Michael Klotz · Matthias Goeken · Martin Fröhlich

IT-Governance

Ordnungsrahmen und Handlungsfelder für eine erfolgreiche Steuerung der Unternehmens-IT

ISACA Germany Chapter

dpunkt.verlag

Prof. Dr. Michael Klotz ist seit 1999 Professor für Betriebswirtschaftslehre, insb. Informationsmanagement, Organisation und Datenverarbeitung an der Hochschule Stralsund. Davor war er 15 Jahre in der IT-Branche als Berater, Projektmanager und Geschäftsführer tätig. Seine fachliche Arbeit dokumentiert sich in über 100 Publikationen zu IT-Governance, IT-Compliance und Projektmanagement.

Prof. Dr. Matthias Goeken ist Professor für Wirtschaftsinformatik an der Hochschule der Deutschen Bundesbank. Zuvor war er Juniorprofessor an der Frankfurt School of Finance & Management und dort Mitbegründer und Leiter einer Forschungsgruppe zum Themengebiet IT-Governance. Zu seinen weiteren Forschungsgebieten zählen Business Intelligence und Machine Learning. Im ISACA Germany Chapter ist er Vizepräsident für Publikationen.

Dr. Martin Fröhlich ist selbstständiger IT-Berater mit den Schwerpunkten Strategie-, IKS-Beratung und IT-Compliance. Davor war er 30 Jahre bei einer Big-Four-Wirtschaftsprüfungsgesellschaft tätig, davon knapp 20 Jahre als Partner verantwortlich für IT-Prüfung und Beratung im Finanzdienstleistungssektor. Dr. Fröhlich ist Mitglied des FAIT beim IDW und Vizepräsident des ISACA Germany Chapter.

Die Autoren sind Mitherausgeber der Zeitschrift »IT-Governance«.

Michael Klotz · Matthias Goeken · Martin Fröhlich

IT-Governance

Ordnungsrahmen und Handlungsfelder für eine erfolgreiche Steuerung der Unternehmens-IT

Edition ISACA Germany Chapter

ISACA Germany Chapter

dpunkt.verlag

Michael Klotz
michael.klotz@fh-stralsund.de

Matthias Goeken
matthias.goeken@bundesbank.de

Martin Fröhlich
mf@martin-froehlich.de

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

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

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

ISBN:
Print 978-3-86490-930-6
PDF 978-3-96910-874-1
ePub 978-3-96910-875-8
mobi 978-3-96910-876-5

1. Auflage 2023

Wieblinger Weg 17
69123 Heidelberg

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

PEFC zertifiziert
Das Papier für dieses Buch stammt aus nachhaltig bewirtschafteten Wäldern und kontrollierten Quellen.
PEFC™
PEFC/04-31-0810 www.pefc.de

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

5 4 3 2 1 0

Vorwort

Die unter dem Begriff »IT-Governance« zusammengefassten Ansätze, Verfahren und Methoden zur Führung und Organisation der Unternehmens-IT haben in den letzten 15 Jahren eine wechselvolle Entwicklung erfahren. Stand IT-Governance noch Anfang dieses Jahrhunderts als wichtiger Baustein zur Steigerung der Effizienz und Effektivität – mithin der Beitrag der IT zur Erreichung von Unternehmenszielen – im Vordergrund auch der wissenschaftlichen Diskussion, ist das Interesse an IT-Governance in Wissenschaft und Praxis in den letzten Jahren angesichts von Entwicklungen, wie Digitalisierung von Geschäftsprozessen, künstlicher Intelligenz oder Blockchain, etwas in den Hintergrund getreten. Erst Finanz- und Unternehmensskandale in jüngerer Zeit haben abermals deutlich gemacht, welchen Stellenwert »gute« bzw. »verantwortungsvolle« Unternehmensführung auch und gerade heute für Unternehmen und deren IT-Einsatz haben muss.

Mit diesem Buch sollen die wissenschaftlichen Erkenntnisse des noch relativ jungen Forschungsgebietes mit den Herausforderungen der Praxis bei der Ausprägung einer Governance für die IT verbunden werden. Zielsetzung ist nicht die Zusammenstellung eines »Kochbuches« mit Patentrezepten, sondern die Darstellung von Bausteinen eines Modells basierend auf wissenschaftlichen Erkenntnissen und Studien sowie Erfahrungen aus der Praxis.

Am Anfang des Buches steht eine Darstellung wesentlicher Forschungsergebnisse zu IT-Governance. Besonderes Augenmerk liegt dabei auf grundlegenden Konzepten und Ansätzen sowie dem Wertbeitrag, den IT-Governance zur Erreichung von Unternehmenszielen liefern kann. Hierzu bedarf es eines Ordnungsrahmens, bestehend aus Mechanismen (u. a. Prozesse, Strukturen) und Maßnahmen (u. a. Regelungen, Verfahren). Die Ausgestaltung dieses Ordnungsrahmens muss sich an Prinzipien orientieren, wie die Trennung von IT-Governance und IT-Management, die Beteiligung aller relevanten Stakeholder oder die Ausrichtung auf die gesamte Unternehmens-IT. Auf diesen methodischen Grundlagen ist die Governance für die IT auszuprägen.

Jedoch werfen die theoretischen Konzepte und Ansätze die Frage der praktischen Umsetzbarkeit auf. Sowohl der Ordnungsrahmen als auch die Prinzipien führen für sich allein nicht zu Vorgaben für die praktische Implementierung von IT-Governance, sondern bilden zunächst nur ein gedankliches Gerüst quasi als Leitplanken für die konkrete Umsetzung. Für die praktische Umsetzung bedarf es verschiedener Handlungsfelder, um IT-Governance zu institutionalisieren, die Beziehungen zu weiteren Managementsystemen, insbesondere für Risikomanagement und Compliance, zu organisieren, Vorgaben für das IT-Management zu machen und Nutzen aus Standards und Normen für die konkrete Ausgestaltung der IT-Governance zu ziehen.

Die Institutionalisierung von IT-Governance beruht auf den drei Säulen Organisation, Akteure und Stakeholder. Das Handlungsfeld IT-Organisation beschreibt verschiedene Organisationsformen und bewertet diese unter dem Gesichtspunkt der Eignung für die organisatorische Verankerung der IT-Governance in Strukturen und Prozessen. Im Handlungsfeld Akteure werden die für die IT-Governance besonders relevanten Personen und Gremien sowie ihre Aufgaben und Verantwortlichkeiten diskutiert. Das Handlungsfeld Stakeholder erweitert die Sichtweise auf die berechtigten Erwartungen und Interessen auch von Organisationseinheiten und Personen, die nicht dem direkt mit IT befassten Personenkreis zugehörig sind.

IT-Governance (G) ist eng mit den Managementsystemen Risikomanagement (R) und Compliance (C) verknüpft, was sich in dem Akronym GRC manifestiert. Aufgabe der Unternehmensführung ist die Identifizierung, Bewertung und die Reaktion auf Risiken, die die Erreichung von Unternehmenszielen gefährden können, sowie die Herstellung der Konformität mit regulatorischen Vorschriften, internen und externen Regelwerken sowie vertraglichen Zusagen. Diese Konformität muss durch ein Compliance-Management-System angestrebt und nachhaltig gesichert werden. Eine ausschließliche Fokussierung auf IT-GRC greift jedoch zu kurz. Weitere Handlungsfelder ergeben sich aus der Bedeutung der Daten für die Unternehmenssteuerung und Entscheidungsfindung (Data Governance) sowie aus der Berücksichtigung der einschlägigen Referenzmodelle, Standards und Normen bei der Gestaltung von Strukturen und Prozessen.

Bei der Entstehung dieses Buches und den vielfältigen Diskussionen zwischen den Autoren ist deutlich geworden, dass das Thema »IT-Governance« viele verschiedene Facetten aufweist. Eine einheitliche Sichtweise auf IT-Governance kann es nicht geben. Jedes Unternehmen wird für sich unterschiedliche Schwerpunkt setzen, bei den einzelnen Handlungsfeldern einen unterschiedlichen Reifegrad haben und bei

der Ausgestaltung der Handlungsfelder unterschiedliche Wege gehen. Den Verantwortlichen in Unternehmen wollen wir am Ende eines jeden Kapitels Handlungsempfehlungen geben, um die praktische Implementierung zu erleichtern und den Blick auf die Aspekte zu lenken, um die es bei dem Thema »IT-Governance« letztlich geht: die IT zu befähigen, einen wertvollen Beitrag zum Unternehmenserfolg zu leisten und sich dabei von den Grundsätzen einer modernen und verantwortungsvollen Unternehmensführung leiten zu lassen.

Wir Autoren freuen uns, dass das Buch in der ISACA-Buchreihe erscheinen kann. Von den Fachdiskussionen in der ISACA-Community konnten wir in den vergangenen Jahren in vielerlei Hinsicht profitieren. Darüber hinaus gilt unser Dank dem dpunkt.verlag für die umsichtige und kompetente Begleitung unseres Buchprojekts und dabei insbesondere Frau Christa Preisendanz, unserer Lektorin!

Michael Klotz, *Matthias Goeken*, *Martin Fröhlich*
Stralsund, Bensheim, Dinslaken im Oktober 2022

Inhaltsübersicht

Inhaltsverzeichnis

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.