Ernst **TIEMEYER**

ENTERPRISE IT-GOVERNANCE

Unternehmensweite IT-Planung und zentrale IT-Steuerung in der Praxis

HANSER

Tiemeyer

Enterprise IT-Governance

Ernst Tiemeyer

Enterprise IT-Governance

Unternehmensweite IT-Planung und zentrale IT-Steuerung in der Praxis

HANSER

Der Autor:
Ernst Tiemeyer, Hamminkeln
ETiemeyer@t-online.de

Bibliografische Information der Deutschen Nationalbibliothek:

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

Lektorat: Brigitte Bauer-Schiewek
Copy editing: Petra Kienle, Fürstenfeldbruck
Coverkonzept: Marc Müller-Bremer, www.rebranding.de, München
Covergestaltung: Max Kostopoulos
Satz: Eberl & Koesel Studio, Kempten
Druck und Bindung: Hubert & Co. GmbH & Co. KG BuchPartner, Göttingen
Printed in Germany

Print-ISBN: 978-3-446-42729-7
E-Book-ISBN: 978-3-446-42963-5
E-Pub-ISBN: 978-3-446-47636-3

Inhalt

Vorwort

Die Leistungsfähigkeit des IT-Personals, die Performance der gesamten IT-Landschaft sowie die Qualität der bereitgestellten IT-Services haben in den letzten Jahren in Unternehmen aller Größenordnungen und in nahezu allen Branchen eine zunehmende Bedeutung für das Geschäft des Unternehmens erlangt. Eine optimale Ausrichtung der IT-Organisation für das Gesamtunternehmen ist damit wesentlich. Diese kann aber nur dann gelingen, wenn sowohl die Planung als auch die Steuerung der IT-Angebote (Applikationen, Informationssysteme, IT- und Cloud-Services) ganzheitlicher betrachtet und umgesetzt werden. Dabei gilt es Planungs-, Entscheidungs-, Steuerungs- und Kontrollaufgaben für die Enterprise IT so zu verankern, dass die Leistungserbringung der IT-Organisation einen hohen Beitrag zum Business-Value des Unternehmens nachhaltig und sicher unter Beachtung der vielfältigen Regularien gewährleistet.

Die Konsequenz: Nahezu alle Unternehmen und Organisationen benötigen für ein erfolgreiches Lösen der anstehenden IT-Aufgaben und Herausforderungen eine „gut aufgestellte" und kundenorientiert arbeitende IT-Organisation; egal, ob es sich um eine klassische interne IT-Abteilung, ein zentrales IT-Competence-Center oder um einen speziellen IT-Dienstleister handelt. Minimumvoraussetzungen dafür sind hochverfügbare IT-Systeme, kompetentes IT-Fachpersonal sowie handhabbare Managementinstrumente. Eine gemeinhin akzeptierte Feststellung lautet: Ohne eine unternehmensweite Planung und eine zentrale Steuerung der IT-Bereiche (IT-Services, IT-Produkte, IT-Prozesse, IT-Projekte) ist eine leistungsfähige IT, die einen umfassenden Beitrag zur Wertschöpfung von Unternehmen und Verwaltungen leistet, heute nicht mehr möglich.

Erfahrungen der Praxis zeigen aber auch: Um unternehmensweit eine wirtschaftliche, hocheffiziente IT zu gewährleisten, sind heute – im Vergleich zu vergangenen Zeiten – konkrete Handlungsfelder und Konzepte für die IT-Governance und das IT-Management zu fokussieren und verstärkt zu etablieren:

- eine stärkere strategische Ausrichtung der IT unter Beachtung der Unternehmensstrategie,
- der Aufbau und die Nutzung von Managementsystemen zur Berücksichtigung von Governance, Risk- und Compliance-Anforderungen (GRC),
- ein Roadmapping mit ganzheitlichen Konzepten zur Planung und Konsolidierung der Enterprise-IT-Architekturen,

- eine unternehmensweite Harmonisierung und bedarfsgerechte Erhebung der Anwenderanforderungen sowie eine
- eine zentrale Planung der IT-Portfolios mit einer abgestimmten integrierten IT-Portfoliosteuerung.

Hinzu kommt die Notwendigkeit, ein wertorientiertes Performance-Management „aufzusetzen", die Einhaltung vielfältiger rechtlicher Vorgaben und interner Richtlinien zu sichern (IT-Compliance) sowie die Institutionalisierung eines IT-Risiko- und Innovationsmanagements zu gewährleisten.

Als Antwort auf die vielfältigen technologischen und organisatorischen Herausforderungen im IT-Bereich hat sich mittlerweile das Konzept „Enterprise IT-Governance" etabliert und in der Praxis eine vielfältige Anwendung gefunden. Durch die vorhandene IT-Komplexität sowie die enormen und raschen Veränderungen und Herausforderungen des Business wird es für die IT-Verantwortlichen immer schwieriger, sich und ihre Abteilungen auf Erfolgskurs zu halten und dabei vor allem den Gesamterfolg des Unternehmens nicht aus den Augen zu verlieren. Eine unternehmensweite IT-Planung und eine zentrale IT-Steuerung gelten deshalb derzeit als wichtiger Ansatzpunkt, wenn es um eine zukunftsorientierte Konzeptentwicklung und Organisation der IT im Unternehmen geht.

Kennzeichen moderner „IT-Governance" ist, dass die Organisation, Steuerung und Kontrolle des IT-Einsatzes in einem Unternehmen zentral durch Personen erfolgen, die in der Unternehmensführung verankert sind (als CIO). Diese Steuerung (engl. „Governance") durch eine zentrale Institution wird als dringend notwendig gesehen. Als wesentliche Gründe können genannt werden:

- Hoher Wert der IT-Assets: Die zunehmende Durchdringung der Unternehmen durch die IT sowie die hohe Komplexität der IT-Lösungen haben zur Folge, dass der Wert der IT-Investitionen und damit der Wert des gesamten IT-Bestands eines Unternehmens im Vergleich zum Gesamtwert des Unternehmens von immer größerer Bedeutung geworden sind.
- IT ist ein wesentlicher Erfolgsfaktor für einen reibungslosen Ablauf und die konsequente Verbesserung der unterstützten Geschäftsprozesse.
- Strategieorientierung ist unverzichtbar: Ohne eine strategische Ausrichtung der IT und die Orientierung an strategischen Zielsetzungen ist eine nachhaltige Entscheidungsfindung auch für den IT-Bereich nicht mehr zu bewerkstelligen.
- Notwendige Risikoorientierung für die IT: IT-Architekturen (bzw. IT-Produkte und IT-Services) verfügen über eine hohe Komplexität, unterliegen damit aber auch einem hohen Ausfallrisiko. So spielen IT-Prozesse – insbesondere die Serviceprozesse – in vielen Unternehmen eine zunehmend wichtige, aber auch kritische Rolle. Ein gezieltes IT-Risikomanagement ist deshalb als Daueraufgabe zu etablieren und weiterzuentwickeln.

Hauptstoßrichtung dieser Publikation ist – nach einer grundlegenden Einordnung von Corporate Governance, GRC (Governance, Risk & Compliance) sowie der Aufgaben der IT-Governance (Evaluate, Direct, Monitor) – die strukturierte Darlegung der Handlungsfelder von Enterprise IT-Governance und deren Umsetzung mittels bewährter Instrumente und Handlungspraktiken. Mit der umfassenden Einführung von Strukturen und Prozessen der Enterprise IT-Governance wird letztlich die konsequente Ausrichtung der IT-Produkte, der IT-Prozesse, der IT-Architekturen und der IT-Portfolios an strategischen Überlegungen und Entscheidungen sowie an den Bedarfen der Kunden/Anwender ermöglicht.

Dieses Buch gibt Ihnen eine ganzheitliche, aber auch praxisnahe Orientierung zu den vielfältigen Herausforderungen und den skizzierten Handlungsfeldern von Enterprise IT-Governance. Eingangs finden Sie eine Einordnung sowie Ausführungen zur Bedeutung von IT-Governance, indem die Anlässe, Herausforderungen und Zielsetzungen angesprochen werden. Weitere Fragenkreise, die in diesem Buch angesprochen werden, sind die Bereitstellung und Nutzung von Frameworks für die Governance der Enterprise IT (insbesondere COBIT) sowie die Organisation und Einführung von Enterprise IT-Governance in die betriebliche Praxis.

In den weiteren Kapiteln des Buchs wird auf wesentliche Handlungsfelder von Enterprise IT-Governance eingegangen, wobei folgende Kernbereiche unterschieden werden:

- Enterprise IT-Planungen (Strategien) vereinbaren und erfolgreich umsetzen
- Enterprise-Architecture – EA-Organisation, Planungen und EA-Governance
- Digitale Transformationen planen, umsetzen und steuern
- IT-Portfoliomanagement und Enterprise IT-Governance – Konzepte und Lösungen
- IT-Investitionsmanagement und wertorientiertes Controlling (Value Management)
- Enterprise IT-Risiko- und Compliancemanagement – Prozesse, Anwendungsformen, Einführung

Insgesamt sind Sie mit Unterstützung der Ausführungen in diesem Buch in der Lage, Strukturen, Verfahren, Projekte und Prozesse zur erfolgreichen Umsetzung von Enterprise IT-Governance zu identifizieren und Roadmaps für Ihre Praxis zu entwickeln. Dabei „erschließen" Sie wichtige Management- und Governance-Aufgaben und erwerben umfassende Methoden- und Managementkompetenzen zur Gestaltung ganzheitlicher Enterprise IT-Governance-Lösungen.

Wesentliche Zielsetzungen und Handlungskompetenzen, die mit dem Lesen dieses Fachbuchs erworben werden können, sind nachfolgend exemplarisch skizziert:

- *IT-Assessments vorbereiten und durchführen:* Mit dem Durcharbeiten des Buchs erwerben Sie u. a. die Kompetenz, IT-Assessments erfolgreich durchzuführen, strategische Business-IT-Planungen vorzunehmen sowie Entscheidungen (zu IT-Portfolios, Investitionen) vorzubereiten und unter Berücksichtigung ausgewählter Kriterien (in Teams/Boards) zu treffen.
- *Handlungsfelder und Aufgaben von IT-Governance und IT-Management identifizieren:* Mit dem Durcharbeiten dieses Fachbuchs erwerben Sie das fachliche Know-how und die Kompetenz, IT-Governance hinsichtlich der Bedeutung für die IT-Praxis einzuschätzen sowie entsprechende Handlungsfelder zu identifizieren.
- *IT-Governance-Prozesse analysieren und gestalten:* Das Fachbuch soll Ihnen helfen, Ihre Handlungsstrukturen in IT-Governance-Prozessen zu erkennen, zu analysieren und so weiterzuentwickeln, dass Sie IT-Governance-Prozesse in der Unternehmenspraxis zielorientiert gestalten und zur Verfügung stehende Instrumente bzw. bewährte Methoden erfolgreich nutzen können.
- *IT-Governance-Tools, Werkzeuge und Methoden nutzen:* Sie erfahren auf anschauliche Weise, wie Sie Ihre Methodenkompetenz auf die beruflichen bzw. geschäftlichen Herausforderungen von Enterprise IT-Governance transferieren können. Gleichzeitig werden Sie so mit den wichtigsten IT-Governance-Werkzeugen vertraut gemacht (wie etwa im Bereich EA-Governance, Digital Governance, Data Governance etc.).

Das Buch richtet sich an das Fach- und Führungspersonal aus der Unternehmens-IT sowie an das Management der Fachbereiche bzw. die Unternehmensführung. Beispielsweise seien genannt:

- IT-Leitung (CTOs), Leitung von IT-Kompetenzzentren, IT-Strategists
- Risk- und Compliance-Manager, GRC-Verantwortliche
- Chief Information Officer (CIOs), Chief Data bzw. Digital Officer (CDOs), CISO
- Unternehmensführung (CEOs, Geschäftsführung)
- Leader EAM (Enterprise Architecture Management), Solution-, Data- und Integration-Architekten
- IT-Verantwortliche verschiedener Schwerpunktbereiche; z. B. Leitung System- und Anwendungsentwicklung, Digital-Platform-Management, Cloud-Management
- IT-Portfolio-Management (Investitionsportfolio, Produkt- und IT-Serviceportfolio)
- Qualitätsmanager in der IT, IT-Controller und IT-Revisoren, IT-Compliance-Manager

Nicht zuletzt dürfte das Handbuch für alle Studierenden beispielsweise der Wirtschaftsinformatik oder anderer angewandter Informatik-Studiengänge an Fachhochschulen und Universitäten höchst interessant und lesenswert sein. Gerade von künftigen Fach- und Führungskräften der Informations- und Kommunikationstechnik sowie im Umfeld digitale Transformation, Automation und KI (intelligente Technologien) wird ein immer komplexeres Management-Know-how erwartet, wollen sie den Herausforderungen der Praxis gerecht werden und ihnen übertragene Aufgaben erfolgreich wahrnehmen.

Danken möchte ich dem Carl Hanser Verlag, hier insbesondere Frau Brigitte Bauer-Schiewek als verantwortliche Lektorin, Frau Irene Weilhart sowie Frau Kristin Rothe, die durch ihre Vorgaben und weiterführenden Hinweise sowie durch ein zielgerichtetes Controlling für die professionelle Umsetzung dieses Buchs gesorgt haben.

Ich wünsche Ihnen viel Spaß beim Lesen sowie Ideen zur Umsetzung des Gelesenen in Ihre Praxis. Über Anregungen zur Verbesserung und Weiterentwicklung des Buchs aus dem Kreis der Leserinnen und Leser würde ich mich freuen.

Hamminkeln, im Oktober 2022

Ernst Tiemeyer

ETiemeyer@t-online.de

1 Enterprise IT-Governance – Positionierung, Aufgabenbereiche, Handlungsfelder

Fragen, die in diesem Kapitel beantwortet werden:

- Inwiefern stellt Corporate Governance einen wesentlichen Ausgangspunkt zur Einführung und Umsetzung von Enterprise IT-Governance dar?
- Wie kann die Enterprise IT-Governance im Unternehmenskontext eingeordnet und „aufgestellt" werden?
- Welcher Wertbeitrag für die Unternehmensorganisation kann durch erfolgreiche Enterprise IT-Governance erwartet werden?
- Welche Handlungsprinzipien und Zielsetzungen kennzeichnen eine moderne Enterprise IT-Governance?
- Inwiefern stellt ein funktionierendes Business IT-Alignment eine wichtige Rahmengröße für eine Enterprise IT-Governance dar?
- Wie kann ein Konzept bzw. die Roadmap für die Einführung und die Weiterentwicklung von Enterprise IT-Governance aussehen?
- Welche Aufgabenbereiche für die Enterprise IT-Governance haben sich in welcher Ausprägung bewährt (Plan, Control, Evaluate, Decide, Monitor)?
- Inwiefern kann zwischen Aufgaben der IT-Governance und des IT-Managements unterschieden werden, und welche Schnittstellen sind gegeben?
- Welche Handlungsfelder umfasst eine zeitgemäße Enterprise IT-Governance?
- Wie können die Handlungsfelder für Management und Governance der Enterprise IT eingeordnet werden und ausgerichtet sein?
- Welche Erfolgsfaktoren und Gestaltungsmerkmale für ein integriertes Management-Informationssystem zur Enterprise IT-Governance sind zu beachten?

1.1 Herausforderung „Enterprise IT-Governance“ – eine Einordnung

Enterprise IT-Governance gewinnt in der Unternehmenspraxis eine immer größere Bedeutung. Dieses einführende Buchkapitel nimmt eine erste Einordnung in die vielfältige Thematik „Enterprise IT-Governance“ vor, skizziert wesentliche Aufgabenbereiche und Handlungsfelder im Rahmen der Enterprise IT-Governance und gibt damit gleichzeitig einen Überblick zu den Inhalten für die nachfolgenden Kapitel.

Im Einordnungsteils werden zunächst die Grundlagen für eine „Verankerung“ von IT-Governance im Unternehmenskontext gelegt. Dazu wird eingangs eine **Positionierung** von Corporate Governance und IT-Governance für die Unternehmenspraxis vorgenommen. Anschließend werden der Weg zur Enterprise IT-Governance aufgezeigt, eine Positionsbestimmung für die Einführung vorgenommen (Vision, Mission) sowie die Festlegung der Zielsetzungen (inkl. Wertbeitragsbestimmung) erläutert.

Ausgehend von wesentlichen **Governance- und Management-Aufgaben** (Plan, Control, Evaluate/Decide, Monitor) werden schließlich die Kern-Handlungsfelder im Überblick skizziert, die mit der Umsetzung von IT-Governance für Enterprises wahrzunehmen sind:

- Dazu zählen insbesondere **Planungsbereiche** (Plan) wie strategische IT-Planung, Enterprise-Architekturplanungen sowie das Planen und Managen diverser Portfolios (beispielsweise zu Business-IT-Projekten, Geschäftsprodukten, Applikationen, Technologien und Business-IT-Services).
- Die **Steuerungsaufgaben** (Control) fokussieren auf EA-Governance, Multi-Projektsteuerung, Data Governance sowie auf das Handlungsfeld der digitalen Transformation und entsprechender Geschäftsfelder bzw. digitaler Produkte und Prozesse (digital governance).
- **Bewertungs- und Entscheidungsaufgaben** (Evaluate/Decide) bedürfen insbesondere im Portfolio- und Risikomanagement sowie im Finanz- und Investitionsmanagement einer besonderen Berücksichtigung. Aufgrund der hohen Bedeutung gilt es, diese Entscheidungen durch geeignete Verfahren und strukturelle Maßnahmen (Boards) nachhaltig abzusichern.
- Aufgaben sowie Handlungsbereiche der **Überwachung und Kontrolle** (Monitor) sind insbesondere für die Bereiche Risikomanagement, IT-Compliance und IT-Performancemanagement (IT-Controlling) sowie für Auditierungen verankert.

Um eine systematische Umsetzung der Management- und Governance-Aufgaben zu realisieren, haben sich in dieser Praxis diverse Handlungsfelder der Enterprise IT-Governance sowie dabei übliche Management- und IT-Governance-Praktiken etabliert. Sie stellen einen wesentlichen Handlungsrahmen im Unternehmenskontext dar. Die Handlungsfelder werden in diesem Kapitel in den Grundzügen beschrieben und eingeordnet. Eine ausführliche Darstellung findet sich dann in den Folgekapiteln.

1.1.1 Ausgangspunkte „Corporate Governance“ und GRC

Aufgrund vielfältiger Herausforderungen in Wirtschaft und Gesellschaft, dem Aufkommen intelligenter Digitalisierungstechnologien sowie dem steigenden Stellenwert der IT sind strategische Themen (Plan, Evaluate, Decide, Control) sowie Governance, Risk- und Compliancemanagement (kurz GRC) in den Mittelpunkt gerückt. Damit verbunden sind auch jene Chancen und Risiken von Bedeutung, welche in Zusammenhang mit der IT, der Digitalisierung sowie der Nutzung intelligenter Technologien (AI/KI, Machine Learning etc.) stehen.

Ausgangspunkt für Überlegungen zu einer Einführung und Weiterentwicklung von Enterprise IT-Governance im Unternehmenskontext ist der Begriff „Corporate Governance“. Damit wurde ursprünglich vor allem der rechtliche und faktische Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens angesprochen. Mittlerweile rechnen zur Coporate Governance erweiternd auch Planungs-, Entscheidungs-, Bewertungs- und Steuerungsaufgaben für das Gesamt-Unternehmen, mit deren Lösung ein wertvoller Beitrag zum Unternehmenserfolg geleistet werden kann.

Merke:

Unter Corporate Governance werden allgemein alle selbstgesetzten und extern vorgegebenen (ethischen) Werte, Grundsätze, Verfahren und Maßnahmen für eine gute und verantwortungsvolle Unternehmensführung zusammengefasst. Sie haben Konsequenzen für alle Betroffenen und Beteiligten am Unternehmensgeschehen (Beschäftigte, Stakeholder sowie für die Unternehmensführung selbst). Damit wird der Unternehmensleitung ein Rahmen für die Ausgestaltung und Implementierung von Planungs-, Entscheidungs- und Kontrollstrukturen im Sinne einer nachhaltigen Wertschöpfung für das Unternehmen gegeben.

Im Wesentlichen geht es bei der Festlegung „guter Corporate Governance“ um folgende Herausforderungen und Fragenkreise, die es zu lösen gilt:

- Wie lassen sich unter Beachtung anerkannter Werte und Grundsätze sowie internationaler und nationaler Regeln und Vorschriften eigne Unternehmensleitlinien entwickeln und erfolgreich implementieren?
- Wie kann die notwendige Transparenz und Offenlegung wichtiger Unternehmensdaten gesichert und geregelt werden (z. B. Nutzung von Unternehmens- und Kundenportalen, Ad-hoc-Berichterstattung versus regelmäßige Reports)?
- Welche Rechte zur Entscheidungsfindung sind den Aufsichtsgremien bzw. den Aktionären vorbehalten (z. B. Entscheidungen über Übernahmegebote), und wo sind die Beschäftigten an Entscheidungsprozessen zu beteiligen?
- Welche Kontrollmechanismen sind notwendig und zu vereinbaren (etwa hinsichtlich des Zusammenwirkens von Aufsichtsrat und Vorstand/Geschäftsführung)?
- Ist eine angemessene und leistungsorientierten Vergütung des Managements (z. B. Beteiligung des Managements am Residualgewinn) sowie der Beschäftigten gegeben?

Überlegungen zu einer Good Governance finden sich im internationalen Kontext in den Corporate Governance-Grundsätzen der Organisation for Economic Co-operation and Deve-

lopment (OECD). Diese Grundsätze, die in vielen Staaten eine Grundlage für nationale Governance-Regularien geschaffen haben, wurden erstmals 1999 publiziert sowie 2004 und 2015 aktualisiert.

Festzuhalten ist:

Corporate Governance richtet sich auf das „Geflecht der Beziehungen zwischen der Geschäftsführung eines Unternehmens, seinem Aufsichtsorgan (Board), seinen Aktionären und anderen Unternehmensbeteiligten (Stakeholdern)“ sowie auf „den strukturellen Rahmen für die Festlegung der Unternehmensziele, die Identifizierung der Mittel und Wege zu ihrer Umsetzung und die Modalitäten der Erfolgskontrolle“ ([OECD15], S. 9).

Die Corporate-Governance-Grundsätze der OECD fanden in Deutschland im Rahmen des „Deutschen Corporate Governance Kodex“ (DCGK) erstmals im Jahr 2002 Berücksichtigung. Der Kodex enthält unter anderem zahlreiche Empfehlungen und Anregungen für die Umsetzung von Corporate Governance. „Im Rahmen eines Corporate Governance Kodex sind im Detail Grundsätze, Empfehlungen und Anregungen zur Leitung und Überwachung börsennotierter Gesellschaften dokumentiert, die national und international als Standards guter und verantwortungsvoller Unternehmensführung anerkannt sind.“ [DCGK19]

Derzeit finden sich zahlreiche Vorstellungen darüber, was Corporate Governance ergänzend an Festlegungen und Orientierungen umfassen sollte. Einvernehmlich wird die Auffassung vertreten, dass Corporate Governance jedenfalls auch Fragenkreise gesellschaftlicher Verantwortung (Corporate Social Responsibility (CSR) mit ökonomischer, sozialer und ökologischer Nachhaltigkeit) und Integrität/Ethik berücksichtigen muss.

Neue gesetzliche und technische Herausforderungen an Organisationen, wie Unternehmenssanktionsrecht, Lieferkettengesetz, Berichterstattung über Nachhaltigkeit in der Lieferkette, Informationssicherheits- und sonstige globale Risiken verstärken den Bedarf der Organisationen an Management-Informationssystemen und offiziellen Nachweisen, dass das Unternehmen auch in den Bereichen Risiko-, Compliance- und Nachhaltigkeitsmanagement (ESG) aktuellen Governance-Anforderungen umfassend Rechnung tragen kann.

Um eine „gute“ Corporate Governance zu gewährleisten, sind die Geschäftsführer einer GmbH bzw. der Vorstand einer AG bereits per Gesetz dazu verpflichtet, ein den Anforderungen des Unternehmens entsprechendes **Internes Kontrollsystem (IKS)** einzurichten. Als IKS wird die Gesamtheit der Methoden und Maßnahmen zur Systematisierung einer ständigen, umfassenden Kontrolle und Information bezeichnet. Es dient insbesondere dazu,

- die vorhandenen Vermögenswerte des Unternehmens zu sichern,
- die betriebliche Leistungsfähigkeit zu steigern,
- die Vollständigkeit und Richtigkeit der geschäftlichen Aufzeichnungen sicher zu stellen,
- die Zuverlässigkeit des Rechnungs- und Berichtswesens zu gewährleisten,
- Vorstand und Geschäftsführung bei ihrer Überwachungsaufgabe zu unterstützen,
- dass das Unternehmensvermögen nicht durch kriminelle oder fahrlässige Handlungen geschädigt wird, sowie
- die betriebliche Effizienz durch Rationalisierungen und Kostensenkungen zu verbessern.

In der Realität stellt die Vielzahl an Unternehmens- und Geschäftsprozessen sowie deren Komplexität die Unternehmensführung oft vor enorme Herausforderungen. So ist es grundsätzlich problematisch, eine ordnungsgemäße Durchführung der Prozesse selbst bei guter Prozessorganisation zu überblicken. Die Einhaltung der Ordnungsmäßigkeit der Prozesse ist allerdings essenziell. Bereits minimale Abweichungen können negative Auswirkungen auf das gesamte Unternehmen haben. Abhilfe bzw. Übersicht schafft ein implementiertes effizientes Internes Kontrollsystem, indem es als Steuerungs- und Überwachungsinstrument bei der korrekten Ausführung der wichtigsten Prozessschritte im Unternehmen unterstützt.

Hinweis:

Ein Internes Kontrollsystem ist ein wichtiges Steuerungs- und Führungsinstrument eines jeden Unternehmens, das einer laufenden Überwachung bedarf.
In der Praxis geschieht dies meist über die interne Revision eines Unternehmens.
Es bietet sich an, die IKS-Systeme in sog. „Integrierte technologiegestützte Managementsysteme“ zu etablieren.

In den letzten Jahren hat sich zunehmend im Kontext der Corporate Governance auch das Kürzel **GRC** (für Governance, Risk, Compliance) eingebürgert. Basierend auf Überlegungen der OCEG (= Open Compliance and Ethics Group) kann GRC als eine integrierte Sammlung von Aufgaben und Fähigkeiten verstanden werden, die es einer Organisation ermöglichen,

- die Unternehmensziele zuverlässig zu erreichen,
- Unsicherheiten und Risiken zu bewältigen sowie
- integer und regelkonform zu handeln.

GRC umfasst im Unternehmenskontext per Definition die Arbeit von Abteilungen wie Innenrevision, Compliance, Risiko, Recht, Finanzen, IT, Personal sowie der Geschäftsbereiche, der Führungsebene und des Vorstands/der Geschäftsführung selbst.

Ein **GRC-System** eines Unternehmens oder einer Organisation stellt mittlerweile einen wesentlichen Bestandteil der Unternehmensführung („Corporate Governance“) dar. Verschiedene Managementfunktionen wie Internes Kontrollsystem, Sicherheitsmanagement, Krisenmanagement, Nachhaltigkeitsmanagement, Risikomanagement sowie Compliance-Management, dienen dazu, das Unternehmen vor Gefahren und Risiken zu bewahren, Chancen und Geschäftspotenziale zu erkennen und so insgesamt den Fortbestand der Institution zu sichern. Um die mit GRC verbundenen Aufgabenbereiche effizient und effektiv erfüllen zu können, bedarf es einer transparenten organisatorischen Ausgestaltung dieser Managementfunktionen sowie der Etablierung eines geeigneten, technologiegestützten Managementinformationssystems.

Im Einzelnen werden folgende Rahmenbedingungen genannt, die ein funktionales GRC-System ermöglichen:

- Um die Bedeutung einer GRC-Initiative sowie die Notwendigkeit entsprechender organisatorischer Verankerungen zu unterstreichen, ist eine Zusammenarbeit zwischen allen Mitgliedern der Leitungsebene unverzichtbar. Ggf. bedarf es die Einrichtung entsprechender Boards, in denen Abstimmungen und Entscheidungen getroffen werden.

- Eine ausgeprägte Risiko- und Security-Awareness ist gegeben. Eine Allokation von Ressourcen, um negative Konsequenzen im Falle des Eintritts von Risiken zu reduzieren, ist erfolgt.
- Eine Vorstandsposition für Informationssicherheit (CISO), die als Kontrollinstanz für andere Abteilungen wie IT, Risikomanagement und Compliance fungieren kann, ist etabliert.
- Eine Kultur, die das Verhalten zum Schutz von Daten und Informationen belohnt und nicht bestraft, ist gegeben.

Als Basis für den Aufbau und Betrieb des integrierten GRC-Systems hat sich das **Three-Lines-Modell** (kurz: 3LM; auch Modell der drei Linien) als ein sehr effektiver Ansatz bewährt. Dieses Modell, das von der European Confederation of Institutes of Internal Auditing (ECIIA) und der Federation of European Risk Management Associations (FERMA) entwickelt wurde, unterteilt eine Organisation in 3 Linien (die sog. **Three-Lines**), indem jeweils die Aufgaben der folgenden drei Gruppen im GRC-Kontext definiert und beschrieben werden:

- 1st Line – Operatives Management (Fachbereichsmanagement)
- 2nd Line – GRC-Funktionen für spezifische Services (z. B. Risikomanagement, IKS, Compliance etc.)
- 3rd Line – Interne Revision

Das Zentrum des Three-Lines Modells stellt das **operative Management** dar. Dieses sind etwa die Abteilungsleiter bzw. Bereichsleiter der Fachbereiche. Sie haben die fachliche Verantwortung aller Prozesse ihrer organisatorischen Einheit. Über diese Prozesse werden die Aufgaben innerhalb der jeweiligen Organisationseinheit strukturiert und vereinbart. Damit einher geht insbesondere auch die Verantwortung für Kennzahlen, Risiken, Kontrollen und die Einhaltung von Compliance-Vorgaben.

Auf der 2nd Line befinden sich die verschiedenen **Querschnitts-Disziplinen** wie Internes Kontrollsystem (IKS), Prozessmanagement, Risikomanagement, Compliance-Management, Corporate Security Management, Arbeitsschutz, Datenschutz (DSGVO), Health Management, Qualitätsmanagement und Umweltschutz. Sie definieren das Vorgehen und die Methode, um die verschiedenen Aufgaben bzw. Pflichten innerhalb der jeweiligen Unternehmensfunktion wahrnehmen und erfüllen zu können.

Die letzte der drei Linien besteht aus der **internen Revision**, welche die Aufgaben der Überwachung des GRC-Systems übernehmen und auf Effektivität und Effizienz prüfen.

Wesentlicher Nutzen und Vorteil des Three-Lines-Modell ist es, dass die Interaktion, Kooperation und Kommunikation zwischen den verschiedenen Management-Disziplinen verbessert werden kann. Dazu trägt insbesondere die konkrete Klärung und Beschreibung der wesentlichen Rollen im Corporate Governance- bzw. GRC-Umfeld bei. Wichtig ist, dass die Verantwortlichen der 2nd Line das Potenzial der Zusammenarbeit erkennen, um Querschnittsthemen gleichermaßen in den fachlichen Funktionsbereichen zu betrachten.

Hinweis:

Welche Empfehlungen werden gegeben, um Corporate Goverance bzw. GRC erfolgreich im Unternehmen zu verankern? Grundsätzlich sollte ein integriertes GRC-System im Rahmen eines Top-Down-Ansatzes etabliert werden. Die entsprechende Einführung müsste von der Unternehmensführung initiiert und geleitet werden. Dabei gilt es alle Beschäftigten des Unternehmens zu befähigen, potentielle Risiken oder Schwachstellen im Unternehmen zu erkennen und zu melden.

1.1.2 IT-Governance – Einordnung und Normen

IT-Governance wird vielfach als Teilbereich der Corporate Governance gesehen. Aufgrund der zunehmenden Bedeutung der IT für den Unternehmenserfolg hat sich dieser Handlungsbereich im Business IT-Bereich mittlerweile etabliert (vgl. auch Definitionen gemäß ISO/IEC 38500:2015 sowie des IT-Governance Instituts (kurz ITGI)).

Einen ersten konkreten Zugang zum Begriff „IT-Governance“ kann die folgende Definition geben: IT-Governance besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die IT die Unternehmensstrategie und -ziele unterstützt. („Leadership and organizational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategy and objectives“; vgl. [ITGI03], S. 11).

Ein übergeordnetes Ziel der IT-Governance wird darin gesehen, dass in der Unternehmensführung die Etablierung und das „Wirken“ einer IT-Organisation eine hohe strategische Bedeutung zugeordnet wird. So soll sichergestellt werden, dass das Unternehmen sowohl Innovationen bzw. Investitionen tätigen kann als auch seinen laufenden Betrieb erfolgreich aufrechterhalten kann. Dazu muss es sich vergewissern, dass es seine benötigten Strategien implementieren und seine Aktivitäten in der Zukunft ausbauen kann. IT-Governance-Praktiken zielen darauf ab, dass die Erwartungen an die IT erfüllt werden, die IT-Leistung gemessen wird und seine Ressourcen gemanagt sowie die Risiken berücksichtigt und abgesichert werden. Um dies zu gewährleisten, sollte vor allem ein ausreichender Einbezug der Stakeholder des Unternehmens erfolgen.

Nachfolgende Ziele stehen bei einer Verankerung von IT-Governance im Zentrum der Überlegungen:

- Ausrichtung des Einsatzes der Informationstechnologie an der Geschäftsarchitektur der Unternehmung
- Verantwortungsvoller und zielorientierter Einsatz der IT-Ressourcen
- Management der mit dem IT-Einsatz in Verbindung stehenden Risiken (Systemrisiken, Projektrisiken, CyberSecurity-Risiken)

- Unterstützung der (Geschäfts-)Prozesse durch Erkennen sowie Ausnützen (neuer) Möglichkeiten und Einsatz der optimalen Technologien und Ressourcen
- Performance Measurement (Kennzahlen zur Unternehmenssteuerung/KPIs)

Bezüglich der Einordnung von IT-Governance ist ergänzend die ISO/IEC-Norm relevant. Der Standard ISO/IEC 3850 mit dem Namen „Corporate Governance in Information Technology" richtet sich als Referenzmodell vor allem an die obere Führungsebene und an die Entscheidungsträger. Diese müssen ihre Verantwortung für eine effektive, effiziente und rechtskonforme Nutzung der IT wahrnehmen. Zentrale Bedeutung haben dabei die systematische Bewertung des IT-Einsatzes (mittels Assessments) sowie die ständige Überwachung der Umsetzung strategischer und taktischer Planungsüberlegungen.

Hinweis:

In der ISO/IEC-Norm 38500 findet sich statt des IT-Governance-Begriffs die Bezeichnung „governance of IT" ([ISO15], S. 2). Dabei wird letztlich auf die Governance der Unternehmens-IT fokussiert. Verstanden wird darunter ein System, durch das die aktuelle und künftige Nutzung der Unternehmens-IT professionell geplant und gesteuert werden kann.

Bild 1.1 zeigt einen Bezugsrahmen, der die Einordnung der verschiedenen Ansprüche an eine Governance-Struktur im Zusammenspiel von Corporate und IT-Governance verdeutlichen soll. Während „die Corporate Governance (…) das Unbehagen der Aktionäre, den Umgang mit den von ihnen bereitgestellten Finanzmitteln (…) abbauen soll, geht es bei der IT-Governance (…) um das Adressieren des Unbehagens beim Top-Management, wenn es um Kosten und Nutzen des Einsatzes von Informationstechnologie im Unternehmen geht" ([RüSG06], S. 4).

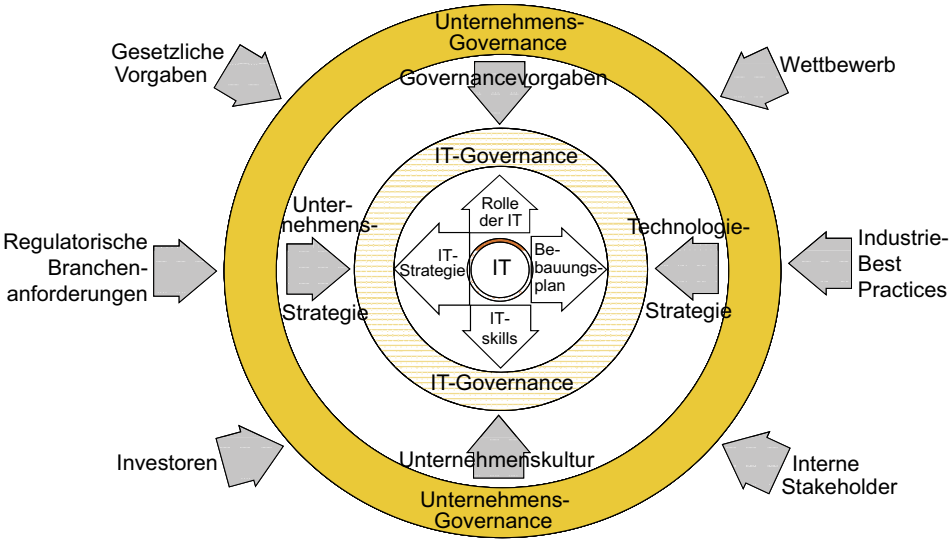

Bild 1.1 Bezugsrahmen für IT-Governance (nach [RÜSG06], S. 5)

Neuorientierungen zur IT-Governance haben im Kontext von Corporate Governance zum Ziel, flexibel Strukturen und Prozesse zu vereinbaren. Dabei gewinnen die Ziel- und Prozessorientierung der Unternehmenssteuerung für die IT (inklusive der Messung und des Controllings der Zielerreichung) eine zunehmende Relevanz. Darüber hinaus haben vor allem Themenkreise wie Risk- und Compliance-Management eine besondere Bedeutung erlangt.

Das Center for Information Systems Research (CISR) am Massachusetts Institute of Technology (MIT) stellt bezüglich der Definition von IT-Governance ergänzend die Entscheidungs- und Verantwortungsstruktur in Bezug auf die Nutzung von IT in den Mittelpunkt. Dabei werden vier Entscheidungsbereiche unterschieden: Grundsätze der IT-Nutzung, die IT-Infrastrukturstrategie, die IT-Architektur in Form von Standards und Richtlinien (für Technologie, Datenverwendung, Anwendungsdesign und Change-Management-Prozesse) sowie Entscheidungen über IT-Investitionen und die damit verbundenen Verfahren zur Generierung und Auswahl von IT-Projekten (vgl. [WeWo02], S. 2 f.).

Merke:

Mittels IT-Governance soll erreicht werden, dass die Chancen und Risiken der IT durch eine zentrale unternehmensweise IT-Planung und IT-Steuerung aktiv gemanagt werden. Ursprünglich war die IT vielfach von Fachbereichsinitiativen getrieben. Sie reagierte mehr, anstatt strategisch auf der Basis von Business-IT-Aligment-Initiativen zu agieren. Ein aktives Business IT-Management, gesteuert durch etablierte Enterprise IT-Governance, ermöglicht es der IT-Organisation, das Erreichen der Unternehmensziele nachhaltig zu unterstützen. Damit erlangt die IT eine wachsende Bedeutung. IT-Governance kann so einen Beitrag zu einer wertorientierten Unternehmensführung leisten (vgl. [Jo07], S. 32 f.).

1.1.3 Enterprise IT-Governance – Management und Governance der IT

Als ein erweiterter Fokus für die IT-Governance kann die Betonung der Aufgabenausrichtung auf die gesamte Unternehmenssicht gesehen werden. So findet sich folgende Begriffseinordnung bei De Haes und van Grembergen: „Enterprise Governance of IT (kurz EGIT) is an integral part of corporate governance, exercised by the Board, overseeing the definition and implementation of processes, structures and relational mechanism in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled business investments.“ ([DeH15], De Haes/van Grembergen 2015)

Die Definition zeigt die Weiterentwicklung im Hinblick auf die vielfältigen Herausforderungen eines Risiko- und Ressourcenmanagements sowie die entsprechende Steuerung durch Monitoring- und Performancemanagement-Lösungen. In besonderer Weise wird auf das Zusammenspiel von IT- und Fachbereich Wert gelegt. Darüber hinaus wird die strategische Ausrichtung am Business betont, wobei eine Unterstützung von Unternehmenszielen und -strategien durch die IT erfolgt. So wird letztlich der Wertbeitrag der IT (zum Business Value) in den Mittelpunkt der Ausrichtung von Enterprise IT-Governance gestellt.

Die erstmals im Jahr 2008 publizierte Norm „ISO/IEC 38500:2008 Corporate governance of information technology“ nimmt bezüglich der Aufgabenorganisation eine „Unterscheidung zwischen Governance und Management“ vor. Der wesentliche Beweggrund für diese Unterscheidung geht darauf zurück, dass beide Disziplinen „mit unterschiedlichen Arten von Aktivitäten verbunden“ sind, unterschiedliche Organisationsstrukturen erfordern und unterschiedlichen Zwecken dienen ([ISACA12a], S. 16).

Auch das dominierende Framework COBIT® geht von der Unterscheidung in IT-Governance- und Managementprozessen aus. Dabei bestehen die Governance-Prozesse im Wesentlichen „aus Praktiken und Aktivitäten, die darauf ausgelegt sind, strategische Optionen zu evaluieren, die IT-Richtung vorzugeben (also die IT zu steuern) und Ergebnisse zu überwachen“ ([ISACA12b], S. 25). Für die Benennung der Governance-Domäne bzw. der zugehörigen IT-Governance-Zielsetzungen werden dabei die drei Begriffe „Evaluate, Direct, Monitor“ (abgekürzt „EDM“) verwendet.

Zu beachten ist, dass die aktuelle COBIT®-Version, COBIT® 2019, diesen Ansatz konsequent fortführt. So wird bezüglich der Einführung von Governance-Systemen eine klare Unterscheidung zwischen Governance- und Management-Strukturen und Aktivitäten angeregt (vgl. [ISACA20], S. 17). Darüber hinaus werden zusätzliche Implementations-Guidelines formuliert, um auf der Basis von Good Practices eine erfolgreiche Umsetzung der beschriebenen Prozesse in die Unternehmenspraxis zu ermöglichen.

Hinweis:

Mit den neuesten Versionen von COBIT werden den Anwendern sog „Good Practices“ zur Verfügung gestellt. Damit kann dann eine Governance der Enterprise IT umgesetzt werden, indem ein umfassender und strukturierter „Implementation Guide“ bereitgestellt wird. Er soll als Grundlage für eine individuelle Einführungsplanung dienen, wobei eine Orientierung auf der Basis eines kontinuierlichen Verbesserungszyklus erfolgt. Eine ausführlichere Darstellung zu COBIT findet sich in Kapitel 2 dieser Publikation!

1.2 Einführung und Wertbeitrag von Enterprise IT-Governance

Um unternehmensweit eine wirtschaftliche, hocheffiziente IT zu gewährleisten, die den Anforderungen der Kunden (Fachabteilungen bzw. Fachbereiche des Unternehmens, Niederlassungen/Werke bzw. Auslandsgesellschaften) in hohem Maße gerecht wird, sind eine strategische IT-Planung, ein ganzheitliches Planen und Managen der Enterprise-Architektur, eine Harmonisierung der Kunden- und IT-Anforderungen (Relationship-Management) sowie eine zentrale Portfolioplanung und steuerung (etwa Portfolios zu Projekten, Applikationen, Technologien oder Services) unverzichtbar. Dies kann nur durch klare Enterprise

IT-Governance-Strukturen und Prozesse gewährleistet werden, so eine Kernthese, die vielfach durch die Praxis gestützt wird.

Eine optimale Ausrichtung der IT-Organisation für das Gesamtunternehmen kann nur dann gelingen, wenn sowohl die Planung als auch die Steuerung der IT-Angebote (Applikationen, Systeme bzw. der IT-Services) einer ganzheitlichen Betrachtung unterliegen und eine angemessene Entscheidungszentralisation verankert wird. Dazu kann eine entsprechende Ausgestaltung des strategischen Handlungsfelds „Enterprise IT-Governance" einen Beitrag leisten. (vgl. zu den folgenden Ausführungen auch [BeTi20], S. 759 ff.)

Um diese Ausgestaltung zu ermöglichen, wird die Entwicklung eines unternehmensspezifischen Frameworks für die Enterprise IT-Governance empfohlen. Dieses kann den Entscheidungsträgern aus Business und IT die hohe strategische Bedeutung, die der IT zukommt, bewusstmachen und eine nachhaltige Umsetzung ermöglichen. So lässt sich durch die Anwendung eines solchen Frameworks sicherstellen, dass das Unternehmen seine Aktivitäten aufrechterhalten und Strategien für zukünftige Aktivitäten implementieren kann. Es bietet Gewährleistung, dass Erwartungen der Business-Organisation an die IT erfüllt werden, wobei gleichzeitig Chancen und IT-Risiken beachtet werden (vgl. auch [ITGI03], S. 51).

Bild 1.2 zeigt eine Einordnung der strategischen IT-Planungsaufgaben sowie der strategischen IT-Steuerung im Kontext eines Enterprise IT-Governance-Frameworks.

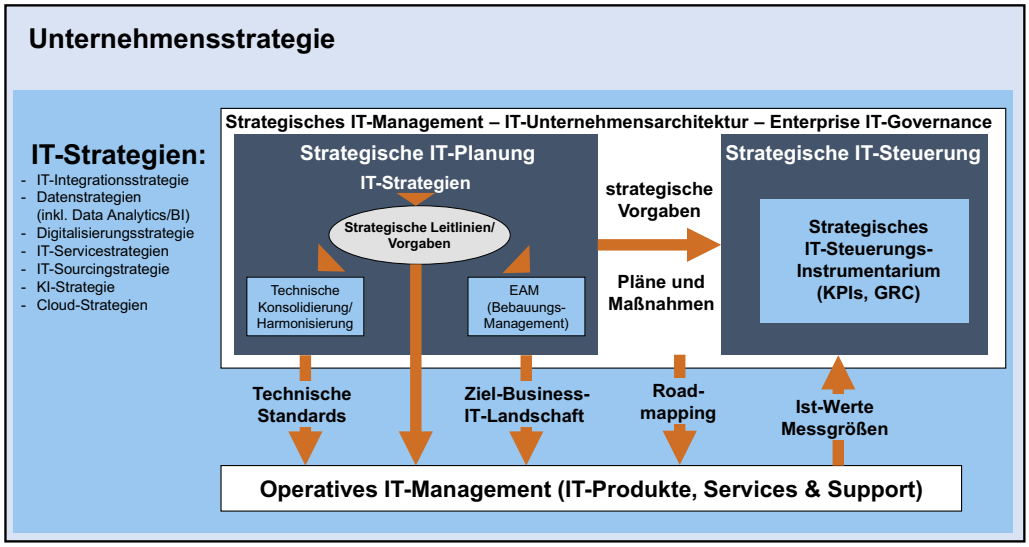

Bild 1.2 Strategische IT-Planung und Enterprise IT-Governance (strategische IT-Steuerung) im Zusammenhang

Hinweis:

Mit einem unternehmensindividuellen Framework für die Enterprise IT-Governance wird die Basis für die Einführung und Umsetzung von IT-Governance im Unternehmenskontext gelegt. Durch die Anwendung des Frameworks werden klare Verantwortlichkeiten und Ziele zur Enterprise IT-Governance definiert. Dabei werden alle involvierten Unternehmensbereiche sowie Stakeholder miteinbezogen.

1.2.1 Zielsetzungen und Handlungsprinzipien von Enterprise IT-Governance

Die Gründe für einen verstärkten Wunsch nach unternehmensweiter IT-Planung und zentraler IT-Steuerung stehen in engem Zusammenhang mit innovativen technologischen und geschäftsbezogenen Notwendigkeiten. Diese Herausforderungen können nur durch klare IT-Governance-Strukturen, die unternehmensweites Handeln ermöglichen, sowie durch darauf abgestimmte Verfahren und Prozesse erfolgreich gemeistert werden. Unternehmensführung und IT-Management sollten in Zusammenarbeit mit den entsprechenden Fachbereichen und den Projekt- sowie Budgetverantwortlichen ein Sollkonzept für die Enterprise IT-Governance formulieren und dabei auch die Handlungsfelder einordnen und vereinbaren. Ein integraler Bestandteil von Enterprise IT-Governance ist dabei die Etablierung von Rahmenbedingungen zur Ermöglichung der kontinuierlichen Verbesserung des Konzepts. Exemplarisch einige Beispiele für derartige Rahmenbedingungen:

- Einrichtung und Weiterentwicklung zweckmäßiger und funktionsbezogener Planungs- und Kontrollsysteme
- Zentrale Steuerung der IT-Ausgaben und -Aufwendungen (IT-Investitionsportfolios inkl. Budgetierungen für den IT-Bereich)
- Klare, marktoffene Auftragnehmer-/Auftraggeber-Beziehung zwischen den Fachbereichen und der IT-Organisation
- Entscheidungsfindung auf Basis eines einheitlichen, verpflichtenden Business-Case-Formats (Kosten-, Nutzen- und Risikobetrachtung) mit anschließendem Nutzeninkasso (Prüfung und Kontrolle des Business Cases)

Neben den Rahmenbedingungen ist vor allem auch der Scope für die Enterprise IT-Governance zu fixieren. Enterprise IT-Governance soll demnach sicherstellen, dass die Umsetzung der IT-Strategie im Sinne der Verantwortungsträger – also der Unternehmensführung – erfolgt. Folgende Anforderungen und Zielsetzungen werden als wesentlich erachtet:

- Enterprise IT-Governance soll die Sicherheit (Integrität, Verfügbarkeit, Vertraulichkeit) und Verlässlichkeit (Einhaltung externer Anforderungen) der Informationen bzw. der IT-Systeme sicherstellen.
- Es soll ein effizienter Einsatz der IT-Ressourcen bei gleichzeitiger Ausrichtung der IT auf die Unternehmensziele hergestellt werden (IT-Strategie als integraler Bestandteil der Business-Strategie eines Unternehmens).
- Durch die Schaffung von Transparenz etwa die strategische und betriebswirtschaftliche Bewertung von Portfolios (z. B. IT-Projekten unter Berücksichtigung von Aspekten des Risikomanagements) – soll auch ein Beitrag zur Kostensenkung und Leistungssteigerung im Bereich der IT geleistet werden.
- Durch klare, revisionssichere Strukturierung der IT-Organisation, Prozesse und Projekte nach allgemeinen Standards (z. B. ITIL, COBIT) wird ein Beitrag zur optimalen IT-Organisation geschaffen.
- Es kann die Erfüllung gesetzlicher Vorgaben (z. B. Ableitung von Sicherheitsanforderungen aus der IT-Risikoanalyse) gewährleistet werden.