Michael Klotz · Matthias Goeken · Martin Fröhlich

IT-Governance

Ordnungsrahmen und Handlungsfelder für eine erfolgreiche Steuerung der Unternehmens-IT

ISACA Germany Chapter

dpunkt.verlag

Inhalt

Cover

Über den Autor

Titel

Impressum

Vorwort

Inhaltsübersicht

Inhaltsverzeichnis

1 Grundlagen der IT-Governance

1.1 Entwicklung der Corporate Governance

1.2 Definitionen für IT-Governance

1.3 IT-Governance nach Weill et al.

1.4 IT-Governance nach der ISO/IEC 38500

1.5 IT-Governance nach COBIT 2019

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

1.7 Verständnis von IT-Governance in diesem Buch

1.7.1 Vorüberlegungen

1.7.2 Darstellung unseres Verständnisses von IT-Governance

1.7.3 Prinzipien gemäß dem IT-Governance-Verständnis

1.8 Handlungsfelder für IT-Governance

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

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

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

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

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

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

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

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

1.9 Handlungsempfehlungen

2 Der Wertbeitrag der IT als Handlungsfeld der IT-Governance

2.1 Prioritäten, Trends und Herausforderungen

2.2 Wertbeitrag in wissenschaftlichen Studien und die Rolle der IT-Governance

2.3 Was bedeutet Wert und was ist der Wertbeitrag der IT?

2.3.1 Terminologie, Verfahren und Methoden

2.3.2 Grundlegendes Verständnis von »Wert« und Wertbeitrag der IT

2.3.3 Grundlegende Probleme und Herausforderungen bei der Ermittlung des Wertbeitrags

2.4 Messung und Messkonzepte für den Wertbeitrag der IT

2.4.1 Kostenorientierte Verfahren

2.4.2 Prozesskosten in Fach- und Geschäftsbereichen

2.4.3 Investitionsrechnung

2.4.4 Nutzwertanalyse

2.4.5 Weitere Verfahren im Überblick

2.4.6 Wert als »Nutzenbündel« (»Bundle of Benefits«-Ansatz)

2.5 Wertbeitrag und Wertbeitragsdimensionen

2.6 Konzepte zur Steuerung und Verbesserung des Wertbeitrags der IT
2.6.1 Business Case
2.6.1.1 Konzept und Grundlagen
2.6.1.2 Entwicklung eines Business Case
2.6.2 Business/IT-Alignment
2.6.2.1 Grundlagen und Definitionen
2.6.2.2 Das Strategic Alignment Model (SAM) und Erweiterungen
2.6.2.3 Alignment-Dimensionen und -Ebenen
2.6.2.4 Strategic Alignment Maturity Model (SAMM)
2.6.3 COBIT EDM02
2.7 Herausforderungen und Handlungsempfehlungen
3 Akteure der IT-Governance
3.1 Der Chief Information Officer
3.1.1 Stelle und Rolle des CIO
3.1.2 Beispiel für eine CIO-Organisation
3.2 Der Chief Digital Officer
3.2.1 Position und Aufgaben des Chief Digital Officer
3.2.2 Chief Digital Officer und Chief Information Officer
3.2.3 Der CDO in der bimodalen bzw. ambidextrischen IT
3.3 Gremien zur Steuerung und Überwachung der IT
3.3.1 Aufsichtsrat
3.3.2 Unternehmensleitung
3.3.3 Ausschüsse
3.4 Handlungsempfehlungen
4 Stakeholder als Handlungsfeld der IT-Governance
4.1 IT-Stakeholder als Adressaten der IT-Governance
4.1.1 Externe Akteure im Unternehmensumfeld
4.1.2 Stakeholder-Begriff

4.1.3 Verantwortung für Einbeziehung von IT-Stakeholdern
4.1.4 Beziehungen zwischen Unternehmens-IT und IT-Stakeholdern
4.1.5 Akteure in der Unternehmensumwelt
4.2 IT-Stakeholder
4.2.1 Unterscheidung zwischen externen und internen IT-Stakeholdern
4.2.2 Interne IT-Stakeholder
4.2.3 Externe IT-Stakeholder
4.3 Ziele der IT-Governance in Bezug auf die IT-Stakeholder
4.4 Abgrenzung zum IT-Stakeholder-Management
4.5 Konstitutive Entscheidungen für das IT-Stakeholder-Management
4.5.1 IT-Stakeholder-Identifizierung
4.5.2 IT-Stakeholder-Analyse
4.5.3 IT-Stakeholder-Einbindung
4.5.4 Qualifizierung für das IT-Stakeholder-Management
4.6 Überwachung des IT-Stakeholder-Managements
4.6.1 IT-Stakeholder-Identifizierung
4.6.2 IT-Stakeholder-Analyse
4.6.3 IT-Stakeholder-Einbindung
4.6.4 Kennzahlen für die Überwachung des IT-Stakeholder-Managements
4.7 Handlungsempfehlungen
5 IT-Organisation als Handlungsfeld der IT-Governance
5.1 Herausforderungen und Anforderungen an die IT-Organisation
5.1.1 Aktuelle Herausforderungen für die IT-Organisation
5.1.2 Gesetzlich-regulatorische Anforderungen an die Organisation der IT
5.2 Begriff und Umfang der IT-Organisation
5.3 Integration der IT-Funktion in die Unternehmensstruktur
5.3.1 Aufgaben, Stellen und Rollen der IT-Funktion
5.3.1.1 Aufgaben der IT-Abteilung

5.3.1.2 Rollen in der IT-Organisation

5.3.2 Aufbauorganisatorische Anbindung der IT-Abteilung

5.3.2.1 Grundformen der aufbauorganisatorischen Eingliederung der IT

5.3.2.2 Center-Konzepte für den IT-Bereich

5.3.3 Einfluss von Outsourcing auf die IT-Organisation

5.3.4 Integration der IT in das Unternehmen nach dem 3-Linien-Modell

5.4 IT-Prozesse

5.4.1 Struktur der IT-Prozesse nach COBIT 2019

5.4.2 Leistungssteuerung der IT-Prozesse nach COBIT 2019

5.4.3 Priorisierung der Prozesse mittels Designfaktoren

5.5 Agile IT-Organisation

5.5.1 Agile IT aus Sicht der IT-Governance

5.5.2 Agile Aufbauorganisation

5.5.3 DevOps

5.5.4 Innovation Labs

5.6 Handlungsempfehlungen

6 IT-Risiken als Handlungsfeld der IT-Governance

6.1 Grundlagen für die Governance von IT-Risiken

6.1.1 Grundlagen in Gesetzen, Standards und Normen

6.1.2 Begriff des IT-Risikos

6.1.3 Systematik der IT-Risiken

6.2 IT-Risiken im Rahmen der IT-Governance

6.2.1 IT-Risiken in der Trias »IT-GRC«

6.2.2 IT-Risiken in der ISO/IEC 38500

6.2.3 Governance von IT-Risiken nach COBIT 2019

6.2.4 IT-Risiken als Teilmenge der Unternehmensrisiken

6.2.5 IT-Risiken im Rahmen des unternehmensweiten Risikomanagements

6.3 Wertbeitrag der Governance von IT-Risiken
6.4 Aufgabenbereiche der Governance von IT-Risiken
6.4.1 Struktur der Aufgabenbereiche
6.4.2 IT-Risikoziele
6.4.3 IT-Risikobewusstsein
6.4.4 IT-Risikokultur
6.4.5 Grundlegende IT-Risikoorientierung
6.4.6 IT-Risikostrategie und IT-Risikorichtlinie
6.4.7 IT-Risiko-Stakeholder
6.4.8 IT-Risikoorganisation
6.4.9 IT-Risikomanagementsystem
6.5 Organisation und Mechanismen des IT-Risikomanagements
6.5.1 Umfeld der IT-Risikoorganisation
6.5.2 IT-Risikomanagementprozess
6.5.2.1 Risikomanagementprozess nach DIN ISO 31000
6.5.2.2 Risikomanagementprozess nach COBIT 2019
6.5.2.3 Risikomanagementprozess nach IDW PS 981
6.5.2.4 Risikomanagementprozess nach DIIR Revisionsstandard Nr. 2
6.5.3 Strukturelle IT-Risikoorganisation
6.5.3.1 Organisationseinheiten
6.5.3.2 Rollen
6.6 IT-Risikomanagementsystem
6.6.1 IT-Risikomanagementsystem nach DIN ISO 31000
6.6.2 IT-Risikomanagementsystem nach IDW PS 981
6.6.3 IT-Risikomanagementsystem nach DIIR Revisionsstandard Nr. 2
6.6.4 Prüfung des IT-Risikomanagementsystems
6.6.4.1 Formen und Zielsetzung der Prüfung
6.6.4.2 Prüfung nach DIIR Revisionsstandard Nr. 2

6.6.4.3 Prüfung nach IDW PS 981

6.7 Handlungsempfehlungen

7 IT-Compliance als Handlungsfeld der IT-Governance

7.1 Grundlagen

7.1.1 Einordnung von IT-Compliance in die Governance

7.1.2 Treiber für IT-Compliance

7.1.3 Wertbeitrag der IT-Compliance

7.2 Methodische Grundlagen

7.2.1 Begriff

7.2.2 Rahmenwerke für IT-Compliance

7.2.2.1 COBIT 2019

7.2.2.2 ISO 37301

7.2.2.3 IDW PS 980 n.F.

7.2.2.4 Weitere Entwicklung der Rahmenwerke

7.3 Regelwerke für IT-Compliance

7.3.1 Klassifizierung der Regelwerke

7.3.2 Rechtliche Vorgaben

7.3.2.1 Gesetze

7.3.2.2 Rechtsprechung

7.3.2.3 Rechtsverordnungen

7.3.2.4 Verwaltungsvorschriften

7.3.3 Verträge

7.3.4 Unternehmensinterne Regelwerke

7.3.5 Unternehmensexterne Regelwerke

7.4 Auswahl von relevanten Regelwerken

7.4.1 Bestimmung des Compliance-Portfolios

7.4.2 Konsolidierung von Regelwerken

7.4.3 Mapping

7.5 Gestaltungselemente der IT-Compliance
7.5.1 Einordnung in die Corporate Compliance
7.5.2 IT-Compliance-Kultur
7.5.3 IT-Compliance-Ziele
7.5.4 IT-Compliance-Risiken
7.5.5 IT-Compliance-Programm
7.5.6 IT-Compliance-Organisation
7.5.6.1 Einflussfaktoren
7.5.6.2 Organisationsformen
7.5.6.3 IT-Compliance-Manager
7.5.6.4 IT-Compliance-Prozess
7.5.7 IT-Compliance-Kommunikation
7.5.8 IT-Compliance-Überwachung
7.6 Nachweis der IT-Compliance
7.6.1 Prüfung nach IDW PS 980 n.F.
7.6.2 Prüfungen nach IDW PS 860
7.6.3 Prüfung nach IDW PS 951 n.F.
7.7 Handlungsempfehlungen
8 Data Governance
8.1 Data Governance im Rahmen der IT-Governance
8.2 Begriff der Data Governance
8.3 Wertbeitrag und Ziele von Data Governance
8.4 Organisation der Data Governance
8.5 Normen und Standards für Data Governance
8.5.1 Data Governance nach DAMA-DMBOK
8.5.1.1 Der »Data Management Body of Knowledge«
8.5.1.2 Zielsetzung und Prinzipien von Data Governance
8.5.1.3 Data Governance und Datenmanagement

8.5.1.4 Prozess der Data Governance

8.5.1.5 Akteure der Data Governance

8.5.1.6 Bewertung des DAMA-DMBOK

8.5.2 Data Governance nach COBIT 2019

8.5.2.1 Managementziel APO14

8.5.2.2 Governance-Ziel EDM04

8.5.2.3 Bewertung von COBIT 2019

8.5.3 Data Governance nach ISO/IEC 38505-1 und -2

8.5.3.1 ISO/IEC 38505-1

8.5.3.2 ISO/IEC 38505-2

8.6 Handlungsempfehlungen

9 Standards und Normen der IT-Governance

9.1 Frameworks, Standards und Normen

9.1.1 Zur Begrifflichkeit

9.1.1.1 Standard

9.1.1.2 Norm

9.1.1.3 Framework

9.1.2 Normungsorganisationen

9.1.3 Allgemeiner Nutzen aus IT-Normen und -Standards

9.2 Für IT-Governance relevante IT-Normen

9.2.1 Die Normenreihe ISO/IEC 3850x

9.2.2 Die Norm ISO/IEC 27014

9.3 COBIT 2019 als Standard für die IT-Governance

9.3.1 Struktur der COBIT-Dokumente

9.3.2 IT-Governance-System nach COBIT 2019

9.3.3 IT-Governance und IT-Managementziele

9.3.4 IT-Prozesse

9.3.5 Zielkaskade

9.4 Handlungsempfehlungen

Anhang

A Abkürzungen

B Literaturverzeichnis

Index

4 Stakeholder als Handlungsfeld der IT-Governance

Ausblick

Im Mittelpunkt jeder IT-Governance müssen die Interessen der verschiedenen internen und externen Stakeholder der Unternehmens-IT stehen. In diesem Kapitel wird erläutert, warum die Bedeutung der Stakeholder-Ausrichtung für die IT stark zugenommen hat. Als IT-Stakeholder werden Akteure eingestuft, die legitimierte Ansprüche an Aktivitäten haben, die die Unternehmens-IT betreffen. Ansprüche werden dann als legitimiert betrachtet, wenn sie auf einer gesetzlich-regulatorischen oder einer vertraglichen Grundlage beruhen. Es wird beschrieben, welche IT-Stakeholder es grundsätzlich gibt und wie sich diese in unternehmensinterne und -externe IT-Stakeholder unterscheiden lassen. Nach der Klärung, welche IT-Stakeholder zu berücksichtigen sind, werden die Ziele der IT-Governance in Bezug auf die IT-Stakeholder dargestellt. Im Hinblick auf die Unterscheidung zwischen IT-Governance und IT-Management wird beschrieben, wie sich die IT-Governance in Bezug auf IT-Stakeholder vom IT-Stakeholder-Management unterscheidet. Als wesentliche Aufgabe der IT-Governance hat diese für das Management der IT-Stakeholder konstitutive Entscheidungen zu treffen. Diese werden ebenso dargestellt wie die Überwachung der Prozesse des IT-Stakeholder-Managements durch die IT-Governance.

4.1 IT-Stakeholder als Adressaten der IT-Governance

4.1.1 Externe Akteure im Unternehmensumfeld

Externe Beziehungen des Unternehmens

Da der Stakeholder-Ansatz nach der Systemtheorie auf der System-Umwelt-Relation basiert, stellen sich Stakeholder aus Sicht eines Unternehmens vor allem als unternehmensexterne Akteure dar, deren Zahl und Einfluss von Unternehmen

zu Unternehmen variiert. Jedes Unternehmen steht mit verschiedensten Einzelpersonen, Gruppierungen und Organisationen in Verbindung, unterhält Geschäftsbeziehungen mit Kunden und Lieferanten und steht im Wettbewerb mit konkurrierenden Unternehmen. Große Unternehmen agieren am Kapitalmarkt und müssen u.a. mit Fremdkapitalgebern und Finanzanalysten kommunizieren und deren Informationsanforderungen erfüllen. In regulierten Branchen müssen Unternehmen gegenüber Aufsichtsinstitutionen auf Anforderung Informationen zusammenstellen und übermitteln sowie verbindlichen Meldepflichten nachkommen. Weiterhin wird das Unternehmensgeschehen von den Gewerkschaften, Arbeitgeberverbänden und sonstigen Wirtschaftsorganisationen (z.B. Industrie- und Handelskammern, Außenhandelskammern) beeinflusst. Parteien, politische Organisationen und die Verwaltung nehmen eine doppelte Rolle ein; sie agieren einerseits als Förderer von Unternehmen, stellen aber andererseits auch vielfältige Ansprüche an ihre Geschäftstätigkeit. Anforderungen an Unternehmen werden zudem von zivilgesellschaftlichen Gruppierungen, z.B. Bürgerinitiativen und Vereinen mit unterschiedlichsten Zielsetzungen, gestellt (siehe Abb. 4–1).

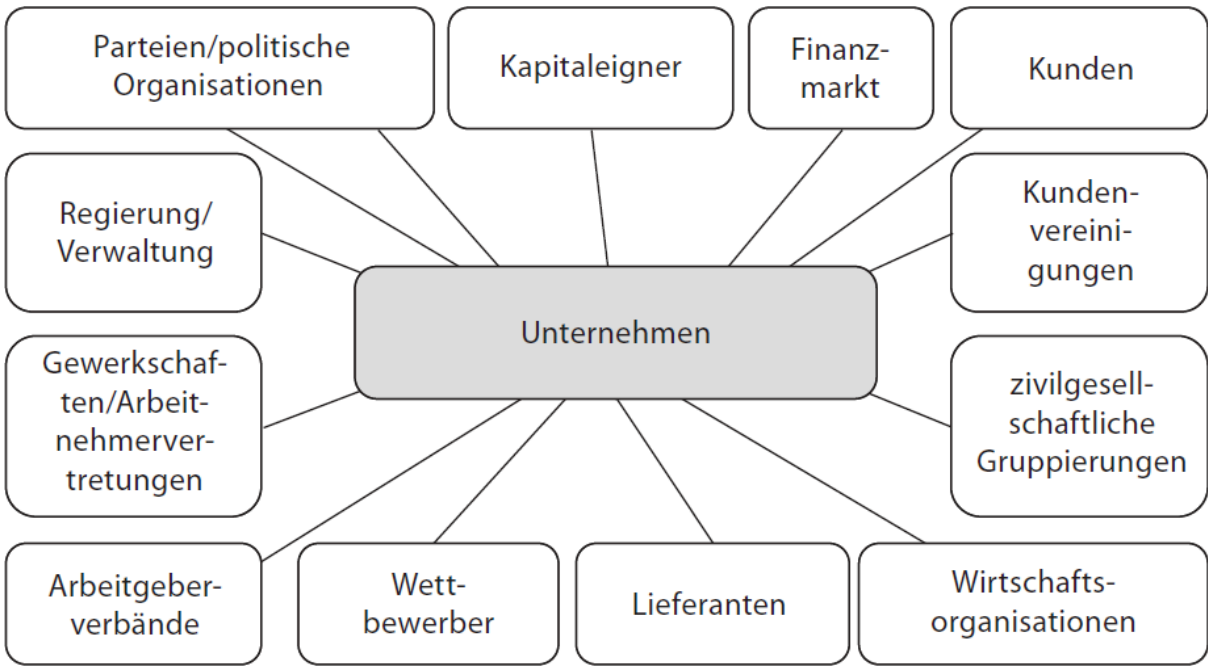

Abb. 4–1 *Externe Akteure des Unternehmens (vgl. [Freeman 1984], S. 25)*

Zusammenhang mit anderen Ansätzen

Als Interessengruppen repräsentieren Stakeholder Ansprüche (weswegen sie häufig auch als »Anspruchsgruppen« bezeichnet werden), die an das Unternehmen herangetragen werden und vom Unternehmensmanagement bei seiner Entscheidungsfindung zu berücksichtigen sind (nach [Schreyögg & Koch 2020], S. 76). Stakeholder-Betrachtungen entstammen dem strategischen Management und gehen insbesondere auf die Arbeit von Freeman zurück. Der

Ansatz wurde in Abgrenzung zum Shareholder-Begriff entwickelt und verweist in diesem Zusammenhang darauf, dass die Unternehmensaktivitäten nicht nur den Kapitaleignern, sondern einem größeren Kreis von Beteiligten nutzen sollen, wenn diese ein berechtigtes Interesse an den Aktivitäten des Unternehmens haben. Insofern wurde das Stakeholder-Konzept zum Kern einer verantwortungsvollen Unternehmensführung, die sich wiederum in der sogenannten Corporate Social Responsibility (CSR) ausprägt.

4.1.2 Stakeholder-Begriff

Stakeholder im DCGK

Nach dem Deutschen Corporate Governance Kodex hat eine nachhaltige Wertschöpfung die Belange der mit dem Unternehmen verbundenen Stakeholder, insbesondere der Anleger, zu berücksichtigen. Als Stakeholder werden Aktionäre, die Belegschaft und sonstige »mit dem Unternehmen verbundene Gruppen« genannt (nach [DCGK 2022, Präambel). Damit sind nicht nur externe, sondern auch unternehmensinterne Akteure zu den Stakeholdern zu zählen.

Definitionen

Die Governance-Norm ISO 37000 (ebenso wie die ISO/IEC 38500) versteht unter »Stakeholder« eine Person oder Organisation, die eine Entscheidung oder Aktivität beeinflussen kann, von ihr beeinflusst wird oder sich selbst als von ihr beeinflusst erachtet (nach [ISO 37000] S. 5). Diese Definition schließt an Freeman an, der jedoch ergänzt, dass die Beeinflussung vom Erreichen der Organisationsziele ausgeht (nach [Freeman 1984], S. 46). Mittlerweile gibt es in der Stakeholder-Theorie zahlreiche Definitionen mit unterschiedlichen Bezügen:

- dem Einfluss, den Stakeholder ausüben oder dem sie ausgesetzt sind,
- den Ansprüchen, die sie an das Unternehmen stellen,
- den Interessen, mit denen sie Sachverhalte, Entscheidungen oder Aktivitäten des Unternehmens verfolgen.

Art der Beziehung

Damit verbunden sind Unterscheidungen nach einer ein- oder zweiseitigen Beziehung zwischen Unternehmen und Stakeholder. Eine zweiseitige Beziehung zeichnet sich dadurch aus, dass Stakeholder sowohl auf Entscheidungen oder Aktivitäten des Unternehmens Einfluss nehmen können als auch von ihnen betroffen sind. Da hier davon ausgegangen wird, dass Unternehmen und Stakeholder grundsätzlich ein gleichgerichtetes Interesse am Erreichen der Unternehmensziele verfolgen, wird in der Regel eine zweiseitige Beziehung zwischen Unternehmen und Stakeholdern bestehen und eine einseitige Beziehung insofern die Ausnahme darstellen.

Eingrenzung

Eine Stakeholder-Definition muss es ermöglichen, relevante Stakeholder zu identifizieren. Hierzu ist es notwendig, dass Stakeholder von sonstigen Akteuren klar abgegrenzt werden können. Nur dann kann der Stakeholder-Ansatz als handlungsleitend für ein Stakeholder-Management betrachtet werden. Mit der Bezugnahme auf bloße Interessen von Akteuren, die dem Unternehmen mitunter auch nicht bekannt sind oder gar nicht bekannt sein können, würde der Stakeholder-Begriff ausufern. Zur Eingrenzung des Stakeholder-Begriffs soll hier deshalb auf legitimierte Ansprüche von Akteuren abgestellt werden, mit denen im Allgemeinen auch eine Einflussmöglichkeit verbunden ist. Als legitimierte Ansprüche sollen nur solche gelten, die auf einer gesetzlich-regulatorischen oder einer vertraglichen Grundlage beruhen. Auf Basis dieser Eingrenzung wird der Stakeholder-Begriff wie folgt definiert:

Definition Stakeholder

Stakeholder sind unternehmensinterne und -externe Personen, Gruppen oder Organisationen, die legitimierte Ansprüche an Entscheidungen oder Aktivitäten des Unternehmens haben.

Im Anschluss an diese Definition lässt sich für die IT-Governance der Stakeholder-Begriff wie folgt fassen:

Definition IT-Stakeholder

IT-Stakeholder sind unternehmensinterne und -externe Personen, Gruppen oder Organisationen, die legitimierte Ansprüche an Entscheidungen oder Aktivitäten der Unternehmens-IT haben.

Stakeholder in COBIT 2019

Stakeholder spielen in COBIT 2019 eine zentrale Rolle. IT-Governance soll sicherstellen, dass Bedürfnisse, Rahmenbedingungen und Handlungsmöglichkeiten der Stakeholder bewertet werden, um ausgewogene, vereinbarte Unternehmensziele festzulegen (nach [ISACA 2020a], S. 13). In der deutschen COBIT-Version wird der Begriff mit »Anspruchsgruppen« übersetzt. Eine der Governance-Zielsetzungen bezieht sich speziell auf die Stakeholder der Unternehmens-IT: »EDM05 Einbindung der Anspruchsgruppen ist sichergestellt«. In der Zielkaskade von COBIT 2019 stellen die Ansprüche der Stakeholder den Ausgangspunkt der Kaskadierung über Unternehmens- und IT-Ziele bis hin zu IT-Governance- und Managementzielen dar (vgl. [ISACA 2020a], S. 30). Trotz dieser zentralen Rolle verwendet COBIT 2019 jedoch keinen eigenen Stakeholder-Begriff.

4.1.3 Verantwortung für Einbeziehung von IT-Stakeholdern

IT-Stakeholder-Governance

Nach dem DCGK ist die Einbeziehung von Stakeholdern und ihren Interessen als Governance-Aufgabe anzusehen. Dies sicherzustellen, obliegt in erster Linie dem Leitungsorgan des Unternehmens. Für die IT-Governance als Teilbereich der Corporate Governance stellt sich dies grundsätzlich nicht anders dar. Auch in der ISO/IEC 38500 wird darauf hingewiesen, dass angemessene Beziehungen zu den

Stakeholdern zur positiven Leistung des IT-Einsatzes beitragen (vgl. [ISO/IEC 38500], S. 4 f.). Damit liegt die Verantwortung für die Einbeziehung der IT-Stakeholder bei den Akteuren der IT-Governance (siehe Kap. 3).

Verantwortungszuordnung in COBIT 2019

Mit Verfolgung der Governance-Zielsetzung »EDM05« soll sichergestellt werden, dass die IT-Stakeholder identifiziert und in das System der IT-Governance eingebunden werden. Zudem sollen die Leistung und die Compliance der Unternehmens-IT in transparenter Art und Weise gemessen und kommuniziert werden. Dies soll auf der Grundlage erfolgen, dass die Ziele und Kennzahlen sowie ggf. erforderliche Verbesserungsmaßnahmen von den IT-Stakeholdern genehmigt werden. Hierdurch soll gewährleistet werden, dass die IT-Stakeholder die IT-Strategie und den dazugehörigen Umsetzungsplan unterstützen, dass die Kommunikation mit den Stakeholdern effektiv und zeitnah erfolgt und dass die Grundlage für eine effektive Berichterstattung geschaffen wird. Mit der Identifizierung von Verbesserungspotenzialen und dem Alignment von Unternehmenszielen und IT-Zielen sowie Unternehmens- und IT-Strategien soll letztlich die Leistung der Unternehmens-IT gesteigert werden (nach [ISACA 2020b], S. 49). Die drei Praktiken der Governance-Zielsetzung richten sich auf die Evaluierung, Steuerung und Überwachung der Einbeziehung der Stakeholder, der Berichtsanforderungen sowie der Kommunikation und Berichterstattung. Die Gesamtverantwortung bzw. Rechenschaftspflicht für alle drei Praktiken liegen bei der Unternehmensleitung, wobei dieser auch in den Positionen des CEO und des CIO die Durchführungsverantwortung obliegt (vgl. [ISACA 2020b], S. 51).

Existiert im Unternehmen kein CIO und engagiert sich auch der CEO nicht für die Einbeziehung der IT-Stakeholder, müsste eine hierarchisch nachgeordnete IT-Leitung die Stakeholder-Verantwortung übernehmen. In dieser Situation müsste die IT-Leitung danach streben, dass die Stakeholder-Thematik aus IT-Sicht auf die Agenda der Unternehmensleitung gelangt. Dies wird sich allerdings dann als schwierig erweisen, wenn die Stakeholder-Sichtweise im Unternehmen nicht oder kaum etabliert ist. In diesem Fall ist das Beziehungsmanagement zu einzelnen kritischen IT-Stakeholdern, z.B. strategischen Lieferanten oder wichtigen Unternehmensbereichen als IT-Anwender, in den Vordergrund zu stellen, um die Aufmerksamkeit der Unternehmensleitung zu erlangen. Auf dieser Grundlage kann eine Governance-Perspektive in Bezug auf die IT-Stakeholder reifen und im nächsten Schritt in die IT-Governance integriert werden.

Konstitutive Entscheidungen

Grundlegend aus Sicht der IT-Governance ist die Haltung, dass für einen nachhaltigen Wertbeitrag der IT eine Einbeziehung von IT-Stakeholdern unabdingbar und operativ in einem IT-Stakeholder-Management umzusetzen ist. Dementsprechend haben die Akteure der IT-Governance als konstituierende Entscheidungen

- IT-Stakeholder als grundlegend relevant für den Wertbeitrag der IT anzusehen,
- zu bestimmen, dass ein IT-Stakeholder-Management etabliert wird,
- Zielsetzungen für das IT-Stakeholder-Management zu verabschieden (dies umfasst auch Strategien für den Umgang mit den wesentlichen Stakeholdern),
- festzulegen, welche Personen, Gruppen oder Organisationen als IT-Stakeholder zu betrachten sind,
- den Rahmen für die Klassifizierung und Bewertung von IT-Stakeholdern festzulegen,
- die Qualifizierung der Akteure des IT-Stakeholder-Managements zu initiieren.

Subjektive Festlegung

Die Festlegung der IT-Stakeholder durch die Akteure der IT-Governance macht deutlich, dass jedes Unternehmen für sich selbst zu entscheiden hat, welche Personen, Gruppen oder Organisationen es als IT-Stakeholder einstuft. Diese Entscheidung erfolgt in der Praxis nicht nur nach objektiven Kriterien. Hier sind auch Erwägungen zu treffen, welche Ressourcen für ein Stakeholder-Management aufgewendet werden sollen. So können sich Unternehmen z.B. dazu entscheiden, nur externe oder nur interne Akteure als IT-Stakeholder zu definieren. In diesem Sinne ist auch unerheblich, ob sich Personen, Gruppen oder Organisationen selbst als Stakeholder verstehen. Dies dürfte sogar häufig dann nicht der Fall sein, wenn externe Akteure der Unternehmens-IT zu Neutralität und Unabhängigkeit verpflichtet sind, so wie dies beispielsweise bei Wirtschaftsprüfern oder Aufsichtsbehörden der Fall ist. Gleichwohl bezieht ein Unternehmen deren Anforderungen und Interessen in die Festlegung von Zielen und Prioritäten ausdrücklich mit ein, wodurch sie aus dessen Perspektive zu Stakeholdern werden können.

Infolge der genannten Entscheidungen haben die Akteure der IT-Governance die Umsetzung ihrer Entscheidungen und insbesondere die Zielerreichung zu überwachen.

4.1.4 Beziehungen zwischen Unternehmens-IT und IT-Stakeholdern

Die Beziehungen, in denen legitimierte Ansprüche der IT-Stakeholder zum Tragen kommen (d.h. beispielsweise erkannt, berücksichtigt, abgewiesen, erfüllt werden), können sich sehr unterschiedlich ausprägen. Dies liegt vor allem an der unterschiedlichen Grundlage der Legitimität. Einige Beispiele sollen dies verdeutlichen:

- Kunden, mit denen ein Unternehmen eine vertraglich geregelte Geschäftsbeziehung unterhält, erwarten von diesem, dass das Unternehmen mit ihren Daten verantwortlich umgeht und diese vor unberechtigtem Zugriff schützt. Sie nehmen ggf. ihre Rechte wahr (z.B. Auskunftsrechte) und verfolgen bei Verletzungen derselben ihre Ansprüche auf dem Rechtsweg.
- Das Management der Fachabteilungen erwartet von der Unternehmens-IT, dass diese die IT-Systeme und sonstige Serviceleistungen – wie in den SLAs vereinbart – bereitstellt bzw. erbringt. Bei Abweichungen werden festgelegte Abhilfemaßnahmen ergriffen oder Eskalationswege beschritten.
- In Bezug auf die gesetzlichen Vorgaben zum Datenschutz existieren mit den zuständigen Landesdatenschutzbeauftragten Einrichtungen, die die Einhaltung der gesetzlichen Verpflichtungen (z.B. hinsichtlich einer Meldung von Vorfällen) nicht nur erwarten, sondern ggf. auch prüfen oder gar sanktionieren.
- Für Betreiber kritischer IT-Infrastrukturen (KRITIS) sind relevante Stakeholder vom Gesetz vorgegeben und umfassen überwachende und auditierende Organisationen, z.B. das Bundesamt für Sicherheit in der Informationstechnik (BSI). Die betreffenden Unternehmen haben insbesondere den jeweiligen vom BSI genehmigten branchenspezifischen Sicherheitsstandard umzusetzen.
- Der Unternehmensleitung werden die IT-Strategie und eine entsprechende Umsetzungsplanung vorgelegt. Diese erwartet eine Unterstützung der Unternehmens-Strategie durch die IT-Strategie und entscheidet, ggf. in Abstimmung mit einem Aufsichtsrat, über ihre Genehmigung und die Freigabe damit verbundener Mittel für IT-Investitionen.
- Unternehmensleitung und Aufsichtsrat erhalten regelmäßige Statusinformationen zu einem Projektprogramm zur Umsetzung der digitalen Transformation des Unternehmens, inkl. der Einführung neuer, datengetriebener Geschäftsmodelle. Akteure der Unternehmens-IT erhoffen sich ein verstärktes Engagement der Unternehmensleitung für das Transformationsprogramm.

Wie an den Beispielen zu sehen ist, variieren die beiderseitigen Ansprüche in Form, Umfang und Bedeutung. Mitunter werden individuelle Personen als IT-Stakeholder adressiert, in anderen Fällen sind es Gruppen oder Institutionen. Abbildung 4–2 zeigt die Bandbreite der legitimierten Beziehungen zwischen der Unternehmens-IT und ihren Stakeholdern.

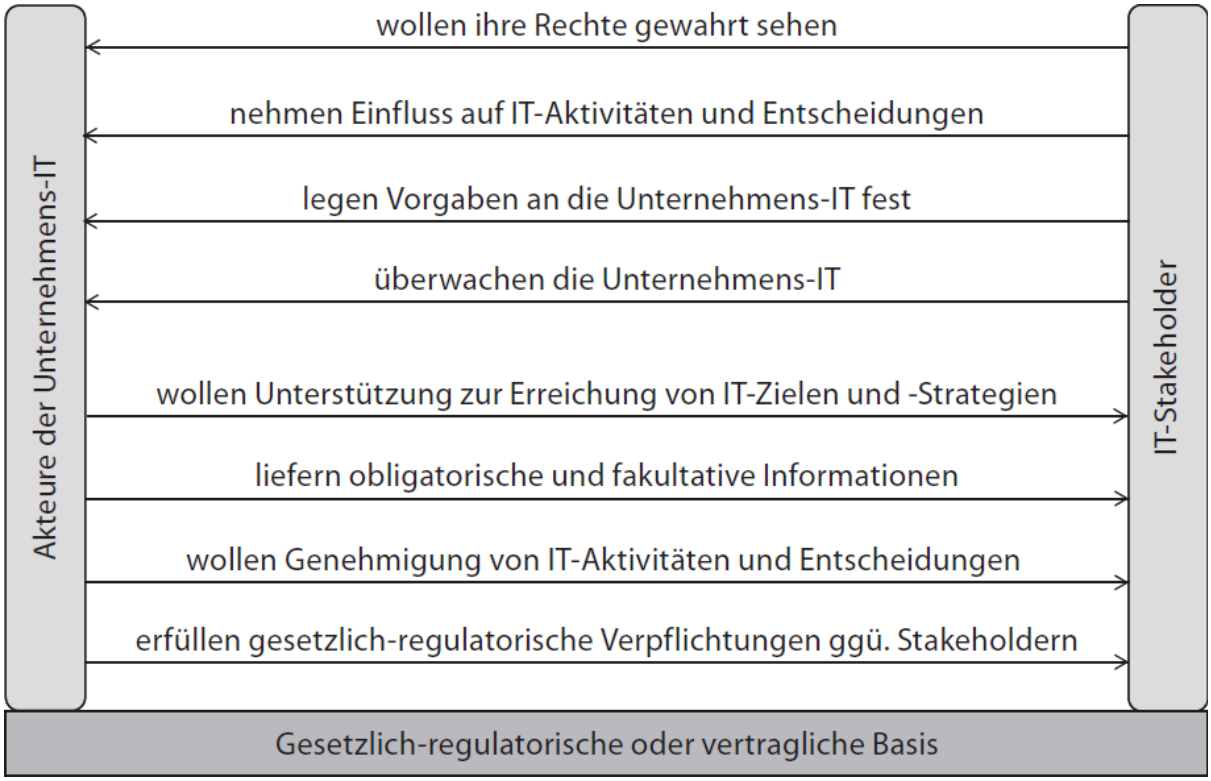

Abb. 4–2 *Zweiseitige Beziehungen zwischen Unternehmens-IT und IT-Stakeholdern*

Identifizierung von Personen

Auch wenn Gruppen oder Organisationen als Stakeholder anzusehen sind, ist es in den meisten Fällen sinnvoll, individuelle Personen – insbesondere für die IT-Stakeholder-Einbindung – zu benennen und Kontaktmöglichkeiten zu kennen. Bei den unternehmensinternen Stakeholdern fällt dies leicht. Bei unternehmensexternen Gruppen oder Organisationen müssen zuständige Stellen und die betreffenden Stelleninhaber, Ansprechpersonen oder verantwortlichen Führungskräfte erst bestimmt werden. Dies können beispielsweise zuständige Personen bei Aufsichtsinstitutionen, Vertriebskräfte und Kundenbetreuer bei IT-Dienstleistern und -Lieferanten, Ansprechpartner und Experten in der Verwaltung und in Verbänden oder auch bei den Medien beschäftigte Journalisten sein.

4.1.5 Akteure in der Unternehmensumwelt

Mit der vorgenommenen Abgrenzung werden zahlreiche Akteure der Unternehmenswelt nicht als Stakeholder der Unternehmens-IT betrachtet. Trotzdem geht von diesen mitunter ein starker Einfluss auf Themen und Maßnahmen der Unternehmens-IT aus. Diese Akteure sind somit den Triebkräften des Umfelds bzw. den geschäftlichen Anforderungen, die an die IT-Governance gestellt werden, zuzurechnen (vgl. Abb. 1–1). Beispiele für Akteure in der Unternehmensumwelt sind konkurrierende Unternehmen als Wettbewerber,

Medien sowie Standardisierungs- und Normungsorganisationen; weitere sind in Abbildung 4–3 genannt.

- **Wettbewerber des Unternehmens**

  Wettbewerber

  In der Gruppe der Wettbewerber des Unternehmens sind diejenigen Konkurrenzunternehmen relevant, denen es durch einen innovativen und effektiven IT-Einsatz gelingt, Wettbewerbsvorteile zu generieren. Hierdurch wird der Wertbeitrag der IT relativ gemindert und der Erfolg der Unternehmens-IT infrage gestellt. In manchen Branchen gilt die IT eines Unternehmens durch Präsentationen auf führenden Konferenzen und sonstigen Publikationen schnell als Best Practice, die es in den Augen der Unternehmensleitung oder der IT-Leitung zu überbieten oder doch zumindest zu egalisieren gilt. Aus Sicht des Konkurrenzunternehmens wird mit einer derartigen Marktkommunikation gerade der Anspruch erhoben, für den innovativen IT-Einsatz als Technologieführer der Branche zu fungieren. Folge für die Unternehmens-IT sind Rechtfertigungs- und Handlungsdruck, z.B. gegenüber der Unternehmensleitung.

- **Medien**

  Medien

  Insbesondere dann, wenn Fernsehsendungen oder Print- und Onlinemedien über negative Sachverhalte (z.B. ein Datenleck oder Ausfall der vom Unternehmen betriebenen Internetplattform) berichten, stellen sie einen wichtigen Akteur dar. Doch haben sie in der Regel keine wesentliche direkte Einflussmöglichkeit auf die Unternehmens-IT (in Bezug auf das gesamte Unternehmen mag dies anders sein). Eine negative Berichterstattung erzeugt jedoch Handlungsdruck für Verbesserungsmaßnahmen, insbesondere in den Bereichen der IT-Sicherheit und des Datenschutzes. Auf der anderen Seite können die Medien als Know-how-Lieferanten die Entwicklung der IT eines Unternehmens, beispielsweise über die Publikation von Best Practices, fördern. Dies gilt auch für Fachverlage, da sie mit ihren Publikationen, die mittlerweile immer umfangreicher auf verlagseigenen Plattformen angeboten werden, Unternehmen mit fachlichem Know-how versorgen.

- **Standardisierungs- und Normungsorganisationen**

  Standardisierungs- und Normungsorganisationen

  Zunehmenden Einfluss auf die Unternehmens-IT haben IT-Normen und -Standards. Im Rahmen der IT-Compliance muss sich die IT-Governance entscheiden, welche IT-Normen und -Standards verpflichtend sind oder als verbindlich angesehen werden sollen. Da Normen und Standards von den sie tragenden Organisationen, z.B. dem DIN, der ISO, der ISACA, in mehr oder minder regelmäßigen Abständen aktualisiert werden, ergibt sich

hieraus auch grundsätzlich ein kontinuierlicher Anpassungsdruck auf die Unternehmens-IT. Dies gilt vor allem für diejenigen Normen und Standards, die sich in der IT durchgesetzt haben, und für die im Geschäftsverkehr eine Zertifizierung erwartet wird. Dies ist beispielsweise für die ISO/IEC 27001 im IT-Sicherheitsmanagement der Fall. Verbindlichkeit erreichen Standards dort, wo sie auf gesetzlicher Grundlage vorgeschrieben werden. Dies ist beispielsweise der Fall bei den branchenspezifischen Sicherheitsstandards (B3S), die von KRITIS-Betreibern zu erfüllen sind.

4.2 IT-Stakeholder

4.2.1 Unterscheidung zwischen externen und internen IT-Stakeholdern

Externe IT-Stakeholder

Stakeholder der Unternehmens-IT lassen sich – wie Stakeholder des Unternehmens insgesamt auch – grundlegend in unternehmensexterne und unternehmensinterne IT-Stakeholder unterscheiden.

- **Externe IT-Stakeholder**

  sind Personen, Gruppen oder Organisationen in der Unternehmensumwelt, mit denen die Unternehmens-IT in Interaktion steht. Zum einen sind dies auf gesetzlicher Basis eingerichtete Aufsichtsinstitutionen, wie das BSI und die Landesdatenschutzbehörden. Auf vertraglicher Basis sind zum anderen die Beziehungen zu Geschäftspartnern, wie IT-Dienstleistern und -Lieferanten, geregelt. Aus den jeweiligen Verträgen ergeben sich gegenseitige Ansprüche als Rechte und Pflichten im Zuge der Vertragserfüllung.

- **Interne IT-Stakeholder**

  sind Akteure, die dem Unternehmen auf einer gesellschaftsrechtlichen oder arbeitsvertraglichen Basis angehören. Dies sind einerseits Anteilseigner, die ggf. auch Mitglied des Aufsichtsrates sind, andererseits Personen, die verschiedene Positionen in der Unternehmens-IT gemäß dem 3-Linien-Modell einnehmen (siehe Abschnitt 5.3.4). Bei angestellten Akteuren ist die im Arbeitsvertrag geregelte Aufgabenzuordnung Grundlage der gegenseitigen Beziehungen. Konkrete Ausgestaltungen von Aufgaben und Arbeitszusammenhang ergeben sich über die Aufgabendelegation mit der Zuweisung von Befugnissen und Verantwortlichkeiten und daraus resultierenden Anrechten, z.B. auf Information oder Beteiligung.

Unterscheidung in COBIT

Auch COBIT 2019 betrachtet sowohl interne als auch externe IT-Stakeholder. Zu den internen Stakeholdern zählen die Unternehmensleitung bzw. die oberste Führungsebene, das Management der Fachbereiche, das IT-Management, externe Prüfer der IT und das Risikomanagement. Externe Stakeholder sind Regulierungsbehörden, Geschäftspartner und IT-Lieferanten (nach [ISACA 2020a], S. 15).

Akteure werden zu IT-Stakeholdern.

Das geschäftliche Agieren des Unternehmens bewirkt einen materiellen, monetären und kommunikativen Austausch mit den Akteuren der Unternehmensumwelt. Dieser Austausch zeigt sich auch darin, dass manche Akteure ggf. zu IT-Stakeholdern werden können und regelmäßig werden, andere Akteure dagegen nicht (siehe Abb. 4–3). Offensichtliche Beispiele für den ersten Fall sind Personen oder Organisationen, die zu Kunden des Unternehmens werden. Ähnlich verhält es sich mit Anbietern von IT-Produkten oder -Dienstleistungen, mit denen ein Unternehmen verhandelt und ihnen schließlich einen Auftrag erteilt. Hierbei ist zu beachten, dass überall, wo vertragliche Vereinbarungen getroffen werden, bereits vorvertragliche, beiderseitige Vertrauens- und Sorgfaltspflichten bestehen, die auch vom Unternehmen zu erfüllen sind. Bei potenziellen neuen IT-Mitarbeitenden, die sich beim Unternehmen um eine Mitarbeit bewerben, ergeben sich ähnliche Ansprüche, die sich zudem auch auf Gleichbehandlung und Datenschutz erstrecken. Insofern umfasst die Legitimität von IT-Stakeholdern grundsätzlich auch einen vorvertraglichen Bereich. Andere Akteure, wie z.B. Medien oder Standardisierungs- und Normungsorganisationen, können nicht IT-Stakeholder werden, da sie mit Unternehmen in der Regel keine formal legitimierte Beziehung eingehen.

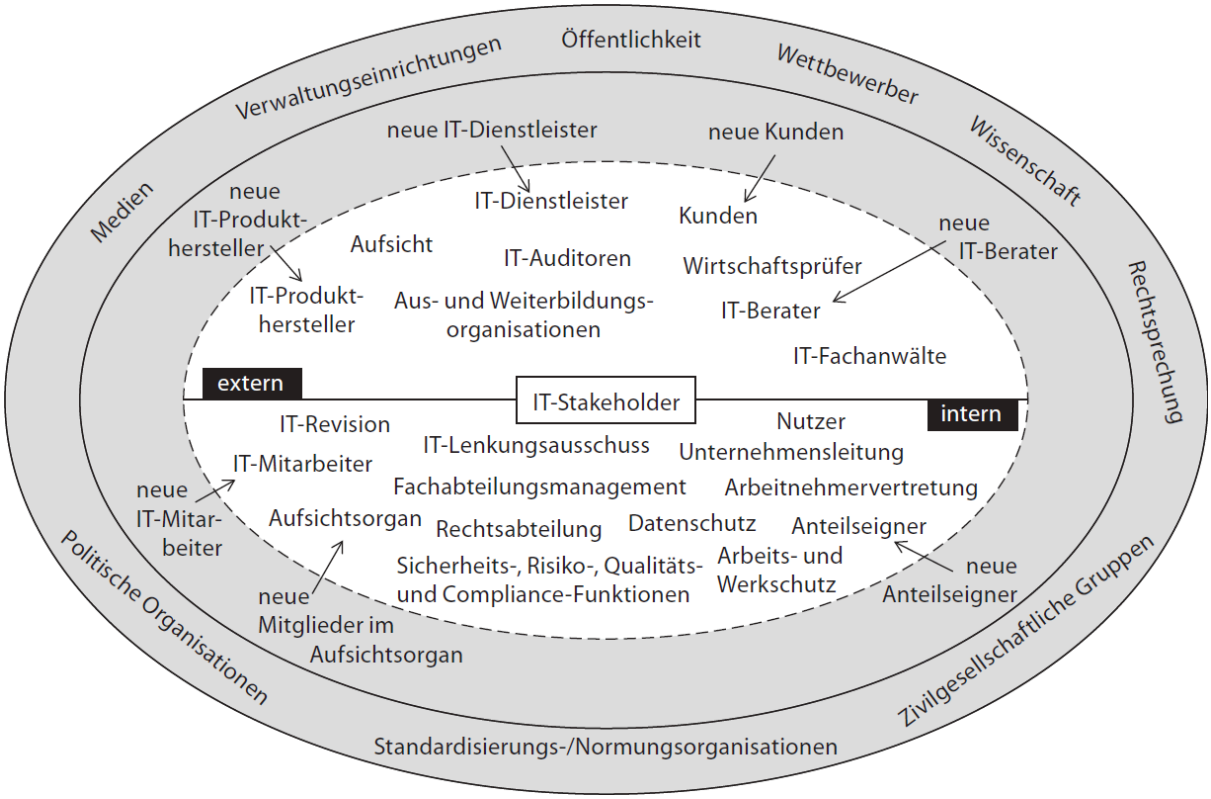

Abb. 4–3 *Interne und externe IT-Stakeholder vs. Akteure der Unternehmensumwelt*

Die in Abbildung 4–3 genannten internen und externen IT-Stakeholder und ihre Ansprüche werden jeweils in den beiden folgenden Abschnitten genauer beschrieben.

4.2.2 Interne IT-Stakeholder

Zu den internen IT-Stakeholdern zählen:

- **Aufsichtsorgan** *Aufsichtsorgan*

  Aufsichtsorgane, wie der Aufsichtsrat einer AG (siehe Abschnitt 3.3.1), haben sich im Rahmen ihrer Überwachungsverantwortung mit dem internen Kontrollsystem, dem Risikomanagement und dem Revisionssystem zu befassen. Hierbei wird auch die Unternehmens-IT fallweise Gegenstand der Überwachung sein, insbesondere dann, wenn entweder ein Schadensfall oder ein Fehlverhalten vorliegt, dessen Ausmaß eine Befassung durch den Aufsichtsrat erforderlich macht. In diesem Fall werden von der Unternehmens-IT Transparenz und Offenlegung von Informationen erwartet, wobei das Aufsichtsorgan diese in der Regel durch Beauftragung von internen oder externen Prüfungen aktiv sicherstellen wird. Zur Vermeidung derartiger Situation wird ein starkes Interesse des Aufsichtsorgans an einem angemessenen und wirksamen IT-Kontrollsystem bestehen. Des Weiteren wird die IT ins Blickfeld des Aufsichtsorgans

geraten, wenn der Wertbeitrag der IT generell oder konkret digitale Geschäftsmodelle bzw. Digitalstrategien auf der Agenda stehen. In diesem Fall wird der CIO oder der CDO die Mitglieder des Aufsichtsorgans mit den gewünschten Informationen zu IT-Zielen und -Strategien zu versorgen haben. Die Entwicklung und Implementierung der IT-Strategien liegen im Ermessen der Unternehmensleitung. Durch das Aufsichtsorgan werden die IT-Strategien im Rahmen einer strategischen Durchführungskontrolle sachlich und zeitlich auf ihren Umsetzungsstand hin überprüft und die Entwicklung der mit ihrer Umsetzung verbundenen Risiken kontinuierlich überwacht (vgl. [Welge & Eulerich 2021], S. 265).

- **Anteilseigner** *Anteilseigner*

  Je nach Rechtsform und Besetzung der Unternehmensorgane können Anteilseigner – insbesondere, wenn sie wesentliche Anteile am Unternehmen halten oder gar Mehrheitseigentümer sind – Einfluss auf die Ausgestaltung der IT nehmen (z.B. als Mitglied des Aufsichtsrats oder der Unternehmensleitung). Wie beim Aufsichtsorgan wird dies dann der Fall sein, wenn wesentliche Problemsituationen vorliegen oder der IT eine wettbewerbsstrategische Bedeutung zukommt. In diesen Fällen werden die Anteilseigner ihre – auch finanziellen – Ansprüche an die Unternehmens-IT gegenüber der Unternehmensleitung äußern und direkt oder indirekt geltend machen.

- **Unternehmensleitung** *Unternehmensleitung*

  Die Unternehmensleitung erwartet von einer IT, die im Wesentlichen eine Unterstützungsfunktion einnimmt, dass sie »funktioniert«, d.h. ihre Leistungen sicher, mit hoher Verfügbarkeit und einem akzeptablen Risikoniveau zu niedrigen Kosten erbringt (»Run the Business«). Dort, wo der IT eine wettbewerbsstrategische Bedeutung zukommt und sie mithin als »Enabler« fungiert«, stehen Ansprüche an den Wertbeitrag der IT sowie an die Flexibilität und Agilität, mit der neue, IT-gestützte Produktbestandteile oder IT-Leistungen generiert werden können, im Vordergrund (»Change the Business«). Da die Unternehmensleitung die konstitutiven Entscheidungen im Hinblick auf die Ausgestaltung der Unternehmens-IT trifft (insbesondere zu Budget, Eingliederung in die Unternehmensstruktur, IT-Strategie) sowie den Erfolg, die Risiken und die Compliance der IT zu steuern und zu überwachen hat, ist sie neben einem eventuellen Aufsichtsorgan der wesentliche interne IT-Stakeholder.

- **IT-Lenkungsausschuss** *IT-Lenkungsausschuss*

  Ein IT-Lenkungsausschuss ist für die Steuerung und Überwachung der IT verantwortlich, wobei sich sein Fokus vor allem auf das Business/IT-

Alignment, also auf die systematische Abstimmung von Business-Anforderungen und IT-Unterstützung richtet. Die Entscheidungen eines IT-Lenkungsausschusses haben Auswirkungen auf die IT-Anwendungslandschaft, aber auch die informations- und kommunikationstechnische Infrastruktur und nehmen hierdurch wesentlichen Einfluss auf den Wertbeitrag der IT.

- **Fachabteilungsmanagement** *Fachabteilungsmanagement*

  Das Fachabteilungsmanagement erwartet von der IT im Wesentlichen die effektive und effiziente Unterstützung der Geschäftsprozesse durch die IT-Systeme und -Services. Dies umfasst auch die entsprechende Wartung und Weiterentwicklung sowie die rechtzeitige Bereitstellung neuer IT-Systeme. Das Fachabteilungsmanagement ist ggf. Mitglied in einem IT-Lenkungsausschuss und ähnlichen Gremien und hat insofern Möglichkeiten der Einflussnahme. Dies ist auch dann der Fall, wenn im Rahmen von Budgetierungen bzw. Profit-Center-Strukturen das Fachabteilungsmanagement als Auftraggeber für die Entwicklungen von IT-Systemen oder im Rahmen von Service Level Agreements als interner Vertragspartner agiert. Damit sind die Mitglieder des Fachabteilungsmanagements wichtige IT-Stakeholder, insbesondere dann, wenn im Unternehmen eine einvernehmliche Verantwortungsteilung für IT-Systeme und IT-Projekte zwischen der IT-Abteilung und den Fachabteilungen z.B. derart erfolgt, dass die Fachabteilungen das Frontend und die IT-Abteilung die zugrunde liegende Plattform verantwortet (nach [Kopper et al. 2017], S. 140). Große, einflussreiche Fachabteilungen können sehr wichtige Stakeholder darstellen, wenn ihre IT-Systeme den Unternehmenserfolg wesentlich beeinflussen und einen Großteil des Entwicklungsportfolios betreffen. In einer solchen Situation kann verbunden mit budgetärer Verfügungsgewalt schnell eine »Schatten-IT« entstehen, die sich der Steuerung und Überwachung der IT-Abteilung entzieht. Hier muss die IT-Governance gegensteuern, z.B. durch einen Kontrahierungszwang zwischen Fachabteilung und IT-Abteilung und klare IT-Richtlinien für Beschaffung, IT-Betrieb, IT-Risiko- und -Sicherheitsmanagement.

- **IT-Revision** *IT-Revision*

  Der Revisionsabteilung hat in ihrer Unterstützungsfunktion für die Unternehmensleitung zu prüfen, »ob und inwieweit die informationsverarbeitenden Systeme, Prozesse und Schnittstellen die anfordernden Geschäftsprozesse in der Erfüllung ihrer Aufgaben unterstützen« ([Thelemann & Bunzel 2011], S. 149 f.). Konkret erfolgt die Prüfung nach Kriterien, wie Vertraulichkeit, Verfügbarkeit, Wirtschaftlichkeit

oder Compliance. Die IT-Revision prüft ergebnisoffen, d.h. objektiv und ohne Erwartungen. Sie hat jedoch Anforderungen an die IT in Bezug auf die Prüfbarkeit der Prüfobjekte und die Unterstützung der Prüfung durch die IT-Abteilung. Mit den Feststellungen als Ergebnis einer Prüfung hängt das »Standing« der IT in den Augen der Unternehmensleitung nicht unbeträchtlich vom Urteil der IT-Revision ab.

- **Rechtsabteilung** *Rechtsabteilung*

  Die Rechtsabteilung fordert von der IT die rechtskonforme Durchführung der IT-Prozesse. Dies geht über Datenschutz und IT-Sicherheit hinaus und umfasst zudem im Rahmen der Beschaffung vertrags-, vergabe- und lizenzrechtliche Anforderungen, im IT-Betrieb arbeitsschutz- und wettbewerbsrechtliche Vorgaben sowie geschäftliche Anforderungen an den elektronischen Geschäftsverkehr. Hierzu steht die Rechtsabteilung der IT als beratende Funktion zur Seite, muss allerdings auch seitens der IT-Funktion einbezogen werden. Soweit die IT-Funktion vertragliche Vereinbarungen eingehen muss, sollte die Pflicht zur Einbeziehung der Rechtsabteilung bestehen oder eine klar geregelte Verantwortungsteilung vorliegen.

- **Datenschutzbeauftragter** *Datenschutzbeauftragter*

  Dem Datenschutzbeauftragten (DSB) obliegt eine Überwachungsfunktion in Bezug auf die Einhaltung der datenschutzrechtlichen Vorgaben nach der Datenschutzgrundverordnung (DSGVO) bzw. dem Bundesdatenschutzgesetz (BDSG). Die gewachsene Bedeutung des DSB resultiert einerseits aus den beträchtlichen potenziellen Bußgeldern im Falle von Verstößen gegen die Vorgaben der DSGVO, andererseits aus seiner Verpflichtung zur Informationsweitergabe an die jeweils zuständige externe Datenschutzaufsichtsinstitution. Hinzu kommen die Prüfrechte, die dem DSB bei der Entwicklung von IT-Systemen oder der Inanspruchnahme von externen IT-Services gewährt werden. Datenschutzrechtliche Non-Compliance zählt in vielen Unternehmen heute zu den wesentlichen Risiken, was die Einordnung des DSB als relevanten Stakeholder rechtfertigt.

- **Sicherheits-, Risiko-, Qualitäts- und Compliance-Management** *Sicherheits-, Risiko-, Qualitäts- und Compliance-Management*

  Unternehmensweite Funktionen, die sich mit Unternehmenssicherheit, Enterprise Risk Management, Qualität und Corporate Compliance befassen, müssen auch die jeweilige Ausprägung in Bezug auf die Unternehmens-IT im Auge haben (2. Linie des TLM, siehe Abschnitt 5.3.4). Gegebenenfalls halten sie hierfür eigene IT-Spezialisten in ihren Organisationseinheiten vor,

z.B. Risikoanalysten, die mittels Process Mining große Bestände an Prozessdaten nach Auffälligkeiten untersuchen (vgl. [Knoll 2019], S. 126). Andernfalls sind sie auf eine Zusammenarbeit mit der IT-Funktion angewiesen, was zu entsprechenden Anforderungen an die Information durch und die Kommunikation mit der IT-Abteilung führt. Da diese überwachenden Funktionen häufig der Unternehmensleitung als Stabsabteilungen zugeordnet sind, können sie ihre Forderungen mit Nachdruck vertreten.

- **IT-Mitarbeiter** *IT-Mitarbeiter*

  Auch die (führenden und ausführenden) IT-Mitarbeiterinnen und -Mitarbeiter als Teil der IT-Abteilung oder ggf. auch der Fachabteilung stellen wichtige IT-Stakeholder dar. Aus Sicht der qualitativen Personalplanung müssen sie über die erforderlichen Fähigkeiten verfügen, um durch die effektive und effiziente Entwicklung und Bereitstellung von IT-Systemen und IT-Services den Wertbeitrag der Unternehmens-IT operativ sicherzustellen. Sollten diese Fähigkeiten nicht verfügbar sein, muss die Personalabteilung sie auf dem Personalmarkt beschaffen oder durch Maßnahmen der Personalentwicklung den Erwerb dieser Fähigkeiten bewirken. Eine Missachtung der Interessen der eigenen IT-Mitarbeiter wird zu unerwünschten Mitarbeiterabgängen führen und gleichzeitig ihren Ersatz erschweren, wenn das Unternehmen auf Jobportalen schlecht bewertet wird (vgl. [Beckmann & Horst 2009], S. 112).

- **Nutzer der IT-Systeme** *Nutzer der IT-Systeme*

  Die Nutzer der IT-Systeme wollen zuverlässige, leicht bedienbare und leistungsfähige IT-Systeme für die Bearbeitung ihrer Aufgaben einsetzen. Hierfür müssen sie sich an Richtlinien und Anweisungen orientieren, die ihren Handlungen Sicherheit geben. Allerdings wollen die IT-Nutzer in ihrer Arbeit nicht behindert werden (vgl. [Baumöl 2012], S. 10). IT-Nutzer können über das jeweils vorgesetzte Management nur indirekt Einfluss nehmen. Eine andere Möglichkeit der Einflussnahme ist der Weg über formale Kanäle, z.B. im Rahmen einer Nutzer-Hotline, eines Hinweisgebersystems oder der in Service Level Agreements geregelten Kommunikations- und Eskalationswege.

- **Arbeitnehmervertretung** *Arbeitnehmervertretung*

  Die Arbeitnehmervertretung nimmt ihre Aufgaben gemäß der ihr gesetzlich zugewiesenen Verantwortung zum Nutzen der Belegschaft wahr. Sie verfügt über die ihr nach dem Betriebsverfassungsgesetz (BetrVG) zustehenden Informations- und Mitbestimmungsrechte. Dies ist nach § 87 Abs. 1 Nr. 6 BetrVG vor allem dann der Fall, wenn IT-Systeme potenziell zur

Überwachung von Arbeitnehmern geeignet sind. Über den Abschluss von Betriebsvereinbarungen hat die Arbeitnehmervertretung die Möglichkeit, im Schutzinteresse der Mitarbeiter auf die Ausgestaltung der IT Einfluss zu nehmen.

- **Werkschutz** *Werkschutz*

  Der gewöhnlich im Facility-Management angesiedelte Werkschutz (bzw. Sicherheitsdienst) sichert u.a. die Liegenschaften eines Unternehmens gegen unbefugten Zutritt, indem er Personen beim Betreten des Werkgeländes oder einzelner Gebäude kontrolliert, Personenbewegungen im Außengelände und in Innenräumen überwacht und Gebäude und Räumlichkeiten gegen gewaltsames Eindringen sichert. Damit ist er Teil der physikalischen Zutrittskontrolle zu IT-Räumen und -Gerätschaften. Mitunter ist der Werkschutz auch für die Überwachung von Teilen der IT-Infrastruktur und bei Vorkommnissen für die Meldung bei Störungen zuständig.

- **Arbeitsschutz** *Arbeitsschutz*

  Ein im Unternehmen institutionalisierter Arbeitsschutz muss heute auch auf Herausforderungen einer digitalen Arbeitswelt reagieren. Der Arbeitsschutz hat die Vorgaben des Arbeitsschutzgesetzes (ArbSchG) bzw. der Arbeitsstättenverordnung umzusetzen. Dies betrifft insbesondere die Anordnung und Ausstattung der IT-Arbeitsplätze, aber auch die ergonomische Organisation der Bildschirmarbeit.

4.2.3 Externe IT-Stakeholder

Zu den externen IT-Stakeholdern zählen:

- **Kunden des Unternehmens** *Kunden*

  Als Nutzer der Unternehmens-IT oder als ihr Adressat, z.B. bei einer auf Basis historischer Kaufdaten individuellen Kundenansprache, ist diese Gruppe sowohl für das Unternehmen insgesamt als auch für die IT-Funktion wichtig. Dies gilt vor allem bei B2C-Geschäftsbeziehungen über das Internet, in denen Kunden verfügbare bzw. zuverlässige, leicht bedienbare und leistungsfähige IT-Systeme bzw. IT-Produkte zur Realisierung ihrer Ziele einsetzen wollen. Auch wenn einzelne Kunden kaum einen wesentlichen Einfluss nehmen können, kann eine Vielzahl von Kunden durch Ausweichen auf IT-Services anderer Anbieter beträchtliche wirtschaftliche Verluste bewirken. Im Extremfall kann ein komplettes Geschäftsmodell durch eine Veränderung des Nutzerverhaltens infrage gestellt werden. Der Kunde ist aber nicht nur handelnder Akteur; seine Daten sind auch Objekt der IT, z.B. dann, wenn im datenschutzrechtlichen Rahmen Kundenprofile erstellt und

ausgewertet werden oder vor dem Hintergrund der Geldwäscheprävention Kundendaten zur Qualifizierung und Identifizierung der betroffenen Person zu verarbeiten sind.

- **Aufsichtsinstitutionen** *Aufsichtsinstitutionen*

  Neben den Kunden des Unternehmens zählen Aufsichtsinstitutionen, wie z.B. das BSI oder in der Finanz- und Versicherungsbranche die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), zu den wesentlichen externen Stakeholdern der Unternehmens-IT. Aufsichtsinstitutionen nehmen eine gesetzlich verankerte Überwachungsfunktion wahr und stellen sicher, dass sich Unternehmen in ihrem IT-Betrieb gesetzeskonform verhalten. Hierzu überwachen sie die Erfüllung der gesetzlichen Vorgaben oder stellen konkrete Anforderungen, wie dies z.B. mit den »Bankaufsichtlichen Anforderungen an die IT« (BAIT) der Fall ist. Ergebnis der Überwachung durch Aufsichtsinstitutionen können infolge von Prüfungen umfangreiche Auflagen, letztlich auch ein Betriebsverbot, oder immense Bußgelder sein. Letzteres ist vor allem vor dem Hintergrund des Datenschutzes sowie der IT-Sicherheit der Fall. Im operativen Tagesgeschäft sind vom Unternehmen Berichtspflichten zu erfüllen, die Grundlage für die Überwachung durch die Aufsichtsinstitutionen sind. Ebenfalls zur Aufsicht zählen die Finanzämter, die durch die Betriebsprüfer – ggf. im Rahmen einer digitalen Betriebsprüfung – die IT-gestützte Buchhaltung des Unternehmens prüfen.

- **IT-Dienstleister** *IT-Dienstleister*

  Das Interesse von IT-Dienstleistern, mit denen das Unternehmen eine strategische Geschäftsbeziehung unterhält, besteht in einer langfristigen und profitablen Geschäftsbeziehung. IT-Dienstleister verfügen in diesen Fällen mitunter über eine beträchtliche Verhandlungsmacht, da es dem Unternehmen schwerfallen kann, zu einem Wettbewerber zu wechseln. Dies ist bei einem umfangreichen IT-Outsourcing der Fall, wo gerade die Beendigung der Geschäftsbeziehung und der Übergang auf einen neuen IT-Dienstleister oftmals nur ungenügend geregelt sind. Aber auch im operativen IT-Betrieb kann ein Unternehmen von seinem IT-Provider abhängig sein, wenn die eigene IT-Infrastruktur aufgegeben wurde und das betreffende Know-how durch Personalabbau nicht mehr vorhanden ist. Insbesondere Unternehmen als KRITIS-Betreiber müssen ihre IT-Dienstleister identifizieren, von denen sie kritische Dienstleistungen beziehen.

- **Hersteller von IT-Produkten** *IT-Produkthersteller*

Werden in den Bereichen ERP, SCM oder CRM umfangreich Standardsoftwarepakete eingesetzt, so ist das Unternehmen auf eine langfristige Zusammenarbeit mit dem jeweiligen Hersteller angewiesen. Diese Zusammenarbeit beginnt bereits in der Auswahl- und Einführungsphase mit Installation, Migration von Altsystemen, Customizing und Schulung. Grundlage der Betriebsphase ist ein Wartungsvertrag, mit dem sich das Anwenderunternehmen Unterstützung bei Problemen im laufenden IT-Betrieb (ggf. über einen Hotline-Service), bei der regelmäßigen Überprüfung der Funktions- und Leistungsfähigkeit, inkl. der Installation von Updates, und bei der Störungsbeseitigung sichern kann (vgl. [Klotz & Dorn 2008], S. 178). IT-Produkthersteller verfolgen – genauso wie IT-Dienstleister – im Wesentlichen geschäftliche Interessen, die nicht immer mit den Interessen ihrer Kundenunternehmen gleichgerichtet sind. Trotz dieser Konfliktsituation müssen beide Parteien ein gemeinsames Interesse an einer für beide Seiten profitablen und nutzbringenden Geschäftsbeziehung haben. Gelingt dies nicht, drohen Auseinandersetzungen und jeweils erhobene Ansprüche, die ggf. auf juristischem Wege verfolgt werden.

- **IT-Berater** *IT-Berater*

  Vom Unternehmen beauftragte IT-Berater, z.B. für Fragen der IT-Strategie, der digitalen Transformation, der IT-Sicherheits- und IT-Risikomanagementsysteme, stellen während der Zusammenarbeit wichtige externe Stakeholder dar. Dies ist vor allem dann der Fall, wenn externe Mitarbeiter als »Manager auf Zeit« IT-Projekte oder -Programme leiten. Von ihren Erfahrungen und der Qualität der Zusammenarbeit wird der Erfolg des jeweiligen Vorhabens abhängen. Zwar sollte durch das Auftragsverhältnis grundsätzlich eine umfangreiche, direkte Beeinflussbarkeit des Auftragnehmers durch das Unternehmen gegeben sein, allerdings sind Möglichkeiten der Steuerung und Überwachung gewöhnlich vertraglich geregelt. Dies umfasst auch Pflichten des Unternehmens dem Auftragnehmer gegenüber.

- **IT-Fachanwälte** *IT-Fachanwälte*

  Das IT-Recht ist mittlerweile so umfangreich, dass Hausjuristen des Unternehmens nicht alle Rechtsgebiete (z.B. Datenschutz-, Urheber-, Domain-, E-Commerce-Recht) abdecken können. Deshalb ist eine kontinuierliche Zusammenarbeit mit externen IT-Fachanwälten keine Seltenheit mehr. Fälle, in denen die Inanspruchnahme externer Rechtsexpertise sinnvoll oder notwendig ist, stellen umfangreiche IT-Verträge dar, wie dies bei IT-Outsourcing die Regel ist. Vor allem bei

internationaler Geschäftstätigkeit im Internet sind die rechtlichen Anforderungen komplex und unterliegen einer hohen Dynamik.

- **Wirtschaftsprüfer**

  Wirtschaftsprüfer

  Vom Unternehmen beauftragte Wirtschaftsprüfer prüfen die IT im Zuge der Jahresabschlussprüfung oder im Rahmen von Sonderprüfungen, z.B. IT-Sicherheitsaudits, projektbegleitende Prüfungen, Softwarezertifizierungen oder auch forensische Datenanalysen bei Betrugsverdacht. Die externen Prüfer haben ähnliche Anforderungen wie die Interne Revision, was die Prüfbarkeit der Prüfobjekte und die Unterstützung der Prüfung durch die IT-Abteilung anbelangt. Eventuelle negative Feststellungen des Wirtschaftsprüfers rücken die IT-Funktion in ein ungutes Licht, geben aber gleichzeitig Anlass für eine Verbesserung von IT-Prozessen und -Systemen.

- **IT-Auditoren**

  IT-Auditoren

  Durch das Unternehmen beauftragte externe IT-Auditoren führen ebenfalls wie die Wirtschaftsprüfer Konformitätsprüfungen der Unternehmens-IT durch. Insofern gibt es Überschneidungen in den Prüfungsgegenständen, z.B. bei Datenschutzaudits. Einen Wettbewerbsvorteil haben IT-Auditoren dann, wenn sie von einer dazu ermächtigten Organisation eine Zertifizierung als Prüfer erhalten. Dies ist z.B. der Fall bei Auditoren, die vom BSI für ISO-27001-Audits auf der Basis von IT-Grundschutz zertifiziert sind (vgl. [BSI 2021]).

- **Aus- und Weiterbildungsorganisationen**

  Aus- und Weiterbildungsorganisationen

  Zum Zwecke der Weiterbildung sind es vor allem Veranstalter von Konferenzen und Seminaren, die das Know-how zu aktuellen IT-Thematiken vermitteln. Das Unternehmen ist hier in der Lage, aus einem breiten Angebot auszuwählen, ohne allerdings selbst Einfluss nehmen zu können (bis auf die Ausnahme unternehmensindividueller Veranstaltungen).

Wachsende Bedeutung von IT-Stakeholdern

Die Vielzahl der hier aufgeführten IT-Stakeholder zeigt, warum die Bedeutung der Stakeholder-Ausrichtung der IT stark zugenommen hat. Neben konventionellen Lieferanten, z.B. von Hardware und Anwendungssoftware, sind mit digitalen Geschäftsmodellen und den daraus resultierenden vielfältigen IT-technischen Verbindungen mit Interessenten und Kunden sowie einem IT-Outsourcing, das mit seinen unterschiedlichen Cloud-Ausprägungen in der Mehrzahl der Unternehmen heute zum IT-Alltag zählt, Stakeholder auf den Plan getreten, ohne die eine effektive und effiziente IT-Nutzung in Unternehmen nicht mehr denkbar ist. Hinzu kommen die zahlreichen allgemeinen und

branchenbezogenen externen Regulierungs- und Aufsichtsinstitutionen, die den Fokus auf IT-Stakeholder aus dem Unternehmensumfeld richten. Mit den zunehmenden gesetzlichen Anforderungen und den damit verbundenen potenziellen hohen Bußgeldern bei Non-Compliance ist auch für den Bereich der IT grundsätzlich mit Schadensersatzforderungen durch Stakeholder zu rechnen, die diese ggf. gerichtlich durchsetzen. In der Summe ergibt sich eine Vielzahl von IT-Stakeholder-Gruppen, die einen Stakeholder-Ansatz als Teil der IT-Governance unumgänglich macht.

4.3 Ziele der IT-Governance in Bezug auf die IT-Stakeholder

Ziele der IT-Stakeholder-Governance

Die Akteure der IT-Governance müssen die Erwartungen, Ansprüche und Bedarfe nicht aller, sondern der wichtigen IT-Stakeholder fokussieren. Dies setzt voraus, dass im Rahmen der Stakeholder-Identifizierung (siehe Abschnitt 4.5.1) die wesentlichen Stakeholder ermittelt wurden. Die Ziele der IT-Governance in Bezug auf diese IT-Stakeholder gehen in drei Richtungen (vgl. Abb. 4–4):

- Erstens ist im Rahmen der IT-Governance die Unterstützung der IT-Stakeholder für die grundsätzliche Ausrichtung der Unternehmens-IT, die IT-Strategie und ihre Umsetzung zu erlangen.
- Zweitens ist die Compliance mit Anforderungen externer IT-Stakeholder sicherzustellen, sodass die Unternehmens-IT nicht in den Fokus von Aufsichtsinstitutionen gerät oder sich der Kritik weiterer wesentlicher Stakeholder ausgesetzt sieht.
- Drittens sollten eine effektive Kommunikation mit den IT-Stakeholdern sowie ihre systematische Einbeziehung eine positive Einstellung der Stakeholder gegenüber der Unternehmens-IT bewirken.

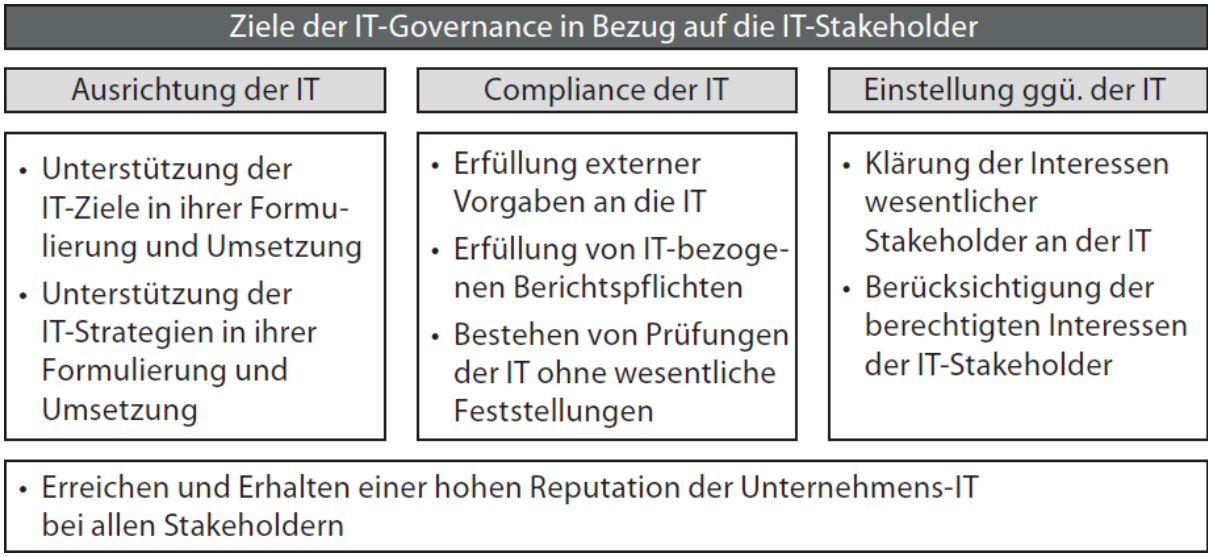

Abb. 4–4 *Ziele der IT-Stakeholder-Governance*

- **Ausrichtung der IT** *Ausrichtung der IT*

  Die IT-Governance muss danach streben, dass die wesentlichen Stakeholder die IT-Ziele und die IT-Strategie des Unternehmens in ihrer Formulierung und Umsetzung unterstützen bzw. sich hinsichtlich der Verfolgung der IT-Ziele und der Umsetzung der IT-Strategie zumindest neutral verhalten. Dies erfordert regelmäßig eine frühzeitige Einbindung der IT-Stakeholder, verbunden mit einer adäquaten Information und einer effektiven Kommunikation.

- **Compliance der IT** *Compliance der IT*

  Die IT-Stakeholder-Governance hat dafür zu sorgen, dass durch externe Stakeholder vorgegebene, verbindliche Compliance-Anforderungen an die Unternehmens-IT erfüllt werden. Dies gilt vor allem für Vorgaben aus Gesetzen, Verordnungen und Verwaltungsanweisungen, deren Einhaltung durch Aufsichtsinstitutionen überwacht wird. Diese Überwachung erfolgt zum einen durch Berichtspflichten, die einem Unternehmen auferlegt sind, oder zum anderen durch Prüfungen der Aufsichtsinstitution. In Bezug auf die obligatorische Berichterstattung bedeutet dies, dass die Anforderungen der betreffenden Stakeholder zu analysieren und zu beurteilen sind, die Pflichtberichte, die diesen Anforderungen entsprechen, validiert und genehmigt werden und durch Überwachungsmaßnahmen die Genauigkeit und Zuverlässigkeit von Pflichtberichten sichergestellt wird (vgl. [ISACA 2020b], S. 50). Auch die Einhaltung wichtiger vertraglicher Vereinbarungen fällt unter diese Zielsetzung.

- **Einstellung gegenüber der IT** *Einstellung gegenüber der IT*

Die Interessen der wesentlichen Stakeholder müssen geklärt und berücksichtigt werden, damit sie gegenüber der IT positiv eingestellt sind. Hier geht es im Wesentlichen um Kommunikationsmaßnahmen zur Klärung der Interessen, eine proaktive Information und eine der jeweiligen Bedeutung der verschiedenen Stakeholder angemessene Partizipation an der Entwicklung und Gestaltung der Unternehmens-IT.

Reputation der IT

Für die Realisierung dieser drei Ziele ist eine hohe Reputation der IT bei allen ihren Stakeholdern zu erreichen und zu erhalten. Anders ausgedrückt liegt es in der Verantwortung der Akteure der IT-Governance, das Vertrauen der Stakeholder in die Unternehmens-IT zu stärken und einen Vertrauensverlust zu vermeiden.

Kommunikation mit wesentlichen IT-Stakeholdern

Diese Zielsetzungen liegen in erster Linie im Interesse der Unternehmensleitung (inkl. CIO und/oder CDO) und der IT-Leitung. Insofern werden sie sich in die Information der wesentlichen IT-Stakeholder und die Kommunikation mit ihnen selbst einbringen müssen.

… mit internen IT-Stakeholdern

Im Fall der internen IT-Stakeholder werden sich Information und Kommunikation auf institutionalisierten Wegen vollziehen, beispielsweise als Tagesordnungspunkt einer Aufsichtsratssitzung, als Bericht des CIO bzw. CDO und Diskussion bei einem Meeting der Unternehmensleitung oder als Teil der Agenda einer Sitzung des IT-Lenkungsausschusses. In all diesen Fällen werden die Stakeholder durch vorbereitende Unterlagen über die zu diskutierenden und ggf. zu entscheidenden Sachverhalte – insbesondere IT-Ziele und IT-Strategien, aber auch wesentliche IT-Probleme – informiert, Diskussionen werden im jeweiligen Gremium geführt und durch die Protokollierung dokumentiert. Die Akteure der IT-Stakeholder-Governance sind an dieser Stelle also persönlich involviert. Sie vertreten selbst die zur Diskussion stehenden Themen, erhalten Rückmeldungen der IT-Stakeholder und müssen diese verarbeiten. Je nach der formalen Ausgestaltung, beispielsweise durch Geschäftsordnungen, können Vorlagen zu IT-Zielen und -Strategien eine Zustimmung wesentlicher IT-Stakeholder erfordern, insbesondere dann, wenn hohe IT-Investitionen Bestandteil der Entscheidungsvorlagen sind oder eine grundlegende Umgestaltung ansteht, was z.B. bei einer Auslagerung der IT-Funktion der Fall wäre.

… mit externen IT-Stakeholdern

Für die Kommunikation mit wesentlichen externen IT-Stakeholdern ist grundsätzlich die Unternehmensleitung verantwortlich. Allerdings wird sie beispielsweise gegenüber Aufsichtsinstitutionen bei Prüfungen oder für die regelmäßige Berichterstattung kaum selbst agieren, sondern die notwendigen Handlungen und Maßnahmen an die Experten der unterstützenden Organisationseinheiten

(Compliance, Rechtsabteilung etc.) oder an die IT-Leitung und das Abteilungsmanagement der IT-Funktion delegieren. Gleiches gilt für strategische IT-Dienstleister, wo IT- und Beschaffungsfunktion gemeinsam mit der Rechtsabteilung die geschäftliche Beziehung in fachlicher, rechtlicher, organisatorischer und technischer Hinsicht wahrnehmen werden. Auch werden Unternehmensleitung und CIO bei wesentlichen Feststellungen durch den beauftragten Wirtschaftsprüfer und beim Abschluss von wichtigen Betriebsvereinbarungen mit der Arbeitnehmervertretung aktiv tätig werden müssen. Für das Vertrauen von externen Stakeholdern spielen effektive interne IT-Richtlinien sowie IT-Standards und -Normen, deren Einhaltung durch Zertifizierungen nachgewiesen werden kann, eine wichtige Rolle.

Qualität der Kommunikation

Die Qualität der Stakeholder-Kommunikation wird wesentlich von der Unternehmenskultur geprägt sein. Formale Strukturen können die Information und Kommunikation in Richtung der internen Stakeholder regeln, aber auch laterale und agile Handlungsweisen in Führung und Kooperation sind hier gefragt. Beispiele in der IT sind Service Level Agreements (SLA) für die geregelte Zusammenarbeit zwischen IT-Funktion und Fachabteilungen oder ein an den Informationsbedürfnissen der Stakeholder ausgerichtetes IT-Reporting,

Ebenengerechte Kommunikation

Idealerweise gelingt es, die IT-Stakeholder zu überzeugen und ihre aktive Unterstützung zu erlangen. Wenn dies jedoch nicht möglich ist, muss zumindest eine neutrale Haltung erreicht werden. Dies ist vor allem bei wesentlichen Stakeholdern, die über ein großes Interesse an der IT und gleichzeitig großen Einfluss haben, wichtig. Eine ebenengerechte IT-Stakeholder-Kommunikation »auf Augenhöhe« (Management zu Management, Fachexperte zu Fachexperte) ist hier entscheidend. Wesentliche IT-Stakeholder sind regelmäßig und umfassend zu informieren, dies aber nicht nur durch ein Standard-Reporting, sondern auch in Meetings und bilateralen Gesprächen. Wo erforderlich, sind diese Stakeholder verantwortlich einzubeziehen, z.B. im Rahmen von Abstimmungs- und Freigabeprozessen.

Balanced Scorecard

Als Instrument zur Unterstützung von Vorständen und Aufsichtsräten bei der Steuerung und Überwachung einer effektiven Corporate Governance wird empfohlen, neben eventuell bereits bestehenden Balanced Scorecards (BSC), die bisher als Managementinstrument genutzt werden, weitere spezialisierte Scorecards für den Aufsichtsrat und die Unternehmensleitung als Governance-Instrument einzusetzen (nach [Welge & Eulerich 2021], S. 304 f.). Hierbei sollte die Kundenperspektive zu einer Stakeholder-Perspektive erweitert werden (vgl. [Welge & Eulerich 2021], S. 316 f.). Ob Belange der IT in eine Governance-BSC integriert werden oder eine für IT-Governance spezialisierte BSC erforderlich ist, hängt von der Stellung der Unternehmens-IT im Unternehmen und ihrem

Wertbeitrag ab. Befindet sich ein Unternehmen auf dem Weg der digitalen Transformation, kann eine IT-BSC für den Aufsichtsrat und die Unternehmensleitung sinnvoll genutzt werden. Dies gilt sowohl für die Entwicklung als auch für die Umsetzung einer Digitalisierungsstrategie. Gerade in der strategischen Planung als Teil der Strategieentwicklung kann die BSC eingesetzt werden, wenn die Perspektiven so gewählt werden, dass sie das digital unterstützte bzw. datengetriebene Geschäftsmodell widerspiegeln (nach [Becker et al. 2019], S. 49). Es ist vor allem die Mehrperspektivenbetrachtung, inkl. der Stakeholder-Perspektive, die die BSC zu einem wirkungsvollen Instrument der Transformation des Geschäftsmodells macht (nach [Becker et al. 2019], S. 51).

4.4 Abgrenzung zum IT-Stakeholder-Management

Governance vs. Management de IT-Stakeholder

Die Aufgaben der IT-Governance in Bezug auf die IT-Stakeholder sind von den Aufgaben des IT-Stakeholder-Managements zu unterscheiden. Stakeholder-Management umfasst alle Prozesse, die sich mit der »Identifikation, Analyse und Behandlung von Stakeholdern (Anspruchsgruppen) befassen« ([Hofmann & Knoll 2012], S. 129). Die Beziehung zwischen Governance und Management der IT-Stakeholder ist bidirektional (siehe Abb. 4–5):

- Die Implementierung eines IT-Stakeholder-Managements bildet eine Voraussetzung für die Erreichung der von der IT-Governance gesetzten Ziele hinsichtlich Wertschöpfung, Sicherung der Wettbewerbsposition und Investitionsschutz (nach [Baumöl 2012], S. 8). Die Ergebnisse des IT-Stakeholder-Managements sind als Leistungsinformation an die Governance-Akteure zu berichten.
- Durch die Governance der IT-Stakeholder wird der Ordnungsrahmen geschaffen, in dem sich die Prozesse des IT-Stakeholder-Managements vollziehen. Hierfür sind durch die Akteure der IT-Governance verschiedene konstitutive Entscheidungen für das IT-Stakeholder-Management zu treffen. Zudem ist das IT-Stakeholder-Management durch eine kontinuierliche Steuerung und Überwachung der Governance-Ebene zu begleiten.

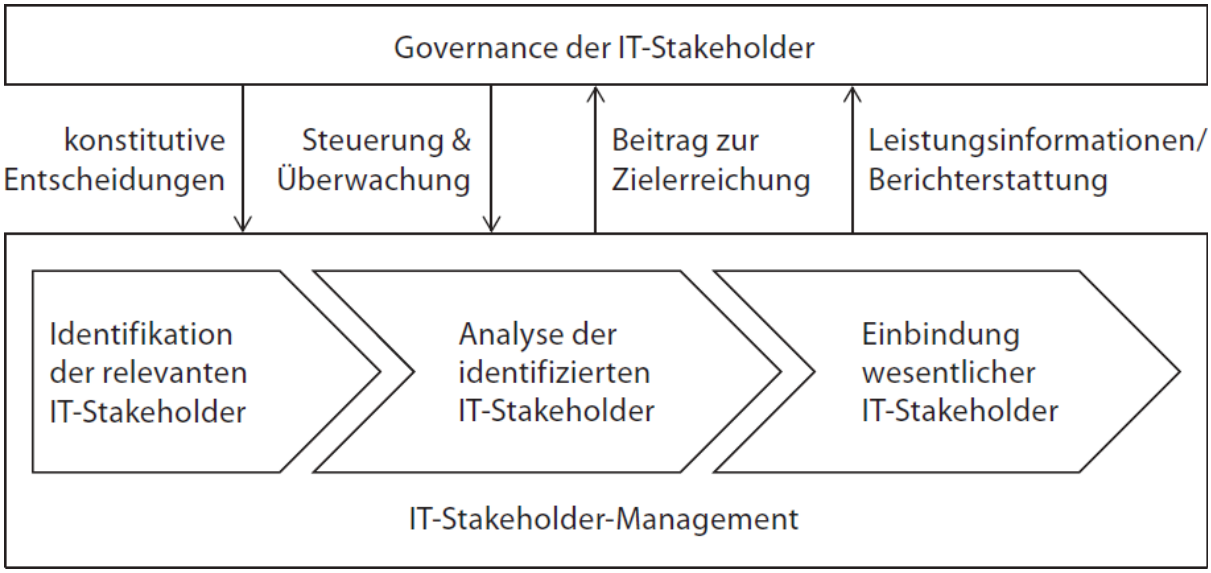

Abb. 4–5 *Zusammenhang von Governance und Management der IT-Stakeholder*

Konstitutive Entscheidungen

Die grundlegende Aufgabe der IT-Governance in Bezug auf die IT-Stakeholder ist die Entscheidung, in der Steuerung und Überwachung der Unternehmens-IT nach einem Stakeholder-Ansatz zu verfahren. Diese Entscheidung haben die Akteure der IT-Governance zu treffen. Voraussetzung der Entscheidung ist die Erkenntnis, dass zumindest einige IT-Stakeholder einen wesentlichen Einfluss auf Unternehmens- und IT-Ziele und damit auch auf den Wertbeitrag der IT nehmen, sodass diese wesentlichen Stakeholder zu identifizieren und in einem erforderlichen Umfang an der Entwicklung der Unternehmens-IT in unterschiedlichen Formen zu beteiligen sind. Hieraus folgt fast notwendig die Entscheidung, ein systematisches IT-Stakeholder-Management zu etablieren. Dieses gliedert sich in drei Prozesse. Nach der Identifizierung der IT-Stakeholder als erstem Prozess folgt als zweiter Prozess die Stakeholder-Analyse, auf der wiederum die Stakeholder-Einbindung mit der Stakeholder-Kommunikation als drittem Prozess basiert. Für jeden der drei Aufgabenbereiche hat die IT-Governance Rahmenbedingungen festzulegen und konstitutive Entscheidungen zu treffen.

Unterscheidung bei COBIT 2019

COBIT 2019 trennt auch für den Umgang mit IT-Stakeholdern ausdrücklich zwischen einer IT-Governance- und einer IT-Managementebene. Die IT-Governance-Zielsetzung »EDM05 Einbindung der Anspruchsgruppen ist sichergestellt« soll gewährleisten, dass die IT-Stakeholder identifiziert und in das IT-Governance-System eingebunden sind. Weiterhin sollen die Messung der IT-Performance und -Compliance sowie die Berichterstattung transparent sein, wobei die Ziele, Kennzahlen sowie notwendige Verbesserungsmaßnahmen durch die IT-Stakeholder zu genehmigen sind (nach [ISACA 2020b], S. 49). Das IT-Stakeholder-Management ist in COBIT 2019 auf verschiedene IT-Management-Zielsetzungen verteilt. Die grundlegende IT-Management-Zielsetzung für das IT-Stakeholder-

Management ist »APO08 Beziehungen sind gemanagt«. Das formalisierte und transparente Management der Beziehungen soll derart erfolgen, dass ein gegenseitiges Vertrauen und ein gemeinsamer Fokus auf das Erreichen der strategischen Ziele innerhalb von Budgetgrenzen und Risikotoleranz sichergestellt werden (nach [ISACA 2020b], S. 109). Diese Zielsetzung wird ergänzt durch weitere IT-Management-Zielsetzungen, die auf spezifische Stakeholder abstellen: »APO07 Personal ist gemanagt« für interne und externe IT-Mitarbeiter, »APO10 Lieferanten sind gemanagt« für die IT-Lieferanten und »BAI11 Projekte sind gemanagt« für IT-Projekt-Stakeholder.

4.5 Konstitutive Entscheidungen für das IT-Stakeholder-Management

4.5.1 IT-Stakeholder-Identifizierung

Identifizierung der wesentlichen IT-Stakeholder

Initiiert wird das IT-Stakeholder-Management durch einen Auftrag zur Identifizierung der relevanten Stakeholder, die legitimierte Ansprüche an die Unternehmens-IT stellen. Die Identifizierung der IT-Stakeholder selbst sowie die Analyse der wechselseitigen Beziehungen und Wirkungen zwischen ihnen und der Unternehmens-IT einerseits und ggf. untereinander andererseits (vgl. Abb. 4–6), die damit in Zusammenhang stehende administrative Verwaltung und die Nutzung entsprechender Managementtools obliegen dem IT-Stakeholder-Management.

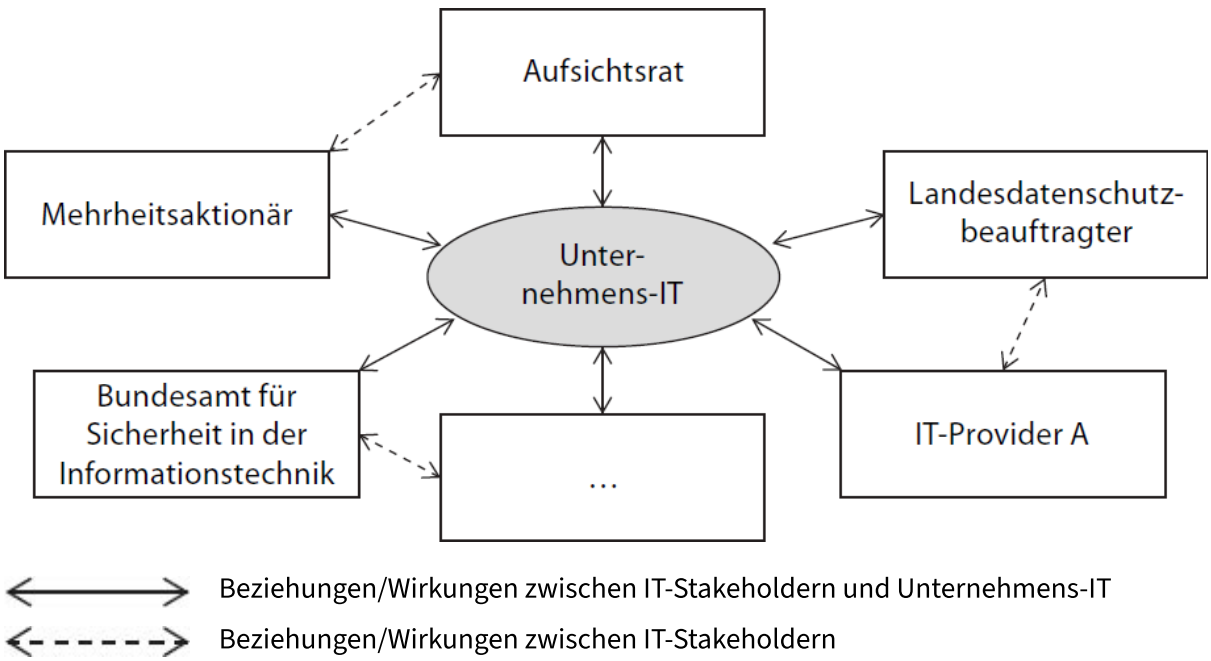

Abb. 4–6 *Wechselseitige Beziehungen und Wirkungen zwischen primären Stakeholdern und Unternehmens-IT*

Das IT-Stakeholder-Management hat zur Einordnung von internen und externen Akteuren als relevanten IT-Stakeholdern eine Entscheidungsvorlage zu erarbeiten. Die Entscheidung darüber obliegt der IT-Governance. Dass dies keine einmalige Aufgabe ist, zeigt zum Beispiel die Entwicklung im Bereich der kritischen Infrastrukturen, wo durch das Gesetz zur Erhöhung der Sicherheit in der Informationstechnik (IT-Sicherheitsgesetz) das BSI der Adressat für die betroffenen KRITIS-Betreiber und damit ein neuer IT-Stakeholder geworden ist.

Beziehungen und Wirkungen analysieren

Die Analyse und die in Abbildung 4–6 gezeigte Darstellung können nutzbringend auf einzelne Bereiche der Unternehmens-IT angewendet werden. Beispielsweise kann es von großem Interesse sein, diejenigen IT-Stakeholder zu ermitteln, die von einer IT-Strategie (die dann in dem Kreis stehen würde) betroffen sind und insofern Ansprüche an ihre Umsetzung stellen. Hierbei sind gerade auch negative Wirkungen in Richtung der Stakeholder zu identifizieren und zu analysieren, um daraus resultierende mögliche Konflikte frühzeitig erkennen und als Risiken der Strategieumsetzung steuern zu können. Ebenso wichtig ist es, die für die Unternehmens-IT positiven oder negativen wechselseitigen Beziehungen der Stakeholder untereinander zu analysieren.

4.5.2 IT-Stakeholder-Analyse

Analyse von Zielen, Motiven und Einstellungen

Für die identifizierten und als relevant eingestuften IT-Stakeholder ist eine Analyse ihrer Ziele, Motive und Einstellungen als Grundlage der Stakeholder-Einbindung vorzunehmen. Hierbei sind neben der grundlegenden Einteilung in interne und externe IT-Stakeholder weitere Klassifizierungen durchzuführen. Mögliche Kriterien hierfür sind z.B. die Macht eines Stakeholders als Umfang seiner möglichen Einflussnahme oder die Dringlichkeit, d.h. die Wichtigkeit bzw. die zeitlichen Anforderungen der Stakeholder-Ansprüche (vgl. [Bruton 2017], S. 80 f.). Mit diesem Schritt sind aus den als relevant eingestuften IT-Stakeholdern die wesentlichen IT-Stakeholder zu ermitteln, deren legitimierten Ansprüchen gegenüber den Ansprüchen anderer Stakeholder höhere Priorität eingeräumt wird. Die hiermit verbundene Entscheidung kann vom IT-Stakeholder-Management vorbereitet werden, die Entscheidung obliegt wiederum den Akteuren der IT-Governance. Das Ergebnis wird häufig in einer grafischen Portfolio-Darstellung dokumentiert.

Analyse der Berichtsanforderungen

Ein weiterer wichtiger Teil der IT-Stakeholder-Analyse besteht in der Ermittlung der Berichtsanforderungen der wesentlichen Stakeholder. Gerade externe Berichtsanforderungen sind genau zu analysieren, um die Informationsanforderung der betreffenden Stakeholder zu erfüllen. So

umfasst z.B. bei Sicherheitsvorfällen die notwendige Meldung Art und Umfang der Auswirkungen, die Ursachen der aufgetretenen Sicherheitsvorfälle sowie Maßnahmen zu deren Behebung und zur zukünftigen Vermeidung derartiger Vorfälle (vgl. [Bundesnetzagentur 2018], S. 17 f.).

4.5.3 IT-Stakeholder-Einbindung

Einbindung der IT-Stakeholder

Ähnlich wie die IT-Governance für die Unternehmens-IT die Risikoneigung für den Umgang mit IT-Risiken grundlegend klären muss, hat sie auch festzulegen, welche grundsätzliche Einstellung hinsichtlich der Erfüllung der Ansprüche von wesentlichen IT-Stakeholdern und damit für ihre Einbindung vorherrschen soll. Dies gilt insbesondere für die Erfüllung von Anforderungen externer Stakeholder. Eine Orientierung bietet hierbei die RDAP-Skala, ein Werkzeug zur Charakterisierung von Haltungen bzw. Einstellungen – hier gegenüber der IT. Die Skala unterscheidet vier grundlegende Einstellungen: reaktiv (reactive), defensiv (defensive), anpassungsfähig (accommodative), proaktiv (proactive) (siehe Tab. 4–1):

Einstufung	Strategie	Erfüllung
1. Reaktiv	Verantwortung ablehnen	Weniger tun als nötig
2. Defensiv	Verantwortung erkennen, aber gleichzeitig abwehren	Das Minimum dessen tun, was erforderlich ist
3. Anpassungsfähig	Verantwortung akzeptieren	Alles tun, was gefordert wird
4. Proaktiv	Verantwortung vorausschauend übernehmen	Mehr tun, als gefordert wird

Tab. 4–1 *RDAP-Skala für den Umgang mit Stakeholder-Anforderungen (nach [Clarkson 1995], S. 109)*

RDAP-Einstufungen

- Eine *reaktive Einstellung* lehnt die Verantwortung für die Erfüllung von Stakeholder-Ansprüchen ab. Dementsprechend werden Ansprüche als nicht berechtigt angesehen und abgewehrt, z.B. indem eine Zuständigkeit verneint wird. Dies führt dazu, dass die Interessen der Stakeholder ganz oder teilweise nicht beachtet werden.
- Bei der *defensiven Einstellung* wird erkannt, dass Stakeholder-Ansprüche bestehen, diese werden aber so weit wie möglich abgelehnt. Nur wenn dies

nicht gelingt, werden Ansprüche erfüllt, beispielsweise dann, wenn ein Gerichtsurteil dies zwingend vorgibt.

- Bei der *Einstellung der Anpassungsfähigkeit* wird die Verantwortung gegenüber den Stakeholdern akzeptiert und die berechtigten Ansprüche werden vollständig erfüllt. Dies wird vor allem bei Prüfungen durch externe Stakeholder der Fall sein, denen man sich nicht entziehen kann.
- Die *proaktive Einstellung* liegt bei einer vorausschauenden Übernahme von Verantwortung vor. Ansprüche der Stakeholder werden antizipiert, sodass letztlich Anforderungen umgesetzt werden, die von den Stakeholdern nicht geäußert werden. Dies ist z.B. dann der Fall, wenn Unsicherheit besteht, wie die Anforderungen neuer Gesetze umgesetzt werden müssen, und wegen dieser Unsicherheit ein Mehr an Maßnahmen ergriffen wird. Eine solche Situation lag in der IT z.B. nach der Verabschiedung der DSGVO vor.

Strategie für IT-Stakeholder-Einbindung

Insgesamt ist somit eine Strategie für die IT-Stakeholder-Einbindung festzulegen. Dies sollte mit Blick auf die allgemeine Stakeholder-Governance des Unternehmens erfolgen. Wird auf Unternehmensebene beispielsweise ein defensives Handeln gegenüber Lieferantenansprüchen praktiziert, wird diese Festlegung nicht durch die IT-Funktion mit einem proaktiven Handeln in Richtung von IT-Dienstleistern konterkariert werden können. Auf der anderen Seite müssen auf der Basis der grundsätzlichen Einbindungsstrategie auch Stakeholder-spezifische Strategien der Erfüllung von Ansprüchen festgelegt werden. Gegenüber den wesentlichen IT-Stakeholdern werden die Akteure der IT-Governance eher nicht eine defensive oder gar reaktive Einstellung verfolgen können. Hierbei sind vor allem Risikoaspekte zu beachten. Dass dies eine sehr realistische Diskussion ist, zeigt der Umgang der Unternehmen mit den datenschutzrechtlichen Vorgaben vor und nach Inkrafttreten der DSGVO. Erst in Folge der mit den potenziellen Bußgeldern verbundenen beachtlichen Risiken wurde umfangreich in den Datenschutz investiert, obgleich die gesetzlichen Verpflichtungen im Großen und Ganzen auch schon vorher bestanden.

4.5.4 Qualifizierung für das IT-Stakeholder-Management

Qualifizierung für IT-Stakeholder-Management

Die IT-Governance sollte weiterhin dafür sorgen, dass die Akteure des IT-Stakeholder-Managements hierfür in ausreichendem Maße qualifiziert sind bzw. werden. Als Basis der Bestimmung der erforderlichen Qualifikationen, einer anschließenden Gap-Analyse sowie der Planung und Durchführung von Qualifizierungsmaßnahmen kann das Kompetenz-Rahmenwerk »Skills Framework for the Information Age« (SFIA) eingesetzt werden. Das Stakeholder-Management

wird hier als »Beziehungsmanagement« bzw. »Relationship-Management« bezeichnet. Hierunter versteht SFIA 7 die »systematische Identifikation, Analyse, Steuerung, Überwachung und Verbesserung von Stakeholder-Beziehungen, um gegenseitig vorteilhafte Ergebnisse zu erzielen und zu verbessern« ([SFIA 2018], S. 139).

Kompetenz-Rahmenwerk SFIA

Die für das IT-Stakeholder-Management in SFIA 7 beschriebenen Qualifikationen sind den höheren Führungs- und Verantwortungsebenen 4 bis 7 zugeordnet. Hierbei beschreibt die Ebene 7 die höchste Verantwortung im Unternehmen. Insofern stellen die hier aufgeführten Kompetenzen diejenige Qualifikation dar, über die die Akteure der IT-Governance selbst verfügen sollten. Hierzu zählen Fähigkeiten und Kenntnisse für

- die Bestimmung der strategischen Herangehensweise, durch die ein Verständnis für die Ziele und Bedürfnisse der IT-Stakeholder erworben werden soll,
- die Definition der Grundsätze für den Aufbau effektiver Beziehungen zwischen den IT-Stakeholdern (einschließlich der Beziehung zwischen der IT-Abteilung und den Fachabteilungen) und Erzielen eines diesbezüglichen Einvernehmens mit den Beteiligten,
- die Zusammenarbeit mit IT-Stakeholdern, um effektive Beziehungen zwischen wesentlichen IT-Stakeholdern zu schaffen, einschließlich der Verantwortung für die Beziehung zwischen IT-Abteilung und Fachabteilungen,
- die Festlegung und Förderung der generellen Art und Weise, wie die Ziele der IT-Stakeholder erreicht werden sollen, und die Festlegung der hierfür notwendigen organisatorischen Rollen und des anzustrebenden Business/IT-Alignments,
- ein aktives Management der Beziehungen zu den wichtigsten IT-Stakeholdern und ein Agieren als letzte Eskalationsinstanz für die Lösung von Problemen (nach [SFIA 2018], S. 139).

Die Führungs- und Verantwortungsebenen 4 bis 6 betreffen die Kompetenzen für das IT-Stakeholder-Management. Tabelle 4–2 listet die hierfür erforderlichen Qualifikationen auf.

Ebene	IT-Stakeholder-Management
6	▪ Leitung der Entwicklung umfassender Strategien und Pläne für das IT-Stakeholder-Management

	▪ Aufbau langfristiger, strategischer Beziehungen zu wichtigen internen und externen IT-Stakeholdern und Förderung der Beziehungen zwischen ihnen ▪ Ermöglichen der Einbindung von IT-Stakeholdern und Agieren als zentrale Anlaufstelle für wichtige IT-Stakeholder ▪ Klärung der Maßnahmen in den unterschiedlichsten IT-Bereichen mit den betroffenen IT-Stakeholdern, sodass diese verstehen, inwiefern ihre Interessen betroffen sind und gewahrt werden; ggf. Treffen angemessener Vereinbarungen hierüber ▪ Beaufsichtigung der Überwachung der Beziehungen, einschließlich erworbener Erfahrungen und des entsprechenden Feedbacks ▪ Einleitung von Maßnahmen zur Verbesserung der Beziehungen und für eine offene Kommunikation mit und zwischen den IT-Stakeholdern
5	▪ Identifizierung der Kommunikations- und Beziehungsbedürfnisse von IT-Stakeholdern ▪ Umsetzung von Strategien für die Kommunikation und die Einbindung von IT-Stakeholdern in konkrete Aktivitäten und Ergebnisse ▪ Ermöglichung einer offenen Kommunikation und Diskussion zwischen den IT-Stakeholdern ▪ Fungieren als zentraler Ansprechpartner bei der Entwicklung, Pflege und Umsetzung von Strategien und Plänen zur Einbindung der IT-Stakeholder ▪ Unterstützung der Kommunikation mit IT-Stakeholdern durch fundiertes Feedback, Förderung des gemeinsamen Verständnisses verschiedener IT-Stakeholder, Ermöglichung unternehmerischer Entscheidungsprozesse sowie Erfassung und Verbreitung informationstechnischer und geschäftlicher Informationen
4	▪ Implementierung von Plänen zur Einbindung von IT-Stakeholdern und zur Kommunikation mit ihnen ▪ Befassung mit Problemen und anstehenden Fragen, Umsetzung von Lösungen, Abhilfemaßnahmen und Lessons Learned sowie Sammlung und Verteilung von relevanten Informationen ▪ Sammlung und Nutzung von Feedback seitens IT-Stakeholdern, um die Effektivität des Stakeholder-Managements zu messen ▪ Unterstützung der Entwicklung und Verbesserung der Beziehungen zu IT-Stakeholdern

Tab. 4–2 *Qualifikationen für IT-Stakeholder-Management (nach ([SFIA 2018], S. 123 f.)*

Die IT-Governance sollte die entsprechenden Analyse- und Qualifizierungsmaßnahmen initiieren, die notwendigen Ressourcen zuweisen und den Fortschritt der Qualifizierungsmaßnahmen überwachen. Die operative

Durchführung wird durch die Personalabteilung gesteuert, die der IT-Governance über den Fortschritt zu berichten hat.

Qualifizierung ernst nehmen

IT-Stakeholder-Management lässt sich nicht mal »eben so« machen. Es handelt sich um eine professionelle Tätigkeit im Rahmen des IT-Managements, die heute ein wichtiger Erfolgsfaktor von IT-Projekten, IT-Programmen und der gesamten digitalen Transformation eines Unternehmens ist. Aus diesem Grunde müssen die Akteure, die das IT-Stakeholder-Management verantwortlich durchführen, hierfür entsprechend qualifiziert sein bzw. werden. Dies sicherzustellen, ist insofern eine wichtige Aufgabe der IT-Governance.

4.6 Überwachung des IT-Stakeholder-Managements

Überwachung des IT-Stakeholder-Managements

Die Überwachungsaufgaben der IT-Governance in Bezug auf die IT-Stakeholder leiten sich wiederum aus den drei Prozessen des IT-Stakeholder-Managements ab. Sie zielen darauf ab, die Genauigkeit, Zuverlässigkeit und Effektivität des IT-Stakeholder-Managements sicherzustellen, insbesondere im Hinblick auf Anforderungen der verschiedenen IT-Stakeholder in Bezug auf Berichterstattung und Kommunikation (vgl. [ISACA 2018b], S. 50).

4.6.1 IT-Stakeholder-Identifizierung

Aktualität der Stakeholder-Identifizierung

Bezüglich der IT-Stakeholder-Identifizierung muss die IT-Governance darauf achten, dass die Identifizierung aktuell ist und die wesentlichen IT-Stakeholder erkannt wurden. Hierzu sind die regelmäßigen Identifizierungsaktivitäten an die Akteure der IT-Stakeholder-Governance zu berichten. Dieser Bericht muss auch einen Rückblick enthalten und kritisch hinterfragen, welche IT-Stakeholder in der Vergangenheit nicht oder zu spät identifiziert wurden. Input erhält diese Analyse aus Fällen, in denen berechtigte Ansprüche mit beträchtlichen Auswirkungen von Personen(gruppen) an das Unternehmen gerichtet wurden, ohne dass diese bereits als relevante bzw. wesentliche IT-Stakeholder eingestuft worden waren. Auf der anderen Seite muss hinterfragt werden, ob die bisherige Einstufung der IT-Stakeholder im Rückblick gerechtfertigt war und für die Zukunft weiterhin aufrechterhalten werden soll.

Verbesserungspotenziale

Aus der Überwachung der Stakeholder-Identifizierung resultieren Hinweise für die Verbesserung des Prozesses und der Instrumente der Stakeholder-Identifizierung. Kriterien für die Identifizierung werden geschärft, ggf. verschiebt sich auch der

Fokus für die Identifizierung, wenn beispielsweise bei einem publik gewordenen Fall von Non-Compliance der Unternehmens-IT Kontakte zu externen Akteuren, z.B. Wirtschaftsprüfer oder IT-Berater, intensiviert werden sollen und damit die entsprechenden IT-Stakeholder eine gesteigerte Bedeutung erfahren.

4.6.2 IT-Stakeholder-Analyse

Kriterien der IT-Stakeholder-Analyse

Die IT-Stakeholder-Analyse ist dahingehend zu prüfen und zu beurteilen, ob die Analyse mittels geeigneter Kriterien erfolgt. Insofern hat die IT-Stakeholder-Governance die Kriterien zu hinterfragen, IT-Stakeholder-Analysen mit alternativen Kriterien anzufordern und ggf. Anpassungen zu verlangen.

Berichtsanforderungen

Hinsichtlich der Berichtsanforderungen der wesentlichen IT-Stakeholder ist zu überwachen, ob und inwieweit diese korrekt analysiert wurden und, ob Veränderungen erkannt und berücksichtigt wurden. Input hierfür ergibt sich aus der IT-Stakeholder-Kommunikation. Bei den internen Stakeholdern werden Verbesserungen der Berichterstattung mehr oder weniger unmittelbar eingefordert. Bei externen IT-Stakeholdern wird sich dies aus der formalen Kommunikation oder aus den Feststellungen infolge von externen IT-Prüfungen ergeben.

4.6.3 IT-Stakeholder-Einbindung

Effektivität der IT-Stakeholder-Einbindung

Der Fokus der Überwachung liegt auf der Bewertung der Effektivität der IT-Stakeholder-Einbindung. Hier müssen die grundsätzliche Einbindungsstrategie ebenso wie die Stakeholder-spezifischen Strategien hinterfragt werden. Ergebnis dieser Überwachung können z.B. häufigere Abstimmungen oder veränderte Berichtszyklen sein.

Kommunikation und Berichterstattung

Ein weiterer wichtiger Punkt ist die Berichterstattung, insbesondere das obligatorische Reporting. Für die Vergangenheit sind eventuelle Verstöße gegen Berichtspflichten zu thematisieren und hinsichtlich der Wirksamkeit von Eskalationsverfahren zu bewerten. Letztlich ist aber die gesamte Kommunikation in ihrer Effektivität und Effizienz zu beurteilen.

4.6.4 Kennzahlen für die Überwachung des IT-Stakeholder-Managements

Kennzahlen für die Überwachun

Zur Unterstützung der Überwachung des IT-Stakeholder-Managements können Kennzahlen

verwendet werden. Diese sollten alle drei Prozesse des IT-Stakeholder-Managements abdecken, so wie dies in Tabelle 4–3 beispielhaft dargestellt ist.

Prozess	Kennzahlen (Beispiele)
IT-Stakeholder-Identifizierung	▪ Aktualität des Berichts zu den Identifizierungsaktivitäten (Datum) ▪ Aktualität der Festlegung von primären IT-Stakeholdern (Datum)
IT-Stakeholder-Analyse	▪ Aktualität der letzten Überarbeitung der Kriterien (Datum) ▪ Aktualität der letzten Überarbeitung der Berichtsanforderungen (Datum) ▪ Anteil der Stakeholder, deren Berichtsanforderungen erfasst werden (Prozentsatz)
IT-Stakeholder-Einbindung	▪ Anzahl der Verstöße gegen die Pflichtberichterstattung (Zahl) ▪ Anteil der Berichte mit Ungenauigkeiten (Prozentsatz) ▪ Anteil der Berichte, die pünktlich geliefert wurden (Prozentsatz) ▪ Grad der Einbeziehung der Anspruchsgruppen in die Prozesse der Unternehmens-IT (Prozentsatz) ▪ Zufriedenheit der IT-Stakeholder mit der Einbindung (Prozentsatz) ▪ Zufriedenheit der IT-Stakeholder mit der Berichterstattung (Prozentsatz)

Tab. 4–3 *Kennzahlen für die Überwachung des IT-Stakeholder-Managements (vgl. [ISACA 2020b], S. 49 f.)*

Aus der kontinuierlichen Überwachung des IT-Stakeholder-Managements resultieren Ansätze für Verbesserungen der IT-Stakeholder-Governance und des IT-Stakeholder-Managements gleichermaßen. Dadurch, dass sich die Akteure der IT-Governance immer wieder mit den wesentlichen IT-Stakeholdern befassen müssen, wird insbesondere die Erfüllung der Ansprüche der externen IT-Stakeholder sichergestellt. Insofern ist die IT-Governance in Bezug auf die IT-Stakeholder eng verknüpft mit der IT-Governance in Bezug auf IT-Risiken und IT-Compliance.

4.7 Handlungsempfehlungen

- **Bedeutung von IT-Stakeholdern bewusst machen!**

  Die grundlegende Voraussetzung für IT-Governance in Bezug auf IT-Stakeholder ist das Bewusstsein, dass IT-Stakeholder den Wertbeitrag der IT wesentlich beeinflussen. Dieses Bewusstsein stellt sich nicht von alleine ein, sondern die Bedeutung von IT-

Stakeholdern ist zu thematisieren, zu diskutieren und zu entscheiden. Die Verantwortung hierfür liegt bei den Akteuren der IT-Governance.

- **Interne und externe IT-Stakeholder unterscheiden!**

  Zu den externen IT-Stakeholdern zählen Personen, Gruppen oder Organisationen in der Unternehmensumwelt, mit denen die Unternehmens-IT in Interaktion steht, z. B. Aufsichtsinstitutionen und IT-Dienstleister, mit denen das Unternehmen Geschäftsbeziehungen unterhält. Interne IT-Stakeholder sind dem Unternehmen auf einer gesellschaftsrechtlichen oder arbeitsvertraglichen Basis zugehörig. Dies sind Anteilseigner des Unternehmens und arbeitsvertraglich gebundene Personen.

- **Relevanz der IT-Stakeholder-Gruppen beachten!**

  IT-Stakeholder sind nur solche Akteure, die legitimierte Ansprüche an die Unternehmens-IT stellen. Die wichtigsten internen IT-Stakeholder sind Mitglieder des Aufsichtsorgans, der Unternehmensleitung und des IT-Lenkungsausschusses, Anteilseigner, der CIO/CDO bzw. die IT-Leitung, der Datenschutzbeauftragte und weitere Organisationseinheiten der 2. Linie. Die wichtigsten externen IT-Stakeholder sind Kunden des Unternehmens, Aufsichtsinstitutionen und IT-Dienstleister, IT-Hersteller, IT-Berater und IT-Fachanwälte, mit denen das Unternehmen eine strategische Geschäftsbeziehung unterhält oder deren Know-how das Unternehmen kontinuierlich nutzt.

- **Die Ziele der IT-Governance in Bezug auf die IT-Stakeholder klären!**

  Ziele der IT-Governance in Bezug auf die IT-Stakeholder gehen in drei Richtungen. Es ist die Unterstützung in der grundsätzlichen Ausrichtung der Unternehmens-IT zu erlangen, die Compliance mit Anforderungen externer Stakeholder sicherzustellen und eine positive Einstellung der Stakeholder gegenüber der Unternehmens-IT zu erreichen. Dort, wo es zu keiner aktiven Unterstützung durch die IT-Stakeholder kommt, sollte zumindest eine neutrale Einstellung erreicht werden.

- **Fokus auf die wesentlichen IT-Stakeholder richten!**

  Wenn Stakeholder umfangreiche legitimierte Ansprüche an die IT und gleichzeitig einen großen Einfluss haben, müssen sich Unternehmensund IT-Leitung in der Pflege der Beziehungen zu diesen Stakeholdern engagieren. Sie vertreten dann selbst die zur Diskussion stehenden Entwicklungslinien der IT, erhalten Rückmeldungen der Stakeholder und müssen diese für die Stakeholder sichtbar verarbeiten.

- **Governance in Bezug auf IT-Stakeholder und IT-Stakeholder-Management gegeneinander abgrenzen!**

  Aufgaben der IT-Governance in Bezug auf IT-Stakeholder sind von den Aufgaben des IT-Stakeholder-Managements zu unterscheiden. Die IT-Governance schafft den Rahmen, in dem sich das IT-Stakeholder-Management vollzieht. Akteure der IT-Governance treffen die konstitutive Entscheidung, in der Steuerung und Überwachung der Unternehmens-IT nach einem Stakeholder-Ansatz zu verfahren und hierfür ein systematisches IT-Stakeholder-Management einzurichten. Weiterhin hat die IT-Governance die Identifizierung der wesentlichen IT-Stakeholder durch das IT-Stakeholder-Management zu beauftragten. Für die IT-Stakeholder-Analyse sind Klassifizierungskriterien festzulegen. Für die IT-Stakeholder-Einbindung gibt die IT-Governance die grundsätzliche Einstellung (reaktiv, defensiv, anpassungsfähig, proaktiv) hinsichtlich der Erfüllung der Ansprüche von IT-Stakeholdern vor. Die Überwachungsaufgabe der IT-Governance richtet sich auf die Überwachung, ob und inwieweit die Vorgaben in den

drei Prozessen des IT-Stakeholder-Managements eingehalten werden und ob das IT-Stakeholder-Management insgesamt effektiv und effizient erfolgt.

- **Qualifikation für IT-Stakeholder-Management sicherstellen!**

  Das Management von IT-Stakeholdern erfordert Qualifikationen in den Bereichen Strategie, Planung, Business/IT-Alignment, Kommunikation sowie Problem- und Konfliktmanagement. IT-Know-how und Soft Skills müssen zusammenkommen, um ein effektives und effizientes IT-Stakeholder-Management zu betreiben. Dies wird in der Regel Qualifizierungsmaßnahmen erfordern. Hierfür muss die IT-Governance die erforderlichen Ressourcen bereitstellen und den Kompetenzaufbau überwachen.

- **Kennzahlen nutzen!**

  Zur Überwachung des IT-Stakeholder-Managements sind Kennzahlen zu verwenden. Diese bilden einen wesentlichen Input für die Überwachungsaufgabe durch die Akteure der IT-Governance. Die verwendeten Kennzahlen sollten alle drei Aufgabenbereiche des IT-Stakeholder-Managements abdecken.

Index

A

Abnahme 472

Agiles Mindset 252, 255

Agilität 138, 195–196, 202, 210, 212, 217, 250–253, 255–256, 260, 262, 471

AktG 145, 196, 272

Aktiengesellschaft 145

Alignment 144, 146, 148, 150–151, 199, 279, 457

Alignment-Dimensionen 100

Ambidextrie 140

Änderungsmanagement 197, 471

Anforderungen 143–144, 250, 260–262, 470–472, 475

Anforderungsanalyse 364

Anforderungskatalog 365

  Aktualisierung 365

Anforderungsmanagement 131, 206, 208–209, 470

Angemessenheit 288, 300, 320, 322, 326

Angemessenheitsprüfung 322

Anwenderbetreuung 204

Anwendungen 124–125, 138, 140, 206, 260–261, 471–472

Anwendungsbetreuung 226

Anwendungsentwicklung 226

Anwendungskontrollen 474

Anwendungsmanagement 131

APO-Domäne 466

Application Service Providing 227

Applikationsportfolio 124

Arbeitnehmervertretung 172
Arbeitsanweisungen 359
Arbeitsstättenverordnung 353
Assurance 130, 394, 475
Audit 469
Auditierung 362
Aufbauorganisation 196
Aufsichtsinstitution 173, 178, 197, 237–238, 298, 451
Aufsichtsorgan 3, 168, 236–237
Aufsichtsrat 122, 141–142, 144, 146, 149, 218, 272, 276, 285, 294, 299, 322
Auftraggeber 219
Ausgründung 263
Auslagerung 400
Ausschüsse 149, 151
B
BaFin 173, 196, 355, 412
BAIT 197, 289, 298, 355, 363
  norminterpretierende Verwaltungsvorschrift 356
  Regelungsbereiche 356
Balanced Scorecard 179
Barcamp 264
Barrierefreie-Informationstechnik-Verordnung 353
BDSG 197
Bedrohungen 207, 273
Bedrohungslandschaft 249
Benchmark 448, 475
Benutzersupport 207
Beratung 144
Berechtigungskonzept 376
Berichterstattung 177
Berichtspflichten 465
Berichtswege 140
Berichtswesen 198, 204, 301, 421, 471
Best Practice 148, 232, 443
Betriebsprüfung 238

Betriebsübergang 230–231
Bewertungsproblem 70
BGB 230
BilMoG 272
Bimodale IT 138, 140, 255
Bindungswirkung 361
  externe Regelwerke 350
  interne Regelwerke 350
  Rechtsnormen 350
  Verträge 350
Blockchain 282, 414
Board 144–146, 150–151
  Portal 144
BSI 197, 238
BSI-C5 362
BSI-Gesetz 284, 296, 352
BSI-Grundschutz
  Basis-Absicherung 378
  Kern-Absicherung 378
  Konzept 378
BSI-Kritisverordnung 353
BSI-Standards 377
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 197
Bundesnetzagentur 197
Bundle of Benefits 77
Business Case 86, 225
  Lebenszyklus 86
  Vorgehensmodell 87
Business Impact 274, 285, 300, 307
Business Model Canvas 263
Business Process Outsourcing 227
Business/IT-Alignment 58, 95, 199, 209, 239, 466
  Alignment-Dimensionen 100
  Alignmenttypen 98
  Definition 95

Enablers 102
Inhibitors (Hemmnisse) 102
Business/IT-Integration 99
Bußgeld 284
B3S 284
C
CEN 446
Change-Management 135, 148, 428
Chapter 257
Chief Data Officer 133, 411, 420, 437
Chief Digital Officer 123, 133–138, 141, 168, 178, 194, 218, 412, 415, 437
Chief Executive Officer 132, 134–137, 145–146, 148–150, 218, 411, 415, 424, 433
Chief Financial Officer 147
Chief Information Officer 122, 126–127, 129–130, 132, 134–137, 139–141, 146–147, 149, 168, 178, 194, 218, 229, 250–251, 253, 278, 295, 308, 411, 415, 423–424, 429, 433, 437
Chief Information Risk Officer 287, 311–312
Chief Operating Officer 147
Chief Risk Officer 278, 292, 308, 311
Chief Technology Officer 123, 218
Citizen Developer 140, 254, 262
Claim-Management 208
Cloud 200, 209, 213
Cloud Computing 283, 301, 414
Cloud-Dienstleister 362
CMMI 230
Coaching 144
COBIT 445
Governance-Praktiken 339
Evaluieren 340
Steuern 340
Überwachen 340
Governance-Ziele 339
Managementziele 339
COBIT 2019 19–20, 22, 45, 123, 134, 146, 152, 160, 166, 181, 214, 219, 240, 243–249, 255, 278–279, 281, 287, 289–290, 293, 306, 312, 340, 363, 431–432, 434, 460
COBIT 5 18, 246

Code of Conduct 370
Colocation 254
Compliance
  Begriff 331
  Verantwortung 369
Compliance-Aufgaben 381
Compliance-Checks 388
Compliance-Funktion
  Alternativen 380
  Sourcing 380
Compliance-Kommunikation 344
  Mitarbeiterschulung 390
Compliance-Kultur 344, 368
  Ausprägung 369
  Verankerung 369
  Verhaltenskodex 369
Compliance-Manager 381
Compliance-Officer 381
Compliance-Organisation 344
  dezentrale Verantwortung 381
  Einflussfaktoren 379
  Kompetenzmodell 382
  zentrale Verantwortung 382
Compliance-Politik 371
Compliance-Portfolio 337, 361, 363
  Nutzer 387
Compliance-Programm 344
Compliance-Prozess 386
  Abweichungsanalyse 388
  Anforderungsanalyse 386
  Berichterstattung 389
Compliance-Risiken 344, 374
Compliance-Verstöße 368
Compliance-Ziele 344, 370
  Unternehmensebene 371

Continuous Delivery 261
Continuous Deployment 261
Continuous Integration 260
Continuous Monitoring 261
Controls 365
Corporate Compliance 367
Corporate Governance 2, 146, 272, 294, 367, 410, 424
Corporate Social Responsibility 159
COSO ERM 273
Cost-Center 223, 226
Covid-19-Pandemie 58, 128, 254, 282, 300, 354, 405
  CoronaEinreiseV 354
  Homeoffice 354
  Infektionsschutzgesetz 354
CRM-System 130
Customizing 206
Cyberangriffe 148
Cyberphysisches System 218
Cyberraum 203
Cyberrisiken 144
Cybersicherheit 200
D
Data Analytics 217
Data Custodian 422
data driven 123, 140, 146, 217, 247
Data Governance 129, 407–408, 414, 424, 437, 454
Data Governance Board 421
Data Management Body of Knowledge 424, 431
Data Owner 411, 421
Data Producer 422
Data Steward 219, 421
  Team 421
Data-as-a-Service 428
Daten 129, 137, 143, 199, 216, 219, 262, 278, 406–407, 413, 422, 434, 454, 469
Datenadministration 407, 422

Datenanalyse 144
Datenarchitektur 424
Datenaufbewahrung 436
Datenbankmanagementsystem 407
Datenerfassung 438
Datenkultur 417, 421, 433, 436
Datenmanagement 129, 407, 409–410, 412–413, 415–416, 421–426, 428, 430–432, 434, 437–438
Datenmodell 408
Datenqualität 282, 408, 411, 414, 421–422, 428, 436, 470
Datenschutz 238, 262, 277, 282, 300, 410, 417
  by Design 351
Datenschutzaudit 238
Datenschutzbeauftragter 171, 197, 237, 300, 303
Datensicherheit 144
Datensicherung 238, 363
  Kontrollmatrix 363
Datenstrategie 411, 421, 436–437
Datenvernichtung 436
DCGK 159, 272, 276, 410
Delegation 196
Demand-Supply-Konzept 209, 226, 267
Design Thinking 263
Designfaktor 248–249, 255
DevBizOps 261
DevOps 138, 194, 226, 250, 252, 255, 260, 283
Digitale Transformation 56, 123, 133–134, 136–137, 141, 143, 146, 149–150, 179, 194, 204, 209, 212, 221, 251, 261, 466
DIIR Revisionsstandard Nr. 2 301, 310, 320, 323
DIN 442, 446
DIN ISO 31000 273, 304, 315
Disruption 142
Diversität 143
Dokumentation 198, 230
Dokumentenmanagement 144
DrittelbG 141
DSGVO 197, 237, 284, 300, 303, 414

DSS-Domäne 473
Due Process 349
Dynamikproblem 70
E
Edge Computing 124
EDM-Domäne 241
Enterprise Architecture Management 151, 199, 206
Enterprise Risk Management 171, 240, 276, 287, 299, 302, 320
Erfassungsproblem 70
ERP-System 130, 138, 205, 225, 408
Eskalation 132, 149, 465, 468, 473
EU-Richtlinien 351
EU-Verordnungen 352
F
Fachabteilung 125, 135, 138, 169, 203, 206–209, 217, 224–226, 236, 254, 467–468
Fähigkeitsstufe 245–247, 249
Finanzen 432
Finanzmanagement 467
First-Level-Support 216
FISG 272
Framework 444
Funktionstrennung 275, 376
G
Gericht 198
Geschäftsmodell 123, 135, 141, 145, 282
Geschäftsprozess 240, 242, 274–275, 292, 307, 411
Geschäftsprozessmanagement 206
Gesetze 196, 198, 350, 475
  allgemeine Rechtsnormen 351
  IT-Gesetze 352
  unbestimmte Rechtsbegriffe 351
Gesundheit 473
GmbHG 196
GoBD 238, 351, 355, 399
  Archivierung 355

Datenzugriff 355
Scannen von Dokumenten 355
Governance-Verantwortung 374
Guild 257
G20 3
G20/OECD 272
Grundsätze der Corporate Governance 3
H
Hackathon 133, 264
Hacker 284
Hausstandard 443
Hinweisgebersystem 294
Hochschulen 264
Homeoffice 254
Homogenität 131
I
IDW PH 9.860.1 238, 397
IDW PH 9.860.2 238
IDW PH 9.860.3 398
IDW PS 860 238, 394
Berichterstattung 396
direkte Prüfung 395
Erklärung 395
Konformität 396
Kriterien 395
Prüfungshinweise 396
Prüfungsurteil 396
Treiber 394
IDW PS 951 235, 362, 400
Adressat 400
IKS des Dienstleisters 400
IDW PS 980 343
Abgleich mit ISO-Normen 345
Berichterstattung 393
CMS-Beschreibung 343, 392

CMS-Grundsätze 343
Entwicklung 343
Grundelemente 343, 392
Musterformulierungen 393
Prüfung 392
Prüfung der Angemessenheit 392
Prüfung der Wirksamkeit 393
Prüfungsurteil 393
IDW PS 981 301, 308, 319, 325
IDW RS FAIT1 200, 363
IEC 446
Industrie 4.0 405
Information Governance 19
Informationssicherheit 200
Managementsystem 207, 469
Informationssicherheitsbeauftragter 198
Infrastrukturmanagement 372
Innovate-Design-Transform 209, 214
Innovation 130, 134, 138, 142, 202, 204, 209–211, 249–250, 466
Innovation Lab 253, 263
Innovationsmanagement 133, 248
Integrität 362
Interne Revision 3, 296, 308, 323
Internes Kontrollsystem 272, 477
Internet of Things 405, 415
Investitionsrechnung 74
Investment-Center 224, 226
ISACA 5, 445, 460
ISAE 3402 235
ISO 446
ISO 19600
Norm Typ B 341
ISO 27002 363
ISO 31000 273
ISO 37000 159

ISO 37301 341
Compliance-Ziele 371
Elemente 341
Regelkreis PDCA 341
Zertifizierungsstandard 341
ISO/IEC TR 38502 453
ISO/IEC TR 38504 454
ISO/IEC TR 38505-2 455
ISO/IEC TS 38501 453
ISO/IEC TS 38505-3 455
ISO/IEC 27001 238
ISO/IEC 27014 456, 458
ISO/IEC 3850x 451
ISO/IEC 38500 7, 160, 277, 434, 451, 458
ISO/IEC 38503 454
ISO/IEC 38505-1 434, 454
ISO/IEC 38505-2 437–438
ISO/IEC 38506 455
ISO/IEC 38507 456
IT-Abteilung 131, 133, 136, 194, 202–204, 207, 209, 214, 220, 222, 254, 293, 299
IT als Enabler 64, 195, 204, 466
IT-Anwender 275, 300
IT-Berater 299
IT-Beschaffung 125, 130
IT-Betrieb 125, 138, 204, 208, 226, 259, 261–262
IT-Betriebsmittel 472, 474
IT-Budget 125, 131, 467
IT-Code of Conduct 370
IT-Compliance 124–125, 130, 144, 146, 151, 203, 209, 212, 236–237, 240, 242, 253, 276, 282, 287, 410, 445, 475
Auditierung 392
aufsichtliche Vorgaben 334
Control-Self-Assessment 391
Definition 336
Facetten 336
Kommunikation 385, 390

Konsistenz zur IT-Strategie 334
Management 131
Manager 381, 384
Aufgaben 384
Ausbildung 385
Berufsbild 385
externe Aufgaben 384
Unabhängigkeit 384
Zuordnung 384
Nutzen 335
Organisation 379
Organisationsformen 380
Programm 376
Rahmenwerke 339
Regelungen 338
Risiko 374
Begriff 374
Szenarien 375
Treiber 332
Überwachung 391
Compliance Audit 392
Interne Revision 391
Vermeidung von Bußgeldern 334
Ziele 370–371
nach Abteilungen 372
nach IT-Prozessen 373
nach Regelwerken 373
Strukturierung 372
IT-Controlling 237, 304
IT-Dienstleister 125, 133, 174, 178, 198–199, 204, 227, 229–230, 233, 298
IT doesn’t matter 61
IT-Fachanwälte 175
IT-Fortbildungsverordnung 354
IT-Funktion 195, 203
IT-Governance 141, 203, 409–410

nach COBIT 2019 19
IT Governance Institute 5
IT-Governance-Mechanismen 24
IT-Governance-System 462, 464
IT-Grundschutz-Methodik 377
ITIL® 219
IT-Infrastruktur 124–125, 130, 199, 205, 207–208, 225–226, 275, 282, 406, 471–472
IT-Investition 143, 145, 223, 225–226, 242, 313, 455, 467
IT-Kontinuitätsmanagement 303
IT-Kontrollen 237, 469
IT-Kontrollsystem 130, 229, 233, 237, 276, 300, 312, 475
IT-Kosten 125, 130, 224, 227, 229, 242, 467
IT-Kostenrechnung 72
IT-Lenkungsausschuss 131–132, 150–151, 169, 239, 313
IT-Lieferanten 125, 208, 468, 471
IT-Mitarbeiter 45, 51, 82, 143, 171, 199–201, 242, 254–255, 263, 282, 360, 368–369, 384, 390, 417, 422, 448, 465, 467
Entwicklung 44, 133, 319
IT-Norm 447
IT-Nutzer 172, 201, 203, 282, 300
IT-Organisation 138, 193, 196, 199–200, 202, 214, 411
IT-Outsourcing 133, 152, 209, 227–228, 230–231, 233, 283, 298, 324, 413
IT-Personal 126, 282
IT-Portfoliomanagement 152, 467
IT-Produkte 208, 467–468, 471
IT-Produkthersteller 299
IT-Programm 152, 199, 205, 470
IT-Programmmanagement 467
IT-Projekt 125, 131, 142, 152, 199, 205, 465, 472
IT-Projektmanagement 207, 218, 472
IT-Projektportfolio 124
IT-Prozess 142, 201, 205, 234, 240, 242, 244–245, 247, 249, 275, 282, 303, 315, 462, 466
IT-Prüfung 125, 238, 473
IT-Qualität 450
IT-Qualitätsmanagement 226, 237, 473
IT-Ressourcen 142, 207–209, 242, 467, 474

IT-Revision 125, 130, 170, 237, 239, 287, 300, 320
IT-Richtlinien 124, 132, 199, 359, 428, 431, 448, 462, 475
IT-Risiken 125, 151, 153, 203, 209, 242, 273–275, 285, 288, 293, 298, 375, 450, 469, 471, 477
IT-Risikoanalyse 310
IT-Risikoanalysten 314
IT-Risikoausschuss 313
IT-Risikobewertung 309–310
IT-Risikobewusstsein 289, 292
IT-Risikoeigentümer 314, 318
IT-Risikoidentifikation 308–310
IT-Risikokommunikation 292, 309, 311
IT-Risikokultur 286, 293, 295–296, 317, 319
IT-Risikomanagement 125, 131, 236–237, 239, 242, 276, 289, 301, 414, 424, 450, 464, 468, 473
IT-Risikomanagementorganisation 321
IT-Risikomanagementprozess 310
IT-Risikomanagementsystem 286, 289–290, 294, 301–302, 315–320, 322, 324–325
IT-Risikomanager 313
IT-Risikoorganisation 302, 314, 329
IT-Risikorichtlinie 289, 297
IT-Risiko-Stakeholder 297–299, 307, 318
IT-Risikosteuerung 283, 296, 309, 311
IT-Risikostrategie 242, 279, 296, 310, 321, 324
IT-Risikoszenarien 469
IT-Risikoziele 290, 296
IT-Service-Provider 227
IT-Services 125, 204, 207–208, 223, 234, 467–468, 471–474
IT-Sicherheit 125, 130, 204, 212, 262, 282–283, 287, 303, 410, 450
IT-Sicherheitsbeauftragter 197
IT-Sicherheitsgesetz 2.0 352
IT-Sicherheitsmanagement 125, 131, 195, 201, 207, 237, 240
IT-Sicherheitsrichtlinie 143
IT-Sourcing 209, 465
IT-Stakeholder 125, 136, 152, 160–162, 166, 176, 181, 214, 227, 236, 239–242, 292, 306, 412, 465–471, 473, 475
  Analyse 183, 188
  Einbindung 183, 186, 188

Identifizierung 182, 187
Kommunikation 186
Management 162, 180, 182, 185
IT-Standards 124, 132, 447
IT-Strategie 124, 130–132, 142–144, 151, 177, 199, 206, 247, 296, 321, 411, 427, 466–467
IT-Strategieausschuss 150
IT-Systeme 471–472
IT-Verträge 471
IT-Wertbeitrag 123, 161, 195, 236, 242, 246, 291, 313, 470
als »Nutzenbündel« 77
IT-Wissen 148
IT-Ziele 177, 199, 204, 247, 306, 320, 427, 466, 476
J
Jahresabschlussprüfung 237
K
KAIT 197–198
Kapazität 471
Kennzahlen 140, 189, 212, 242, 279, 421, 464
Kernkompetenzen 227
Kommodisierung 61
Kommunikation 149, 197, 233, 249, 471
Komplexitätsproblem 70
Konfigurationsmanagement 472
Konflikt 136, 141
Konsolidierung 362
Regelwerke 362
Kontinuierliche Verbesserung 468
Kontinuität 143–144, 146
Kontinuitätsmanagement 474
KonTraG 272
Kontrollen 429
Kontrollmatrix 363
Kontrollsystem 3
Kontrollziele 364, 401
Kostenarten 72

KRITIS-Betreiber 212, 284, 293, 296
Kulturwandel 144
Kunden 173, 250
Kundenorientierung 206
Künstliche Intelligenz 144, 194, 282, 414, 456
L
Lebenszyklus 472
Leitungsorgane 122, 127, 153, 249, 277, 285, 292, 294–295, 322–323
Lieferantenauswahl 232
Lieferantenmanagement 208
Lieferkettensorgfaltspflichtengesetz 284
Liquidität 145
Lizenzrechte 436
Low Code 261–262
M
Machine Learning 414
Managementsystem 337
  integriertes 338
  Module 338
Mapping 366
  Regelwerke 366
  Zweck 366
MaRisk 289, 355, 412
  prinzipienorientierte Aufsicht 355
Massachusetts Institute of Technology 5
MEA-Domäne 474
Metadatenmanagement 415
Metriken 233, 242, 475
Mindset, agiles 252, 255
Minimal Viable Product 263
N
Nearshoring 209
NIST 362
Non-Compliance 284, 374, 414, 464, 475
Normen 360, 443

Normungsorganisation 360, 445
Notfallplanung 143, 200, 474
Nutzendimensionen 80
Nutzwertanalyse 75

O

OECD 3
Offshoring 133, 209, 211
Open Data 415
Ordnungsrahmen 180
Organisationsformen 380
Organisationsverschulden 196
Outsourcing 358

P

Personalbeschaffung 254
Personalentwicklung 467
Personalplanung 467
Personenbezogene Daten 197
Pflichtberichterstattung 242
PH 9.860.2 398
PH 9.860.4 399
Plan-Build-Run 200, 206, 208, 211–212, 260
Plan-Measure-Control 211, 214
Plattformen 407
Plattformökonomie 282
Problemmanagement 428, 473
Process Mining 261
Process Owner 217, 300
Product Owner 257
Produktivitätsparadoxon 61
Profit-Center 130, 224, 226
Programmänderungen 376
Programmierung 260
Projektdokumentation 204
Projekt-Management-Office 153, 206, 428
Proof of Concept 263

Prototyping 263
Prozesskosten 74
Prozessorganisation 196
Prüfungsausschuss 272, 276, 322

Q

Qualifikation 448, 467
Qualifizierung 249
Qualitätsmanagement 207, 469
  System 469

R

RACI 240, 243
Ransomware 274
RDAP-Skala 183
Rechnungslegung 237, 281
Rechnungswesen 467
Rechtsbefolgung 369
Rechtsprechung 353
Rechtstreue 369
Rechtsverordnungen 353
Regelkonformität 331
Regelwerke
  Bindungswirkung 349
  Cloud 348
  Herkunft 347
  ISO-Normen 349
  Klassifizierung 347
  Normgeber 348
  Normgebungsverfahren 349
  Themen 348
Reifegradstufen 247
Rentabilität 145
Retained Organisation 231
Re-Zertifizierung 448
Risikoakzeptanz 130, 283, 376
Risikoanalyse 305

Risikoappetit 288–289, 291, 295, 320
Risikoausschuss 312
Risikobereitschaft 236, 242, 285
Risikobeurteilung 305
Risikobewertung 275, 305
Risikodaten 306, 308, 316
Risikoeigentümer 217, 237, 287, 300
Risikoereignis 308
Risikoidentifikation 305
Risikokategorien 280
Risikomanagement 375
  Office 313
Risikomanagementprozess 304, 308
Risikomanagementsystem 3
Risikoorientierung 285
Risikopolitik 249
Risikoprofil 279–280, 307
Risikosteuerung 273, 305
Risikostrategien 376
Risikotoleranz 242, 279, 288–289, 291, 295, 469
Risikotragfähigkeit 130, 283, 288–289, 295, 320
Risikovermeidung 375
Rollen 136, 216, 218–219, 243, 246, 257, 313

S

SAM 97
SAMM 103
Sarbanes Oxley Act 122
Schadensersatz 196
Schatten-IT 210, 261
Schulung 197–198
Schutzbedarf 201
Schutzbedarfsanalyse 377
Schwachstelle 273, 275
Schwachstellenanalyse 389
SCM-System 130

Scrum 217, 250–251, 263
Self-Assessment 125, 475
Sensibilisierung 197–198, 249, 292, 469
Service Level Agreement 179, 199, 207, 229, 234, 361, 468–469, 473
SFIA 231
Shared-Service-Center 225–226
Social Media 405
Societas Europaea 145
Softwareentwicklung 217, 250, 255
Softwarelizenzen 472
Sorgfaltspflichten 196, 288
Source-Make-Deliver 207, 209, 213
Squad 256
Stakeholder 3, 157, 159–160
Stammdatenmanagement 408, 415, 419, 421
Stand der Technik 351, 358
Standards 235, 360, 442
  COSO 360, 395
  DIIR-Standards 360
  IDW-Prüfungsstandards 360
Standardsoftware 206
Start-up 134, 263
Störungen 473
T
Testmanagement 207, 226, 261
Time-to-Market 251
TKG 197, 352
TOGAF 52, 419, 445, 466
Tone at the top 285, 294, 319
Total Cost of Ownership 73
  Verfahren 230
Transparenz 136, 204
Tribe 257–258
TTDSG 352
Typ-1-Bericht 235

Typ-2-Bericht 235

U

Überwachung 125, 141, 152, 196–197, 203–204, 233, 238, 470, 473, 475

Unbestimmte Rechtsbegriffe 351

Unified Compliance Framework 378, 445

Unsicherheitsproblem 70

Unternehmen 297

Unternehmensexterne Regelwerke 360

Unternehmensinterne Regelwerke 359

- Arbeitsanweisungen 359
- IT-Richtlinie 359

Unternehmenskultur 135

Unternehmensleitung 122, 130–134, 136–137, 141, 145, 149–150, 169, 178, 195–196, 198, 218, 221, 236–238, 278, 285, 294, 297, 304, 411, 413, 423–424, 437, 450, 454, 465

Unternehmensrisiken 375

Unternehmensstrategie 144, 242, 247, 249, 296, 464–465, 470, 472

Unternehmensüberwachung 2

Unternehmenswerte 369

Unternehmensziele 3, 466, 476

Urheberrechte 436

Use Case 137, 263

User Experience 262

V

Veränderungsmanagement 211

Verfahrensdokumentation 238

Verfügbarkeit 138, 207, 212, 274, 283, 471, 474

Verordnung 196

Verträge 356

- Dienstvertrag 357
- Kaufvertrag 357
- Mietvertrag 357
- Softwareüberlassungvertrag 357
- Werkvertrag 358

Vertragliche Verpflichtungen 361

Vertragsmanagement 208, 359

Vertragstypen 357
Vertrauen 149
Verwaltungsanweisung 196
Verwaltungsvorschriften 354
  norminterpretierend 354
  normkonkretisierend 354
Vorgehensmodell 138
Vorstand 141, 272

W

Wartung 208
Wasserfallmodell 251
Weiterbildung 144
Wert
  als Beitrag zur Zielerreichung 68
  als Überschuss/Nettoeffekt 67
  attributiver 67
  substanzieller 67
Wertbeitrag 287, 436, 464, 467
  immaterieller 78
  Referenzmodell 83
  schwer quantifizierbarer 78
Wertbeitrag der IT 61
  COBIT 109
  Definitionen 65
  empirische Untersuchungen 62
  Rolle der IT-Governance 65
  und IT-Governance-Mechanismen 63
Wertbeitragsdimensionen 79
  Referenzmodell 84
Wertschöpfungsmanagement 86
Wettbewerb 133, 204
Whistleblower 294
Wiederherstellung 473
Wirksamkeit 288, 300, 320, 322, 326
Wirksamkeitsprüfung 322

Wirtschaftsprüfer 175, 178, 234–235, 238, 299
Wissensmanagement 472

Z

Zertifizierung 448
Zielkaskade 160
Zugangsrechte 474
Zugriffskontrolle 216
Zurechenbarkeitsproblem 70

Ziffern

1. Linie 277, 300
2. Linie 276, 299–300
3-Ebenen-Modell 383
3-Linien-Modell 125, 236–237, 239–240, 276, 287
3. Linie 299