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).

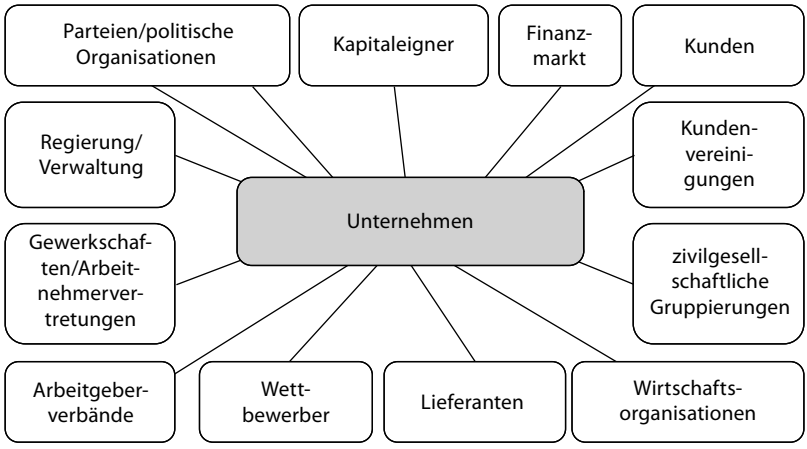

Abb. 4–1
Externe Akteure des Unternehmens (vgl. [Freeman 1984], S. 25)

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 da-

rauf 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-Manage-

ment 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.

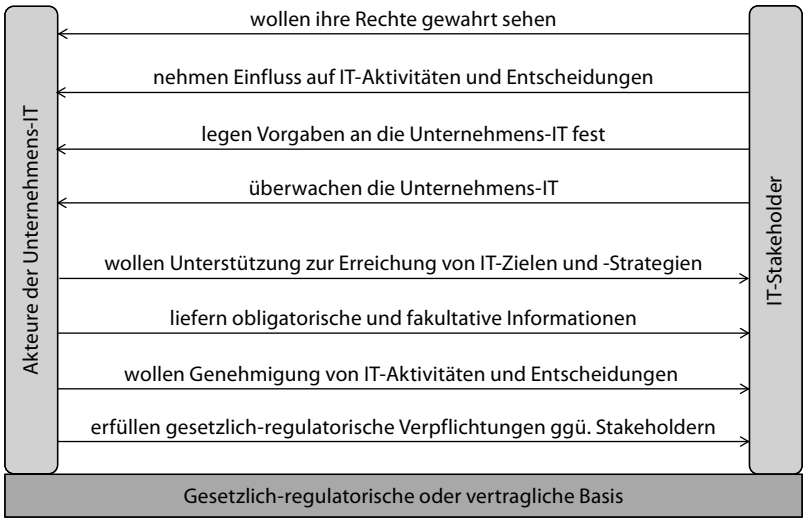

Abb. 4–2
Zweiseitige Beziehungen zwischen Unternehmens-IT und IT-Stakeholdern

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.

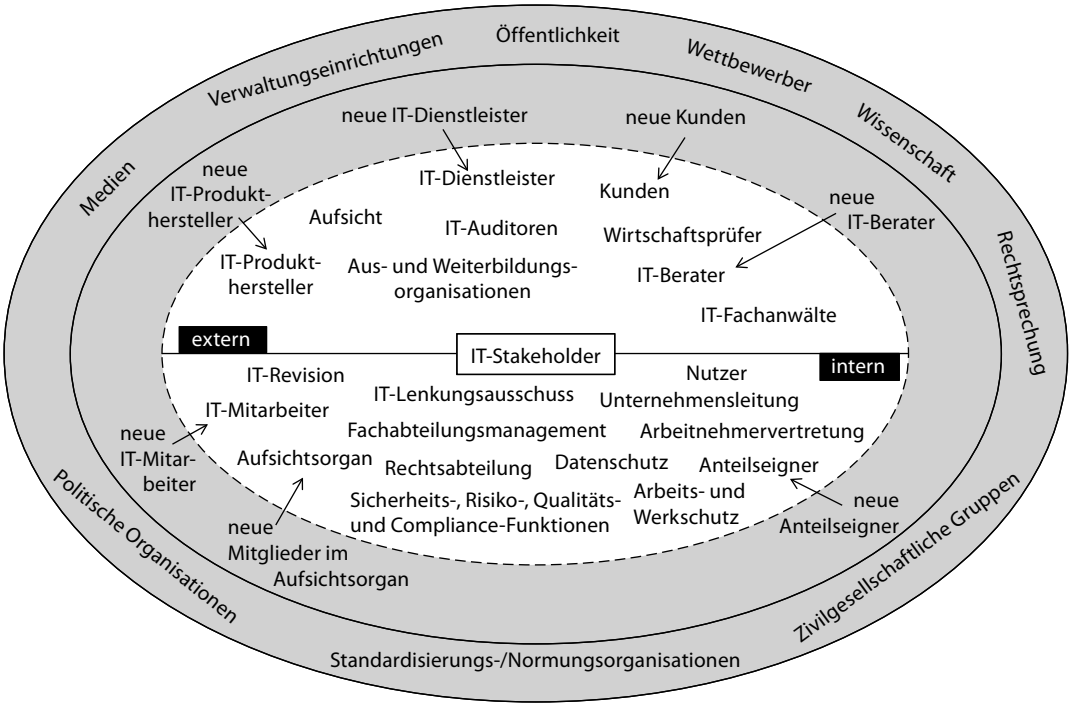

Abb. 4–3 *Interne und externe IT-Stakeholder vs. Akteure der Unternehmensumwelt*

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 Mitar-

beiterabgängen 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.

IT-Produkthersteller

Hersteller von IT-Produkten

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 abhän-

gen. 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.