente enthalten Vertiefungen und ergänzende Themen. So wird z. B. das Modell der IT-Governance näher beschrieben und ein Implementierungsleitfaden gibt Empfehlungen zur Einführung von IT-Governance. Data Governance wird in einer eigenen Norm behandelt, die mehrere Teile umfasst. Zudem liegen Normen und Spezifikationen zur Datenklassifikation in Zusammenhang mit Data Governance, zur Bewertung der IT-Governance oder den Folgen des KI-Einsatzes für die IT-Governance vor.[2]

1.5 IT-Governance nach COBIT 2019

COBIT als umfassendes Rahmenwerk (Framework)

COBIT 2019 versteht sich als Framework für die »Governance der unternehmensweiten I&T« (enterprise governance of information and technology – EGIT)« und stellt mit »Information & Technology« nicht nur auf die Informationstechnologie ab.[3]

»I&T« und »Information Governance«

Während sich im Modell der ISO der Bezug auf das Gesamtunternehmen (»Corporate Governance of IT« bzw. »Governance of IT for the organization«) andeutet, wird von der ISACA eine Ausweitung in eine andere Richtung angestrebt, weg von der (Informations-)Technologie und hin zu Technologie und Information: Die eigentliche Information, also der Rohstoff bzw. das Zwischen- und/oder Endprodukt der Informationsverarbeitung, soll durch diese Namensgebung verstärkt in den Blick genommen werden. Im Zuge dessen wird und wurde vermehrt auch über »Information Governance« als Konzept und Managementansatz nachgedacht (vgl. [Johannsen & Goeken 2017]; [Tallon et al. 2013], beispielsweise auch [Information Governance Initiative o. J.]). Dies scheint sachlogisch, wenn man bedenkt, dass Information als Produktionsfaktor angesehen wird und – so [Broadbent et al. 2003] – Technologie die Verpackung ist: »IT [information technology] does matter, but not because of hardware or even standard commercial software. It

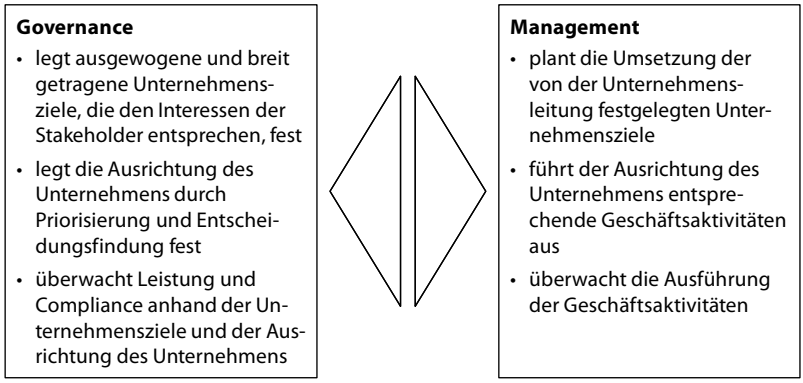
2. Einen Überblick über die Normenreihe ISO/IEC 3850x beinhaltet der Abschnitt 9.2.1.
3. Eine ausführlichere Betrachtung von COBIT findet sich in Abschnitt 9.3; eine umfangreiche Darstellung bei [Gaulke 2020].

is because the intelligent and innovative application of information solves business problems and creates customer value.« Gleichwohl hat »Information Governance« eine eher begrenzte Resonanz in Praxis und Forschung gefunden und auch in COBIT selbst steht die Informationstechnologie nach wie vor im Mittelpunkt.

Organisatorische Aufhängung und Abgrenzung zwischen Governance und Management

Auch für COBIT ist IT-Governance integraler Bestandteil der Corporate Governance. Ihre Ausgestaltung obliegt der Unternehmensleitung, die die Definition und Implementierung von Prozessen, Strukturen und Arbeitszusammenhängen im Unternehmen überwacht, sodass sowohl die Fachabteilungen (das »Business«) als auch die Unternehmens-IT in der Lage ist, die jeweilige Verantwortung hinsichtlich des Business/IT-Alignments und der Wertschöpfung durch IT-Investitionen wahrzunehmen (nach [ISACA 2020a], S. 11). Die Abgrenzung zwischen Governance und Management zeigt Abbildung 1–2.

Abb. 1–2
Abgrenzung zwischen Governance und Management nach COBIT 2019 (vgl. [ISACA 2020a], S. 13)



Governance- und Management-Domänen

Den Kern von COBIT 2019 bildet ein Referenzmodell für Governance- und Managementziele, die über eine Kaskadierung letztlich zu einer Vielzahl von IT-Governance- und IT-Managementpraktiken führen. Hierbei werden die Zielsetzungen für die IT-Governance in der Governance-Domäne »Evaluate, Direct, Monitor (EDM)« (dt.: Evaluieren, Vorgeben, Überwachen), die Zielsetzungen für das IT-Management in vier Management-Domänen abgebildet (nach [ISACA 2020b], S. 11):

- *Evaluate, Direct and Monitor (EDM) – Evaluieren, Vorgeben, Überwachen*: umfasst die Evaluierung strategischer Optionen, die Steuerung der gewählten strategischen Optionen und die Überwachung der Umsetzung der IT-Strategie.
- *Align, Plan and Organize (APO) – Anpassen, Planen, Organisieren*: befasst sich mit der Gesamtorganisation, der Strategie und den unterstützenden Planungs- und Koordinationsaktivitäten für IT.
- *Build, Acquire and Implement (BAI) – Aufbauen, Beschaffen, Implementieren*: behandelt die Definition, Beschaffung und Implementierung von IT-Lösungen und ihre Integration in Geschäftsprozesse.
- *Deliver, Service and Support (DSS) – Bereitstellen, Betreiben, Unterstützen*: richtet sich auf die operative, sichere Bereitstellung und Unterstützung von IT-Services.
- *Monitor, Evaluate and Assess (MEA) – Überwachen, Evaluieren und Beurteilen:* befasst sich mit der Leistungsüberwachung in Bezug auf interne Leistungs- und Kontrollziele und der Compliance der IT mit externen Anforderungen.

IT-Governance- und IT-Management-Domänen beinhalten u.a. IT-Prozesse und zugehörige Praktiken. Diese sind über ein Input/Output-Modell für informationelle und materielle Beziehungen miteinander verbunden. Auf diese Weise lassen sich die komplexen Zusammenhänge zwischen der Governance-Domäne und den Management-Domänen nachvollziehen.

Beispiel

Eine der IT-Governance-Zielsetzungen von COBIT 2019 ist die sichergestellte Lieferung von Wertbeiträgen des IT-Einsatzes (EDM02). Dieses Ziel wird durch verschiedene Governance-Praktiken erreicht, wobei die Steuerung der Wertoptimierung eine dieser Governance-Praktiken ist (EDM02.03). Abbildung 1–3 zeigt die Input-/Output-Beziehungen dieser Governance-Praktik mit insgesamt vier Managementpraktiken. Zwei dieser Praktiken sind dem IT-Managementziel »Gemanagtes Portfolio« zuzurechnen, während sich die anderen beiden Praktiken auf die IT-Managementziele »Gemanagte Programme« bzw. »Gemanagte Projekte« beziehen.

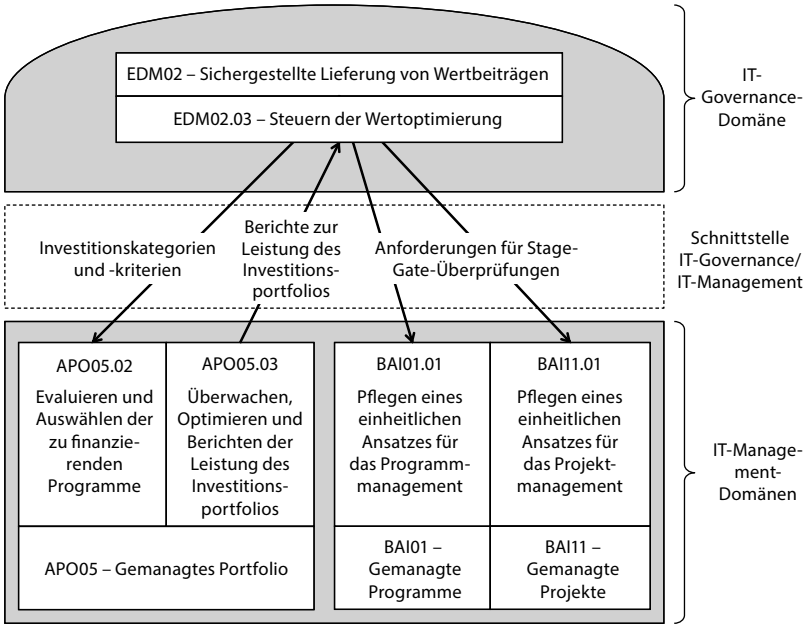


Abb. 1–3
Zusammenhang zwischen IT-Governance- und IT-Management-Domänen nach COBIT 2019

Die IT-Governance-Praktik erhält einen Input aus der Managementpraktik »APO05.03 Überwachen, Optimieren und Berichten der Leistung des Investitionsportfolios«, nämlich Leistungsberichte in Bezug auf das IT-Investitionsportfolio. Diese Berichte werden benötigt, um im Rahmen der Steuerung der Wertoptimierung erforderliche Änderungen am IT-Investitionsportfolio vorzunehmen, damit die betreffenden Investitionen und IT-Services sich (wieder) an den Unternehmenszielen bzw. Beschränkungen des Unternehmens ausrichten.

Durch die Durchführung der IT-Governance-Praktik entstehen zwei Outputs, die in drei Managementpraktiken verwendet werden. So richtet sich die Governance-Praktik zum einen u.a. auf die Definition und Kommunikation von Investitionskategorien und -kriterien für die IT-Investitionsentscheidungen. Diese stellen damit die notwendige Grundlage dar, auf der im Rahmen der Managementpraktik »APO05.02 Evaluieren und Auswählen der zu finanzierenden Programme« IT-Investitionsmöglichkeiten mit adäquaten Wertbeiträgen identifiziert, klassifiziert, bewertet und entschieden werden können. Zum anderen werden Anforderungen für Stage-Gate-Überprüfungen definiert, die – im Rahmen der beiden Managementpraktiken BAI01.01 und BAI11.01 – als Element eines hausinternen Standards für das Vorgehen im Programm- und Projektmanagement festzulegen und weiterzuentwickeln sind. Die Anforderungen richten sich z.B. auf die Bedeutung der IT-Investition für das Unternehmen, die damit verbundenen Risiken, Finanzierungs-

pläne, die erforderlichen Schlüsselqualifikationen und den laufenden Wertbeitrag.

Integration von Normen und Standards

Bei der Beschreibung der einzelnen Praktiken verweist COBIT 2019 auf Normen und Standards, die in die jeweilige Praktik eingegangen sind. Zum Beispiel wird für die Steuerung der Wertoptimierung die ISO/IEC 38500:2015 angeführt (vgl. [ISACA 2020b], S. 37). Die in dieser Praktik beschriebenen Aktivitäten sollen das Strategieprinzip abdecken, nach dem durch die IT-Governance die Ausrichtung des IT-Einsatzes an der Unternehmensstrategie sicherzustellen ist und die aktuellen und künftigen Potenziale der IT im Rahmen der strategischen Planung zu berücksichtigen sind.[4]

1.6 IT-Governance nach Van Grembergen/De Haes et al.

Definition

Die Definitionen von Van Grembergen bzw. De Haes et al. (siehe Tab. 1–2) beziehen sich nicht nur auf die »Enterprise Governance of IT« als organisatorische Fähigkeit (sogenannte EGIT-/IT-Governance-Mechanismen), sondern auch auf die angestrebten Ergebnisse.

»Enterprise Governance of IT (EGIT)« statt »IT-Governance«

Bemerkenswert ist, dass die Autoren den Begriff IT-Governance abzulösen versuchen. Sie argumentieren, dass durch die Fokussierung auf »IT« die Diskussion über IT-Governance hauptsächlich im IT-Bereich geführt wurde und dort verblieb. Jedoch reiche diese Fokussierung, obwohl in der Praxis viele IT-Governance-Vorhaben von der IT vorangetrieben und verantwortet werden, nicht aus. Ein Wertbeitrag und Wirkungen auf Prozesse und Geschäftsmodelle können so nicht erzielt werden. Vielmehr sei die Einbeziehung der Ziele, Anforderungen und Bedarfe der Fachbereiche von entscheidender Bedeutung, was mit der Verschiebung der Definition von »IT-Governance« hin zu »Enterprise Governance of IT (EGIT)« (d.h. mit Schwerpunkt auf die Einbeziehung des Unternehmens) zum Ausdruck gebracht werden soll (vgl. [De Haes et al. 2020a]; [De Haes & Van Grembergen 2009]).

Erweiterter Fokus

Wie bereits in der Definition zum Ausdruck kommt, ist Enterprise Governance of IT ein integraler Bestandteil der Corporate Governance, für die der Vorstand als solcher verantwortlich ist. Sie umfasst die Definition und Implementierung von Prozessen, Strukturen und Beziehungsmechanismen, die es sowohl den Geschäfts- als auch den IT-Stakeholdern ermöglichen, ihre Verantwortlichkeiten zur Unterstützung der Ausrich-

4. Mithilfe von COBIT 2019 lässt sich ein IT-Governance-System konzipieren. Für die maßgeschneiderte Implementierung eines derartigen Systems ist die sogenannte Zielkaskade von COBIT 2019 von besonderer Bedeutung. Abschnitt 9.3 enthält hierzu – nach einer kurzen Darstellung der verschiedenen COBIT-Dokumente – vertiefende Erläuterungen.

tung von Business und IT (Alignment) sowie zur Schaffung und zum Schutz eines IT-Wertbeitrags wahrzunehmen. Enterprise Governance of IT geht demnach über die IT-bezogenen Verantwortlichkeiten hinaus und erstreckt sich auch auf Geschäftsprozesse, was für die Schaffung und die Sicherung eines Wertbeitrags der IT erforderlich ist. Dies korrespondiert mit der Namensgebung von ISO/IEC, die 2008 die neue globale Norm zur »Corporate Governance of IT« (ISO/IEC 38500:2008) veröffentlicht hat.

De Haes und Van Grembergen gestehen zwar ein, dass – vordergründig – die Änderung der Bezeichnung und des Schwerpunkts von »IT-Governance« zu »Enterprise Governance of IT« spitzfindig und nicht bahnbrechend erscheinen mag, sie plädieren jedoch vehement dafür, dass es eines entscheidenden Wandels in der Denkweise der Unternehmensakteure bedarf. Die führende Rolle der IT-Stakeholder bei der IT-Governance sei schon immer paradox gewesen – ähnlich wie bei anderen IT-unterstützten Vorhaben wie Prozessoptimierung und Reengineering (vgl. [De Haes et al. 2020a], S. 4).

Auch an anderer Stelle zeigen sie, dass empirische Evidenz darauf hinweist, dass Führungskräfte und Aufsichtsgremien eben nicht in dem Maße in die IT-bezogene strategische Entscheidungsfindung und Kontrolle eingebunden sind, wie es wünschenswert und nötig wäre. Dies sei insbesondere auch bei der »Digitalisierung« bzw. der »digitalen Transformation« ein entscheidendes Hindernis (vgl. [De Haes et al. 2020b], S. 1 ff.).

IT-Governance-Mechanismen

Neben dem modifizierten Grundverständnis spielen bei Van Grembergen et al. die verschiedenen IT-Governance-Mechanismen eine zentrale Rolle. Aufbauend auf relevanten Vorarbeiten der IT-Governance-Forschung schlagen sie vor, dass ein IT-Governance-Arrangement aus Strukturen, Prozessen und Beziehungsmechanismen bestehen solle (vgl. [De Haes et al. 2020a], S. 17 ff. insbesondere S. 19 und 23 ff.) – siehe Abb. 1–4).

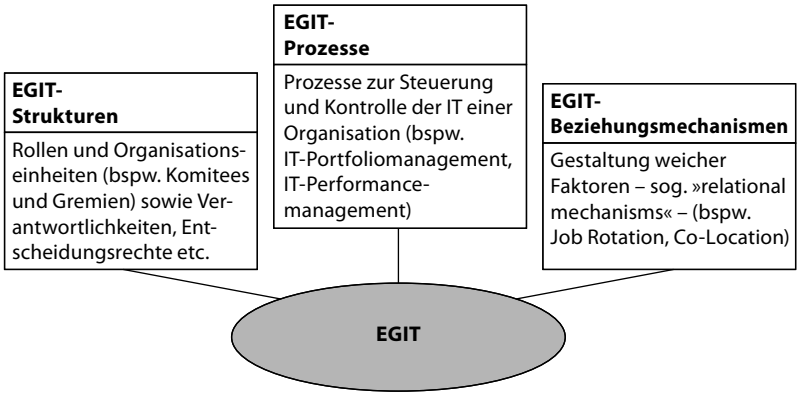


Abb. 1–4
Strukturen, Prozesse und Beziehungsmechanismen im IT-Governance-Modell von Van Grembergen et al.

Strukturen

- EGIT-Strukturen umfassen Organisationseinheiten, Gremien und Komitees sowie Rollen, die für IT-Entscheidungen verantwortlich sind und strukturelle Verbindungen zwischen den Geschäftsfunktionen und dem IT-Management herstellen (z. B. IT-Lenkungsausschuss).

Prozesse

- EGIT-Prozesse beziehen sich auf die Formalisierung und Institutionalisierung von strategischen IT-Entscheidungs- und IT-Überwachungsverfahren, um sicherzustellen, dass die tägliche und gelebte Praxis mit den Richtlinien übereinstimmt und angemessen gesteuert und kontrolliert wird, also Feedback und Rückkopplungen vorgesehen sind (z. B. Portfoliomanagement).

Beziehungsmechanismen (»relational mechanisms«)

- Bei den EGIT-Beziehungsmechanismen schließlich geht es um eher »weiche Faktoren«, die die aktive Beteiligung von und die Zusammenarbeit zwischen den Führungskräften des Unternehmens, der IT-Leitung und der Geschäftsleitung sicherstellen; dazu gehören beispielsweise Job-Rotation, Kommunikations- und Schulungsmaßnahmen.

Ein wesentliches Ergebnis ist eine Menge von 33 EGIT-/IT-Governance-Mechanismen in den drei Gruppen, die von De Haes und Van Grembergen (vgl. [De Haes & Van Grembergen 2009]) identifiziert wurden und sowohl von ihnen als auch von anderen Autoren in empirischen Studien analysiert und auf ihren Beitrag für eine effektive und effiziente IT-Governance hin untersucht worden sind und in aktuellen Arbeiten untersucht werden (siehe Tab. 1–8).

IT Governance Practice IT-Governance-Mechanismen		
IT governance structures Strukturen	**IT governance processes** Prozesse	**IT governance relational mechanisms** Beziehungsmechanismen
IT strategy committee at level of board of directors IT-Strategieausschuss auf Vorstandsebene	**Strategic information systems planning** Strategische Informationssystem-planung	**Job-rotation** Job-Rotation
IT expertise at level of board of directors IT-Kompetenz auf Vorstandsebene	**IT performance measurement (e.g. IT balanced scorecard)** IT-Leistungsmessung (z.B. IT Balanced Scorecard)	**Co-location** IT-Personal in Fachabteilung u/o vice versa
(IT) audit committee at level of board of directors (IT-)Prüfungsausschuss auf Vorstandsebene	**Portfolio management (incl. business cases, ROI, payback)** Portfoliomanagement (inkl. Business Cases, ROI, Payback)	**Cross-training** Cross-Training/Hospitation u.Ä.
CIO on executive committee CIO im Vorstand	**Charge back arrangements – total cost of ownership (e.g. activity based costing)** Verrechnungskosten – Total Cost of Ownership (z.B. Prozesskostenrechnung)	**Knowledge management (on IT governance)** Wissensmanagement (zu IT-Governance)
CIO reporting to CEO and/or COO CIO-Berichterstattung an CEO und/oder COO	**Service level agreements** Service-Level-Vereinbarungen	**Business/IT account management** Business/IT-Account-Management
IT steering committee (IT investment evaluation/prioritization at executive/senior management level) IT-Lenkungsausschuss (IT-Investitions-bewertung/Priorisierung auf Führungs-ebene)	**IT governance framework COBIT** IT-Governance-Framework COBIT	**Executive/senior management giving the good example** Executive/Senior Management mit gutem Beispiel vorangehen
IT governance function/officer IT-Governance-Funktion/-Beauftragter	**IT governance assurance and self-assessment** IT-Governance-Assurance und Self-Assessments	**Informal meetings between business and IT executive/senior management** Informelle Treffen zwischen Fach- und IT-Führungskräften/Senior Management
Security/compliance/risk officer Beauftragter für Sicherheit/ Compliance/Risiko	**Project governance/management methodologies** Project-Governance/Management-methoden	**IT leadership** IT-Leadership
IT project steering committee IT-Projekt-Lenkungsausschuss	**IT budget control and reporting** IT-Budgetkontrolle und Reporting	**Corporate internal communication addressing IT on a regular basis** Unternehmensinterne Kommunikation, die regelmäßig IT-Themen adressiert
IT security steering committee Lenkungsausschuss IT-Sicherheit	**Benefits management and reporting** Management des Wertbeitrags und Reporting	**IT governance awareness campaigns** IT-Governance-Aufklärungskampagnen

→

IT Governance Practice IT-Governance-Mechanismen		
Architecture steering committee Lenkungsausschuss Architektur		
Integration of governance/alignment tasks in roles & responsibilities Integration von Governance-Alignment in Rollen & Verantwortlichkeiten		

Tab. 1–8 *EGIT-/IT-Governance-Mechanismen nach Van Grembergen und De Haes*

1.7 Verständnis von IT-Governance in diesem Buch

1.7.1 Vorüberlegungen

Unterschiedliche Perspektiven

Wie die Ausführungen zum Begriff der IT-Governance in den vorherigen Abschnitten und zu den unterschiedlichen Ansätzen und Modellen gezeigt haben, gibt es zahlreiche Blickwinkel auf IT-Governance. Die einzelnen Definitionen und Ansätze setzen unterschiedliche inhaltliche Schwerpunkte und priorisieren verschiedene Handlungsfelder. Diese Verschiebung von Perspektiven und neuen Fokussierungen im Zeitablauf verweisen auch immer auf Veränderungen im praktischen Handlungsbedarf und damit auf notwendige Anpassungen der Aufgaben der IT-Governance, was in dem hier entwickelten Verständnis reflektiert werden soll.

Begriffskombinationen

Besonders deutlich zeigt sich dies daran, dass an verschiedenen Stellen der Begriff »IT-Governance« als zu eng betrachtet und abgelöst wird:

- *Corporate Governance of IT*

  Die ISO/IEC 38500:2008 spricht von »Corporate Governance of IT«. Diese Sichtweise in der ersten Version der Norm adressiert die Governance der Managementprozesse, die sich auf die Informations- und Kommunikationsservices einer Organisation richten. Wie in Abschnitt 1.4 beschrieben, wird durch die Definition hervorgehoben, dass IT-Governance einen Teilbereich der Corporate Governance darstellt.

- *Governance of IT for the Organization*

  »Governance of IT for the Organization«: Diese Bezeichnung wird von der aktuellen Version der Norm ISO/IEC 38500:2015 gewählt. Im Begriffsteil der Norm wird klargestellt, dass die Bezeichnung synonym mit »Enterprise Governance of IT« zu verstehen ist (vgl. [ISO/IEC 38500], S. 2). Damit kommt zum einen zum Ausdruck, dass die ISO/IEC 38500 neben Unternehmen Organisationen aller Art adressiert. Zum anderen wird in der zweiten Version der Norm mehrmals betont, dass die Leitungsorgane vor allem Compliance-Risiken in der Unternehmens-IT durch die Umsetzung der in der Norm

enthaltenen Empfehlungen begegnen können (vgl. [ISO/IEC 38500], S. 5).

»Enterprise Governance of IT« (EGIT)

- Die von De Haes u.a. gewählte Bezeichnung »Enterprise Governance of IT« (EGIT)« dient vor allem dazu, die Beschränkung der Perspektive auf »die IT« aufzulösen und damit zu vermeiden, dass sich die Leitungsorgane des Unternehmens nicht für die Unternehmens-IT verantwortlich fühlen (siehe auch Abschnitt 1.6). Es sollte verdeutlicht werden, dass die Governance der IT eben nicht nur die IT-Abteilung betrifft, sondern das gesamte Unternehmen, da die Geschäftsprozesse insgesamt und durchgängig von IT-Systemen und -Services unterstützt werden (vgl. [De Haes et al. 2020a], S. 3 f.).

I&T Governance

- »I&T Governance« bzw. »Enterprise Governance of Information & Technology«: Das Verständnis der ISACA hat sich darüber hinaus noch insofern gewandelt, als dass neben der Technologie auch der Rohstoff »Information« explizit berücksichtigt wird. Damit hat COBIT eine umfassende Entwicklung durchlaufen, von einem Werkzeug für Revisoren und IT-Prüfer über ein IT-Governance-Framework hin zu einem Ansatz, der das gesamte Unternehmen abdeckt und sich nicht nur auf die IT-Funktion, sondern auf alle Technologien und die gesamte Informationsverarbeitung bezieht, die das Unternehmen zur Erreichung seiner Ziele einsetzt, unabhängig davon, wo sie im Unternehmen angesiedelt ist (vgl. [ISACA 2020a], S. 17).

In diesem Buch verwenden wir weiterhin den Begriff »IT-Governance« – auch im Titel – und bevorzugen, keine weitere Begriffsinnovation hinzuzufügen. Zum einen, weil sich im Deutschen keine Entsprechung zu den zuvor genannten Phrasen und Formulierungen anbietet und etabliert hat. Zum anderen, weil beispielsweise »Governance der Unternehmens-IT« sich nur auf erwerbswirtschaftliche Betriebe bezöge und damit öffentliche Unternehmen und Non-Profit-Organisationen ausschließen würde.

Allerdings meinen wir »IT-Governance« in einem umfassenden Verständnis, das die Fachdiskussion der letzten 20 Jahre integriert und die aktuellen Herausforderungen und Anforderungen an die Planung, Steuerung und Überwachung der Unternehmens-IT adressiert. Im Folgenden wird dies mit einer eigenen Definition und durch die Formulierung von Prinzipien verdeutlicht.

»Schlüsseldimensionen« nach Gregory et al.

Die Verschiebungen und Erweiterungen im Verständnis von IT-Governance werden ebenfalls in dem bereits referenzierten Beitrag von ([Gregory et al. 2018], S. 1227) analysiert. Für ihre historische Betrachtung und den Vergleich von Definitionen und Konzepten identifizieren sie drei sogenannte Schlüsseldimensionen:

Focus – »what to govern«

Als Fokus (»Focus« – »what to govern«) bezeichnen sie den Gegenstand der IT-Governance, d.h., welche IT-bezogenen Aktivitäten und Artefakte mit der Unternehmensstrategie und den Unternehmenszielen in Einklang gebracht werden sollen, und nennen IT-Strategie, Infrastruktur, Systeme und IT-Investitionen als Beispiele. Diese Dimension weist eine erkennbare Nähe zu den Entscheidungsdimensionen, die Weill et al. nennen, auf (siehe Abschnitt 1.3). Allerdings zeigt sich auch, dass in der Literatur – je nach Erkenntnisinteresse – andere Aktivitäten und Artefakte betrachtet werden. Zuvor wurde bereits beschrieben, dass beispielsweise »Information« verstärkt in den Fokus gerückt ist; an anderer Stelle werden »Stakeholder« als relevante Artefakte einbezogen [Tiwana et al. 2013]. Der so beschriebene Fokus der IT-Governance dürfte im Zeitablauf mit dem Aufkommen neuer Schwerpunkte, Technologien und ggf. Managementkonzepte dynamisch sein. In unserem Verständnis von IT-Governance adressieren wir das »what to govern« als »Handlungsfelder«.

Scope – »who to govern«

Unter Umfang der IT-Governance (»Scope« – »who to govern«) verstehen Gregory et al. Akteure und Interessengruppen, die sicherstellen, dass die IT einen Beitrag zur Organisation leistet. Wie zuvor skizziert, hat sich der »Scope« in der Hinsicht verschoben, dass zunehmend über »die IT« als organisatorische Einheit hinaus die Geschäftsseite und die Unternehmensleitung einbezogen und deren Bedeutung für die IT-Governance hervorgehoben werden. In unserem Verständnis von IT-Governance adressieren wir verschiedene Akteure und Stakeholder und ihre unterschiedlichen Rollen.

Patterns – »how to govern«

Als Muster der IT-Governance (»Patterns« – »how to govern«) werden Maßnahmen bezeichnet, die eingerichtet und definiert werden, um »wünschenswerte« IT-bezogene Aktivitäten und Ergebnisse zu gewährleisten. Gregory et al. beziehen sich hier auf die von Van Grembergen et al. (siehe Abschnitt 1.6) identifizierten und in vielen Studien verwendeten Mechanismen[5] (Strukturen, Prozesse, Beziehungsmechanismen). In unserem Verständnis von IT-Governance betrachten wir diese ergänzt um weitere Maßnahmen wie zum Beispiel Leadership (vgl. [ITGI 2001]), Grundsätze und Verfahren (vgl. [Meyer et al. 2003]), Policies und Richtlinien (vgl. [ISO/IEC 38500]) sowie Managementsysteme (vgl. [Peterson 2004], S. 8).

5. Mittlerweile hat sich in der akademischen Literatur an dieser Stelle der Begriff »Mechanismus« (mechanism) als Terminus technicus etabliert und wird in vielen Publikationen verwendet. Zuvor war das Gemeinte mit »IT Governance Practices« bezeichnet worden (vgl. [De Haes & Van Grembergen 2008 und 2009]). Insbesondere in seiner deutschen Übersetzung ist nach Ansicht der Verfasser der Begriff »Mechanismen« nicht besonders intuitiv. Wir verwenden ihn jedoch, um anschlussfähig an die Fachdiskussion zu sein.

Zweck – »why to govern«

Nach Ansicht der Verfasser und für unser Verständnis bietet es sich darüber hinaus an, die genannten »Schlüsseldimensionen« um eine explizite Beschreibung der Ziele bzw. des Zwecks zu erweitern (»why to govern«). Zwar definieren Gregory et al. ([Gregory et al. 2018], S. 1227) IT-Governance als den »Rahmen für Entscheidungsrechte und Rechenschaftspflichten«, der »dazu dient, das Alignment der IT-bezogenen Aktivitäten mit der Strategie und den Zielen der Organisation sicherzustellen«. Jedoch ist Alignment nach Ansicht der Verfasser nicht ein finales Ziel, sondern »Mittel zum Zweck« und in diesem Sinne eher ein Zwischenziel.

1.7.2 Darstellung unseres Verständnisses von IT-Governance

Anknüpfend an die Vorüberlegungen sowie die Darstellung der Definitionen und Konzepte in diesem Kapitel wird im Folgenden das IT-Governance-Verständnis für dieses Buch beschrieben und definiert. Es benennt neben einer allgemeinen Charakterisierung die Komponenten (how), den Zweck (why), Handlungsfelder (what) sowie Akteure (who):

IT-Governance ist der Ordnungsrahmen für die gesamte IT einer Organisation und als solcher Bestandteil der Corporate Governance.

Komponenten des Ordnungsrahmens

Er besteht aus Mechanismen (Prozesse, Strukturen, Beziehungsmechanismen) und Maßnahmen (Regelungen, Managementsystemen, …), die ein ganzheitliches und balanciertes System bilden.

Zweck von IT-Governance

Er ist so zu gestalten und zu definieren, dass die Zielerreichung der Organisation sichergestellt wird, d.h. Ziele erreicht werden und die Zielerreichung nicht gefährdet wird. Die Ziele werden als Interessen und Anforderungen von Stakeholdern und der Umwelt eingebracht und sind durch die IT-Governance abzustimmen und festzulegen.

Handlungsfelder der IT-Governance

Der Ordnungsrahmen fokussiert die gesamte IT, d.h., er bezieht sich auf Handlungsfelder, die sich aus den Elementen des Informationssystems einer Organisation ergeben.

Akteure

Da IT die gesamte Organisation durchdringt (Informationsverwendung/-verarbeitung und Technologie), betrifft auch die IT-Governance die gesamte Organisation; sie ist entsprechend auf der Leitungsebene angesiedelt (bzw. anzusiedeln). Der Ordnungsrahmen wird von den Leitungsorganen und ggf. weiteren Akteuren gestaltet und definiert, die auch die Umsetzung von Mechanismen und Maßnahmen bzw. deren Beachtung und Einhaltung überwachen.

Zwecke der IT-Governance

Mit Blick auf die Zwecke ist das formulierte Verständnis bewusst offen. In den obigen Definitionen anderer Autoren werden verschiedene Zwecke genannt, die von dem eher vagen »erwünschten Verhalten bei der Nutzung von IT« über die Unterstützung von Zielen und Strategien bis hin zu sehr konkreten organisatorischen und ökonomischen Zielen gehen.[6] Aus unserer Sicht scheint es passend, als generischen Zweck der IT-Governance die Unterstützung einer Organisation mit Blick auf die Erreichung ihrer (v.a. strategischen) Ziele anzusehen. Hierbei ist – wie erwähnt und in den Abschnitten 2.2 und 2.6.2 vertieft diskutiert – Alignment »Mittel zum Zweck«. Welche konkreten Ziele der IT dann aus übergeordneten Zielen resultieren, wird für verschiedene Organisationen unterschiedlich sein.

Informationssystem (IS) einer Organisation

Darüber hinaus ergeben sich nach dem hier vertretenen Verständnis Handlungsfelder der IT-Governance u.a. durch die Elemente eines (betrieblichen) Informationssystems. Allerdings wird – obwohl zentral in der Wirtschaftsinformatik – der Begriff »Informationssystem« recht unterschiedlich definiert (vgl. [Ferstl & Sinz 2013], S. 11 f.). So sind bei ([Schwarzer & Krcmar 2014], S. 9) »Informationssysteme … sozio-technische Systeme, die menschliche und maschinelle Komponenten (Teilsysteme) umfassen«; dabei verwenden sie den Begriff Informationssystem synonym zu »Anwendungssystem«.

Andere Autoren verstehen unter Informationssystem »das Teilsystem eines Unternehmens bzw. Unternehmensausschnitts …, dessen Aufgaben auf Informationen ausgerichtet sind« ([Benker & Jürck 2016], S. 25 ff.]; ähnlich [Ferstl & Sinz 2013], S. 35). Es umfasst alle zur Erfüllung der informationsbezogenen Aufgaben erforderlichen Elemente bzw. konkret die »vorhandenen Ressourcen, d.h. die Daten, die Datenbank-Software, die nötige Rechner-Hardware, die Personen, welche die Daten benutzen und verwalten, die relevante Anwendungssoftware sowie die Programmierer, die diese entwickeln« [Vossen 2008].

---

6. Aus den Definitionen in Tabelle 1–2: »desirable behavior« (erwünschtes Verhalten); »use of IT is directed and controlled« (Nutzung von IT wird gesteuert und kontrolliert); »organisation's IT sustains and extends the organisation's strategies and objectives« (IT unterstützt die Strategien der Gesamtorganisation); »control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT« (die Formulierung und Umsetzung der IT-Strategie zu kontrollieren und auf diese Weise die Integration von Geschäft und IT zu gewährleisten); IT-Einsatz, sodass »die Geschäftsziele abgedeckt, Ressourcen verantwortungsvoll eingesetzt und Risiken angemessen überwacht werden«; »enable both business and IT stakeholders to execute their responsibilities in support of business/IT alignment, and the creation and protection of IT business value« (sowohl die Geschäfts- als auch die IT-Akteure sind in der Lage, ihre Aufgaben zur Abstimmung von Business und IT sowie zur Schaffung und zum Schutz des Wertbeitrags der IT wahrzunehmen).

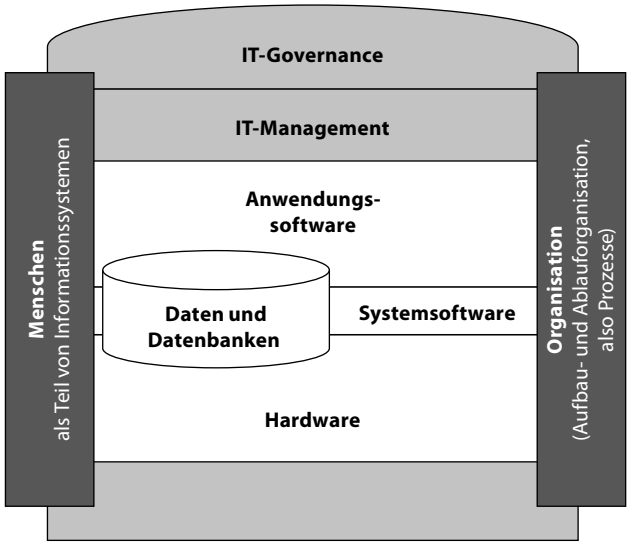
IS im engeren Sinne

Gemäß der ersten Auffassung könnte man von »Informationssystem im engeren Sinne« sprechen und davon, dass eine Organisation viele Informationssysteme für verschiedene Einsatzbereiche hat (operative, analytische, im Rechnungswesen etc.) – so auch ([Hansen et al. 2019], S. 4 ff.). Dadurch, dass der Begriff aber synonym zu Anwendungssystem ist, ist eigentlich einer der beiden Begriffe entbehrlich.

IS im weiteren Sinne

Die zweite Begriffsauffassung ließe sich entsprechend als »Informationssystem im weiteren Sinne« bezeichnen; sie beinhaltet, dass man sinnvollerweise davon spricht, dass eine Organisation *ein* Informationssystem hat – bestehend aus den o.g. Elementen. Seine Zwecke sind vielfältig, beispielsweise Erfüllung von Anforderungen und Informationsbedarfen, Unterstützung oder Automatisierung von Geschäftsaktivitäten und Erreichung der Unternehmensziele (vgl. [Vossen 2008]).

Abb. 1–5
Informationssystem einer Organisation



IT-Governance und Informationssystem

Das IT-Governance-Verständnis in diesem Buch greift auf die zweite Begriffsauffassung zurück. Abbildung 1–5 veranschaulicht diese. Ein Informationssystem besteht demnach aus *Hardware*, *Software* und *Daten/Datenbanken* sowie *Menschen*, die die genannten Elemente nutzen, betreiben und verwalten, ihren Einsatz steuern und kontrollieren und/oder entwickeln bzw. weiterentwickeln. Teil des Informationssystems ist auch eine *Organisation* im Sinne von organisatorischen Regelungen für Aufbau- und Ablauforganisation mit Blick auf die Nutzung, den Betrieb, die Entwicklung und das Management der Elemente oder von Kombinationen der Elemente. *IT-Governance* und *IT-Management* sind dann die »verbindende Klammer« oder eben der Ordnungsrahmen, der die

Zielerreichung des Unternehmens durch die Steuerung und Kontrolle des Informationssystems und seiner Komponenten unterstützt.

Handlungsfelder der IT-Governance und Informationssystem

Dem Systemgedanken folgend können aus den Elementen eines Informationssystems Teilsysteme gebildet werden. Diese Teilsysteme oder auch die einzelnen Elemente werden hier als Handlungsfelder der IT-Governance betrachtet (siehe insbesondere Abschnitt 1.8): So bezieht sich »Data Governance« vornehmlich auf »Daten/Datenbanken« sowie »Menschen« und organisatorische Regelungen mit Blick auf Daten; das Handlungsfeld »Stakeholder« fokussiert insbesondere die IS-Komponente »Menschen« (Akteure und Interessengruppen); »IT-Investitionen« sind die Verwendung finanzieller Mittel für Infrastrukturen und/oder Anwendungssysteme, die selbst aus »Hardware«, »Software« und »Daten« bestehen und durch die ein Wertbeitrag erzielt werden soll.

Zwar gelingt durch den gewählten Fokus auf das Informationssystem einer Organisation keine vollkommen konsistente Begründung und Ableitung aller in der Literatur und auch in diesem Buch angesprochenen (und denkbaren) Handlungsfelder oder »Domänen« (im Sinne von Weill et al.) der IT-Governance. Gleichwohl scheint uns die Systemmetapher zweckmäßig, da sie zum einen verdeutlicht, dass sämtliche technischen und menschlichen Systemelemente einer Organisation, die mit Informationen befasst sind, für die IT-Governance relevant sind oder sein können. Zum anderen verdeutlicht sie, dass das Informationssystem und der Ordnungsrahmen, den die IT-Governance setzt, selbst wiederum Elemente eines übergeordneten Systems sind, nämlich des Systems Unternehmen und der Corporate Governance.

Abbildung 1–6 fasst das formulierte Verständnis zusammen und benennt – neben den Zwecken der IT-Governance und den Komponenten des Ordnungsrahmens – auf der untersten Ebene die in diesem Buch adressierten Handlungsfelder. Dabei wird auch angedeutet, dass die genannten Zwecke, Komponenten und Handlungsfelder nicht als abgeschlossene Listen angesehen werden.

Abb. 1–6 *Das IT-Governance-Verständnis in diesem Buch*

1.7.3 Prinzipien gemäß dem IT-Governance-Verständnis

Neben dieser begrifflichen Einordnung orientiert sich das Verständnis von IT-Governance in diesem Buch an den im Folgenden dargestellten Prinzipien. Sie knüpfen an die bis hierhin diskutierte Literatur an und ergeben sich aus dieser sowie aus der Definition des vorangegangenen Abschnitts; darüber hinaus reflektieren sie praktische Erfahrungen. Die bewusst normative Formulierung als Prinzipien mag auch geeignet sein, eine kritische Reflexion und Diskussion zu fördern oder sogar direkten Widerspruch zu provozieren.

Während die ersten fünf Prinzipien die grundlegende Positionierung und Ausrichtung einer IT-Governance betrachten, adressieren die weiteren Prinzipien die aktuell im Mittelpunkt stehenden Zwecke und Ziele von IT-Governance. Sie sollen demnach den im nachfolgenden Abschnitt 1.8 diskutierten Handlungsfeldern als übergeordnet vorangestellt werden.

Prinzipien für IT-Governance

1. IT-Governance ist integraler Bestandteil der Corporate Governance.

Eine IT-Governance kann nicht losgelöst von der Corporate Governance gestaltet, implementiert und praktiziert werden. Vielmehr muss sich das gesamte System der IT-Governance in das System der Corporate Governance integrieren. Dies fängt beim Governance-Verständnis an und umfasst in der Folge die Konsistenz von Zielen und Zwecken, Handlungsfeldern, Maßnahmen und Mechanismen sowie die Einbindung von Stakeholdern und Akteuren.

2. IT-Governance ist von den Leitungsorganen und dem IT-Management gleichermaßen wahrzunehmen.

IT-Governance liegt nicht allein und zuvorderst in der Verantwortung des CIO und des Managements der einzelnen IT-Bereiche. Die Leitungsorgane (Aufsichtsrat, CEO und weitere Mitglieder der Unternehmensleitung) müssen sich insbesondere in Zeiten der digitalen Transformation mit der Planung, Steuerung und Überwachung der Unternehmens-IT befassen und mit dem IT-Management (CIO, IT-Bereichsleitungen) sowie mit Zentralfunktionen, insbesondere Corporate Compliance und Corporate Riskmanagement, kooperieren. Gerade dem Zusammenspiel zwischen CEO und CIO kommt eine entscheidende Bedeutung zu (vgl. Abschnitt 3.3.2).

3. IT-Governance hat die IT-Stakeholder an der Entwicklung der Unternehmens-IT zu beteiligen.

Governance hat generell zum Ziel, das Zusammenwirken zahlreicher verschiedener Akteure abzustimmen – sei es in der Politik, in Unternehmen oder mit Blick auf die Unternehmens-IT. Die IT-Governance hat daher die Identifizierung der wesentlichen IT-Stakeholder (und ihrer Interessen) zu initiieren und ein Stakeholder-Management zu etablieren. Das bedeutet, dass relevante Stakeholder zum einen an der Entwicklung und Definition von IT-Zielen und -Strategien zu beteiligen sind. Zum anderen sind Stakeholder eine notwendige Voraussetzung für den Geschäftserfolg und den Erfolg der IT, sodass eine Stakeholder-Governance deren Einbeziehung sicherstellen muss.

4. IT-Governance ist auf die gesamte Unternehmens-IT gerichtet.

Als Unternehmens-IT (oder allgemeiner: IT einer Organisation) wird die gesamte Bandbreite der digitalen Lösungen verstanden, unabhängig davon, wo oder von wem sie im Unternehmen geplant, beschafft, entwickelt, betrieben oder genutzt werden. Zuvor wurde auf den Begriff des Informationssystems Bezug genommen, der die Elemente feingranular benennt. Diese werden zu Anwendungssystemen, Infrastruktur, (Business-/IT-)Services und/oder IT-Produkten zusammengefügt, die direkt oder indirekt der Informationsverwendung/-verarbeitung in einem umfassenden Sinne dienen.[7] Hieraus werden die oben genannten »Handlungsfelder« abstrahiert. Dabei ist unsere Auflistung und Betrachtung von Handlungsfeldern nicht als abschließend zu betrachten, sondern sie deckt die aus unserer Sicht zurzeit wichtigsten Themen ab.

5. IT-Governance und IT-Management sind klar zu trennen.

IT-Governance ist als Verantwortung und ganzheitliches Handlungsfeld dem IT-Management übergeordnet. Das IT-Management vollzieht sich in dem von der IT-Governance geschaffenen Ordnungsrahmen. Entsprechend sind Verantwortlichkeiten und Aufgaben von IT-Governance und IT-Management einerseits klar voneinander zu trennen, andererseits über definierte Schnittstellen miteinander zu verbinden.[8]

---

7. »Umfassenden Sinne« deshalb, weil hier nicht versucht werden soll, alle möglichen Tätigkeiten mit Blick auf Information aufzulisten. Eine recht umfangreiche Übersicht über mögliche »Tätigkeiten« mit Blick auf Information bietet: *https://glossary.atis.org/glossary/information-system/*.
8. Theoretisch-konzeptionell mag diese Unterscheidung zwar grundsätzlich einleuchtend sein – im Unternehmensalltag wird die Grenze jedoch oft mit Blick auf konkret zu treffende Entscheidungen verschwimmen. So wird beispielsweise die Entscheidung einer Organisation, »den Weg in die Cloud« anzutreten, aufgrund ihrer Tragweite (u. a. finanziell und organisatorisch) gewiss oft als eine »Governance-Entscheidung« angesehen; nach der hier geforderten klaren Trennung sollte IT-Governance jedoch »nur« den Prozess und die Entscheidungsrechte definieren, in deren Rahmen das IT-Management Entscheidungen trifft. Die scheinbare konzeptionelle Unschärfe dürfte zum Teil aber auch dadurch entstehen, dass dieselben Akteure einerseits den Ordnungsrahmen setzen, andererseits aber eben auch – beispielsweise aufgrund der Investitionssumme – die Entscheidung treffen.

6. IT-Governance ist ein Ordnungsrahmen für den erfolgreichen IT-Einsatz.

IT-Governance ist weder eine Abteilung noch eine isolierte Aufgabe. Sie ist der faktische Ordnungsrahmen, der von den Leitungsorganen und den Führungskräften der IT geschaffen und gesetzt wird, um das Informationssystem zweckmäßig und zielorientiert (also erfolgreich) zu gestalten. In einer statischen Sichtweise meint IT-Governance dann den Ordnungsrahmen, der vor dem Hintergrund bestimmter Ziele definiert ist und für eine bestimmte Zeit Gültigkeit hat. In einer dynamischen Sicht wird deutlich, dass dieser Ordnungsrahmen vor dem Hintergrund von Zielen zum einen eingeführt und angepasst (weiterentwickelt) werden muss und zum anderen seine Umsetzung und das Handeln der Akteure hinsichtlich der Einhaltung von Mechanismen und Maßnahmen zu überwachen ist.

In unserer Definition wurde die Unterstützung der Zielerreichung als generischer Zweck der IT-Governance genannt und argumentiert, dass verschiedene Organisationen jeweils verschiedene konkrete Ziele verfolgen. Dies ergänzend und konkretisierend lassen sich Zielkategorien aus der IT-Governance-Literatur, die ein hohes Maß an Allgemeingültigkeit haben, nennen. Nach ([De Haes et al. 2020a], S. 3): »Essentially, the ultimate goal of governing IT is to enhance IT's delivery of business value and to mitigate IT risks«, wobei sie die zwei genannten Ziele noch um »Resource management« und »Performance measurement« erweitern. In den folgenden Prinzipien wird auf diese Zielkategorien Bezug genommen. Gleichwohl scheint uns wichtig, darauf hinzuweisen, dass die Nennung von Zielen und Zwecken keineswegs als abschließend anzusehen ist und dass – je nach Unternehmensspezifika – durchaus andere Ziele von einschlägiger Bedeutung sein können (denkbar und naheliegend sind zurzeit sicherlich Informationssicherheit und Cybersecurity oder auch Nachhaltigkeit).

7. IT-Governance zielt auf die Sicherung und Steigerung des Wertbetrags der IT sowie auf die effiziente Nutzung von Ressourcen.

Zum einen manifestiert sich erfolgreicher IT-Einsatz darin, dass einerseits positive Wertbeiträge und Nutzeneffekte erzielt werden, indem die Unternehmensstrategie und die Erreichung der Unternehmensziele unterstützt werden, und andererseits auf eine optimale Ressourcennutzung im Sinne eines Effizienzgedankens hingearbeitet wird.

Inzwischen ist durch empirische Studien gut belegt, dass eine bessere IT-Governance einen mittelbaren oder unmittelbaren Einfluss auf

den Wertbeitrag der IT hat, sie also mit Blick auf den Wertbeitrag ein entscheidendes »Mittel zum Zweck« ist.

8. IT-Governance fokussiert IT-Risiken und IT-Compliance, ist aber nicht darauf beschränkt.

Zum anderen manifestiert sich erfolgreicher IT-Einsatz darin, dass Risiken der IT angemessen gemanagt werden und Compliance der IT (und auch durch IT) hergestellt wird. Risiken und Compliance werden vom DCGK miteinander in Beziehung gesetzt und deswegen oft in einem Zuge mit Governance genannt (»GRC«). Insofern ist auch von »IT-GRC« als »Trias« die Rede (siehe Abb. 6–2). Auch wenn dieser Zusammenhang einer besonderen Aufmerksamkeit bedarf und aufgrund von hohen IT-Risiken und zunehmenden gesetzlich-regulatorischen Anforderungen zweifellos seine Berechtigung hat, wäre eine Begrenzung von IT-Governance auf IT-GRC eine Verkürzung, da dadurch zahlreiche Handlungsbereiche und weiter gehende Zwecke der IT-Governance unbeachtet blieben.

9. IT-Governance hat ein ganzheitliches Business/IT-Alignment sicherzustellen.

Da ein Wertbeitrag der IT nur im Zusammenspiel von Geschäfts- und IT-Bereichen entsteht, gilt es, das Zusammenspiel beider Seiten zu gestalten bzw. zu harmonisieren. Dies ist eine originäre Governance-Aufgabe, weil verschiedene Akteure mit ihren verschiedenen und sich möglicherweise widersprechenden Zielen, Zwecken und Interessen zu koordinieren sind. Dieses »In-Einklang-Bringen« beider Seiten wird auch als Business/IT-Alignment bezeichnet. Dessen direkte (positive) Wirkung auf den Wertbeitrag der IT ist in vielen Studien empirisch belegt. Entsprechend kann man annehmen, dass auch andere Zielkategorien besser adressiert werden, wenn das Alignment von Business und IT verbessert wird bzw. einen höheren Reifegrad aufweist.

Zunehmend setzt sich die Erkenntnis durch, dass sich ein Business/IT-Alignment nicht nur auf die Ebene der Strategien und Ziele bezieht, sondern auch andere Aspekte »in Einklang zu bringen« sind, sodass es mehr und mehr als ein vielschichtiges Konzept angesehen wird, das auch organisatorische, kulturelle und soziale Aspekte umfasst.

10. IT-Governance muss vor dem Hintergrund interner und externer Herausforderungen Flexibilität und Stabilität balancieren.

Die IT eines Unternehmens muss zahlreichen Anforderungen genügen; entsprechend muss die IT-Governance verschiedenste Interessen austarieren. Dabei soll sie zum einen ein stabiler Ordnungsrahmen sein, der angemessen Orientierung bietet. Zum anderen muss sie vor dem Hintergrund neuer Ziele und Zwecke (beispielsweise digitale Transformation, Analytik, Sicherheit und Nachhaltigkeit) sowie Mechanismen und Maßnahmen (beispielsweise agiler Methoden und organisationaler Ambidextrie) sich aber auch als anpassbar und flexibel erweisen und bereit sein, auf diese angemessen zu reagieren. Auch dieser Gegensatz zwischen Stabilität und Flexibilität erfordert ein Austarieren, das im Rahmen eines kontinuierlichen Verbesserungsprozesses der IT-Governance selbst zu gestalten ist.

11. IT-Governance muss sicherstellen, dass die digitalen Chancen genutzt werden.

Die Entwicklung schreitet mit technologischen Neuerungen, wie Cloud Computing, KI, Blockchain, cyberphysischen Systemen oder Quantencomputing, schnell voran und eröffnet Chancen für neue Produkte, Services und datengetriebene Geschäftsmodelle. In diesem Sinne wird in nahezu allen Organisationen die »digitale Transformation« angestrebt oder zumindest diskutiert. Der Einsatz von Informationstechnologie ist allerdings nicht nur ein Technikthema, sondern ihr Zusammenspiel mit und ihre Ausrichtung auf fachliche Prozesse und Aufgaben muss durch Management und Governance geplant, gesteuert und kontrolliert werden. IT-Governance hat in diesem Zusammenhang zu gewährleisten, dass sich das Unternehmen systematisch mit IT-Innovationen auseinandersetzt, deren Potenziale, Risiken und Nutzen bewertet und Neuerungen in abgestimmter Weise im Rahmen eines Portfoliomanagements umsetzt.

Situative Anwendung

Für das einzelne Unternehmen werden nicht alle genannten Prinzipien in der unternehmensindividuellen Ausgestaltung der IT-Governance von gleicher Bedeutung sein. Unternehmen müssen sich somit entscheiden, welchen dieser Prinzipien sie folgen wollen. Die Integration von Corporate und IT-Governance, das Engagement der Leitungsorgane und des IT-Managements sowie das Business/IT-Alignment sind jedoch unverzichtbar für eine effektive IT-Governance.

1.8 Handlungsfelder für IT-Governance

Im Folgenden werden die in Abbildung 1–6 dargestellten Handlungsfelder jeweils kurz beleuchtet. Dies rundet zum einen das einleitende Kapitel ab; zum anderen wird hierdurch ein Ausblick auf die Kapitel 2 bis 9 in diesem Buch gegeben.

1.8.1 Messung und Management des Wertbeitrags der IT im Rahmen der IT-Governance

Wertbeitrag der IT und IT-Governance

Im Standard ISO/IEC 38500 und auch bei Van Grembergen et al. wird deutlich, dass es Aufgabe der IT-Governance ist, die geschäftlichen Anforderungen und Erwartungen der Stakeholder zu erfassen und zu evaluieren sowie – hierauf aufsetzend – Vorgaben für das Management zu machen. Daraus folgt, dass IT-Governance über IT-bezogene Verantwortlichkeiten hinausgeht. Die Anforderungen und Erwartungen von außerhalb der IT beziehen sich typischerweise auf ökonomische und/oder fachliche Ziele und Zwecke, die mit IT-Einsatz und IT-Investitionen angestrebt werden. Regelmäßig fällt hierunter der Wunsch, einen Beitrag der IT für den Unternehmenserfolg zu generieren.

Ungeklärte grundlegende Fragen

Der Wertbeitrag der IT und verwandte Konzepte (beispielsweise »Nutzen«, »Performance« etc.) sind seit vielen Jahren Gegenstand von Diskussionen und wissenschaftlichen Auseinandersetzungen. Gleichwohl sind wesentliche Fragen wie die folgenden kaum eindeutig beantwortet:

- Was versteht man unter Wertbeitrag der IT?
- Wie misst man den Wertbeitrag von IT?
- Wie steuert und realisiert man Wertbeitrag durch IT-Einsatz und IT-Investitionen?
- Welche Mechanismen und Maßnahmen der IT-Governance unterstützen die Generierung eines Wertbeitrags der IT?

Herausforderungen der IT-Governance

Dass solche grundlegenden Fragen nicht eindeutig geklärt sind, bringt verschiedene Herausforderungen für IT-Governance-Verantwortliche in Organisationen mit sich: Sie müssten eine Reihe von unternehmensindividuellen und -spezifischen Festlegungen treffen, um Vorgaben für ein Management des Wertbeitrags zu machen. Entsprechend werden im nächsten Kapitel praktische Anregungen mit Blick auf jene Aspekte gegeben, für die Festlegungen erforderlich erscheinen.

Ausblick auf Kapitel 2

Kapitel 2 betrachtet den Stand der Diskussion in Theorie und Praxis. Am Anfang stehen empirische Befunde, die die aktuellen Erwar-

tungen und Anforderungen an die IT konkretisieren, und der Bezug zwischen diesen und dem Ordnungsrahmen, den die IT-Governance setzt, wird aufgezeigt. Nach einer grundlegenden begrifflichen und methodischen Betrachtung werden Konzepte zur Messung des Wertbeitrags dargestellt und kritisch beleuchtet. Hierbei zeigt sich, dass traditionelle betriebswirtschaftliche Verfahren, die zum Beispiel der Kosten- und Investitionsrechnung entstammen, in der Regel zu kurz greifen. Eine ganzheitliche Planung und Steuerung des Wertbeitrags der IT sollte stattdessen umfassendere Messkonzepte zugrunde legen. Eine Auswahl von in der Literatur zu findenden und etablierten Konzepten zur Steuerung und Verbesserung des Wertbeitrags der IT werden abschließend dargestellt.

1.8.2 Aufgaben und Verantwortlichkeiten der Akteure der Unternehmens-IT und ihre Positionierung in der Organisation

Strukturen als Komponente des Ordnungsrahmens

In der strukturellen Sichtweise von IT-Governance, die in dem Ansatz von Weill et al. im Vordergrund steht, wird ein besonderes Augenmerk auf Entscheidungsrechte und Rechenschaftspflichten gelegt. Auch bei Van Grembergen et al. (siehe Abschnitt 1.6) sind strukturelle EGIT-Mechanismen ein Teil von drei Mechanismen eines IT-Governance-Arrangements. In dem zuvor hier formulierten Verständnis in Abschnitt 1.7.2 steht Struktur neben weiteren Maßnahmen wie Prozessen, Beziehungsmechanismen, Grundsätzen, Richtlinien, Verfahren und Managementsystemen. Diese stellen die wesentlichen Komponenten des Ordnungsrahmens dar, den die IT-Governance bildet.

… zur Erfüllung geschäftlicher Anforderungen und zur Zielerreichung

Zentral ist dabei, die Verantwortungsteilung zwischen den beteiligten Akteuren vor dem Hintergrund der geschäftlichen Anforderungen und der Erwartungen der Stakeholder angemessen und unternehmensspezifisch zu gestalten. Empirische Befunde zeigen in diesem Zusammenhang recht eindeutig, dass eine adäquate Gestaltung der strukturellen Komponente des Ordnungsrahmens zu positiven Effekten führt, u. a. hinsichtlich der Generierung von Wertbeiträgen, der Herstellung von Compliance und der Beherrschung von Risiken. Auch die digitale Transformation von Unternehmen und das Hervorbringen innovativer Lösungen sind Ziele, die durch Veränderungen und Ergänzungen traditioneller Organisationsstrukturen unterstützt werden.

Definition von Rollen und Organisationseinheiten

Konkret ausgeprägt werden die Verantwortungsteilung und die strukturellen Aspekte des Ordnungsrahmens durch die Definition von Rollen und Organisationseinheiten. Als besonders hervorzuhebende Rollen werden der CIO (Chief Information Officer) und der CDO (Chief Digital Officer) betrachtet, die nach aktuellem Verständnis wesentlich für die

Erreichung der genannten geschäftlichen Anforderungen und Ziele sowie zur Herstellung eines stabilen IT-Betriebs sind.

Dabei ist der CIO die Führungskraft, die für die Abstimmung von IT- und Geschäftsstrategien sowie für die Planung, Beschaffung und das Management der Bereitstellung von IT-Services und -Lösungen verantwortlich ist. Der CDO hingegen ist für die Planung, Steuerung und Umsetzung digitaler Initiativen in die Praxis verantwortlich und damit mehr als der CIO für das Hervorbringen und Implementieren von Innovationen.

Ausblick auf Kapitel 3

In Kapitel 3 werden die vielfältigen Aufgaben und Verantwortlichkeiten, die dem CIO bzw. dem CDO im Rahmen der IT-Governance zugewiesen werden können, sowie die Varianten, die sich für die beiden Rollen in der Praxis dadurch ergeben, dargestellt. Es werden die Möglichkeiten und Grundformen ihrer Positionierung in der Unternehmensorganisation und die potenziellen Abgrenzungsprobleme und Konflikte, die auf diese Art und Weise entstehen können, veranschaulicht. Vor dem Hintergrund der digitalen Transformation und des Hervorbringens von Innovationen werden in jüngerer Zeit die bimodale bzw. ambidextrische IT als Ergänzungen vorgeschlagen. Diese Konzepte sind ebenfalls Gegenstand dieses Kapitels.

Neben einzelnen Rollen haben Organisationseinheiten – temporäre wie dauerhafte – wesentliche Bedeutung für die Gestaltung des Ordnungsrahmens der IT-Governance. Wie bereits angemerkt, ist die IT-Governance auf der Leitungsebene einer Organisation anzusiedeln. Dementsprechend werden in Kapitel 3 der Aufsichtsrat und die Unternehmensleitung als Akteure der IT-Governance mit ihren Aufgaben, Verantwortlichkeiten und Entscheidungsrechten diskutiert. Insbesondere Ausschüsse sind, da sie auf unterschiedliche Art und Weise mit Mitarbeitern aus der Unternehmensleitung sowie den Fach- und IT-Bereichen besetzt werden können (siehe die Archetypen in Abschnitt 1.3 bei Weill et al.), von wesentlicher Bedeutung bei der Abstimmung zwischen Fachbereichen und IT. Sie sind damit ein wichtiger Mechanismus zur Herstellung des sogenannten »Business/IT-Alignments« und werden in diesem Sinne betrachtet.

1.8.3 IT-Stakeholder als Adressaten der IT-Governance – Stakeholder in die Entwicklung der Unternehmens-IT einbeziehen

Bedeutung der IT-Stakeholder

Der Wertbeitrag der IT und der gesamte IT-Einsatz werden durch IT-Stakeholder wesentlich beeinflusst. Sich der Bedeutung der IT-Stakeholder bewusst zu werden, ist Aufgabe der für die Steuerung und Überwachung der IT-Verantwortlichen. Grundlage ist die Klärung, welche Stakeholder-Gruppen einbezogen werden sollen. Hierzu ist zwischen internen und externen IT-Stakeholder-Gruppen zu unterscheiden.

- Interne IT-Stakeholder sind Akteure, die dem Unternehmen auf einer gesellschaftsrechtlichen oder arbeitsvertraglichen Basis angehören.
- Externe IT-Stakeholder sind Personen, Gruppen oder Organisationen in der Unternehmensumwelt, mit denen die Unternehmens-IT in Interaktion steht.

IT-Stakeholder

IT-Stakeholder finden sich demnach im Unternehmen und im Unternehmensumfeld. Primäre interne IT-Stakeholder sind z. B. Mitglieder des Aufsichtsorgans oder der Unternehmensleitung und Anteilseigner. Wichtige externe IT-Stakeholder sind aus Sicht einer Organisation z. B. Kunden des Unternehmens, Aufsichtsinstitutionen sowie IT-Hersteller und -Dienstleister, mit denen das Unternehmen eng zusammenarbeitet. Die Ziele der IT-Governance in Bezug auf die IT-Stakeholder gehen in drei Richtungen:

- Erlangen der Unterstützung in der grundsätzlichen Ausrichtung der Unternehmens-IT
- Sicherstellen der Compliance mit Anforderungen externer Stakeholder
- Erreichen einer positiven Einstellung der Stakeholder gegenüber der Unternehmens-IT

Beziehungen zu IT-Stakeholdern

Dort, wo keine aktive Unterstützung durch die Stakeholder erreicht werden kann, muss man sich mit einer neutralen Einstellung begnügen. Wenn primäre Stakeholder ein großes Interesse an der IT und gleichzeitig einen großen Einfluss haben, müssen sich Unternehmens- und IT-Leitung ggf. in der Pflege der Beziehungen zu diesen Stakeholdern engagieren.

Aufgaben der IT-Governance

Aufgaben der IT-Governance in Bezug auf die IT-Stakeholder sind von den Aufgaben des IT-Stakeholder-Managements zu unterscheiden. Die IT-Stakeholder-Governance schafft den Rahmen, in dem sich das IT-Stakeholder-Management vollzieht. Die IT-Stakeholder-Governance trifft hierfür konstitutive Entscheidungen. Am Anfang steht die initiale

Entscheidung, nach einem Stakeholder-Ansatz zu verfahren und hierfür ein systematisches IT-Stakeholder-Management einzurichten. Die Überwachungsaufgabe der IT-Stakeholder-Governance richtet sich auf die Kontrolle, ob und inwieweit Governance-Vorgaben vom IT-Stakeholder-Management eingehalten werden und das IT-Stakeholder-Management insgesamt effektiv und effizient erfolgt. Zur Überwachung des IT-Stakeholder-Managements sind Kennzahlen, die alle Aufgabenbereiche des IT-Stakeholder-Managements abdecken, zu verwenden.

Ausblick auf Kapitel 4

Kapitel 4 stellt die Stakeholder der Unternehmens-IT in den Fokus. IT-Stakeholder werden als Akteure und Adressaten der IT-Governance beschrieben. Zur Orientierung wird eine grundlegende Klassifizierung in interne und externe Gruppen von Stakeholdern verwendet. Nach Klärung der potenziellen IT-Stakeholder werden die Ziele der IT-Governance in Bezug auf die IT-Stakeholder diskutiert. Im Sinne einer Abgrenzung gegenüber dem IT-Stakeholder-Management werden die notwendigen konstitutiven Entscheidungen für das IT-Stakeholder-Management dargestellt. Auch eine Festlegung der für die Aufgaben des IT-Stakeholder-Managements benötigten Qualifikationen und die Überwachung des IT-Stakeholder-Managements werden als Aufgaben der IT-Governance eingestuft und betrachtet.

1.8.4 Organisation der Unternehmens-IT – interne und externe Anforderungen an die IT in Strukturen und Prozessen abbilden

Betroffene Akteure

Um aus der digitalen Transformation des Unternehmens einen maximalen Wertbeitrag der IT zu erreichen, muss – wie dargestellt – das Zusammenwirken der verschiedenen Akteure und Stakeholder organisiert werden. Unter anderem müssen sich Aufsichtsrat und CEO in IT-Themen intensiv engagieren. Hierfür müssen CEO und CIO eine gemeinsame IT-Vision teilen und im Unternehmen durchsetzen. Der CIO oder ein Chief Digital Officer (CDO) wiederum hat die digitale Transformation des Unternehmens voranzutreiben und zu steuern. Dabei erfordert die Entwicklung von digitalen Geschäftsmodellen u. a. die Koordination mit der Organisations-, der Prozess-, der Technologie- und der Mitarbeiterentwicklung. Wesentliche Aufgabe der IT-Governance ist es dabei – im Sinne der oben dargestellten Komponenten des Ordnungsrahmens –, die Verantwortung für die IT und die Zuordnung von Entscheidungsrechten sowie die Zusammenarbeit der Leitungsorgane und ihrer Mitglieder zu organisieren. Dies betrifft ggf. einen Aufsichtsrat, die Unternehmensleitung (mit CEO und CIO) und den CDO.

Organisatorischer Gestaltungsbedarf

Organisatorische Vorgaben, die durch die IT-Governance zu machen sind, betreffen jedoch nicht nur die obersten Führungskräfte und -gremien. Sie beziehen sich auch auf die Zusammenarbeit der Mitarbeiterinnen und Mitarbeiter der IT mit denen der Geschäftsbereiche. In dieser Hinsicht ergeben sich vielfältige weitere Herausforderungen:

- Einführung agiler Methoden,
- Stärkung der IT-Sicherheitsstrukturen und -prozesse,
- Management des Kulturwandels,
- Sicherstellung des Personalaus- und -aufbaus,
- systematisches Skill- und Kompetenzmanagement,
- Optimierung der Business/IT-Schnittstelle und
- Einrichtung flexibler Organisationsstrukturen.

Vor allem die gesetzlich-regulatorisch vorgeschriebenen Stellen der IT-Organisation sind einzurichten, allen voran eine Datenschutzorganisation mit dem Datenschutzbeauftragten an der Spitze.

Konstitutive Festlegungen

Konstitutive Entscheidungsfelder der IT-Organisation richten sich auf die aufbauorganisatorische Anbindung der IT-Abteilung, den Stellenaufbau der IT-Abteilung, die Integration der IT in das Unternehmen, die Gestaltung der IT-Prozesse und die Einrichtung von Stellen und Gremien zur Leitung und Überwachung der IT. Diese organisatorischen Festlegungen zu treffen, ist eine der zentralen Aufgaben der IT-Governance. Die herkömmliche Struktur der IT-Abteilung ist zu verändern, um IT-Innovationen und eine Unterstützung der digitalen Transformation zu bewerkstelligen und um sichere, hochverfügbare und anforderungsgerechte IT-Services zu betreiben. Hierbei hilft vor allem das 3-Linien-Modell als Blaupause für eine grundlegende IT-Governance-Struktur. Für die Gestaltung der IT-Prozesse und eine darauf basierende strategiegerechte Priorisierung kann auf den IT-Governance- und -Management-Standard »COBIT 2019« zurückgegriffen werden.

Herausforderungen der Agilität

Die Einführung agiler Vorgehensmodelle resultiert aus steigenden Anforderungen und Erwartungshaltungen von internen und externen Kunden. Hierauf müssen die IT-Governance-Verantwortlichen reagieren. In agilen Strukturen nehmen vor allem Aufgaben der Kommunikation, der Information und des Wissensmanagements einen größeren Anteil ein. Führungsaufgaben sind auf verschiedene Rollen verteilt. Autonomie wird in Form von Verfügungs- und Entscheidungsbefugnissen gewährt. Zurzeit kommen agile Strukturen vor allem im Bereich der Anwendungsentwicklung und -bereitstellung zum Einsatz; in der Zukunft möglicherweise auch vermehrt bei Transformations- und Innovationsprojekten. Der DevOps-Ansatz – oder gar der DevBizOps-Ansatz – er-

laubt eine schnellere Bereitstellung neuer oder verbesserter Anwendungen. Letztlich muss aber die gesamte Unternehmens-IT agiler werden, um die digitale Transformation erfolgreich bewältigen zu können.

Ausblick auf Kapitel 5

Kapitel 5 vermittelt den aktuellen Stand der für die Unternehmens-IT diskutierten organisatorischen Konzepte, Modelle und Entwicklungslinien. Einführend werden die aktuellen Herausforderungen für die IT-Organisation beschrieben. Als externe Anforderungen stehen die gesetzlich-regulatorischen Anforderungen an die Organisation der Unternehmens-IT im Vordergrund. Eine Strukturierung von IT-Aufgaben und eine darauf aufbauende Organisationsstruktur der IT-Abteilung kann auf die verschiedenen verfügbaren Konzepte zurückgreifen: Plan-Build-Run, Source-Make-Deliver, Innovate-Design-Transform und Plan-Measure-Control. Diese Konzepte werden einzeln vorgestellt und in ein integriertes Modell überführt. Da die Organisation der Unternehmens-IT nicht nur die IT-Abteilung umfasst, wird das weitverbreitete Rollenkonzept, das insbesondere auch in der agilen Organisation Anwendung findet, dargestellt. Für die Eingliederung der Unternehmens-IT wird das 3-Linien-Modell herangezogen. Hieraus ergibt sich eine Grundstruktur für die Steuerung und Überwachung der Unternehmens-IT. Diesbezügliche Aufgaben liegen im Tagesgeschäft wesentlich bei den Leitungsorganen des Unternehmens, d.h. Aufsichtsrat, Unternehmensleitung und einzelnen, unterstützenden Gremien. Konkret werden die C-Rollen des CEO, des CIO und des CDO diskutiert.

1.8.5 IT-Risikomanagement – Managen von Unsicherheit durch Bewertung, Steuerung und Überwachung der Risiken

Bedeutung von IT-Risiken

Gemäß dem zuvor dargestellten Verständnis dient IT-Governance dazu, einen erfolgreichen IT-Einsatz sicherzustellen. Dieser konkretisiert sich in verschiedenen Zielen und Zwecken unter anderem darin, den Wertbeitrag von IT, die Einhaltung von Regulierungen und eben auch IT-Risiken zu bewerten, zu steuern und zu überwachen.

Knapp und kurz formuliert meint Risiko hier die Auswirkung von Unsicherheit auf Ziele, also mögliche Zielabweichungen, die positiv oder negativ ausfallen können.

IT-Risiken als geschäftliche Anforderungen

Die Bedeutung des Managements von Risiken wird in Regularien und Gesetzen sowie in einschlägigen Definitionen von und Ansätzen der IT-Governance unterstrichen:

- So fordert der Deutsche Corporate Governance Kodex [DCGK 2022] in Grundsatz 4, dass der verantwortungsvolle Umgang mit den Risiken der Geschäftstätigkeit eines angemessenen und wirksamen internen Kontrollsystems und Risikomanagementsystems bedarf.

- ISO/IEC 38500 macht deutlich, dass im Rahmen der IT-Governance der Einsatz von IT von einem angemessenen Risikomanagement zu begleiten ist, d.h., dass unter anderem bei der Bewertung von IT- und Anwendungssystemen Risiken einzubeziehen sind, dass diese bewertet werden sollen und zu kommunizieren sind.
- Ähnlich schlägt COBIT Praktiken und Aktivitäten zum Evaluieren (evaluate), Vorgeben (direct) und Überwachen (monitor) von Risiken vor.
- Hinzu kommen branchenspezifische Regulierungen wie zum Beispiel in der Finanzbranche die MaRisk (Mindestanforderungen an das Risikomanagement) und die BAIT (Bankaufsichtliche Anforderungen an die IT), die das Risikomanagement adressieren.
- Neben Regulierungen spielen jedoch auch die Risikoerwägungen und -präferenzen der relevanten Stakeholder einer Organisation und ihre Erwartungen mit Blick auf den Umgang mit Risiken eine wesentliche Rolle.

IT-Risiken als Handlungsfeld der IT-Governance

Vor diesem Hintergrund muss IT-Governance sich mit der Auswirkung von Unsicherheit auf die vielfältigen Ziele und geschäftlichen Anforderungen befassen und den Ordnungsrahmen so gestalten, dass verantwortungsvoll mit ihnen umgegangen wird. IT-Risiken sind entsprechend ein wesentliches Handlungsfeld der IT-Governance.

Ausblick auf Kapitel 6

Kapitel 6 beleuchtet den State of the Art zum Thema »IT-Risiken« im Kontext der IT-Governance. Fokussiert werden die Planung, Steuerung und Überwachung des Risikomanagements, da diese einen wesentlichen Teil der Governance-Verantwortung ausmachen. Neben einer Darstellung von Grundlagen, die die Definition und Systematisierung von Risiken umfassen, wird betrachtet, wie IT-Risiken in verschiedenen Ansätzen der IT-Governance behandelt werden. Hierauf aufsetzend werden die Aufgabenbereiche der Governance von IT-Risiken beschrieben, die vielfältige Aspekte, wie zum Beispiel Ziele und strategische Aspekte, aber auch »weiche Mechanismen«, wie Risikokultur und Risikobewusstsein, umfassen. Im Zusammenhang mit der Organisation des IT-Risikomanagements werden strukturelle und prozessorientierte IT-Governance-Mechanismen vertieft und mit Blick auf ihre Bedeutung im Ordnungsrahmen dargestellt. Schließlich werden umfangreiche Ansätze und Vorgehensmodelle zur Durchführung des IT-Risikomanagements beschrieben. Hierfür wird auf etablierte Konzepte zurückgegriffen, die Vorschläge für ein IT-Risikomanagementsystem machen. Dargestellt werden die Norm »DIN ISO 31000«, der DIIR Revisionsstandard Nr. 2 und der Prüfungsstandard »IDW PS 981«.

1.8.6 Compliance der Unternehmens-IT – Konformität mit gesetzlich-regulatorischen Vorgaben, IT-Standards und -Normen sowie internen IT-Richtlinien gewährleisten

Sicherstellung von Compliance

»IT-Compliance« bezeichnet einen Zustand, in dem alle verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben, die die IT des Unternehmens betreffen, nachweislich eingehalten werden (nach [Klotz 2020], S. 849). Der »Deutsche Corporate Governance Kodex« (DCGK) verpflichtet die Leitungsorgane von Aktiengesellschaften explizit auf Compliance. Für alle Unternehmensformen zählt die Sicherstellung von Compliance mit gesetzlich-regulatorischen Vorgaben zu den Sorgfaltspflichten der Unternehmensleitung. Diese müssen somit auch für die Rahmenbedingungen der IT-Compliance sorgen und sich in der Steuerung und Überwachung der IT-Compliance engagieren.

Verbindlichkeit von Vorgaben

Den Kern von IT-Compliance bilden IT-bezogene Vorgaben aus Gesetzen und Verordnungen. In hoch regulierten Branchen sind weiterhin aufsichtliche Vorschriften zu beachten. Welchen Stellenwert Vorgaben aus IT-Standards und -Normen haben, hängt davon ab, ob sie lediglich aus fachlichen Gründen Verwendung finden oder ob sie eine höhere Verbindlichkeit dadurch erlangen, dass

- sie in obligatorischen Vorschriften referenziert werden,
- ihre Anwendung mit einer Zertifizierung verbunden ist,
- sie eine generelle Voraussetzung für einen Marktzugang darstellen oder
- ihre Einhaltung von wichtigen Kunden gefordert wird.

Integration der IT-Compliance

In organisatorischer Hinsicht sollte die IT-Compliance der Corporate Compliance zugeordnet werden. Die Integration der IT-Compliance in die Corporate Compliance hat in struktureller, personeller, operativer und finanzieller Hinsicht zu erfolgen. Vor allem die Integration von Risiken, Zielen und Maßnahmen der IT-Compliance in das Compliance-Management-System des Unternehmens ist aus Effektivitäts- und Effizienzgründen erforderlich. Nicht zuletzt sollte die Compliance-Kultur des Unternehmens auch für die IT-Compliance maßgebend sein, um die Bildung von Compliance-Subkulturen zu vermeiden.

Governance und Management von IT-Compliance

Es ist eine klare Abgrenzung der Verantwortlichkeiten für »Governance« und »Management« von IT-Compliance zu treffen. Die IT-Governance setzt den Rahmen für das Management der IT-Compliance, d.h. Ziele, Grundsätze und Prinzipien für die IT-Compliance. Es ist die Aufgabe der Governance-Akteure, Compliance-Verantwortlichkeiten zu delegieren, Stellen und Prozesse für IT-Compliance zu etablieren, in ihrer Leistung zu steuern und hinsichtlich ihrer Angemessenheit und Wirk-

samkeit zu überwachen. Insbesondere ist ein IT-Compliance-Managementsystem zu etablieren, wofür auf verschiedene Standards und Normen zurückgegriffen werden kann. Angemessenheit und Wirksamkeit des IT-Compliance-Managementsystems sind zu überwachen, z.B. durch Selbstprüfungen, anlassbezogene Prüfungen der IT-Revision oder durch externe, von Wirtschaftsprüfern vorgenommene Prüfungen.

Wertbeitrag von IT-Compliance

Der Wertbeitrag von IT-Compliance liegt wesentlich in der Sicherstellung der Ordnungsmäßigkeit der IT-gestützten Rechnungslegung und der Vermeidung monetärer Schäden, z.B. durch Bußgelder. Zudem werden in vielen Branchen auch aufsichtliche Vorgaben für die Unternehmens-IT zahlreicher. Diesen Herausforderungen lässt sich durch IT-Compliance begegnen – wenn sie von den Akteuren der IT-Governance gesteuert und überwacht wird.

Ausblick auf Kapitel 7

Kapitel 7 befasst sich mit der IT-Compliance aus der Governance-Perspektive. Insofern wird die Frage behandelt, wie sich IT-Compliance in die IT-Governance, aber auch in die Corporate Compliance integriert. Konzeptionelle Hinweise hierfür werden der Norm »ISO/IEC 38500« und dem Standard »COBIT 2019« entnommen. Hinsichtlich der Organisation der IT-Compliance werden Einflussfaktoren der organisatorischen Gestaltung und ein grundlegendes 3-Ebenen-Modell der IT-Compliance-Organisation diskutiert. Besondere Beachtung findet die Stelle des IT-Compliance-Managers, dessen Aufgaben von operativen und analytisch-konzeptionellen Tätigkeiten über die Umsetzung von IT-Compliance-Maßnahmen bis hin zur Überwachung der Ordnungsmäßigkeit von IT-Systemen und -Prozessen reichen. Die Möglichkeiten der Ausgestaltung des IT-Compliance-Managementsystems werden anhand des Prüfungsstandards »IDW PS 980 n.F.« sowie der Normen »DIN ISO 19600« und »DIN ISO 37301« dargestellt.

1.8.7 Wert von Daten durch Data Governance sichern – Ziele, Verantwortlichkeiten und Rollen für ein erfolgreiches Datenmanagement festlegen

Daten als Produktionsfaktor

Die Metapher der Daten als Öl des 21. Jahrhunderts vermittelt die grundlegende Bedeutung, die der Ressource »Daten« für die IT-Infrastruktur, die IT-Systeme und -Services zukommt. Daten sind aber auch ein Kosten- und Risikofaktor. Die Abhängigkeit der Leistungserstellungsprozesse von der Verfügbarkeit qualitativ hochwertiger Daten führt zu ihrer Einstufung als Produktions- bzw. Wettbewerbsfaktor. Daten können auch selbst zum Produkt bzw. zur Ware werden. Hierdurch und hinsichtlich neuer, datengetriebener Geschäftsmodelle fungieren Daten als wesentlicher Enabler. Gerade die Sichtweise der Daten als einem Vermögens-

wert macht bei verteilter Datennutzung und dezentralen Datenbeständen eine zentrale Steuerung und Kontrolle durch eine Data Governance erforderlich. Data Governance ist ein integraler Bestandteil der IT-Governance und insofern dafür verantwortlich, einen Ordnungsrahmen für ein erfolgreiches Datenmanagement vorzugeben und hierdurch das Business/IT-Alignment in Bezug auf die Datennutzung sicherzustellen. Data Governance zeichnet sich dadurch aus, dass

Data Governance

- sie als Verantwortung von den Leitungsorganen und dem Topmanagement der IT gleichermaßen wahrzunehmen ist,
- Anforderungen der IT-Stakeholder an das Data-Governance-Programm zu berücksichtigen sind,
- sie vom Datenmanagement klar zu trennen und hierfür eine Schnittstelle zu definieren ist,
- ihre Regelungen die gesamte Unternehmens-IT betreffen und
- sie insbesondere Risiken und Compliance der Datennutzung fokussiert.

Ziele von Data Governance

Die Ziele von Data Governance richten sich z. B. auf die Schaffung einer datenbewussten Kultur, die Sicherstellung einer hohen Datenqualität, die Minimierung von Risiken und Non-Compliance der Datennutzung oder die Monetarisierung der Daten. Da Data Governance derzeit in den wenigsten Unternehmen fest etabliert ist, sollte der Nutzen von Data Governance durch das Verfolgen konkreter Zielsetzungen, z. B. die Erhöhung der Datenqualität für gesamtunternehmensbezogene Entscheidungen, in begrenzten Umsetzungsprojekten nachgewiesen werden.

Institutionalisierung

Für eine Institutionalisierung von Data Governance sollte ein differenziertes Rollenmodell über eine exekutive, strategische, taktische und operative Ebene umgesetzt werden. Eine minimale Struktur besteht hierbei aus den drei Rollen Auftraggeber, Konzern-Data-Steward und fachlichen/technischen Data Stewards. Die Definition und Zuweisung von Rollen hat den Vorteil, dass eine Data-Governance-Organisation in eine bestehende Linienstruktur integriert und somit ein zentralistisches Organisationsmodell vermieden werden kann.

Standards und Normen

Zur Ausgestaltung der Data Governance, insbesondere der Schnittstelle zum Datenmanagement, können IT-Normen und -Standards genutzt werden. Der Standard »Data Management Body of Knowledge« (DAMA-DMBOK) gliedert Data Governance in Prozessbereiche und Einzelprozesse. Dieses Prozessmodell wird durch ein rollenbasiertes Organisationsmodell ergänzt. Noch umfangreicher als der DAMA-DMBOK beschreibt die Norm »ISO/IEC 38505-1« Prinzipien und Aufgaben der Data Governance. Die zahlreichen Handlungsempfehlungen der Norm

können für eine Standortbestimmung der Ausgestaltung der Data Governance im Unternehmen herangezogen werden.

Ausblick auf Kapitel 8

Kapitel 8 stellt das noch junge Konzept der Data Governance als integralen Teil der IT-Governance vor. Vor allem die Schnittstelle zwischen Data Governance und Datenmanagement wird ausführlich behandelt, da es hier in der Fachdiskussion immer wieder zu unklaren Abgrenzungen kommt. Als neues Gebiet der IT-Governance müssen Ziele und Wertbeitrag der Data Governance vermittelt werden und sie werden deshalb in einem eigenen Abschnitt behandelt. Für die Organisation der Data Governance wird ein ausdifferenziertes Rollenmodell, das mehrere Ebenen umfasst, dargestellt. Dieses kann als Grundlage verwendet werden, um ein an eine spezifische Unternehmenssituation angepasstes Rollenmodell zu entwickeln. Als Orientierung für die konzeptionelle Ausgestaltung einer Data Governance im Unternehmen können einschlägige IT-Normen und -Standards herangezogen werden. Behandelt werden die Standards »Data Management Body of Knowledge« und »COBIT 2019« sowie die beiden Teile der Norm »ISO/IEC 38505«.

1.8.8 Standards und Normen der IT-Governance – bewährte Konzepte und Modelle für die Ausgestaltung der IT-Governance nutzen

IT-Standards und -Normen

Governance- und managementorientierte IT-Standards und -Normen beinhalten Vorgaben oder Empfehlungen, wie in einem bestimmten Handlungsbereich in systematischer Weise zu agieren ist. Unternehmen können an dem Wissen zahlreicher Fachleute, die an der Entwicklung der Standards und Normen mitgearbeitet haben, partizipieren. Vorteile der Nutzung von IT-Standards und -Normen zeigen sich z. B. in einem geringeren Risiko durch Rückgriff auf bewährte Konzepte, durch den Anschluss an eine einheitliche Begriffswelt und in der daraus resultierenden Arbeitsstrukturierung bei der Anwendung der Standards und Normen. Ist das Erlernen einer Norm oder eines Standards mit dem Erwerb eines persönlichen Zertifikats verbunden, resultiert dies in einer höheren Qualifikation und Motivation der Mitarbeiter, die durch nachweisbare Kenntnisse der verschiedenen IT-Standards und -Normen ihren »Marktwert« steigern. Der Nutzen der Anwendung von IT-Normen und -Standards realisiert sich in der Praxis vor allem in den vier Bereichen Marktzugang, Qualität, Sicherheit und Risiken:

Nutzen

- Mitunter stellen bestimmte IT-Standards und Normen (z. B. IT-Sicherheitszertifikate) Markteintrittsbarrieren dar. Ohne ihre Erfüllung könnten Aufträge nicht erlangt und damit Umsatzpotenziale nicht erschlossen werden.

- Die Umsetzung der Empfehlungen und Vorgaben aus IT-Standards und -Normen trägt zu einer höheren Qualität der Unternehmens-IT, insbesondere zu Transparenz und Effektivität von IT-Prozessen und IT-Services bei.
- Einen großen Nutzen hat die Anwendung von IT-Normen und -Standards für die IT-Sicherheit. Gerade für die Einführung und den Betrieb eines Informationssicherheits-Managementsystems bieten verschiedene IT-Standards und -Normen eine wesentliche Hilfestellung.
- Die Reduzierung von IT-Risiken folgt aus der Anwendung entsprechend spezialisierter Normen (z.B. der ISO/IEC 27005) und Standards. Die Erhöhung der Transparenz und Sicherheit in der Durchführung von IT-Prozessen führt regelmäßig auch zur Reduzierung von Risiken.

Reflektierte Nutzung

Allerdings dürfen IT-Standards und -Normen nicht unreflektiert eingesetzt werden. Insbesondere darf kein wettbewerbskritisches Wissen verloren gehen, damit sich ein Unternehmen weiterhin von der Konkurrenz differenzieren kann. Die Nutzung von IT-Standards und -Normen bedeutet immer auch eine Investition, die mit der Erlangung und Aufrechterhaltung des Know-hows für die Implementierung und Nutzung von Standards und Normen verbunden ist. Dies gilt vor allem auch für Zertifizierungen und Rezertifizierungen, die oftmals als bürokratisch und langwierig empfunden werden.

Ausblick auf Kapitel 9

Kapitel 9 beschreibt ausgewählte IT-Normen und -Standards, auf die in den Kapiteln dieses Buches wiederholt Bezug genommen wird. Während in diesem ersten Kapitel die »ISO/IEC 38500« als grundlegende Norm für die IT-Governance beschrieben wurde, wird im neunten Kapitel ein Überblick über die gesamte Normenreihe »ISO/IEC 3850x« gegeben. Für die Governance der Informationssicherheit kann die Norm »DIN EN ISO/IEC 27014« genutzt werden. Daneben wird vor allem COBIT 2019 beschrieben, das als der zentrale IT-Standard für IT-Governance und IT-Management anzusehen ist.

1.9 Handlungsempfehlungen

Wie die folgenden Kapitel schließt auch dieses mit anwendungs- und praxisorientierten Hinweisen und Schlussfolgerungen, die als konkrete Handlungsempfehlungen zu verstehen sind.

- **Verständnis für IT-Governance aus der Corporate Governance ableiten**
  Corporate Governance zielt nach dem Deutschen Corporate Governance Kodex (DCGK) auf den Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens ab. Demgemäß richtet sich die IT-Governance als Teil der Corporate Governance auf die Planung, Steuerung und Überwachung der Unternehmens-IT. Das System und die Strukturen der IT-Governance müssen mit dem System und den Strukturen der Corporate Governance korrespondieren. Begrifflich zeigt sich dieser Zusammenhang bereits in den Definitionen des Cadbury Report und der ISO/IEC 38500.
- **IT-Governance in vollem Umfang verstehen**
  IT-Governance stellt als Teil der Corporate Governance einen Ordnungsrahmen für den erfolgreichen IT-Einsatz in allen seinen Formen dar. Er ist im Wesentlichen auf das Business/IT-Alignment ausgerichtet, wozu sich die Leitungsorgane des Unternehmens in der Planung, Steuerung und Überwachung der Unternehmens-IT richtungsweisend engagieren müssen. Wichtige IT-Stakeholder sind hierbei einzubeziehen. IT-Governance bezieht sich auf die gesamte Unternehmens-IT, insbesondere IT-Entwicklungen und -Innovationen. Risiken und Compliance der Unternehmens-IT erfahren eine besondere Aufmerksamkeit, IT-Governance wird jedoch nicht auf diese Handlungsfelder verkürzt.
- **Empfehlungen der ISO/IEC 38500 bei der Ausgestaltung der IT-Governance zur Orientierung heranziehen**
  Die ISO/IEC 38500 gibt Empfehlungen für die IT-Governance. Sie beinhaltet sechs Prinzipien in den Bereichen Verantwortlichkeit, Strategie, Beschaffung, Performanz, Konformität und Verhalten. Die Anwendung dieser Prinzipien erfolgt in den drei übergeordneten Governance-Aufgaben »Evaluieren, Vorgeben und Überwachen«. Diese Aufgaben werden für jedes einzelne der sechs Prinzipien konkretisiert. Weiterhin legt die Norm in ihrem Konzept der IT-Governance Wert auf die klare Trennung von Governance und Management.

→

- **COBIT 2019 als Basis für die Konzeption und Implementierung eines IT-Governance-Systems nutzen**
  Der IT-Standard »COBIT 2019« bildet ein Referenzmodell für Governance- und Managementziele, die über eine Kaskadierung letztlich zu einer Unterscheidung von IT-Governance- und IT-Managementzielen führen. Hierbei werden die Zielsetzungen für die IT-Governance in der Governance-Domäne »Evaluate, Direct, Monitor (EDM)« beschrieben. Über die In- und Outputs der zu den Zielsetzungen zugehörigen IT-Prozesse bzw. Praktiken ergeben sich die Schnittstellen zum IT-Management.