



## **IT-Management und IT-Governance im Überblick und als synergetische Konstruktion**

188.249, Projektpraktikum im betrieblichen Umfeld  
(mit Bakkalaureatsarbeit)  
Semester SS06

eingereicht bei o. Univ.-Prof. Mag. Dipl.-Ing. Dr. Gerti Kappel  
Ko-Betreuung: Mag. Jimmy Heschl (KPMG)

Paul-Daniel Gruber  
8871331

Wien, 23. September 2007

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b> .....	<b>2</b>
<b>2</b>	<b>IT-Management</b> .....	<b>5</b>
2.1	Einleitung .....	5
2.1.1	Erläuterung des Begriffs „Management“ .....	5
2.1.2	Erläuterung des Begriffs „Business Service Management“ .....	7
2.2	Definitionen und Interpretationen .....	7
2.3	Gründe für IT-Management .....	9
2.4	Teilbereiche .....	10
2.5	Ziele .....	12
2.6	Treiber .....	15
2.6.1	IT-Management nahe Treiber .....	15
2.6.2	Periphere Treiber .....	17
2.7	Prozesse .....	18
2.8	Rollen und Verantwortlichkeiten .....	21
<b>3</b>	<b>IT-Governance</b> .....	<b>25</b>
3.1	Einleitung .....	25
3.1.1	Erläuterung des Begriffs „Governance“ .....	25
3.1.2	Erläuterung des Begriffs „Corporate Governance“ .....	27
3.1.3	Erläuterung des Begriffs „Internes Kontrollsystem“ .....	29
3.2	Definitionen und Interpretationen .....	29
3.3	Gründe für IT-Governance .....	31
3.4	Ziele .....	32
3.5	Treiber .....	33
3.5.1	Nicht-IT-Governance spezifische Frameworks und Anleitungen .....	34
3.5.2	IT-Governance spezifische Frameworks und Anleitungen .....	36
3.5.3	Gesetzliche Rahmenwerke .....	37
3.6	Domänen .....	38
3.7	Prozesse .....	40
3.8	Rollen und Verantwortlichkeiten .....	43
<b>4</b>	<b>Vergleich von IT-Management und IT-Governance</b> .....	<b>51</b>
4.1	Unterschiede .....	51
4.2	Synergien .....	57
<b>5</b>	<b>Zusammenfassung</b> .....	<b>61</b>

Abbildungsverzeichnis .....	63
Tabellenverzeichnis.....	64
Quellenverzeichnis .....	65
Literatur .....	65
Onlinequellen (Webseiten) .....	68
Präsentationen / Vorträge / Veranstaltungen .....	71

## Kurzfassung

Nach wie vor sehen sich Unternehmen mit hohen IT-Kosten konfrontiert, weswegen die IT den Ruf eines Kostentreibers noch nicht ablegen konnte. Oft mangelt es der IT auch an Steuerungskraft aufgrund inadäquater Prozesse und strukturellen Gegebenheiten. Ein weiteres noch immer weitverbreitetes Problem stellt die mangelnde Unterstützung informationstechnischer Lösungen durch das Top-Management dar, welcher Umstand mit fehlendem Know-How und einer geringen personellen Verankerung der IT zu erklären ist. Gesetze verlangen aufgrund vergangener Ereignisse immer mehr Kontrolle bzw. Nachvollziehbarkeit von Prozessen und Aktionen.

All diese Probleme und andere nicht genannte führen dazu, dass der IT oft nicht genügend Aufmerksamkeit geschenkt wird. Dies hat zur Folge, dass technologische Möglichkeiten nicht vollkommen ausgeschöpft werden, IT Lösungen teuer produziert und betrieben werden, der Nutzen unter den Erwartungen und damit die Akzeptanz gering bleibt. Zustände wie diese haben nicht nur Auswirkungen auf Unternehmen, sondern auch auf Kunden und damit die Gesellschaft.

Einen adäquaten Umgang mit Möglichkeiten und Schwierigkeiten ermöglicht ein angemessen konzipiertes und durchgeführtes IT-Management und IT-Governance. Wichtig ist hierbei Unterschiede und Schnittstellen zu erkennen und IT-Management sowie IT-Governance zu einem synergetischen Gebilde zu formen. Ein wesentliches Ziel ist daher dieses Gebilde im gesamten Unternehmen zu integrieren. Dabei helfen Frameworks und Empfehlungen, weswegen es von großem Vorteil ist, diese zu kennen und zu nutzen.

IT-Management und IT-Governance sind nicht als Religion zu betrachten. Sie ermöglichen hohe Ansprüche an die Informationstechnologie zu erfüllen und sind in einer Zeit immer komplexer werdender Lösungen unabdingbar. Ein gut verankertes IT-Management und IT-Governance hilft die IT nicht nur effizienter, sondern auch effektiver zu gestalten und ihren innewohnenden Wert zu aktivieren.

# Kapitel 1

## **Einleitung**

Die Gesellschaftsformen haben sich schon viele Male gewandelt. Die allgemein bekannteste Entwicklung ist die von der Agrar- zur Industriegesellschaft und von der Industrie- zur Dienstleistungsgesellschaft. Seit kurzer Zeit vollzieht sich der Wandel zur Informations- und Wissensgesellschaft, in welcher der Wert von (guter) Information bzw. von (gutem) Wissen allgemein erkannt wird und die Informationen bzw. das Wissen auf breiter Basis zugänglich gemacht werden kann. Dieser Wandel wurde maßgeblich durch die Entwicklung der IT gestützt und nun intensivieren sich diese beiden Entwicklungen gegenseitig.

Damit hat sich auch der Fokus auf unterschiedliche Begrifflichkeiten geändert. Eine Fokusverschiebung nach [Katz06] ist Tabelle 1.1 zu entnehmen.

Vokabular und Denkweise der Vergangenheit	Vokabular und Denkweise der Zukunft	Vokabular und Denkweise der Vergangenheit	Vokabular und Denkweise der Zukunft
Materie	Entropie	Energie	dissipative Systeme
Raum, Zeit	Evolution	Ordnung	Chaos
Mechanik	Selbstorganisation	Linearität	Nichtlinearität
eindimensional	Mehrdimensional	Deterministisch	stochastisch
Gleichgewicht	Fern vom Gleichgewicht	Daten	Informationen
kompliziert	Komplexität (oder einfach komplex)	stetig	diskontinuierlich
diskret	kontinuierlich	geschlossen	offen
technisch	sozio-technisch	Hierarchie	Netzwerke
künstlich	natürlich	allopoietisch	autopoietisch
autoritär	situativ	zentralisiert	dezentralisiert
Starrheit	Flexibilität	kleine Kontrollspannen	große Kontrollspannen
hohe Regelungsdichte	niedrige Regelungsdichte	Misstrauensorganisation	Vertrauensorganisation
triviale Maschinen	nicht-triviale Maschinen	Bürokratie	Kreativität
Taylorismus	Prozessdenken	gerichtete Information	Kommunikation
Organigramme	flexible Teams	Prognose	Alternativensuche
Planwirtschaft	Marktwirtschaft	Economies of Scale	Economies of Speed
Belehrung	Moderation	Machbarkeit	Gestaltbarkeit
Führermentalität	Demokratie	Beseitigung von Widersprüchen	Bewahrung von Widersprüchen
Statik	Dynamik	Know-How	Learn-How

Tabelle 1.1: Vokabular der Vergangenheit und Zukunft [Katz06]

Die IT selbst hat eine vielfältige Wandlung bzw. Weiterentwicklung durchlaufen, wie sie in groben Schritten in Abbildung 1.1 zu erkennen ist.

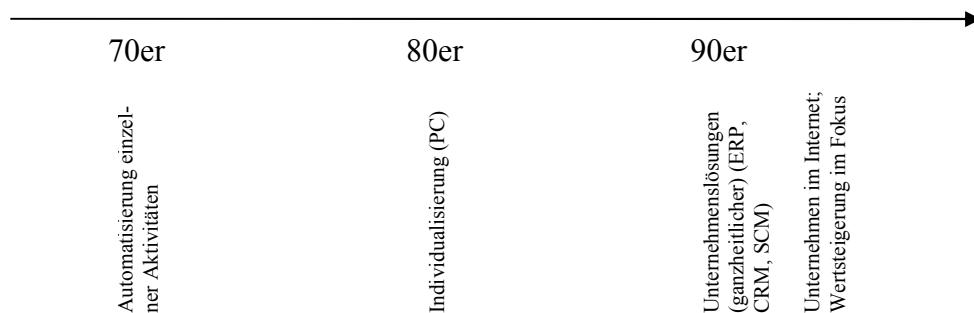


Abbildung 1.1: Geschichte der IT (basierend auf [Buch05])

Es ist nicht allzulange her und in manchen Institutionen noch immer zu beobachten, dass Probleme zwischen der IT und dem Business herrschen. Sprachliche Probleme bzw. für die jeweils andere Seite schwer nachvollziehbare Begrifflichkeiten (vgl. [Rüte06], [Buch05]) und Fehlen einer ganzheitlichen an der Unternehmensstrategie ausgerichteten IT-Strategie sind nur zwei der Vielzahl an Unstimmigkeiten. Diese führten weiters zu geringer Akzeptanz und dem Bild der IT als notwendiges Übel und auch des Kostentreibers, da der Nutzen als nicht kalkulierbar galt [Buch05]. Bestenfalls wurde die IT als reines Rationalisierungsinstrument betrachtet [Tiem06].

Heute wird die IT auch als „Enabler“ bzw. Werttreiber gesehen und man versucht ihren Wertbeitrag zu steigern. (s. Abb. 1.2)

Es sei angemerkt, dass in [Goek06] der zum Begriff „Enabler“ äquivalente Begriff „Value Center“ genannt wird (vgl. auch [Buch05], [Tiem06]).

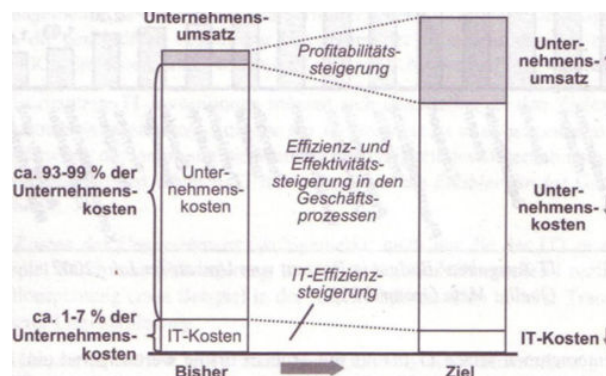


Abbildung 1.2: Wertbeitrag der IT [Buch05]

Die Forderung der Ausrichtung der IT am Business ist keine Neuerung, jedoch wurde und wird sie nicht überall forciert [Goek06].

Um eine Wertsteigerung voranzutreiben, ist es notwendig die künstliche Hülle der IT transparent zu gestalten, um diese gezielt steuern zu können. Proaktiv statt ausschließlich reaktiv gilt hier das Credo.

Zur gezielten Steuerung der IT benötigt man adäquate Mechanismen, die in Kombination eine Ausrichtung am Business und eine Wertsteigerung sicherstellen (können). An dieser Stelle setzen IT-Management und IT-Governance an, welchen sich diese Arbeit in den nächsten Kapiteln widmen wird.

Es sei noch angemerkt, dass für das Wort „Kunde“ nicht nur der externe Kunde gemeint ist. Auch interne Abteilungen können Kunden sein, welche intern hergestellte Produkte oder intern erbrachte Dienstleistungen in Anspruch nehmen.

In dieser Arbeit bezeichnet der Begriff „Unternehmen“ auch andere Institutionen wie beispielsweise öffentliche Rechtsträger.

## Kapitel 2

# IT-Management

In diesem Kapitel wird zu allererst eine Einleitung in die Materie „IT-Management“ geboten. Darauf folgen Definitionen, um die Sicht auf das IT-Management zu schärfen. Nach unterschiedlichen Begründungen für IT-Management werden die Teilbereiche und Ziele erläutert. Unterschiedliche Treiber aus der Praxis, welche IT-Management noch greifbarer gestalten, werden anschließend präsentiert, bevor verschiedene Prozesse, sowie Rollen und Verantwortlichkeiten dargelegt werden.

### 2.1 Einleitung

Um den/die LeserIn durch kleinere verständliche Schritte an IT-Management heranzuführen, wird die Brücke über „Management“ und „Business Service Management“ geschlagen.

#### 2.1.1 Erläuterung des Begriffs „Management“

„Management“ ist sowohl früher wie heute ein schillernder Begriff, der jedoch oft unterschiedlich interpretiert wird. Gerade aufgrund seiner schillernden Eigenschaft, wird heute nahezu keine Gelegenheit ausgelassen etwas mit diesem Begriff oder verwandter Begrifflichkeiten zu schmücken, was sich in der gesteigerten Verwendung und sprießenden MBA-Lehrgängen mit wahrscheinlich sehr unterschiedlicher Qualität widerspiegelt. Ohne den ehrenwerten Beruf eines Hauswarts zu schmälern, wird ein Facility Manager wohl nicht glücklich sein, sollten seine Tätigkeiten mit jenen eines Hauswarts gleichgesetzt werden, wie dies immer wieder der Fall ist. Um ein klareres Bild des Begriffs „Management“ zu erlangen, folgen aus diesem Grund Definitionen und Interpretationen.



[Thom02]. „Management“ wird in [Thom02] als „Gestaltungs- und Steuerungsfunktion“ beschrieben. „Oft werden [...] unter dem Begriff Management sämtliche Führungsaufgaben verstanden, während mit Führung nur die Mitarbeiterführung gemeint ist.“

[Stein05], [Koon55]. [Stein05] unterscheidet im Begreifen des Begriffs Management zwischen der institutionellen und der funktionalen Perspektive. Die institutionelle Perspektive versteht unter „Management“ „Personen, die in einer Organisation mit Anweisungsbefugnissen betraut“ sind. Im Gegensatz zum deutschsprachigen Raum, ist der Begriff „Management“ jedoch weitaus breiter gefasst als nur auf die oberen Führungsebenen bezogen. Die funktionale Perspektive wendet sich in der Erklärung des Begriffs „Management“ den Aufgaben zu, „die zur Steuerung des Leistungsprozesses erfüllt werden müssen.“ Bei diesen Aufgaben handelt es sich um Managementfunktionen, welche nach [Koon55] in Planung, Organisation, Personaleinsatz, Führung und Kontrolle unterteilt und zu einem Managementprozess geformt werden.

[Wojd05]. Als zentrale Managementaufgaben werden in [Wojd05] „Informieren“, „Probleme erkennen“, „Ziele vereinbaren“, „Delegieren“, „Koordinieren“, „Organisieren“, „Kontrollieren“, „Planen“, „Entscheiden“, „Mitarbeiter auswählen, beurteilen, fördern“ genannt.

[Rüeg02]. „Management“ wird gemäß dem St. Galler Management-Konzept (vgl. auch [Wojd05], [Thom02], [Tiem06]) in „normatives, strategisches und operatives Management“ unterteilt. Das normative Management befasst sich demnach mit der Unternehmensverfassung, der Umsetzung der Unternehmenspolitik in „Missionen“ und der Unternehmenskultur. Das strategische Management hingegen setzt bei den Organisationsstrukturen an, befasst sich mit Programmen und Problemverhalten, während das operative Management noch feingranulierter in seiner Betrachtung der Unternehmenswelt ist und sich daher organisatorischen Prozessen, Dispositionssystemen, Aufträgen und dem Leistungs- sowie Kooperationsverhalten widmet.

[Tiem06]. [Tiem06] fasst die Tätigkeiten und Prozesse „Entwicklung, Überwachung und Steuerung“ unter dem Begriff „Management“ zusammen.

Oft wird noch die taktische Ebene als Zwischenschritt von der strategischen zur operativen Ebene genannt.

Diese Interpretationen sollen die Grundlage des Verständnisses für weitere Ausführungen in dieser Arbeit bilden. Es ist zu erkennen, dass Führung gleichzeitig auch Management, aber nicht immer Management gleich Führung impliziert. Auch Herr Dr. Pramböck von MLP sprach bei seinem Vortrag „Karriereplanung für Wirtschaftsinformatiker“ am 23.05.2006 davon, dass die vielen zu ihm kommenden Stu-

denen ihm gegenüber äußern, sie wollen Manager/in werden. Er sieht in diesem Bestreben allerdings den Wunsch Führungskraft zu werden, was bestätigt, dass Management nicht gleich Führung bedeutet.

### 2.1.2 Erläuterung des Begriffs „Business Service Management“

„Business Service Management“ (BSM) ist ein noch recht junger Begriff. Er enthält ein Wort, das sich immer größerer Beliebtheit erfreut – das „Service“. „Service“ wird mit dem Wort „Dienstleistung“ assoziiert (vgl. Kapitel 1) und deutet einen Paradigmenwechsel an. Es verlangt die Ausrichtung am Kunden und betrachtet nicht das Produkt als Selbstzweck. Die Tage, an denen das Zitat „Sie bekommen das Auto in jeder Farbe – Hauptsache, sie ist schwarz“, welches Henry Ford<sup>1</sup> zugeschrieben wird, noch aktuell war, sind gezählt [Stuc04]. Der Begriff „Business“ in Kombination mit „Service“ sorgt für die Ausrichtung der Dienstleistungen (Services) am Kerngeschäft und damit an den Geschäftsprozessen des jeweiligen Unternehmens.

BSM ist nicht unbedingt ein Begriff, den man unmittelbar mit IT in Verbindung bringen würde. Tatsächlich besteht jedoch eine enge Verbindung zur IT, hat dort sogar seinen Ursprung.

Forrester Research definiert *BSM* wie folgt: „Business Service Management verbindet geschäftsfokussierte IT-Services dynamisch mit der darunter liegenden IT-Infrastruktur.“ Ein BSM-System zeichnet sich nach Forrester Research außerdem durch die Erfassung der Geschäftsprozesse, die Erfassung der Infrastrukturreourcen, die dynamische Verbindung von Prozessen und Infrastruktur und durch die Unterstützung eines End-To-End-Management durch Monitoring (Überwachung) und Reporting aus [CIO].

Durch die Adressierung von Geschäftsprozessen und IT-Services ist auch ein Konnex zwischen Geschäftsprozessmanagement und IT-Service-Management herzustellen, welches insbesondere ab Abschnitt 2.4 erläutert wird.

In diesem Kapitel werden verschiedene IT-Managementbereiche angeschnitten, wobei serviceorientiertes Management im Zentrum der Betrachtungen stehen wird.

## 2.2 Definitionen und Interpretationen

Eine allgemeine Definition für IT-Management ist nicht einfach zu finden. Dies mag vor allem darin begründet sein, dass IT-Management ein abstrakter Begriff ist, von dem sich eine Reihe konkreterer IT-Managementbereiche ableiten lassen. Im nächs-

---

<sup>1</sup> Gründer des Automobilherstellers Ford Motor Company.

ten Kapitel wird sich zeigen, dass IT-Governance schon etwas konkreter gefasst ist. Im Folgenden werden Möglichkeiten beschrieben, *IT-Management* zu definieren.

**1. Möglichkeit.** Eine Möglichkeit besteht darin, die bisher bekannten Definitionen von „Management“ für IT-Management zu adaptieren. Ein sehr allgemeiner Versuch wäre beispielsweise: „IT-Management bedeutet die Gesamtheit der IT, gegebenenfalls mit Elementen der Führungskomponente zu gestalten, den Betrieb der IT zu steuern, mit dem Ziel, die Geschäftsprozesse zu unterstützen und dem Kunden adäquate (Dienst)Leistungen zu bieten.“

**2. Möglichkeit.** Eine andere Möglichkeit ist, die Literatur nach Definitionen und Interpretationen zu durchforsten. [Tiem06] unterscheidet aufgrund der verschiedenen Management-Definitionen zwischen strategischem und operativem IT-Management. Dabei wird in dieser Quelle unter „strategisches IT-Management“ die Synchronisierung der Unternehmensziele mit der Informationssystem-Strategie, die Festlegung von IT-Zielen und Strategien für die operative Umsetzung in IT-Leistungsprozessen sowie Planung und Priorisierung von IT-Vorhaben verstanden. „Operatives Management“ kennzeichnet die wirtschaftliche Nutzung der IT-Ressourcen, die wirtschaftliche Durchführung von IT-Leistungsprozessen, die effektive Entwicklung von IT-Lösungen, den kontinuierlichen IT-Betrieb, als auch die Weiterentwicklung und Wartung der Informationssysteme. Die Steuerung geschieht durch Kennzahlen und Berichte. Dabei stehen die Wirksamkeit und insbesondere die Wirtschaftlichkeit im Vordergrund.

[Buch05] unterscheidet zwischen vier Reifegraden von IT-Management, dargestellt in Abbildung 2.1.

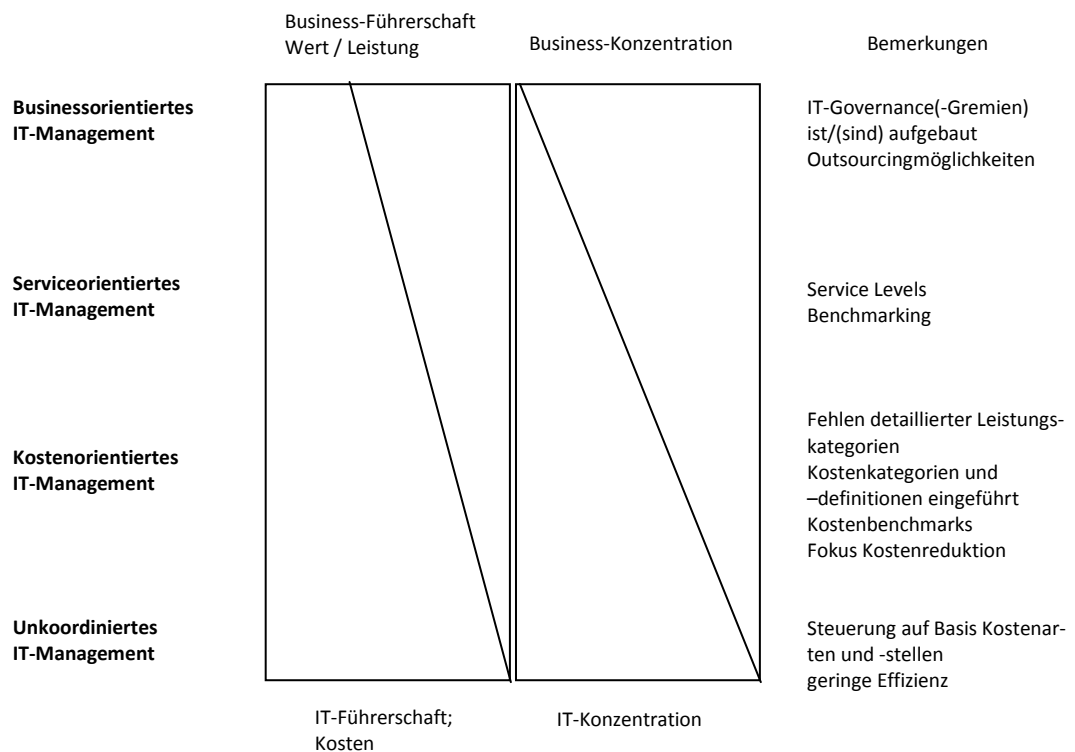


Abbildung 2.1: Reifegrade des IT-Managements (basierend auf [Buch05])

**3. Möglichkeit.** Diese Möglichkeit erfordert die Betrachtung der einzelnen IT-Managementbereiche. Grundsätzlich kann man den meisten Managementarten „IT-“ voranstellen, um den Fokus auf die IT zu lenken. Der/die LeserIn soll an dieser Stelle aber nicht mit diesem Gemeinplatz zurückgelassen werden, weshalb sich diese Arbeit in Abschnitt 2.4 den einzelnen Bereichen widmet. Definitionen der einzelnen Teilbereiche anzuführen und zu erläutern wäre Inhalt detaillierterer Arbeiten über IT-Management bzw. über die einzelnen IT-Managementbereiche.

## 2.3 Gründe für IT-Management

IT ohne Management derselben würde in ihrem Wesen einem Staat in Anarchie gleichen. Einige negative und wahrscheinliche Umstände aufgrund einer *anarchischen IT* sind:

- geringe Effektivität
- geringe Wirtschaftlichkeit
- geringer ROI
- Selbstzweck der IT
- geringe Kundenadressierung
- hohe Kosten (bei geringem Nut-
- inadäquate Kunden- und Lieferantenverträge
- unkoordinierter Support
- geringe Qualität
- „Optimierung“ maximal von feingranularen Tätigkeiten

- zen)
- hohe Time-to-Market
- geringe Flexibilität
- viele Einzellösungen, viele Medienbrüche
- Durchschaubarkeit eingeschränkt
- Datenfriedhöfe
- keine Fokussierung auf notwendige Daten
- veraltete Hard- und Software
- keine konsequente Absicherung von Risiken
- geringe Sicherheitsmaßnahmen
- schlechtes pro- und reaktives Handeln bei widrigen Umständen
- erhöhte Gefahr der vorsätzlichen und unbeabsichtigten Missachtung von Gesetzen und Regulativen
- euphorischer und zu rascher Einsatz von neuen Technologien, Instrumenten und Werkzeugen
- fehlen von effektiven Motivatoren (vgl. Herzberg in [Wojd05])
- fehlen von durchgängigen Prozessen und klaren Schnittstellen
- keine unternehmensweiten Lernprozesse
- geringe Wissensdurchdringung
- Fehlen der strategischen Komponente

## 2.4 Teilbereiche

Die von IT-Management adressierten Bereiche sind sehr vielfältig. [Tiem06] hebt besonders folgende *Bereiche*<sup>2</sup> hervor:

- IT-Servicemanagement
- IT-Architektur, IT-Infrastrukturmanagement
- IT-Sicherheitsmanagement
- IT-Qualitätsmanagement
- IT-Daten- und -Wissensmanagement
- IT-Applikationsentwicklung
- IT-Projektmanagement
- E-Business bzw. IT-Business-Management lt. [Goek07]
- IT-Controlling
- IT-Rechtsmanagement
- IT-Strategieentwicklung
- IT-Organisationsmanagement und -Führung

[Köhl06] erwähnt zusätzlich noch explizit das IT-Risikomanagement.

Weitere Teilbereiche, die sich über einige der oben genannten Teilbereiche erstrecken oder sich überschneiden, sind IT-Portfoliomanagement, welches sich von der IT-Strategie ableitet [Goek06], IT-Produktmanagement, IT-Anforderungsmanagement und IT-Ressourcen- bzw. -Assetmanagement.

---

<sup>2</sup> Manche Begriffe wurden zur einheitlichen Präsentation leicht abgeändert.

Diese Bereiche sind keineswegs separat zu betrachten, sondern überlagern und unterstützen einander gegenseitig.

*IT-Architektur* und *IT-Infrastrukturmanagement* liegen nahe beisammen [Tiem06], [Köhl06]. IT-Architektur konzentriert sich vor allem auf die einzelnen Architekturen wie Netzwerke, Hardware-Systeme, Applikationen sowie Daten und Informationen. Infrastrukturmanagement hingegen betrachtet insbesondere die Zusammenhänge.

*IT-Ressourcen-* bzw. *-Assetmanagement* ist etwas breiter gefasst als IT-Architektur und Infrastrukturmanagement. [ITGI03] zählt zu den Assets IT-Ressourcen, Humanressourcen, Daten und Wissen, Anwendungen, Facilities und Technologie.

*E-Business* verwendet elektronische Medien, um über das E-Procurement - also über die Beschaffung - in weiterer Folge über die Produktion, und letztendlich den E-Commerce - also den finanziellen Kontakt mit dem Kunden -, durch ein ganzheitliches E-Supply Chain Management, die Geschäftsprozesse zu unterstützen und die Kontakte mit den Stakeholdern auf adäquate Weise aufrecht zu erhalten. Das Customer Relationship Management befasst sich speziell mit den Kunden.

Im *IT-Controlling* liegt der Fokus auf der Kontrolle und Steuerung der IT durch Kennzahlen wie ROI, Komplexitätsgrad, Mitarbeiterqualifikation, Benutzerzufriedenheit, IT-Umsatz und IT-Kosten. Aber auch Werkzeuge wie IT-Prozessmanagement mit Prozessmodellierung kommen zum Einsatz [Tiem06].

*IT-Servicemanagement* kann wie in Abschnitt 2.1.2 indirekt erwähnt als Dach für die anderen IT-Management-Teilbereiche bzw. als einen die anderen IT-Management-Teilbereiche durchdringenden Begriff gesehen werden. Kernbereiche eines IT-Servicemanagements sind die Definition und Wartung von Dienstleistungen (Services), Verträgen und Vereinbarungen.

Später wird noch aus einem High-Level-View das Framework namens „IT Infrastructure Library“ (ITIL) präsentiert, welche einige der oben genannten Bereiche intensiver behandelt.

In Abbildung 2.2 sind nochmals Bereiche bzw. Aufgaben in einer Prozesssichtdarstellung nach [Goek06] zu erkennen.

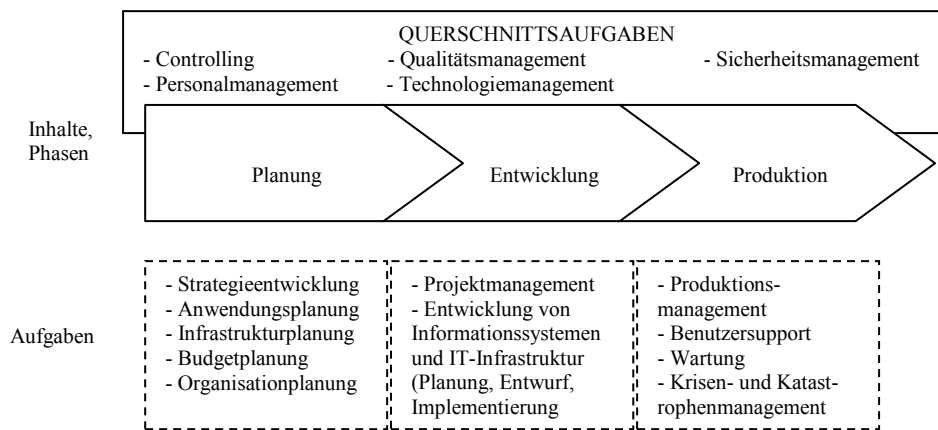


Abbildung 2.2: Aufgaben des IT-Managements (basierend auf [Goek06])

Abschließend sei noch zu erwähnen, dass die einzelnen IT-Management-Teilbereiche nicht in jedem Unternehmen gleich stark ausgeprägt sind oder sein müssen. Es können sogar IT-Managementbereiche ohne Nachteil für das Unternehmen fehlen. Nicht jedes Unternehmen benötigt beispielsweise „IT-Applikationsentwicklung“. Letztendlich entscheiden vor allem Nutzen und Kosten über die Ausprägung eines IT-Managementbereichs.

## 2.5 Ziele

Im Folgenden werden einige wesentliche (Teil-/Zwischen-/End-)Ziele nach IT-Managementteilbereich aufgelistet:

### IT-Servicemanagement

- Prozessorientierung
- Kundenorientierung (bei Lieferung und Support)
- Individualisierbarkeit der IT-Services und angepasste Service-/Operational-Level-Agreements (SLAs/OLAs)
- Angemessene Kosten der Services

### IT-Projekt- und –Programmmanagement

- Gute Koordination der Programme und der Projekte mit deren Tätigkeiten
- Gute Planung
- Projekte zum definierten Zeitpunkt, zur definierten Qualität mit vorgegebenen Budget<sup>3</sup> abschließen
- Schnelle Abwicklung

<sup>3</sup> Unter der Voraussetzung, dass das Budget optimal mit den Erfordernissen abgestimmt wurde und daher als realistisch angesehen werden kann.

### IT-Architektur und Infrastrukturmanagement

- Adäquate Anpassung der Architektur und Infrastruktur an technologische Entwicklungen und Optimierung
- Beherrschung der Schnittstellenkomplexität und Vereinfachung der Systemlandschaft
- Systemanpassung der IT-Architektur und IT-Infrastruktur

### IT-Ressourcen-/Assetmanagement

hierbei handelt es sich insbesondere um eine Mixtur aus IT-Architektur und Infrastruktur- sowie -Daten- und -Wissensmanagement.

### IT-Sicherheitsmanagement

- Gewährleistung von Integrität, Vertraulichkeit, Verfügbarkeit, Authentizität und nach [Kapp06] auch Anonymität
- Gestaltung von Sicherheitsrichtlinien, Prozessen, Organisationsstrukturen
- Sicherstellung eines organisationsweiten Sicherheitsbewusstseins

### E-Business

- Gutes E-Supply-Chain-Management
- (Elektronische) Unterstützung der Geschäftsprozesse und multilateralen Beziehungen zwischen Stakeholdern

### IT-Anforderungsmanagement

- Adäquate Abstimmung von Kundenanforderungen mit Möglichkeiten zur Erfüllung der Anforderungen
- Schaffung eines für alle Seiten gleiches, konsistentes und verständliches Bild über die Anforderungen

### IT-Controlling

- Steigerung der Effizienz und Effektivität der IT
- Senkung der Kosten

### IT-Prozessmanagement

- Kürzere Durchlaufzeiten
- Einfachere Prozesse
- Durchgängige, ganzheitliche Prozesse

### IT-Rechtsmanagement

- Rechtliche Sicherheit
- Gute Compliance

### IT-Strategieentwicklung

- Gut auf das Umfeld abgestimmte IT-Strategie
- Flexibilität, Effektivität, Wirtschaftlichkeit, Qualität der Applikationen, Daten, Technologie, Sicherheit, Prozesse, Organisation, Abwägung der Stärken, Abbau der Schwächen, Nutzen von Chancen, bekämpfen von Risiken



**IT-Qualitätsmanagement**

- Dokumentation
- Überwachung, Messung und kontinuierliche Verbesserung von Ressourcen, Daten, Prozessen, Produkten/Dienstleistungen

**IT-Daten- und –Wissensmanagement**

- Verfügbarkeit von relevanten Daten in der richtigen Qualität, zur richtigen Zeit, am richtigen Ort
- Organisationsweites Lernen

**IT-Applikationsentwicklung**

- Technologisch ausgereifte Applikationen mit hohem Nutzen
- Kurze Entwicklungszeiten
- Angemessene Portabilität und Skalierbarkeit
- Gute Koordination der Beteiligten

**IT-Portfoliomanagement**

- Gute Auswahl an Projekten/Tätigkeiten/etc. gemäß unterschiedlichen Dimensionen wie strategische Bedeutung, Risiko, Nutzen und Kosten, Notwendigkeit

**IT-Risikomanagement**

- Angemessenes Risikoakzeptanz/Risikoabsicherungsverhältnis

**IT-Produktmanagement**

- Auf Kunden abgestimmte Gestaltung des Produkts

**IT-Organisationsmanagement und -Führung**

- Organisatorische Flexibilität
- Angemessene Kosten
- Motivierte Mitarbeiter
- Prozessunterstützende Organisation

Die oben angeführten Ziele der jeweiligen IT-Managementteilbereiche basieren auf [Fran05], [ISO05], [ITGI03], [Köhl06], [Tiem06], [Wojd05], [Wojd06], [Zuse04] und eigenen Überlegungen.

Bei allen oben genannten Bereichen ist die Ausrichtung am Geschäft das übergeordnete Ziel.

Weiters wird darauf hingewiesen, dass die Teilbereiche einen Querschnitt durch andere Teilbereiche bilden können, sich gegenseitig beeinflussen und unterstützen. Kurz gesagt ist eine systemische Sichtweise notwendig. Es wurde darauf geachtet, nur möglichst spezifische Ziele zu den einzelnen Teilbereichen zu nennen. Beispielsweise erfordert ein IT-Projektmanagement auch ein adäquates IT-Risiko- und -Qualitätsmanagement und hat somit auch entsprechende Ziele. E-Business erfordert manchmal eine IT-Applikationsentwicklung, beispielsweise um virtuelle Marktplätze zu schaffen oder Bezahlungssysteme zu entwickeln. In [Tiem06] wird IT-Portfoliomanagement als Werkzeug des IT-Controllings erachtet. Weiters hängen IT-

Sicherheitsmanagement und IT-Risikomanagement in manchen Bereichen stark zusammen.

## 2.6 Treiber

Es gibt unzählige Frameworks und Empfehlungen je IT-Managementteilbereich. Aus diesem Grund wird an dieser Stelle nur eine Auswahl an wesentlichen Treibern präsentiert.

Auch die hier genannten peripheren Treiber sind für IT-verwandte Themen aufgrund der Verwobenheit der IT mit anderen Unternehmensbereichen bzw. -prozessen relevant. Weiters können auch wesentliche Konzepte für IT-Management aus den nicht unmittelbar verwandten Themenbereichen extrahiert werden.

In Abbildung 2.3 sind nicht alle Zwischenschritte dargestellt. Jedenfalls ist eine der früheren Versionen und die zum Zeitpunkt der Verfassung dieser Arbeit aktuelle Version abgebildet. Diese Abbildung erhebt keinen Anspruch auf Vollständigkeit.

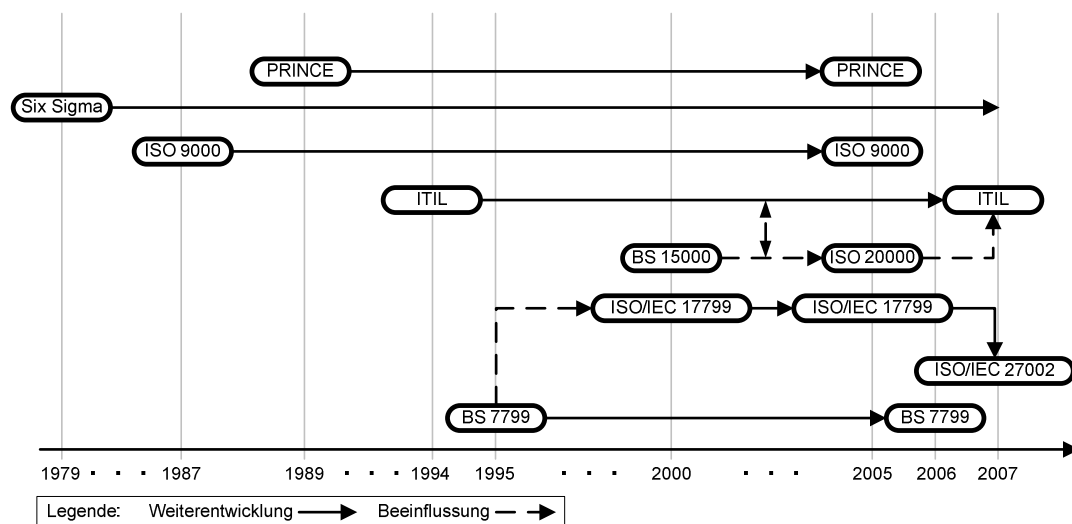


Abbildung 2.3: IT-Managementtreiber im Zeitablauf

### 2.6.1 IT-Management nahe Treiber

**ISO/IEC 17799 (Information Technology – Security Techniques – Code of Practice for Information Security Management).** ISO/IEC 17799 ist ein im Jahr 2000 von der „International Organization for Standardization“ und der „International Electrotechnical Commission“ herausgegebener internationaler Standard, welcher auf dem britischen Standard BS 7799 basiert, der im Jahr 1995 erstmals veröffentlicht wurde und von dem es schon eine Version des dritten Teils aus dem Jahr 2006 gibt. Von ISO/IEC 17799 ist jedoch schon eine neuere Version aus dem Jahr 2005

erhältlich. Im Jahr 2007 wurde vorgeschlagen, den Standard in die ISO/IEC 27 Familie mit der Nummer 27002 zu integrieren. Er adressiert insbesondere die taktische und operationelle Ebene der Informationssicherheit. Dabei behandelt er die Organisation derselben, Personalressourcen mit ihren Rollen und Verantwortlichkeiten, die physische und umgebungsbezogene Sicherheit, die Kommunikation, die Zugriffskontrolle, das Management von Applikationen, das Asset Management, die Kontinuität und mögliche Incidents. Auch die Compliance, die vor allem im nächsten Kapitel eine Rolle spielen wird, steht in der Betrachtung dieses Standards. Informationen von [Hesc07] zufolge ist dieser Standard jedoch obsolet bzw. wurde dieser vor in etwa zwei Monaten durch den oben erwähnten ISO/IEC 27002:2007 ersetzt und existiert somit nicht mehr [ISO05], [Rüte06], [Völk05].

**ISO/IEC 20000.** ISO/IEC 20000 ist ebenfalls ein internationaler Standard der „International Organization for Standardization“, der im Jahr 2005 basierend auf dem British Standard BS 15000 aus dem Jahr 2000 und ITIL v2 (lt. [Hesc07]) publiziert wurde. Bei diesem Standard handelt es sich um ein Werk über IT-Service-Management. Er ermöglicht qualitativ hochwertige IT-Serviceprozesse zu gestalten und diese zu bewerten [Köhl06].

**IT Infrastructure Library (ITIL).** ITIL ist ein IT-(Service-)Management-Framework, gehört zu den Public-Domain-Modellen und wurde in den Jahren 1989 bis 1994 von der „Central Computer and Telecommunications Agency“ (CCTA), einer Dienstleistungsorganisation der britischen Regierung, entwickelt. Frameworks, die zu den Public-Domain-Modellen gehören, sind frei zugänglich im Gegensatz zu den kommerziellen Varianten. Seit 2001 ist sie unter dem Namen „Office of Government Commerce“ bekannt und entwickelt ITIL weiter [Köhl06], [Fran05]. Mittlerweile gibt es schon die dritte Version, welche dieses Jahr (2007) erschienen ist. Sie soll eine noch stärkere Ausrichtung des IT-Service-Managements auf die Unternehmensstrategie ermöglichen. Vor allem wird die lt. [Hesc07] in ITIL v2 fehlende strategische Planung, Entwicklung und Überführung in den Betrieb adressiert. Eine Zertifizierung nach ITIL ist nur für Personen aber keine Organisationen möglich, da ITIL „nur“ ein „de facto Standard“ ist [ITIL1]. Es besteht aber die Möglichkeit die Organisation nach ISO/IEC 20000 zertifizieren zu lassen. [ITIL2]<sup>4</sup> erachtet ITIL als den am breitest anerkannten IT-Service-Management-Ansatz. ITIL konzentriert sich auf das „Was“ und nicht auf das „Wie“. Es gibt zu ITIL Version 2 jedoch ein Buch mit dem Titel „Planning to Implement IT Service Management“. ITIL liefert „Best-Practices“ und vereinigt einige Bereiche des IT-Managements, wobei das Herz das

---

<sup>4</sup> Office of Government Commerce

IT-Service-Management bildet. Die Prozesse werden in Abschnitt 2.7 noch etwas näher beleuchtet.

**CobiT.** Auch CobiT stellt einen wesentlichen Treiber für IT-Management dar. Da dieser jedoch in der durch den Autor studierten Literatur insbesondere im Rahmen von IT-Governance behandelt wurde, wird dieser erst im Kapitel betreffend IT-Governance im Abschnitt 3.5.2 näher erläutert. Weitere Ausführungen in dieser Arbeit werden den Unterschied insbesondere zu ITIL und seine Einordnung „zwischen“ IT-Management und IT-Governance verdeutlichen.

Es gibt noch viele weitere (mitunter in den Eckpunkten ähnliche) Ansätze für IT-(Service-)Management wie das KPMG Maturity Model, Microsoft Operations Framework und IT-Service-Management (ITSM) von HP [Tiem06].

### 2.6.2 Periphere Treiber

**ISO 9000.** Bei der im Jahr 1987 herausgebrachten und der derzeitigen, aus dem Jahr 2005 stammenden, veränderten und aktualisierten Version der ISO 9000 Familie handelt es sich nicht um einen IT-Management-spezifischen Standard. Es handelt sich hierbei um einen Qualitätsmanagementstandard. Er adressiert das Management von Ressourcen, das Management von Produkten, die Messung, Analyse und (kontinuierliche) Verbesserung, die Verantwortungen der Leitung, die Kunden und die Lieferanten. Auch hier ist eine Zertifizierung möglich, die regelmäßig erneuert werden muss, um längerfristig nach ISO 9000 zertifiziert zu sein. Trotz dem nicht spezifischen IT-Management-Bezug ist es möglich, diesen gewinnbringend für das IT-Management einzusetzen [ISO900], [Köhl06], [Fran05], [Golt06].

**Six Sigma.** Six Sigma hat seinen Ursprung bei Motorola im Jahr 1979. Bei Motorola und bei anderen Unternehmungen führte Six Sigma zu Erfolgen durch statistische Analysen über Geschäftsprozesse, durch Identifikation der Fehler und dem konsequenten Handeln zur Steigerung der Qualität. Es wird dabei das Paradigma „Plan, Do, Check, Act“ (PDCA) als qualitätssichernder Kreislauf angewendet. Wichtig ist hierbei vor allem das Messen und das Handeln danach, um aus den Analysen über Handlungen auch (positive) Wirkungen erzielen zu können [4Man], [Köhl06].

**Projects in Controlled Environments (PRINCE).** PRINCE wurde 1989 von der „Central Computer and Telecommunication Agency“ (CCTA) ins Leben gerufen und wird heute durch das „Office of Government Commerce“ weiterentwickelt. Seit 2005 gibt es die neue Version PRINCE 2. Es handelt sich hierbei um eine Projektmanagementmethode. PRINCE 2 erachtet die Organisation, die Planung und das Controlling eines Projekts als Komponenten des Erfolgs. Es unterstreicht weiters die

Bedeutung der Verarbeitung von Anforderungen, die Erstellung einer Dokumentation, der Definition von Rollen und die Beachtung von Risiken [Köhl06].

## 2.7 Prozesse

Die in Abschnitt 2.4 präsentierten Teilbereiche sind nicht als Funktionen gedacht, die von jeweils genau einer auf den jeweiligen IT-Management-Teilbereich spezialisierte Abteilung oder Person bekleidet werden. Sie sind als Prozesse zu sehen, die sich über mehrere organisatorische Einheiten erstrecken und auch innerhalb unterschiedlicher Tätigkeiten Fuß fassen.

Wie bei den Zielen der Teilbereiche und den Empfehlungen für die Teilbereiche gibt es klarerweise auch hier eine Unmenge an Prozessen, wenn man bedenkt, dass jeder Teilbereich sich in (Sub)prozesse aufspaltet. Es wird daher als sinnvoller erachtet, diesen Abschnitt dem allgemein anerkannten - in Abschnitt 2.6.1 angesprochenen - ITIL-Framework v2 in etwas detaillierterer Weise zu widmen, welches für IT-Management repräsentativ ist und sich durch seinen serviceorientierten Charakter auszeichnet. Aufgrund der Neuheit von ITIL v3 und der geringeren Anzahl an (guter) Literatur, bildet hier die Version 2 die Grundlage für weitere Erläuterungen. Die Basis des Verständnisses wird jedoch durch diesen Umstand nicht erschüttert.

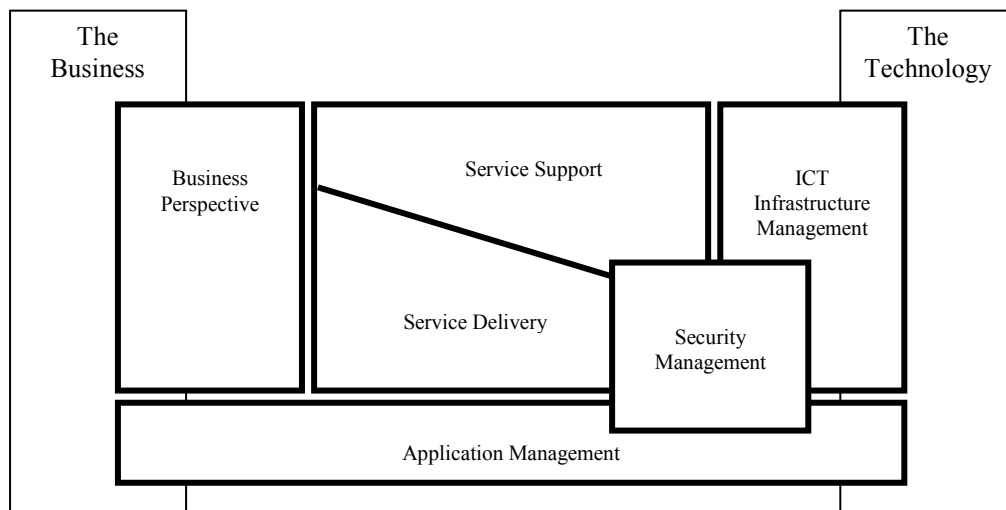


Abbildung 2.4: ITIL-Übersicht (basierend auf [ITIL1])

In Abbildung 2.4 sind sechs durch stärkere Umrahmungen gekennzeichnete Prozesse zu erkennen, welche bildlich wie auch inhaltlich die Brücke zwischen Geschäft und IT bilden sollen.

Der Servicemanagement-Prozess bildet das Herzstück von ITIL, welches eine serviceorientierte Ausrichtung ermöglicht. Er umfasst die zwei Subprozesse Service Delivery und Service Support.

*Service Delivery* besteht aus fünf Prozessen. Der IT-Service-Management-Prozess gestaltet insbesondere den Service Katalog, die Service-Level-Agreements (SLA) mit den Kunden und die Operational-Level-Agreements (OLA) sowie Underpinning Contracts mit den Lieferanten und liefert Service Level Reports. Bei OLAs handelt es sich um firmeninterne Lieferanten. „Underpinning Contracts“ stellen Verträge mit externen Lieferanten dar. Bei dem Capacity-Management-Prozess steht der Kapazitätsplan mit der Capacity Management Database im Vordergrund. Dabei werden auch Kostenvoraussagen, Grenzwerte und verschiedene Reports bezüglich Auslastung und Kapazität erstellt. Der Availability-Management-Prozess sorgt vor allem für adäquate Verfügbarkeit der Services mit ihren Komponenten, für Wartungspläne, Schwachstellenanalysen sowie Havarie- und Backup-Pläne. Die Vorbeugung von Risiken und die Erfüllung der Verfügbarkeitsanforderungen stehen demnach hier im Vordergrund. Der Continuity-Management-Prozess versucht mittels Continuity-Plänen, Havarietests, Kooperations- und Versicherungsverträgen die Risiken in Grenzen zu halten und die Aufrechterhaltung der Services bzw. Geschäftsprozesse sicherzustellen. Auch gilt die Devise „angemessenes proaktives Handeln ermöglicht adäquates reaktives Handeln“. Last but not least gibt es noch den Financial-Management-Prozess der stark an das in Abschnitt 2.4 erwähnte IT-Controlling erinnert, sich hier aber gemäß dem Namen auf die monetäre Komponente konzentriert. Durch Kostenstellen- und Kostenträgerpläne, Preislisten, Plan- und Budgetvorgaben, TCO- und ROI-Berechnungen, Berichte und Prognosen lässt sich die IT steuern und eine höhere Effizienz erzielen.

*Service-Support* umfasst ebenfalls fünf Prozesse. Sollten Störungen auftreten, so ist der erste anzustoßende Prozess der Incident-Management-Prozess. Mit diesem werden möglichst rasch Störungen behoben, Requests for Changes und Reports erstellt. Bei diesem Prozess steht das reaktive Handeln im Vordergrund. Beim Problem-Management-Prozess ist proaktives Handeln dagegen angebracht, um in Zukunft Störungen zu vermeiden. Dazu werden Lösungen gefunden, Requests for Changes getätigt und vorbeugende Maßnahmen gesetzt. Im Change-Management-Prozess werden Requests for Changes abgewogen und eventuell in die Tat umgesetzt. Der Release Management-Prozess ermöglicht dann das eigentliche Release. Wichtig dabei ist eine einwandfreie Dokumentation. Dem Configuration-Management-Prozess obliegt die Gestaltung und Verwaltung der Configuration Management Database (CMDB), die aus Configuration Items (CIs) besteht. Auch wenn diese Begriffe sehr technisch klingen mögen, so sei an dieser Stelle erwähnt, dass beispielsweise auch Personen mit ihren Verantwortlichkeiten Configuration Items abbilden. Dieser Prozess bildet somit die Datengrundlage der Assets und ihrer Beziehungen im Unter-

nehmen ab. Er erinnert insbesondere an Asset-, Ressourcen-, Architektur- und Infrastruktur-Management. [Köhl06] versteht unter „Assets“ die „Bestandsaufnahme der vorhandenen physikalischen Infrastruktur [...]“. An dieser Stelle wird jedoch die breitere in Abschnitt 2.4 verwendete Interpretation aus [ISO05] herangezogen.

Der *Service Desk* stellt keinen Prozess dar, er ist eine Funktion. Er bildet die Schnittstelle zwischen Service Delivery und Service Support und dem Kunden. Jegliche Meldungen seitens des Kunden langen bei ihm in erster Instanz ein. Verhältnismäßig einfache Meldungen können sofort bearbeitet und abgeschlossen werden.

Eine grafische Darstellung der Vernetzung der Prozesse kann neben der Originalliteratur unter anderem auch auf [ITIL1] gefunden werden.

Der *Information-and-Communications-Technology-Infrastructure-Management-Prozess (ICTIM)* besteht im Allgemeinen aus dem ICT-Design and Planning Process, dem ICT-Deployment Process, dem ICT-Operations Process und dem ICT-Technical Support Process. In diesen Prozessen wird insbesondere die Infrastruktur für die Information und Kommunikation adressiert.

Der *Application-Management-Prozess* verwendet einen erweiterten PDCA-Prozess (Plan, Do, Check, Act): Requirements, Design, Build, Deploy, Operate, Optimise. Hierbei geht es dementsprechend um die Entwicklung von Datenverarbeitungssystemen sowie deren Betrieb und Verbesserung. Wie in anderen Prozessen können auch hier andere Frameworks und Empfehlungen Eingang finden. Ein Beispiel für den Entwicklungsprozess ist der Unified Process (s. beispielsweise [Zuse04]), der zu den agilen Softwareentwicklungsprozessen gehört.

Der *Security-Management-Prozess* soll die Datensicherheit und den Datenschutz gewährleisten. Die Vorgaben kommen aus der strategischen und der taktischen, aber auch aus der gesetzlichen und regulativen Ebene. Von der unternehmensweiten Security Policy bis zum Sicherheitsbewusstsein und der Sicherheitskompetenz des einzelnen Mitarbeiters erstreckt sich dieser Prozess. Dabei werden beispielsweise ein Security Plan und Security Audit Reports erstellt und die Mitarbeiter geschult. Sicherheit ist nicht auf technische Belange beschränkt. Sie ist für Assets (auch personelle) und organisatorische Belange relevant.

In der *Business-Perspective* werden Business Continuity, Surviving Change, Business Practice Transformation und Partnerships and Outsourcing adressiert. Hier liegen strategische Gesichtspunkte im Vordergrund. Es handelt sich um einen wesentlichen Part, der bei einem IT-Management nicht fehlen darf. Sie ermöglicht ein durchgängiges IT-Alignment, gestaltet eine Corporate Strategy mit IT-Bezug, stellt (IT-)Asset Management sicher, sorgt für eine Wissensdurchdringung im gesamten Unter-

nehmen und stellt den strategischen Konnex zum Kunden und den Lieferanten her. Ebenso ist IT-Governance ein Thema. Auch hier spielen Gesetze und Regulative eine Rolle, welchen sich diese Arbeit im nächsten Kapitel widmen wird.

In [Köhl06] werden für die IT-Service-Managementprozesse, dem Security Management- und ICT-Infrastructure-Management-Prozess Key-Performance-Indikatoren (KPI) präsentiert, die zwecks Feststellung der Wirksamkeit eines Prozesses gemessen werden. Aber auch in anderen Prozessen lassen sich Key Performance Indikatoren definieren.

Alle Prozesse haben jedenfalls eines gemeinsam – sie unterstützen die Geschäftsprozesse, sind in diese integriert oder bilden diese sogar selbst ab.

ITIL ist demgemäß ein IT-Service-Management-Framework, welches aber auch wesentliche Komponenten des allgemeinen IT-Managements integriert und Schnittstellen definiert.

Wichtig ist, dass bei der Implementierung von ITIL Bezug zu anderen Frameworks und Empfehlungen genommen wird. Dies wird auch in ITIL selbst empfohlen. Wie schon erwähnt, ist die Fülle an Empfehlungen für die einzelnen Spezialgebiete groß. Beispielsweise sollte ISO 17799 beim Security Management eine Rolle spielen oder Six Sigma und ISO 9000 beim Qualitätsmanagement.

Die Basis für obige Erläuterungen bildeten sowohl [Köhl06] als auch [ITIL1].

## **2.8 Rollen und Verantwortlichkeiten**

IT-Management erstreckt sich über alle hierarchischen Unternehmensebenen – vom Top-Management bis zum Management auf niedrigeren Ebenen. Dem Top-Management sind dabei die strategischen Entscheidungen vorbehalten, während das Management auf niedrigerer Ebene auf der taktischen und operationalen Ebene agiert. Allerdings steht bei der allgemeinen Verwendung des Begriffs IT-Management die taktische und operationale Ebene im Vordergrund.

Gemäß einem Rollenkonzept stehen „Person“ und „Rolle“ in einer m:n-Beziehung, was bedeutet, dass eine Person mehrere Rollen (Anzahl n) annehmen und eine Rolle von mehreren Personen (Anzahl m) angenommen werden kann. Es kommen auch noch andere Dimensionen wie die Zentralisierung oder Dezentralisierung der Rollen hinzu. Beispielsweise kann es Personen mit gleichen Rollen auf gleicher Ebene, aber physisch auf verschiedene Niederlassungen des Unternehmens verteilt geben, oder physisch am selben Ort, jedoch auf unterschiedlichen Ebenen. Dies sind spezifische



Themen der Aufbauorganisation, hinsichtlich welcher der/die LeserIn in themenbezogenen Büchern fündig wird.

Kurz und bündig und doch umfassend alle Rollen zu behandeln, kann Stoff für eine eigene Arbeit bilden. Einheitliche Bezeichnungen sind eher selten anzutreffen. Schon alleine der Blick in Jobangebote verrät die Fülle an Rollen mit unterschiedlichen Schattierungen, was zeigt, dass Tätigkeiten in einer komplexen Welt nicht in eine feste Struktur nach einem „One-Best-Way“ gepresst werden können.

[Tiem06] unternimmt jedoch den Versuch (beispielhafte) *Rollen* wie folgt zu segmentieren:

<b>Führungsfunktionen</b>	<b>IT-Betrieb</b>	<b>Projektmanagement</b>
– Chief Information Officer (CIO)	– Gruppenleiter	– Projekt-Gruppenleiter
– IT-Leitung	– Prozessverantwortliche	– Arbeitspaket-Verantwortliche
– Rechenzentrum-Management	– Mitarbeiter im Help-Desk und IT-Support	
– IT-Serviceleitung	– Datenbank-Administratoren	<b>Verwaltung</b>
– Leitung Project Office	– IT-Security-Experten	– Assistenz und ähnliche Rollen mit Stabsaufgaben
<b>IT-Planung / -Controlling</b>	<b>Applikationsentwicklung / -integration</b>	
– IT-Koordinatoren	– Programmierer/Software-Architekten	
– IT-Controller	– Systemintegratoren	
– IT-Beschaffung	– Datenbank- und Systementwickler	
– IT-Quality-Manager		
– Informations- und Wissensmanagement		

Natürlich nehmen auch Führungskräfte aus dem Geschäftsbereich, Fachbereichsleiter und Mitarbeiter der einzelnen Fachbereiche Aufgaben wahr, was Voraussetzung für wirksames IT-Alignment ist. Eine Ausrichtung der IT am Geschäft ohne Unterstützung durch das Geschäft würde die Ausrichtung ad absurdum führen.

Abschließend werden noch *Rollen und Gruppierungen nach ITIL* der einzelnen ITIL-Prozesse genannt, die in [Köhl06] erläutert werden.

<p><b>Service Delivery</b></p> <ul style="list-style-type: none"> <li>– Availability Manager</li> <li>– Continuity Manager</li> <li>– Capacity Manager</li> <li>– IT-Controller</li> <li>– Service Level Manager</li> </ul>	<p><b>ICT Infrastructure Management</b></p> <ul style="list-style-type: none"> <li>– ICT-Manager</li> <li>– Technical Support Manager</li> <li>– Technical Support Specialist</li> <li>– Technical Planner</li> <li>– Technical Support Analyst</li> </ul>	<p><b>Security Management</b></p> <ul style="list-style-type: none"> <li>– (Chief) Security Officer</li> <li>– Datenschutzbeauftragte</li> </ul>
<p><b>Service Support</b></p> <ul style="list-style-type: none"> <li>– Configuration Manager</li> <li>– Configuration-Support-Personal</li> <li>– Incident Manager</li> <li>– Incident-Support-Personal</li> <li>– Problem Manager</li> <li>– Problem-Support-Personal</li> <li>– Change-Manager</li> <li>– Change Advisory Board</li> <li>– Release Manager</li> <li>– Expertengruppe für ein spezielles DV-Verfahren (bei Release-Management)</li> </ul>	<p><b>Applications Management</b></p> <p>Basierend auf PRINCE 2, HERMES in [Köhl06]</p> <ul style="list-style-type: none"> <li>– Projektauftraggeber (Executive)</li> <li>– Hauptnutzer (Senior User)</li> <li>– Kundenvertriebsbeauftragter (Customer Account Manager)</li> <li>– Hauptlieferant (Senior Supplier)</li> <li>– Entwicklungsabteilung (Supplier Skill Management)</li> <li>– Projektleiter (Projekt Manager)</li> <li>– Gruppenleiter (Team Manager)</li> <li>– Risikoverantwortlicher</li> <li>– Qualitätsverantwortlicher</li> </ul>	<p><b>Business Perspective</b></p> <ul style="list-style-type: none"> <li>– Chief Information Officer (CIO)</li> <li>– Mitarbeiter in Fachabteilungen</li> <li>– etc.</li> </ul>

Es verwundert nicht sehr, dass die Namensgebung mit den Namen der einzelnen ITIL-Bereiche bzw. –Prozesse korreliert.

Es wäre für diese Arbeit zu umfangreich, alle einzelnen Rollen zu besprechen. Es wird dem/der LeserIn intuitiv überlassen, die geeigneten Verantwortlichkeiten aus den oben beschriebenen Prozessen abzuleiten. Dennoch werden zu manchen Rollen Ergänzungen angeführt.

Der *Service Level Manager* inkorporiert auch Verantwortlichkeiten eines IT Account Managers [Rüte06]. Auch die Aufnahme der Anforderungen und deren Verarbeitung der Anforderungen liegen in seinem Bereich.

Das *Change Advisory Board (CAB)* besteht aus einer Gruppe von Entscheidungsträgern relevanter Bereiche (z. B. technisch, fachbereichsspezifisch). Diese haben einen Überblick über die für die Entscheidungen wichtigen Datenverarbeitungsverfahren. Auch Vertreter des Kunden können dieser Gruppe beiwohnen.

Die *Expertengruppe* für ein spezielles Datenverarbeitungsverfahren ist im Release-Management für die Entwicklung, das Testen und die Implementierung bzw. das Roll-Out zuständig.

Der *Technical Support Manager* ist für den effektiven und kosteneffizienten Einsatz der Technical Support Prozesse verantwortlich. Während der Technical Support Specialist technische Sachverhalte analysiert, ICT-Komponenten administriert und testet sowie Empfehlungen abgibt, überwacht der Technical Planner die Märkte hinsichtlich Technologien und Trends und plant deren Einführung. Technical Support Analyst zu sein bedeutet die bestehende ICT-Infrastruktur zu überwachen und Relationen zu neuen Komponenten zu analysieren. Die Erstellung von Dokumentationen und Reports zählt ebenfalls zu seinen Verantwortlichkeiten.

Abschließend sei noch zur Business Perspective folgendes angemerkt. In [Köhl06] werden keine speziellen Rollen außer den oben genannten erwähnt. Dies liegt an der Fülle der Rollen, welche je nach Branche in einem Unternehmen existieren, denn schließlich geht es bei „Business Perspective“ vor allem um das Geschäft selbst mit Bezug zur IT. Der CIO bildet die strategische Schnittstelle zu den im jeweiligen Unternehmen befindlichen Geschäftsbereichen.

## Kapitel 3

# IT-Governance

Im ersten Abschnitt wird eine ausführliche Einleitung zu IT-Governance gegeben, um den/die LeserIn mit den Grundlagen vertraut zu machen. Danach widmen sich die Abschnitte gänzlich der IT-Governance. Es werden sowohl Begründungen für IT-Governance angeführt als auch Ziele genannt. Die Beschreibungen der Treiber schaffen die Quelle für die letzten drei Abschnitte, welche sich den Domänen, den Prozessen sowie den Rollen und Verantwortlichkeiten widmen.

### 3.1 Einleitung

Um den/die LeserIn durch kleinere verständliche Schritte an IT-Governance heranzuführen, wird die Brücke über „Governance“, „Corporate Governance“ und „Internes Kontrollsystem“ geschlagen.

#### 3.1.1 Erläuterung des Begriffs „Governance“

Ursprünglich leitet sich „Governance“ vom griechischen Wort „Kybernân“ ab, welches für die Bedeutungen „ein Schiff lenken“ bzw. „führen“ steht (lt. [Hesc07] und [Stut06]). Herr [Hesc07] beschrieb „Governance“ mit Hilfe eines analogen Beispiels. Er beschrieb das Ereignis eines Segelturns für welchen Ziele festgelegt und die Rahmenbedingungen überwacht und sichergestellt werden müssen. Verkörpert man diese Tätigkeiten in einer Person, so ist diese für die Erreichung der Ziele durch die zuvor erwähnten Tätigkeiten verantwortlich. Als Ziele sind im Kontext eines Segelturns beispielsweise bestimmte Punkte in einem Ozean oder Häfen, die erreicht werden müssen bzw. werden sollen und als Rahmenbedingungen zum Beispiel der Wind, das Wetter im Allgemeinen, das Meer, das Boot, die Mannschaft, der Provi-

ant, die Ausrüstung und Regeln zu nennen. Bei den Rahmenbedingungen handelt es sich demgemäß um interne und externe Faktoren.

In Tabelle 3.1 werden einige *Übersetzungen* von „Governance“ aus Wörterbüchern aufgelistet.

Langenscheidt Englisch-Deutsch	PONS5	Wörterbuch-Info	LEO
<p>[Will91]<sup>6</sup> regieren, regeln, leiten, lenken, führen, verwalten, regulieren, steuern, herrschen</p> <p>[Merz02] Entscheidungsstrukturen, Kontrolle, Leitung, Verantwortliches Handeln (bez. Führung von Unternehmen und Behörden), Herrschaft, Gewalt, Staatsführung, Regierungsgewalt, Regierungsform</p>	<p>[Agba05] regieren, regeln</p> <p>[Coll04] regieren</p> <p>iFinger<sup>7</sup> von PONS regieren, leiten, regeln</p>	<p>[IWört] Regierungsform, Regierungsgewalt, Gewalt (über), Herrschaft, Kontrolle</p>	<p>[LEO] Herrschaft, Regieren, Regierung, Regierungsführung, Regierungsgewalt, Staatsführung, Steuerung</p>

Tabelle 3.1: Übersetzungen von "Governance" und verwandten Wörtern

Das Zentrum der Bedeutung des Begriffs „Governance“ und von verwandten Begriffen bilden die Wörter „herrschen“, „leiten“, „kontrollieren“, „regeln“ und „steuern.“

[Meyers]. Meyers(-Lexikon) versteht unter Governance einen „sozialwissenschaftlichen Begriff, der dem Gebiet der Wirtschaft entstammt (Corporate Governance) [...]“. Weiters sei dies ein in der Politikwissenschaft gebräuchlicher Begriff. Es werden Wörter wie „Government“, „Verwaltung“, „Rahmenbedingungen“ und „Regelungsstrukturen“ erwähnt.

<sup>5</sup> Suchbegriff „govern“

<sup>6</sup> Suchbegriff „govern“

<sup>7</sup> Übersetzungsprogramm (Deutsch-Englisch / Englisch-Deutsch)

[WB]. Worldbank definiert Governance „as the traditions and institutions by which authority in a country is exercised for the common good. This includes (i) the process by which those in authority are selected, monitored and replaced, (ii) the capacity of the government to effectively manage its resources and implement sound policies, and (iii) the respect of citizens and the state for the institutions that govern economic and social interactions among them.”

Hierbei sind vor allem Wörter wie „monitor“, „manage resources“, „policies“ und „interactions“ für spätere Betrachtungen in diesem Kapitel hervorzuheben.

Im folgenden Abschnitt wird der Begriff „Governance“ speziell auf Unternehmen bezogen betrachtet.

### 3.1.2 Erläuterung des Begriffs „Corporate Governance“

Nachdem der Begriff „Governance“ im letzten Abschnitt näher erläutert wurde, steht nun die Corporate Governance im Mittelpunkt dieses Abschnitts.

Um einen guten High-Level-View zu erlangen, werden nun einige *Definitionen und Interpretationen* präsentiert.

[Meyers]. Bei Corporate Governance handelt es sich um „Standards beziehungsweise spezielle Rahmenbedingungen für Strukturen und Prozesse der Führung, Verwaltung und Überwachung börsennotierter Unternehmen. [...] Berücksichtigung rechtlicher, ökonomischer, kultureller und sozialer Besonderheiten [...]“.

[CFAC92]. Der Cadbury Report 1992 besagt: „Corporate Governance is the system by which companies are directed and controlled.”

[ITGI07]. CobiT 4.1 definiert den Begriff „Enterprise governance“ als „A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise’s resources are used responsibly.”

[OECD04]. „Corporate Governance involves a set of relationships between a company’s management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and shareholders and should facilitate effective monitoring.” Weiters sollen durch

die Corporate Governance die Ressourcen effizient genutzt werden. [RMG99] (Bank for International Settlements) verwendet ebenfalls diese Definition.

Aus den soeben aufgelisteten Definitionen kann eine Konzentration auf Führung, die Festlegung von Strukturen und Prozessen, die Wahrung einer ganzheitlichen Sicht, die Steuerung und Kontrolle, Stakeholder, die Ausrichtung an Unternehmenszielen und die effiziente Ressourcennutzung festgestellt werden.

[Mali02], [Gälw90]. [Mali02] und [Gälw90] stellen die Führung in den Mittelpunkt der Corporate Governance. Angemessene Führung soll die Erzielung eines guten Wirtschaftsergebnisses ermöglichen. Dabei sei darauf zu achten, nicht nur die Größen des Rechnungswesens als Stütze adäquater Führung zu gebrauchen.

[Rüte06]. Wie in Abbildung 3.1 zu erkennen, werden unterschiedliche Einflussfaktoren auf die Corporate Governance identifiziert. Aufgabe der Corporate Governance ist es, diese Einflussfaktoren in Regeln und Vorgaben zu transformieren.

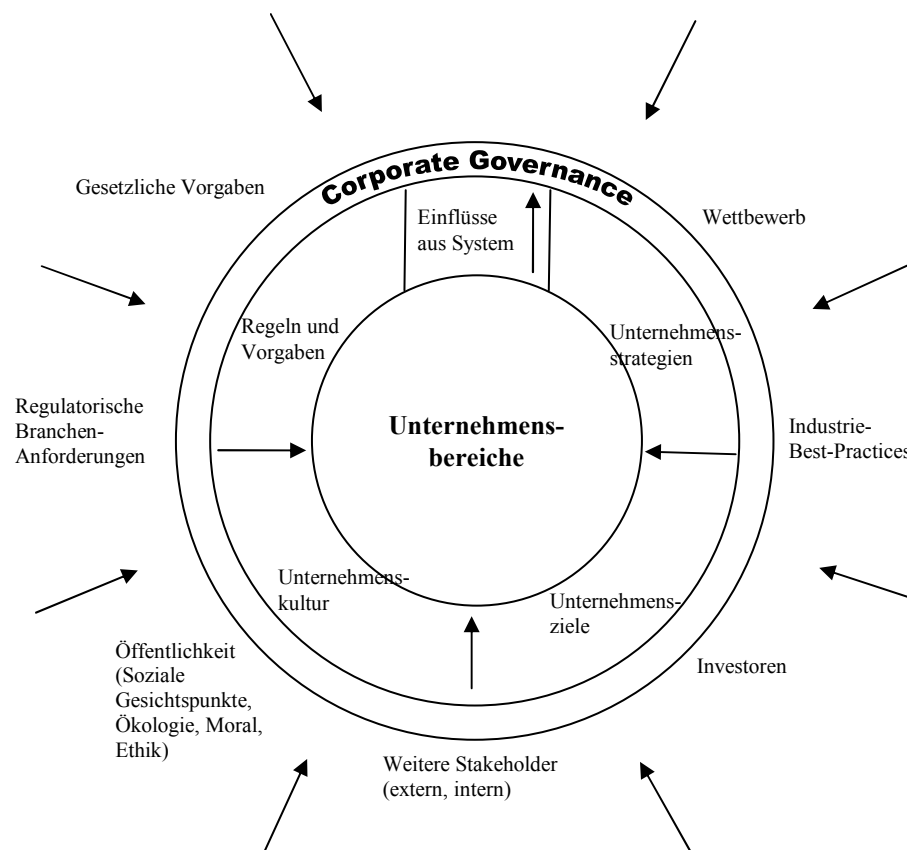


Abbildung 3.1: Innen- und Außensicht von Corporate Governance (basierend auf [Rüte06], [ITGI03])

Weiters verwendet [Rüte06] den Begriff „Metasicht“ als ein charakterisierendes Element von Regelwerken der Kategorie „Governance“. Hier wird die Regulierung

und Kontrolle angedeutet, welche das Unternehmen mit seinen Komponenten und Prozessen in einem bewusst festgelegten Rahmen halten soll.

Die Definitionen und Interpretationen von Corporate Governance spiegeln (klarerweise) die Definitionen und Interpretationen von Governance wider, allerdings erweitern sie diesen Begriff um unternehmensspezifische Belange.

### **3.1.3 Erläuterung des Begriffs „Internes Kontrollsystem“**

Das „Committee of Sponsoring of the Treadway Commission“ (COSO) definiert *interne Kontrolle* als einen Prozess, ausgeführt durch Topführungskräfte, das Management und anderes Personal das die Erreichung der Unternehmensziele hinsichtlich der Kategorien „Wirksamkeit und Effizienz von Tätigkeiten“, „Zuverlässigkeit und Vertrauenswürdigkeit des Finanzreportings“ und „Compliance“ angemessen sicherstellen soll.

COSO teilt interne Kontrolle in fünf zueinander in Beziehung stehende Komponenten ein. Diese sind „Control Environment“, „Risk Assessment“, „Control Activities“, „Information and Communication“ und „Monitoring“.

Die Komponenten stellen die Bereiche dar, die vorhanden sein müssen, um die oben genannten Zielkategorien zu erreichen.

Ein internes Kontrollsystem kann jedoch den Erfolg nicht garantieren. Sehr wohl hilft es jedoch durch Performancemessung, die Steuerung des Unternehmens zu unterstützen und eine gezielte Steuerung zu ermöglichen.

Für ein gut funktionierendes internes Kontrollsystem ist die Verteilung von Verantwortlichkeiten im gesamten Unternehmen auf allen Ebenen notwendig, wobei natürlich das Top-Management die Hauptaufgaben beinhaltet und das Kontrollsystem steuert.

Die Basis für obige Erläuterungen bilden [COSO92] und [SZF06].

## **3.2 Definitionen und Interpretationen**

Nachdem die Begrifflichkeiten „Governance“, „Corporate Governance“ und „Internes Kontrollsystem“ erläutert wurden, beginnt mit diesem Abschnitt die Konzentration auf IT-Governance. Ähnlich den vorigen Abschnitten werden in diesem Kapitel zunächst einige Definitionen und Interpretationen präsentiert, die eine gute Vorstellung, worum es sich bei IT-Governance handelt, ermöglichen sollen.



**[Buch05].** [Buch05] versteht unter IT-Governance die Schaffung eines strukturellen Rahmens und die Definition der Steuerung der IT, um einen effektiven und effizienten Einsatz der IT zu gewährleisten.

**[IMPA05].** “IT Governance covers the culture, organisation, policies and practices that provide this kind of oversight and transparency of IT – IT Governance is part of a wider Corporate Governance activity but with its own specific focus.” [IMPA05] wurde durch CobiT beeinflusst.

**[Tiem06].** Mit IT-Governance “soll ausgedrückt werden, dass mittels Führung, Organisationsstrukturen und Prozessen sicherzustellen ist, dass die IT die Unternehmensstrategie und –ziele unterstützt.“ Sie „liegt in der Verantwortung des Vorstands sowie des Managements und ist damit ein wesentlicher Bestandteil der Unternehmensführung.“

**ISACA.** IT-Governance ist nach der Information Systems Audit and Control Association „a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise’s goals by adding value while balancing risk versus return over IT and its processes.“ [Rüte06].

**[ITGI07].** “IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise’s IT sustains and extends the organisation’s strategies and objectives.” Das IT Governance Institute ist aus der ISACA entstanden.

**[Weil04].** IT-Governance spezifiziert “the decision rights and accountability framework to encourage desirable behaviour in using IT”.

In den oben angeführten Definitionen werden die Themenbereiche Beziehungsgeflechte, Prozesse, Kontrolle, Unternehmensziele und -strategien, Balancierung von Risiken und Nutzen aus der IT, Führungsverantwortung, Organisationsstrukturen, Schaffung eines strukturellen Rahmens und Steuerung der IT adressiert.

Im Rahmen der IT-Governance gilt es auch die Demand- und Supply-Seite im Sinne der Ganzheitlichkeit und der Unterstützung der Unternehmensziele sinnvoll zu verbinden [Buch05].

Es wurde nun die Brücke von Governance über Corporate Governance zu IT-Governance geschlagen.

### 3.3 Gründe für IT-Governance

Für die IT ist in den letzten Jahren ein neues Zeitalter angebrochen. Sie hat sich von der Eigenschaft eines reinen Rationalisierungsinstruments zu einem *Werttreiber*, oft „Enabler“ genannt, und Dienstleister entwickelt. In [Tiem06], [Hesc05] und [IMPA05] wird IT-Governance als wesentlich erachtet, um die werttreibende Eigenschaft der IT zu aktivieren und zu gewährleisten.

Die IT ist mittlerweile stark mit den *Unternehmensprozessen* verwoben. Dieser Umstand generiert, wie erwähnt, Unternehmenswert, aber es resultieren daraus auch viele Risiken. Diese *Risiken* gilt es zu kontrollieren, wodurch ein Kontrollsystem notwendig wird, welches auch die *Performance* der Prozesse und der Organisation zum Zwecke strategischer Belange, der Vergleichbarkeit mit anderen Unternehmen und der Qualitätssicherung misst [Hesc05], [IMPA05], [ITGI03], [Rüte06], [ITGI07].

Ein evolutionäres Entwickeln einer Organisation ist bei passenden Bereichen nicht nachteilig und sogar modern bzw. kann es die Zukunft sein, jedoch müssen *Grenzen* gesteckt und eine umfassende *Steuerung* des Unternehmens implementiert werden, um ungewünschte Entwicklungen zu unterbinden, die den Unternehmenszielen widerstreben.

*Sicherheit* ist ein immer stärker diskutiertes Thema (auch hinsichtlich des Datenschutzes) und die Notwendigkeit sicherer Unternehmen und damit auch sicherer IT ist unbestritten. Grund genug um eine unternehmensweite Sicherheitspolitik mit definierten Steuerungsmechanismen, Berechtigungskonzepten und klaren Entscheidungsstrukturen im Sinne einer „Business Resilience“ zu gestalten [Hesc05], [IMPA05], [Rüte06].

Durch die *Globalisierung* und *Vernetzung* steigt auch der Kompliziertheitsgrad und die Komplexität der Prozesse bei Unternehmen/Organisationen/etc. unabhängig von deren Größe. Eine systemische und ganzheitliche Führung ist daher notwendig.

Eine *prozessorientierte Sicht* macht aufgrund der sich oft rasch ändernden Bedingungen in Märkten und ihren Umgebungen sowie aufstrebenden Technologien eine schnelle Anpassungsfähigkeit notwendig. Oft muss daher auch die Organisationsstruktur überholt und adaptiert werden. Schon Charles Darwin erkannte: „Es sind nicht die Stärksten der Spezies die überleben, nicht die Intelligentesten, sondern die, die am schnellsten auf Veränderungen reagieren.“ [IUK].

Nicht nur externe Faktoren machen Änderungen im Unternehmen notwendig, sondern auch der interne Wille, besser zu werden. *Kontinuierliche Verbesserung* im ge-

samten Unternehmen nach beispielsweise KAIZEN ist daher für das langfristige Überleben von Unternehmen unabdingbar. KAIZEN steht für Kontinuierliche Verbesserung im japanischen Raum (KAI = Wandel, Änderung; ZEN = das Gute) [Wojd05].

Nicht zuletzt wird IT-Governance auch durch immer mehr und umfassendere Gesetze und Regulative getrieben. Skandale wie Enron sollen sich womöglich nicht wiederholen [IMPA05]. Ein Schlagwort in diesem Zusammenhang ist „*Compliance*“. Mit „*Compliance*“ ist „[...] ein regelkonformes Verhalten eines Unternehmens in Bezug auf die gesetzlichen und regulativen Bestimmungen [...]“ gemeint. Sie „[...] soll sicherstellen, dass die unternehmerischen Risiken erkannt, bewertet und durch die Implementierung technischer Lösungen erfüllt werden.“ [ITWiss]. (Verhaltenssicht) (Fortsetzung mögl.weise auf nächster Seite) „IT-Compliance bzw. IT-compliant zu sein bezeichnet einen Zustand, in dem alle für die Unternehmens-IT relevanten Gesetze oder in ihrer allgemeinen Geltungsanordnung von diesen abgeleiteten Rechtsnormen nachweislich eingehalten werden.“ [Goek07] (Zustandssicht) Viel Geld wird zur Sicherstellung von Compliance aufgewendet, wobei ein Drittel in IT investiert wird. Das ist ein Indiz für die Bedeutung eines Regelmechanismus [Rüte06], [Tiem06]. Compliance ist aber nicht mehr als notwendiges Übel, sondern als Wettbewerbsfaktor zu sehen [Dami05], [Hesc05]. Als (wichtiges) Beispiel wird der Sarbanes-Oxley Act in Abschnitt 3.5.3 kurz erläutert.

Der *Wettbewerbsfaktor* äußert sich insbesondere darin, dass Investoren bereit sind oder zumindest bereit waren, um ca. 18 – 41 % mehr in Unternehmen mit guter Governance zu investieren [MK02]. Ein anhaltender Trend ist, nicht zuletzt wegen Negativbeispielen durch fehlende Corporate Governance, zu erwarten.

Da nun theoretisch verdeutlicht wurde, warum IT-Governance notwendig ist, fehlt noch die praktische Komponente. Ohne vorgefertigte Standards oder Empfehlungen als Stütze kann IT-Governance ein aufwendiges, aber auch ein womöglich risikoreiches Unterfangen darstellen. Es existieren Standards und Empfehlungen, welche die Implementierung von IT-Governance unterstützen sollen. Einige davon werden in Abschnitt 3.5 kurz erläutert.

### 3.4 Ziele

Aus den weiter oben präsentierten Definitionen und Interpretationen und den Gründen für IT-Governance lassen sich Ziele der IT-Governance ableiten, welche im Folgenden aus einem High-Level-View betrachtet werden. Es gibt unzählige Unterziele

und Maßnahmen zu jedem hier angeführten Ziel, welche jedoch den Rahmen der hier vorliegenden Arbeit sprengen würden und daher nicht erläutert werden.

*Ziele* der IT-Governance sind

- als Führungsaufgabe die Einbindung der Entscheidungsträger, sprich der Führungskräfte, in die Geschehnisse der IT,
- die Konzentration auf das Kerngeschäft des Unternehmens,
- die Ausrichtung der IT und damit der IT-Strategie auf die Unternehmensziele und damit die Unternehmensstrategie,
- die Schaffung klarer Organisationsstrukturen und Beziehungen,
- die Schaffung klarer Verantwortlichkeiten,
- eine prozessorientierte Sicht,
- die Überwachung, Performancemessung und –analyse,
- den verantwortungsvollen Umgang mit Ressourcen,
- das Management und Minimierung der Risiken,
- die Einrichtung und den Betrieb eines Kontrollsystems, Kontrolle der Prozesse inklusive ihrer In- und Outputs,
- die Sicherheit,
- angemessene Kosten und angemessenes Budget,
- und Compliance

mit der übergeordneten Zielperspektive der Steigerung des Unternehmenswerts durch den Einsatz der IT sicherzustellen [Dami05], [IMPA05], [ITGI03], [ITGI07], [Tiem06].

Abschließend wird das in [ITGI03] in einem Satz erwähnte Hauptziel der IT-Governance genannt, nämlich “die Anforderungen an die IT sowie die strategische Bedeutung von IT zu verstehen, um den optimalen Betrieb der Unternehmensziele sicherzustellen und Strategien für die zukünftige Erweiterung des Geschäftsbetriebs zu schaffen“.

### **3.5 Treiber**

In der Folge werden nicht-IT-Governance-spezifische und IT-Governance-spezifische Frameworks und Anleitungen besprochen. Die nicht-IT-Governance-spezifischen Frameworks und Anleitungen sind aufgrund der schon erwähnten starken Verwobenheit der IT mit anderen Unternehmensbereichen bzw. –prozessen auch Gegenstand einer für IT-Governance relevanten Betrachtung. Weiters können auch für IT-Governance aus den nicht unmittelbar verwandeten Themenbereichen wesentliche Konzepte extrahiert werden.

In den folgenden Unterabschnitten dieses Abschnitts wird eine Auswahl an breit diskutierten Gesetzen und Regulativen behandelt. Allerdings gibt es in den meisten Ländern noch weitere Gesetze und Regulative, wie beispielsweise zur Datensicherheit und zum Datenschutz oder Abwandlungen von weiteren internationalen Gesetzen und Regulativen.

In Abbildung 3.2 sind nicht alle Zwischenschritte dargestellt. Jedenfalls ist eine der früheren Versionen und die zum Zeitpunkt der Verfassung dieser Arbeit aktuelle Version abgebildet. Diese Abbildung erhebt keinen Anspruch auf Vollständigkeit.

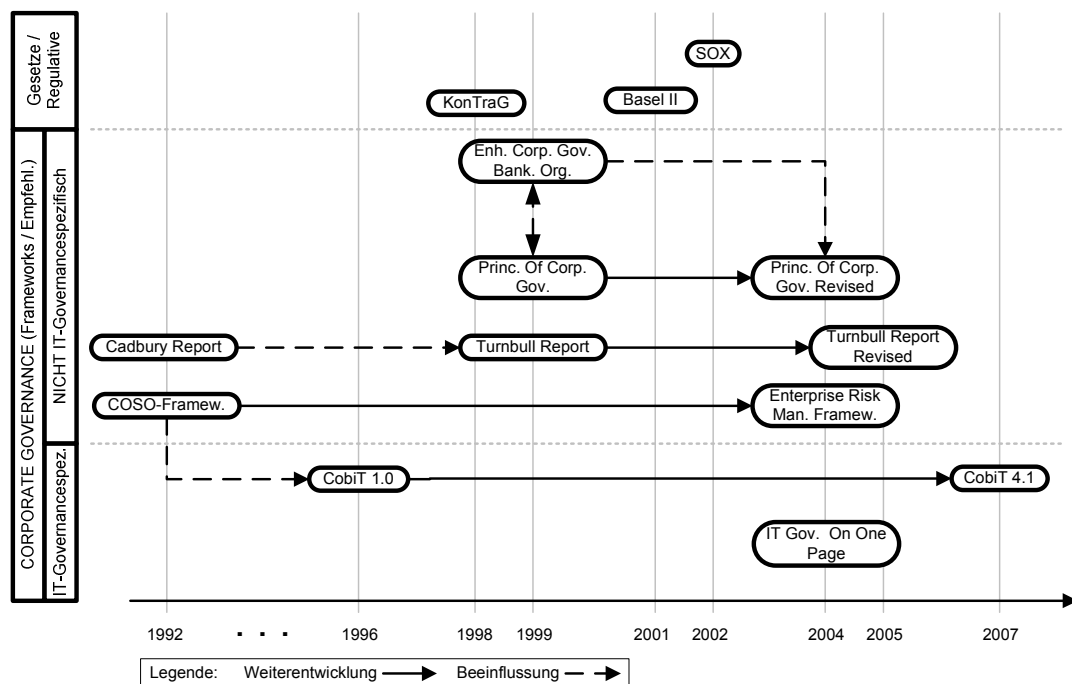


Abbildung 3.2: IT-Governance-Treiber im Zeitablauf

### 3.5.1 Nicht-IT-Governance spezifische Frameworks und Anleitungen

**Cadbury Report.** Der 1992 in Großbritannien vom „Committee on the Financial Aspects of Corporate Governance“ und „Gee and Co. Ltd.“ verfasste Report, der insbesondere unter dem Namen „Cadbury Report“ bekannt ist, rückte die Corporate Governance stärker ins Rampenlicht. Die Definition des Cadbury Reports von „Corporate Governance“ wurde in Abschnitt 3.1.2 dargelegt. Bei diesem Report handelt es sich nicht um IT-Governancespezifische Empfehlungen, sondern um Good-Practices für Führungskräfte und Aufsichtsratsmitglieder im Bereich Finanzberichterstattung und Audit. Er adressiert die Verantwortlichkeiten der Führungskräfte und Aufsichtsratsmitglieder. Weiters empfiehlt er die Förderung von Standards und die

Kontrolle des Geschäfts. Auch organisatorische Belange werden angesprochen [CFAC92], [ITGI03].

**Turnbull Report.** Die 1999 in Großbritannien vom “Institute of Chartered Accountants in England & Wales“ herausgegebene Anleitung, die insbesondere unter dem Namen „Turnbull Report“ bekannt ist, hob besonders die Bedeutung eines internen Kontrollsystems im Sinne einer guten Corporate Governance hervor. Auch bei diesem Report handelt es sich nicht um IT-Governancespezifische Empfehlungen. Dieser verlangt jedoch die Implementierung adäquater und effektiver Prozesse, um Risiken zu überwachen und auf ein sinnvolles Ausmaß zu senken. Die Führungskräfte sind verantwortlich für das Funktionieren eines internen Kontrollsystems [ICA99], [ITGI03], [FRC05].

**Enhancing Corporate Governance in Banking Organisations.** Die 1999 vom “Basel Committee on Banking Supervision“ der „Bank for International Settlements“ (BIS) herausgegebenen Richtlinien konzentrieren sich speziell auf den Bankensektor. Auch wenn diese Richtlinien nicht speziell die IT-Governance adressieren, sei an dieser Stelle erwähnt, dass Banken eine hohe IT-Affinität aufweisen. Immerhin geben bzw. gaben Banken laut einer Studie der Meta Group im Jahr 2002 (vgl. [Buch05]) im Durchschnitt 5,37 % des Umsatzes für IT aus und liegen damit an dritter Stelle von vierzehn betrachteten Branchen und nur um 1,27 % unter der Spitze, welche die Finanzdienstleister bilden. Die Definition von Governance-Aktivitäten der BIS wurde schon in Abschnitt 3.1.2 gegeben. Diese Richtlinien empfehlen organisationsweite strategische Ziele und Unternehmenswerte, Verantwortlichkeit, qualifizierte Führungskräfte, ein Risikomanagement, die Überwachung und interne Kontrolle und eine durchschaubare Corporate Governance. Ad-hoc-Entscheidungen sollen vermieden werden [ITGI03], [RMG99].

**Principles of Corporate Governance.** Die 1999 von der „Organisation for Economic Co-operation and Development“ (OECD) herausgegebenen „Principles of Corporate Governance“ gliedern Corporate Governance Konzepte in fünf Bereiche: 1. Die Rechte der Aktionäre, 2. Die Gleichbehandlung der Aktionäre, 3. Die Rolle der Stakeholder, 4. Veröffentlichung und Transparenz, 5. Die Verantwortung der Unternehmensführung. Die darin enthaltenen Empfehlungen lassen sich auch direkt für IT-Governancespezifische Zwecke nutzen, was durch die Betonung der Bedeutung von Strategien, Masterplänen, Risikopolitik, Budgets, Geschäftsplänen, Performancezielen, Überwachung des Unternehmens, Compliance und dem Vorhandensein relevanter, präziser und zeitgerechter Information deutlich wird [ITGI03], [OECD99], [OECD04].

**Internal Control – Integrated Framework.** Das 1992 vom “Committee of Sponsoring Organisations of the Treadway Commission” (COSO) herausgegebene Public-Domain-Framework, welches naheliegend auch COSO-Framework genannt wird, rückt einmal mehr interne Kontrollen der Finanzberichterstattung in den Mittelpunkt der Betrachtungen. Die Definition nach COSO bezüglich interner Kontrollen wurde in Abschnitt 3.1.3 dargelegt. In diesem wurde auch erläutert, was COSO unter „interne Kontrolle“ versteht. Mittlerweile gibt es eine Erweiterung mit Änderungen aus dem Jahr 2004 – das „Enterprise Risk Management – Integrated Framework“. „Control Environment“ wird zu „Internal Environment“. Dazu kommen die Komponenten „Objective Setting“, „Event Identification“ und „Risk Response“, welche in Kombination mit den im Abschnitt 3.1.3 erwähnten Komponenten einen zu durchlaufenden Prozess abbilden. Die Zielkategorien bilden „Strategic“, „Operations“, „Reporting“, „Compliance“ ab. Mit der organisatorischen Dimension entsprechen die Komponenten zusammen mit den Zielkategorien einem Würfel, der alle drei Dimensionen verbindet. COSO beeinflusste auch CobiT maßgeblich und wird mittlerweile auch als bedeutendes Framework für die Compliance mit dem § 404 des Sarbanes-Oxley Acts wahrgenommen [ITGI03], [COSO92], [COSO04].

### 3.5.2 IT-Governance spezifische Frameworks und Anleitungen

**IT-Governance on One Page.** Dies ist nun das erste hier präsentierte IT-Governance-Framework. Es wurde von Peter Weill und Jeanne W. Ross des „Center for Information Systems Research“ (CISR) der „Sloan School of Management“ des „Massachusetts Institute of Technology“ entwickelt und 2004 veröffentlicht. Was CISR unter IT-Governance versteht, wurde im Abschnitt 3.2 präsentiert. Mit diesem Framework soll die kosteneffiziente Verwendung der IT, die effektive Verwendung der IT zur Auslastung der Assets, für Wachstum und für die Flexibilität des Unternehmens gewährleistet werden. Es konzentriert sich insbesondere auf die organisatorische Komponente, die Ausrichtung der IT an den Unternehmenszielen (Stichwort: Alignment) und Bewertung der IT-Governance im Allgemeinen [Weil04].

**Control Objectives for Information and related Technology (CobiT).** Das wahrscheinlich bekannteste Framework für die Unterstützung der IT-Governance ist das 1996 von der „Information Systems Audit and Control Association“ (ISACA) entwickelte und veröffentlichte Public-Domain-Framework, welches ab dem Jahr 1998 von dem „IT Governance Institute“ weiter entwickelt wurde und dessen letzte Version 4.1 im Jahr 2007 erschienen ist. Laut [Hesc05] hat CobiT eine Entwicklung von einer Audit-Fokussierung über eine Control- und Managementfokussierung zu einer Governancefokussierung erfahren. Durch seinen direkten und starken Bezug zu den

durch das IT Governance Institute definierten und in Abschnitt 3.6 behandelten Bereichen der IT-Governance hat es seine Stellung als IT-Governance unterstützendes Framework erhalten. Da CobiT durch das COSO-Framework beeinflusst wurde, erscheint es logisch, dass auch CobiT zur Erfüllung der Anforderungen des § 404 des Sarbanes-Oxley Act beiträgt, wobei nur ein Teil der CobiT-Kontrollen für diesen relevant sind [Rüte06]. Dies macht deutlich, dass CobiT nicht das COSO-Framework ersetzt. Jenes Framework behandelt, *was* umgesetzt werden soll, jedoch nicht *wie* etwas umgesetzt werden soll. Es gibt jedoch umfangreiche Informationen über Prozesse, deren IT-Prozess- und Aktivitätsziele und Schlüsselmetriken. Es besteht aus vierunddreißig Prozessen, über dreihundert Kontrollzielen, definiert weiters Elemente zur Leistungsmessung, kritische Erfolgsfaktoren und ein Reifegradmodell [ITGI03], [ITGI07].

### 3.5.3 Gesetzliche Rahmenwerke

**Basel II.** Im Jahr 2001 wurde in Basel II eine Änderung der Eigenkapitalregelung mit stärkerer Ausrichtung an Kreditrisiken eines Kreditnehmers<sup>8</sup> von Banken vorgeschlagen - mit dem Ziel Kreditgeber vor Fehlern in internen Verfahren, durch Menschen und Systeme oder bei Kreditnehmern zu schützen. Seit 2004 ist eine überarbeitete Rahmenvereinbarung des „Basler Ausschuss für Bankenaufsicht“ mit dem Titel „Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen“ erhältlich. Die IT-Sicherheit wird durch Anforderungen an Business Continuity-, Contingency Pläne, an die Risikobewertung und das Risikomanagement, an Dokumentationsrichtlinien und sowohl Backup- als auch Havariekonzepte adressiert [Köhl06], [BAB05].

**Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG).** Bei KonTraG handelt es sich um eine Sammlung von Änderungen in anderen deutschen Gesetzen. KonTraG wurde im Jahr 1998 im Bundesgesetzblatt Nr. 24 veröffentlicht. [Köhl06] sieht darin einen Versuch des Gesetzgebers, eine „Corporate Governance“ festzulegen. Auch das Aktiengesetz spielt in diesem Bereich eine Rolle. Ziel ist es in beiden Fällen, die Risiken zu kontrollieren und zu steuern und in diesem Sinne ein Überwachungssystem einzurichten [Köhl06], [Bund98], [DAkt].

**Sarbanes-Oxley Act (SOX).** Im Jahr 2002 wurde vom amerikanischen Kongress der Sarbanes-Oxley Act verabschiedet. Anstoß waren die Skandale um Enron und Worldcom und die Verstrickung von Banken, Analysten und Wirtschaftsprüfern. Bilanzfälschungen sollten sich für börsennotierte Unternehmen schwieriger gestalten.

---

<sup>8</sup> hier: Staat oder Unternehmen



ten, welcher Umstand sich in strengeren Bilanzierungsvorschriften sowie Haftungsvorschriften für Vorstandsvorsitzende und Finanzvorstände niedergeschlagen hat. SOX gilt insbesondere für Unternehmen, welche bei der „Securities and Exchange Commission“ registriert sind, gleichgültig ob es sich um Unternehmen amerikanischer Herkunft handelt. Weiters wurde die Veröffentlichungspflicht ausgeweitet, interne Kontrollen (implizit auch der IT) wurden adressiert, das „Public Company Accounting Oversight Board“ zur Überwachung börsennotierter Unternehmen gegründet und die Aufbewahrungsdauer von Wirtschaftsdaten festgelegt. Die lange Aufbewahrungsdauer stellt(e) neue Herausforderungen an die Dokumentenverwaltung und die IT-Sicherheit im Allgemeinen [Köhl06], [Dami05], [Rüte06].

### **3.6 Domänen**

Dieser Abschnitt sowie der nächste ist stark an dem für IT-Governance bedeutenden Framework ausgerichtet.

IT-Governance besteht nach [ITGI07] vor allem aus folgenden *Bereichen* in Tabelle 3.2, welche als „Focus Areas“ bezeichnet werden.

<b>Strat. Ausrichtung der IT (Strategic alignment)</b>	<ul style="list-style-type: none"> <li>– Definition der IT-Strategie</li> <li>– Definition von Managementprozessen</li> <li>– Ausrichtung der IT an Geschäftsprozessen</li> </ul>	<b>Kommunikationsstrategie und Unternehmenskultur</b> aus [IMPA05]
<b>Nutzengenerierung durch IT (Value delivery)</b>	<ul style="list-style-type: none"> <li>– Sicherstellung korrekter Durchführung der IT-Strategie</li> <li>– Optimierung der Kosten</li> <li>– Erreichung von Zufriedenheit der Stakeholder</li> <li>– Berücksichtigung von Time to Market, Qualität und monetärem Nutzen</li> </ul>	
<b>IT Ressourcen Management (Resource management)</b>	<ul style="list-style-type: none"> <li>– Investition in, Optimierung und Adressierung i. Allg. von Applikationen, Informationen, Infrastrukturen und Menschen</li> </ul>	
<b>Management von IT Risiken (Risk management)</b>	<ul style="list-style-type: none"> <li>– Festlegung der Risikofreudigkeit</li> <li>– Kontrolle der Risiken</li> <li>– Steuerung der Risiken durch Risikoreduktion, -transfer oder -akzeptanz</li> <li>– Festlegung von Verantwortlichkeiten</li> <li>– Gewährleistung von Compliance</li> </ul>	
<b>IT-Performance (Performance measurement)</b>	<ul style="list-style-type: none"> <li>– Überwachung der Durchführung der Strategie, Projekte, Prozesse und Dienstleistungen</li> <li>– Sicherstellung der Benchmarkfähigkeit</li> </ul>	

Tabelle 3.2: Focus Areas (basierend auf [ITGI07], [ITGI03])

Hier wird der Begriff „Bereich“ anstatt „Domäne“ verwendet, um der Verwechslung der „Focus Areas“ mit den „Domains“ vorzubeugen. Tatsächlich werden aber auch die in [ITGI07] ausgewiesenen Focus Areas in unterschiedlicher Literatur, wie beispielsweise in [Goek07] als Domänen aufgefasst – sogar in der CobiT-nahen Literatur [ITGI03].

Weiters werden laut [IMPA05] auch die Themen Reifegradmodelle, Architektur und Informationssicherheit angesprochen, welche bei näherer Betrachtung von CobiT auch darin Eingang gefunden haben. Das Reifegradmodell in CobiT hilft, die Reife von Prozessen zu bestimmen und diese dadurch zu überwachen und zu steuern. „Architektur“ ist insbesondere als Querschnitt zu „Strategic Alignment“ und „Resource Management“ zuzuordnen, wobei „Informationssicherheit“ insbesondere in „Risk Management“ Beachtung findet. Es sei an dieser Stelle wie in [IMPA05] auf die Bedeutung von finanziellen Gesichtspunkten hingewiesen, deren Quelle die Unterneh-

mensziele sind und die über Strategie, Art, Qualität und Quantität der Ressourcen bestimmen.

In [Rüte06] werden zusätzlich noch IT-Portfoliomanagement und IT-Sourcing, welche beide strategische Gesichtspunkte inkorporieren, als *Entscheidungsdomänen* bezeichnet. Sourcing ist auch ein Thema in „Resource management“.

Die in CobiT als *Domänen* ausgewiesenen Begriffe<sup>9</sup> sind

- Planung und Organisation (Plan and Organise)
- Beschaffung und Implementierung (Acquire and Implement)
- Betrieb und Unterstützung (Deliver and Support)
- Überwachung und Bewertung (Monitor and Evaluate).

Diese bilden mit ihren Prozessen einen Querschnitt über die Focus Areas. Deren Prozesse werden im nächsten Kapitel zwecks eines tieferen Einblicks aufgelistet.

IT Governance on One Page führt als *Entscheidungsdomänen* „IT Principles“, „IT Architecture“, „IT Infrastructure Strategies“, „Business Application Needs“ und „IT Investment“ an. Die „IT Principles“ behandeln die strategische Komponente im Speziellen.

### 3.7 Prozesse

Wie im letzten Abschnitt erwähnt, ist auch dieser Abschnitt stark an das bedeutende CobiT-Framework angelehnt.

Im letzten Abschnitt wurden unter anderem die in CobiT definierten Domänen in aller Kürze präsentiert. CobiT legt für jede dieser Domänen eine gewisse Anzahl unterschiedlicher *Prozesse* fest.

---

<sup>9</sup> Sinngemäße Übersetzung nach [Goek06].

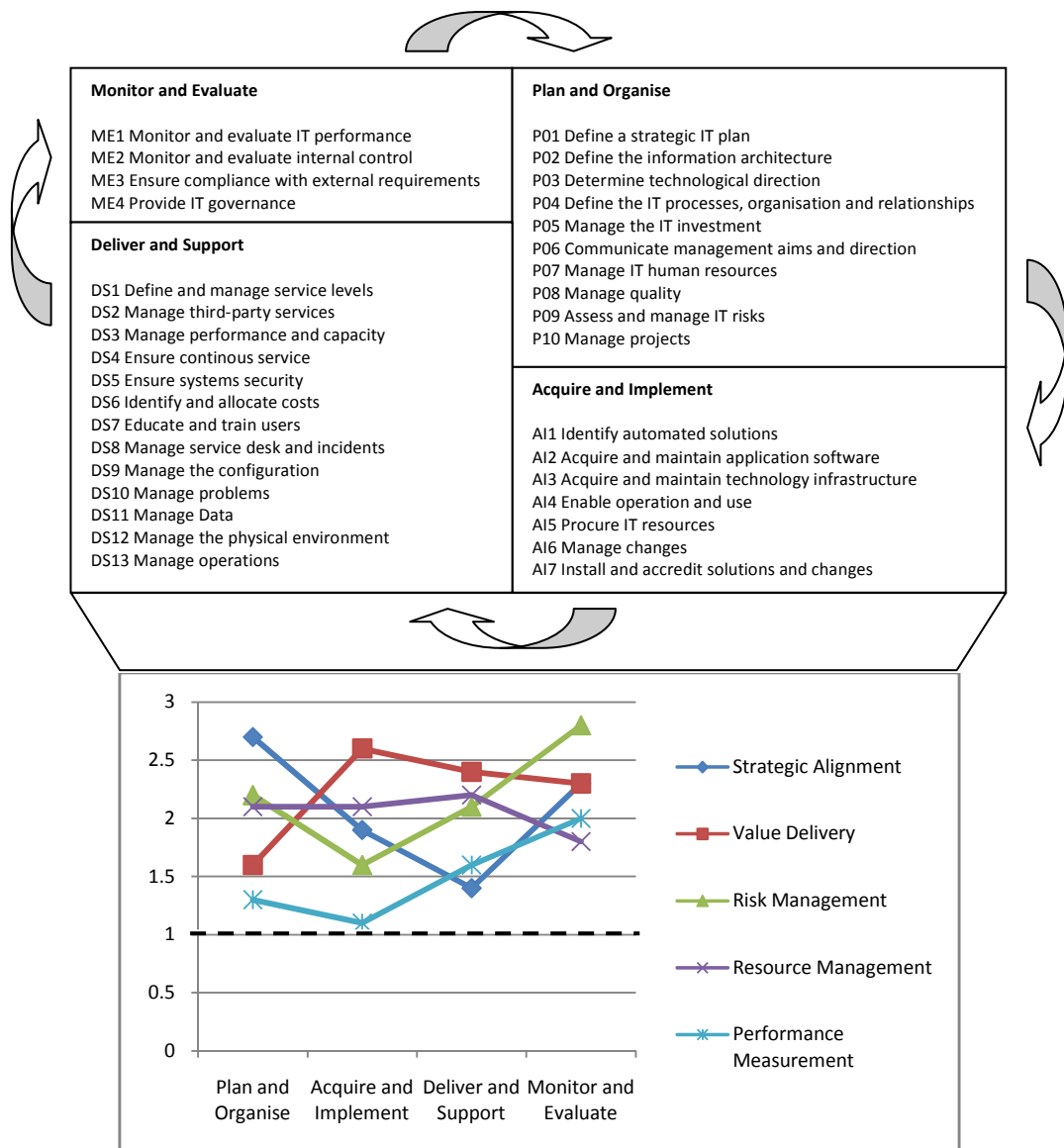


Abbildung 3.3: CobiT-Prozesse in der jeweiligen Focus Area und die Adressierung der Focus Areas in den IT-Governance-Domains (basierend auf [ITGI07])

In Abbildung 3.3 sind die in CobiT definierten Prozesse der einzelnen Domänen zu erkennen. CobiT sieht den Durchlauf der Prozesse als iterativen Vorgang, ähnlich zu beispielsweise PDCA. Jeder Prozess adressiert Focus Areas mehr oder weniger stark. Diese Stärke wird in Abbildung 3.3 durch das in der Mitte dargestellte profilartige Diagramm, in dem die Prozesse zu ihren zugehörigen Domains aggregiert werden, zum Vorschein gebracht. Auf drei Weisen können diesem Diagramm Informationen entnommen werden. *Erstens* betrachtet man jede Domäne für sich alleine. Dabei erkennt man, dass in „Plan and Organise“ besonders die Focus Area „Strategic Alignment“ ein Thema ist. Bei „Acquire and Implement“ und „Deliver and Support“ ist es die „Value Delivery“ und bei „Monitor and Evaluate“ ist es „Risk Manage-

ment". *Zweitens* betrachtet man die Adressierung im Verlauf des Kreislaufs. Man erkennt, dass „Strategic Alignment“ zu Beginn an der Spitze der Betrachtung steht, dann absinkt und bei der letzten Domain im Kreislauf wieder an Bedeutung gewinnt. „Value Delivery“ spielt hingegen beim Planen und Organisieren eine untergeordnete Rolle, dafür in den nächsten Focus Areas eine sehr wichtige. „Risk Management“ gewinnt insbesondere mit den zwei letzten Domains an Bedeutung. „Resource Management“ spielt in allen bis auf die letzte Domain eine große Rolle. Ähnlich wie mit „Risk Management“ verhält es sich auch mit „Performance Measurement“. Es erscheint intuitiv logisch, dass die Messung der Performance ihren Höhepunkt in „Monitor and Evaluate“ erreicht. *Drittens* betrachtet man die Gesamtlage der Linien der einzelnen Focus Areas. Dabei ist die hohe Bedeutung, die der Focus Area „Value Delivery“ zugesprochen wird, zu erkennen. Wenngleich sicherlich nicht unwichtig, so hat „Performance Measurement“ nicht die höchste Priorität. Verdeutlicht wird dies durch die Annahme, die Konzentration läge nur auf der Performance Messung. Performance Messung ohne zumindest zu versuchen, Wert zu generieren, ist zwecklos. Durch die starke Adressierung von „Value Delivery“ wurde versucht, das Denken, IT als reinen Kostenverzehr oder gar als Kostentreiber anzusehen, zu verbannen und den Blick auf die Wertgenerierung durch IT zu lenken. Folgende vereinfachte Annahmen für die angestellten Berechnungen wurden getroffen: alle Prozesse unterscheiden sich in keiner Weise außer durch das adressierte Thema, evtl. Domain und Focus Area. (Beispielsweise wurden keinerlei Gewichtungen vorgenommen.) Es sei angemerkt, dass 1 die unterste Bewertung ist und 3 die höchste. 0 wurde nicht zur Bewertung vergeben, da in manchen Prozessen doch ein gewisser Bezug, wenngleich auch ein geringer, zu der gerade betrachtenden Focus Area bestehen kann.

Zu einer vollständigen Prozessbeschreibung gehören selbstverständlich auch der Input und der Output der Prozesse. Dies ist hier allerdings nicht das Ziel und würde auch bezüglich des Detaillierungsgrades aus dem Rahmen dieser Arbeit fallen.

Die im Framework dargelegten *Informationskriterien* „Effectiveness“, „Efficiency“, „Confidentiality“, „Integrity“, „Availability“, „Compliance“ und „Reliability“ stellen Anforderungen des Geschäfts an Informationen dar. Die Bedeutung für den jeweiligen Prozess ist [ITGI07] (CobiT) ebenfalls zu entnehmen.

In [Buch05] schenkt man besonders dem IT-Innovationsmanagement, der IT-Projektplanung und -steuerung und dem IT-Controlling, die dort als IT-Governance-Prozesse definiert sind, besondere Aufmerksamkeit. IT-Innovationsmanagement findet zyklisch in größeren Abständen unter Anwendung eines Top-down-Ansatzes statt, welcher das gesamte Unternehmen betrachtet, und unter einem Bottom-up-Ansatz, der die Tochter- und Beteiligungsgesellschaften betrachtet. Bei der IT-

Projektplanung und –steuerung geht es insbesondere um die aufeinander abgestimmte Koordination mehrerer Projekte im Sinne eines unternehmensweiten Projektportfolios. Der IT-Controlling-Prozess lenkt den Blick auf Nutzen und Kosten. Hinsichtlich des Nutzens gilt es, *Performanceindikatoren* zwecks der Ermittlung der Qualität der IT zu finden.

Eine kurze Einführung zu „IT Governance on One Page“ wurde schon im Abschnitt 3.5.2 gegeben. Weill und Ross konzentrieren sich allerdings nicht auf konkrete Prozesse. Es werden mehr die Bereiche und Organisationsstrukturen adressiert, welche adäquate Prozesse beinhalten sollen [Weil04].

### 3.8 Rollen und Verantwortlichkeiten

In [PWC07] werden als Triebkraft die (Top-)Führungskräfte für IT-Governance erachtet, welchen Tenor die Literatur im Allgemeinen wiedergibt. Es stellt sich die Frage auf welcher Ebene agiert wird, was und wie etwas in Angriff genommen wird und ob dies zentral oder dezentral erfolgt.

Unternehmen hinterlassen einen bestimmten Abdruck in der *Matrix* von IT Governance on One Page, die Abbildung 3.4 zu entnehmen ist.

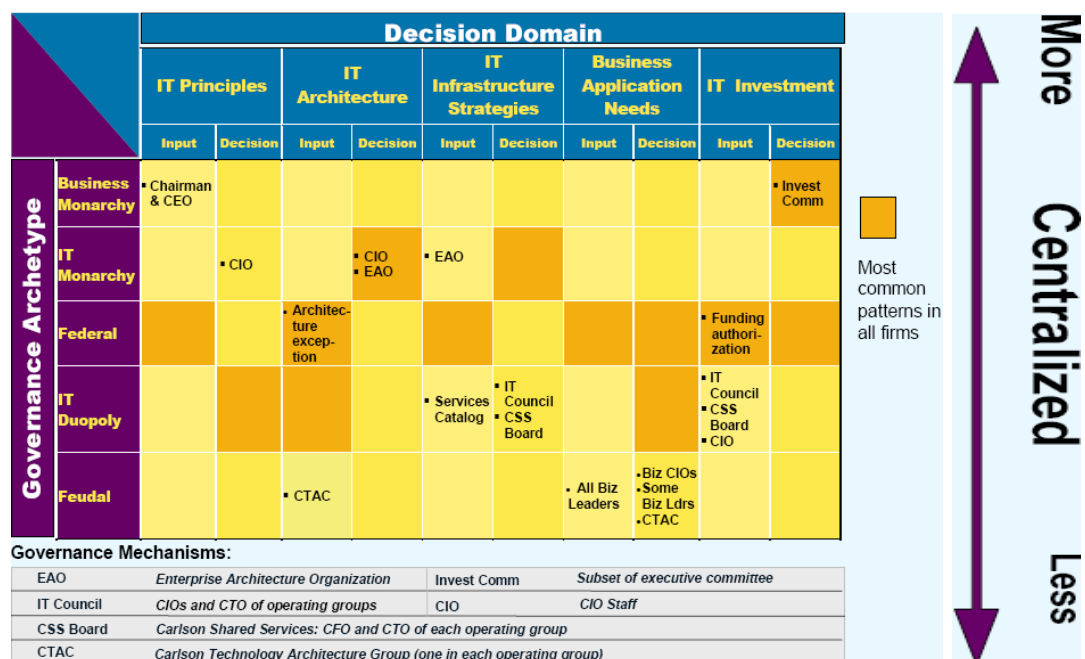


Abbildung 3.4: IT Governance on One Page<sup>10</sup> [Weil04]

Die Analyse unterschiedlicher Firmen anhand dieses Frameworks durch das MIT Sloan Center for Information Systems Research zeigte, dass Firmen mit Fokus auf

<sup>10</sup> „all firms“ in Abbildung 3.4 bezieht sich auf alle Firmen der Carlson Companies.

ROE<sup>11</sup>, ROI<sup>12</sup> und der Profit Margin (Net Income/Net Sales Revenue) eine eher zentralisierte, Firmen mit Fokus auf Wachstum gemessen an der prozentuellen Veränderung des Jahresumsatzes eine eher dezentralisierte und Firmen mit Fokus auf ROA<sup>13</sup> eine hinsichtlich des Zentralisierungsgrads hybride Governance betreiben.

Das Senior Management muss jedenfalls im Sinne einer guten IT-Governance die Vor- und Nachteile von Synergien und Autonomien abwägen und seine Entscheidungen im gesamten Unternehmen umsetzen und umsetzen lassen. Weiters muss die Organisationsstruktur festgelegt und immer wieder verbessert werden, um die Unternehmensziele optimal zu unterstützen. Management Teams müssen IT-bezogene Verhaltensweisen auch innerhalb der Organisationsstruktur steuern, denn neue Anforderungen an die Governance bedeuten nicht immer eine Veränderung der Organisationsstruktur. Bedeutend ist auch das organisationsweite Lernen.

Dieses Framework hebt besonders den strategischen Fokus der IT-Governance hervor. Dennoch ist die Implementierung der IT-Governance auch mit taktischen und operativen Tätigkeiten verbunden.

Abbildung 3.6 zeigt die Stärke der Adressierung der einzelnen *Rollen* im CobiT-Framework, welche auf der Nennung in den einzelnen Prozessen und Tätigkeiten basiert. Es ist die Bedeutung des oberen Managements zu erkennen, welches vor allem in der Domain „Plan and Organise“ tätig ist. Stark operationale Rollen wie der Problem Manager werden in dieser Domain weniger angesprochen. Beispielsweise inkorporiert der Project Management Officer (PMO) aber auch operationale Komponenten. Die stärkste Rolle in der Überwachung ist der CIO. Die große Bedeutung von Compliance, Kontrolle, Risikokontrolle und Sicherheit wird durch die Größe des Balkens für die Rolle bzw. Funktion von „Compliance, Audit, Risk, Security“ hervorgehoben.

---

<sup>11</sup> Return on Equity (Eigenkapitalrentabilität)

<sup>12</sup> Return on Investment (Gesamtkapitalrentabilität)

<sup>13</sup> Return on Assets

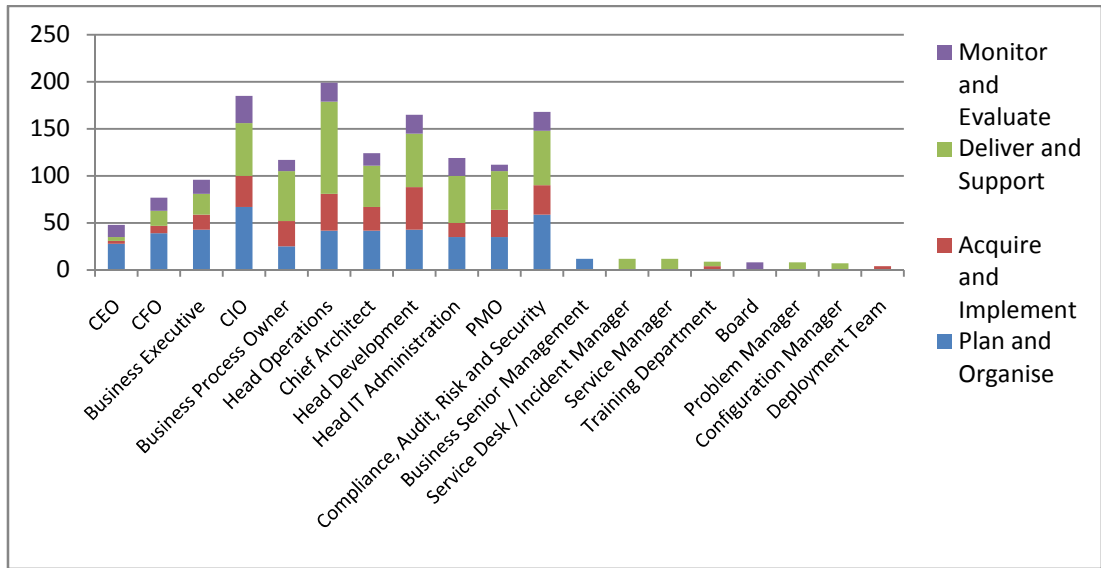


Abbildung 3.5: Rollen, CobiT-Domains nach [ITGI07] und Relevanz der einzelnen Domains für die jeweilige Rolle (y-Achse: absolute Anzahl der Nennungen)

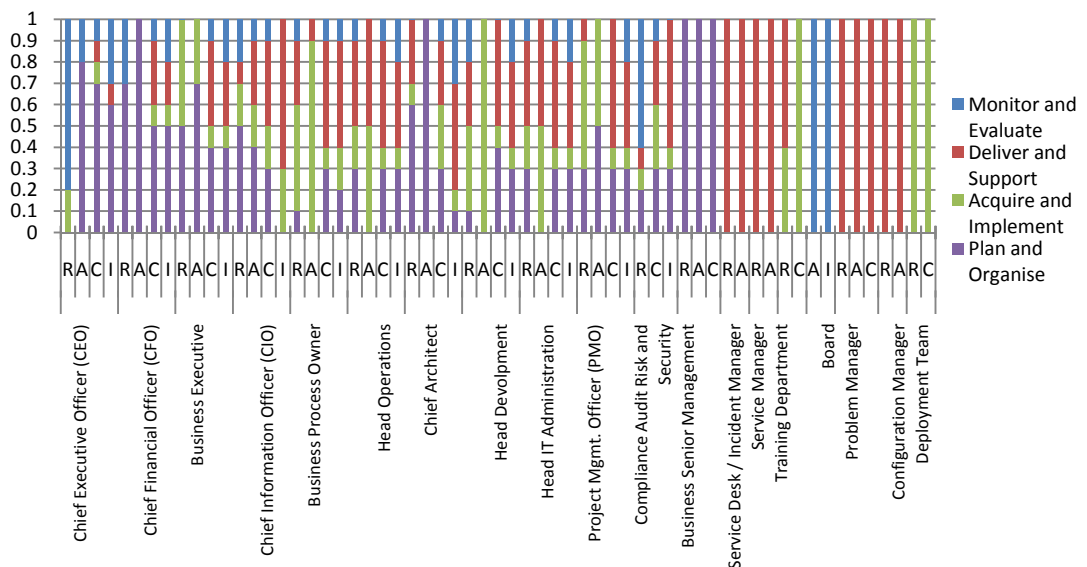


Abbildung 3.6: Rollen, RACI-Eigenschaften, CobiT-Domains nach [ITGI07] und Relevanz der einzelnen Domains für die jeweilige Rolle und RACI-Eigenschaft pro Rolle

Das Akronym RACI steht für Responsible (= verantwortlich für die Durchführung einer Tätigkeit), Accountable (= trägt Verantwortung), Consulted (= beratend/wird befragt), Informed (= wird informiert). Abbildung 3.6 zeigt die in CobiT erwähnten Rollen mit den RACI-Eigenschaften pro Domain. Diese Abbildung lässt erkennen, welche grob granulierten Verantwortlichkeiten (RACI) die einzelnen Rollen pro Domain besitzen. Beispielsweise nimmt der CEO hat vorwiegend planende, organisierende und überwachende Aufgaben. Der CIO nimmt in allen Domänen Aufgaben wahr. Unterschiede gibt es im Vergleich der RACI-Eigenschaften.



[ITGI03] adressiert insbesondere das Top-Management, das IT Strategy Committee, den CEO, den CIO und das Linienmanagement. Alle haben Verantwortlichkeiten in allen Focus Areas. Nach *Rollen* und allgemeinen *Tätigkeitsarten* zusammengefasst ergeben sich in Tabelle 3.3 folgende Verantwortlichkeiten:

CEO	<p><b>Bereitstellung / Gestaltung</b></p> <ul style="list-style-type: none"> <li>– IT-Strategie und –Betrieb an Unternehmenszielen ausrichten und integrieren und auf Organisation abstimmen</li> <li>– Steuerung der Optimierung der IT-Kosten</li> <li>– Zuweisung von Ressourcen</li> <li>– Gestaltung von Organisationsstrukturen und Verantwortlichkeiten unterstützen</li> <li>– (letzter Punkt auch im Risk-Management)</li> <li>– Anwendung von Frameworks im Governancebereich</li> </ul>	<p><b>Sicherstellung</b></p> <ul style="list-style-type: none"> <li>– Abstimmung - Geschäft und Technologie</li> <li>– IT-Kostenverantwortung etablieren und für Erfassung der IT in Finanzberichterstattung sorgen</li> <li>– Reale IT Investitionspläne gewährleisten</li> <li>– Maximierung von Information und Wissen in der Organisation</li> <li>– Einfluss des CIO gewährleisten</li> </ul>	<p><b>Überwachung</b></p> <ul style="list-style-type: none"> <li>– Risiken überwachen</li> </ul> <p><b>Bewertung</b></p> <ul style="list-style-type: none"> <li>– Evaluation von Performance, Kontrolle, Risiken und Investitionen</li> </ul>
Top-Management	<p><b>Bereitstellung / Gestaltung</b></p> <ul style="list-style-type: none"> <li>– Bereitstellung von Investitionen für Wachstum</li> <li>– Überwachung der High-Level-Performance der IT festlegen</li> </ul> <p><b>Sicherstellung</b></p> <ul style="list-style-type: none"> <li>– Sicherstellung eines effektiven Planungsprozesses durch das Management</li> <li>– Ausrichtung der IT-Organisationsstrukturen an Kerngeschäft</li> <li>– Sicherstellung der Definition der Prozesse und Vorgaben für Focus Area</li> </ul>	<p>– Sicherstellung nach ausgewogenem Risiko- / Nutzenverhältnis bei Investitionen</p> <p><b>Freigabe</b></p> <ul style="list-style-type: none"> <li>– Freigabe der Ausrichtung zwischen Kerngeschäft und IT-Strategie</li> </ul> <p><b>Überwachung</b></p> <ul style="list-style-type: none"> <li>– Überwachung des Management bei der Bedarfsermittlung und –ausrichtung an Zielen</li> </ul>	<ul style="list-style-type: none"> <li>– High-Level-Performance der IT</li> </ul> <p><b>Bewertung</b></p> <ul style="list-style-type: none"> <li>– Überwachung der IT-Risiken durch Management</li> <li>– Leistungen der IT-Strategien und des Top-Managements</li> </ul>

IT Strategy Committee	<p><b>Bereitstellung / Gestaltung</b></p> <ul style="list-style-type: none"> <li>– Vorgabe der strategischen Ausrichtung</li> <li>– Vorgabe für IT-Ressourceneinsatz</li> </ul> <p><b>Sicherstellung</b></p> <ul style="list-style-type: none"> <li>– Sicherstellung der strategischen Ausrichtung</li> </ul>	<ul style="list-style-type: none"> <li>– Etablierung gemeinsamer Verantwortung für IT-Kosten</li> <li>– Sicherstellung der Ressourcen für ein angemessenes Risikomanagement</li> </ul> <p><b>Überwachung</b></p> <ul style="list-style-type: none"> <li>– Überwachung Bestätigung des maximalen Wertbeitrags durch IT</li> </ul>	<ul style="list-style-type: none"> <li>– Überwachung der Finanzierung der IT</li> <li>– Review der Bewertung der Performance</li> </ul>
CIO	<p><b>Bereitstellung / Gestaltung</b></p> <ul style="list-style-type: none"> <li>– Erstellung und Umsetzung IT-Strategie, IT-Standards und Policies</li> <li>– Ausbildung des Linienmanagements</li> <li>– Definition und Erhöhung des Wertbeitrags</li> <li>– Budget mit Zielvorgaben abgleichen</li> <li>– Klarer Rahmen für IT Projektmanagement</li> <li>– Bereitstellung der IT-Infrastruktur und Ressourcen</li> </ul>	<ul style="list-style-type: none"> <li>– Einführung und Verbesserung des IT-Kontroll-Frameworks</li> <li>– Implementierung eines Messmechanismus<sup>14</sup> für die Performance</li> </ul> <p><b>Sicherstellung</b></p> <ul style="list-style-type: none"> <li>– Wertgenerierung sicherstellen</li> <li>– Einhaltung der Budgetvorgaben</li> <li>– Angemessene Rollen für Wertmaximierung</li> <li>– Standardisierung der Architektur und Technologie</li> </ul>	<ul style="list-style-type: none"> <li>– Sicherstellung der Rol- lendefinition und – Besetzung für IT- Risikomanagement</li> <li>– Verifikation von IT- Prozessen und Kontrol- len</li> </ul> <p><b>Bewertung</b></p> <ul style="list-style-type: none"> <li>– Bewertung von Risiken</li> </ul>

<sup>14</sup> Z. B. (IT) Balanced Scorecard

Linienmanagement		
<b>Bereitstellung / Gestaltung</b> <ul style="list-style-type: none"> <li>– Verständnis über IT Infrastruktur schaffen</li> <li>– Definition der Anforderungen des Kerngeschäfts</li> <li>– Sponsoring für IT-Projekte</li> <li>– Beschaffung neuer IT Services</li> <li>– Zuweisung von Ressourcen für effektive IT-Governance</li> <li>– Durchführung von Business Impact Assessment</li> </ul>	<b>Freigabe</b> <ul style="list-style-type: none"> <li>– Freigabe von Service Levels</li> <li>– Freigabe der Messmechanismen<sup>15</sup></li> </ul> <b>Überwachung</b> <ul style="list-style-type: none"> <li>– Überwachung von Service Levels</li> <li>– (auch im Performance Management)</li> </ul>	<b>Bewertung</b> <ul style="list-style-type: none"> <li>– Bewertung des operativen Nutzens durch IT-Investitionen</li> </ul>
		Strategic Alignment Value Delivery IT Resource Management Risk Management Performance Management

Tabelle 3.3: Tätigkeiten nach Kategorien und Rollen (basierend auf [ITGI03])

---

<sup>15</sup> Z. B. (IT) Balanced Scorecard

Die oben aufgelisteten Tätigkeiten, geordnet nach unterschiedlichen Kategorien wurden mit Farben für die jeweilige Focus Area unterlegt. Die Unterlegung mit Farben dient rein der Zuordnung und hat nicht den Zweck, durch größere Flächen eine höhere Bedeutung für die jeweilige Rolle oder Rollenkategorie und Tätigkeitskategorie zu konstatieren.

In [ITGI03] werden auch noch das “IT Steering Committee”, “Technology Council” und “IT Architecture Review Board” mit ihren Tätigkeiten beschrieben. Jene Rollenkategorien bzw. Vereinigungen von Rollen haben einen unterstützenden Charakter für das Executive Management und den CIO. Das CIO Project Office, Architekten, Technologieverantwortliche oder andere übernehmen die Koordination des IT Steering Committee, Technologie Council und IT Architecture Review Board. Das IT Steering Committee befasst sich insbesondere mit dem Projektportfolio in den unterschiedlichen Focus Areas. Das Technology Council ist gemäß seines Namens für technologische Belange zuständig, wobei ebenfalls immer der Blick auf das Geschäft gerichtet bleibt. Dabei erstellt es Richtlinien, nimmt eine beratende und lenkende Position ein. Die Aufgaben des IT Architecture Boards beinhalten ebenfalls das Erstellen von Richtlinien für Architekturen und die Ausübung einer beratenden und lenkenden Tätigkeit.

[Rüte06] ordnet in Abbildung 3.7 Rollen und Verantwortlichkeiten folgendermaßen ein:

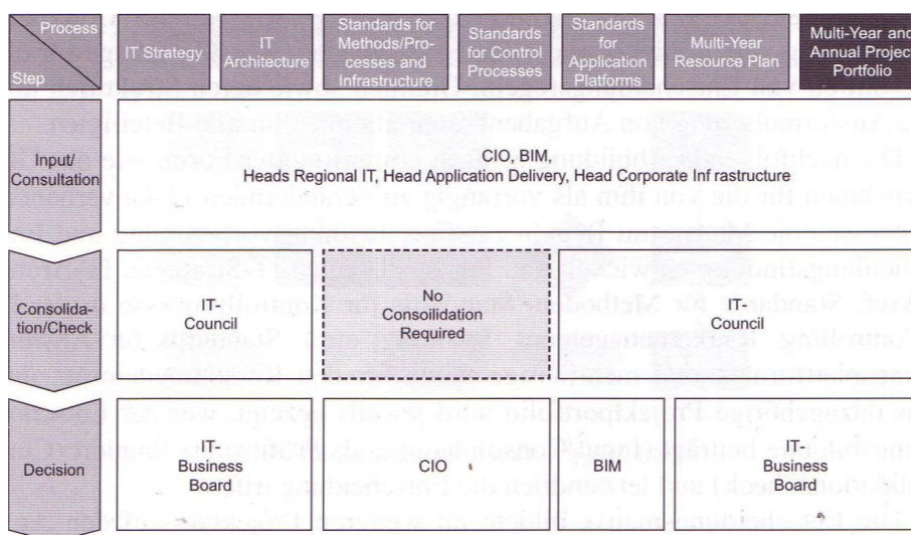


Abbildung 3.7: Rollen und Verantwortlichkeiten (basierend auf [Rüte06])

## Kapitel 4

# Vergleich von IT-Management und IT-Governance

Nachdem dem/der LeserIn einen Einblick in IT-Management und IT-Governance gegeben wurde, werden die zwei Teile nun über ihre Unterschiede zu einem synergetischen Gebilde zusammengeführt.

### 4.1 Unterschiede

Eine Trennlinie zwischen IT-Management und IT-Governance zu ziehen ist aufgrund der fließend verlaufenden Grenzen keine leichte Aufgabe. Beim Studium der Literatur findet der/die LeserIn wiederholt eine Propagierung von IT-Governance als Teil des IT-Managements vor, aber auch gegenteilige Sichtweisen sind implizit vorzufinden.

Erwähnt sei an dieser Stelle, dass im Falle der ersteren Sichtweise mit „IT-Management“ die höheren Funktionen in der IT gemeint sind [Rüte06], [Tiem06]. Hierbei fallen somit auch beispielsweise der CIO darunter, der vor allem im Bereich IT-Governance eine Rolle spielt.

[Tiem06] geht sogar noch weiter und erwähnt CobiT als Referenz-Prozessmodell für IT-Governance unter der Überschrift „Referenz-Prozessmodelle für IT Service Management“. CobiT spricht zwar auch das Service Management an, da die Serviceorientierung populär geworden ist, aber der Fokus liegt nicht alleine darauf. In [Rüte06] und [Goek07] wird ITIL auch als relevantes Modell für IT-Governance erwähnt. Dem ist teilweise zuzustimmen. Schließlich behandelt die Business Perspective in ITIL explizit auch IT-Governance. Der/die LeserIn wird immer wieder auch auf Standards wie den ISO/IEC 17799 im Rahmen von IT-Governance stoßen, wie in

[Goek07], welcher Umstand einmal mehr die enge Verzahnung von IT-Governance und IT-Management aufzeigt. Während CobiT vor allem auf der Effektivitätsebene eine Rolle spielt, ist ITIL auf der darunterliegenden Effizienzebene tätig [Goek07].

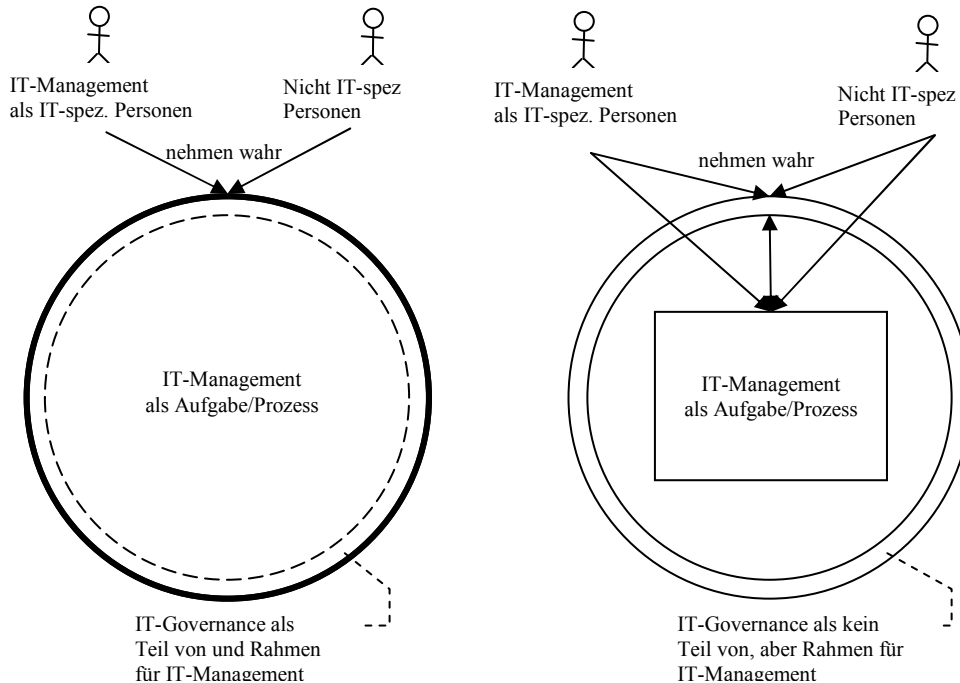


Abbildung 4.1: Zwei Sichtweisen über die Einordnung von IT-Management und IT-Governance

Abbildung 4.1 lässt die beiden unterschiedlichen *Sichtweisen* erkennen. In der einen ist IT-Governance ein Teil von IT-Management und in der anderen nicht, wobei jedoch in beiden Fällen IT-Governance den Rahmen für IT-Management bildet. IT-Management und IT-Governance kann von verschiedenartigen Personen betrieben und unterstützt werden. Beispielsweise zählt der CIO zur jeweils linken Gruppe der Personen und der CEO tendenziell zur rechten. Bei diesen Gruppen sind sowohl führende als auch nicht führende Manager integriert, wobei die nicht führenden bei IT-Governance nicht die Hauptrolle darstellen und mehr taktische und operationale Handlungen durchführen. Die folgende Formulierung für die rechte Darstellung macht die Bedeutung der Unterscheidung zwischen IT-Management als Gruppe von Personen und IT-Management als Aufgabe/Prozess deutlich „Das IT-Management nimmt IT-Governance-, aber auch IT-Managementspezifische Aufgaben wahr“. Obwohl nach der Denkweise in der rechten Darstellung IT-Management und IT-Governance nicht eins sind, so wird beides vom IT-Management wahrgenommen. In der Praxis spielen die obigen unterschiedlichen Sichtweisen keine große Rolle. Jedoch sind sie für die Unterscheidung zwischen IT-Management und IT-Governance

von Bedeutung. Entweder es wird nach der linken Darstellung IT-Governance und IT-Management (überlappend) oder IT-Governance und restliches IT-Management (disjunkt) verglichen oder nach der rechten Darstellung IT-Governance und IT-Management (disjunkt), was zweiterem gleichkommt. Zur Erweiterung der Abbildung 4.1 kann man sich noch die Corporate Governance als allumfassenden Rahmen vorstellen.

In Abschnitt Teilbereiche 2.4 wird IT-Rechtsmanagement als Teil des IT-Managements genannt, wobei dies jedoch nicht mit Compliance zu verwechseln ist. IT-Rechtsmanagement bewegt sich einerseits auf einer anderen Ebene wie auch Tabelle 4.1 verdeutlichen wird, aber auch die Tätigkeitsarten sind teils unterschiedliche wie beispielsweise das Management von Verträgen.

IT-Portfoliomanagement, welches in Abschnitt 2.4 ebenfalls zu IT-Management gezählt wurde, wird in [Rüte06] hingegen als IT-Governance-Entscheidungsdomäne erwähnt. Der Begriff „Entscheidungsdomäne“ hilft aus den Zuordnungsschwierigkeiten. IT-Portfoliomanagement gehört zum strategischen Teil des IT-Managements, jedoch müssen auch Entscheidungen hinsichtlich Governance-Mechanismen für diesen Bereich getroffen werden.

Ähnliches gilt für IT-Ressourcen-Management, welches allerdings in [Rüte06] nicht als IT-Governance-Entscheidungsdomäne eingeordnet wird.

In Abbildung 3.3 sind auch ITIL-verwandte Rollen zu erkennen. Allerdings liegt der Fokus bei CobiT nicht auf diesen Rollen. Sie zeigt aber die enge Verzahnung von CobiT und ITIL sowie IT-Governance und IT-Management.

In Tabelle 4.1 und weiteren Ausführungen wird zur Unterscheidung die rechte Darstellung in Abbildung 4.1 herangezogen, da diese eine klarere Linie zwischen IT-Management und IT-Governance zu ziehen erlaubt und ebenso wie die linke Darstellung von der Literatur unterstützt wird.



Tabelle 4.1 zeigt qualitativ wesentliche *Unterschiede* zwischen IT-Management und IT-Governance auf.

	<b>IT-Management</b>	<b>IT-Governance</b>
<b>Normativ/ Strategisch/Taktisch/Operational</b>	vor allem taktisch/operational	vor allem strategisch, aber auch normativ und taktisch
<b>Detailheitsgrad</b>	höher	niedriger
<b>Lokalität</b>	höher	niedriger <sup>16</sup>
<b>IT-Strategie</b>	Gestaltung/Umsetzung	Gestaltung
<b>Geschäftsorientierung<sup>17</sup></b>	intern	intern/extern
<b>Zeitorientierung<sup>18</sup></b>	Gegenwart	Gegenwart/Zukunft
<b>Hebelwirkung IT Alignment</b>	tendenz. etw. geringer	tendenz. etw. höher
<b>Fokus</b>	Erreichung der Unternehmensziele, Umsetzung der IT-Governancevorgaben, Umsetzung der IT-Strategie, Effizienz, Continuity, Rahmenbedingungen optimal nutzen, IT Service Management, direkter Kontakt zu Kunden, IT Verwaltung, Direkte Wertgenerierung,	Strategie IT-Alignment, High-Level-Zielsetzung, (Risiko-)Kontrolle, Audit, Regulierung, Compliance, Rahmen, Richtlinien, Organisationskultur, Organisationsstruktur, organisationsweite (Performance-)Messung, Setzung organisationsweite IT-Ziele, Effektivität
<b>Hierarchieebenenadressierung</b>	insbes. mittleres und unteres Management <sup>19</sup>	höhere Ebenen
<b>Rollenanzahl</b>	höher	niedriger
<b>Gesetzadressierung</b>	niedriger	höher
<b>Anzahl Frameworks Empfehlungen u. Vorschriften</b>	höher	niedriger
<b>ungefährer anfänglicher Zeitraum stärkerer Beachtung</b>	90er Jahre	90er Jahre <sup>20</sup>

Tabelle 4.1: High-Level-Unterschiede zwischen IT-Management und IT-Governance

<sup>16</sup> Organisationsweit; was „Organisation“ im Konkreten bedeutet, hängt von der Implementierung der IT-Governance ab (vgl. [Weil04]).

<sup>17</sup> Speziell nach [Grem04].

<sup>18</sup> Speziell nach [Grem04].

<sup>19</sup> Ausgenommen CIO, der ebenfalls eine Rolle spielt.

<sup>20</sup> Jedoch später und in geringerer Intensität als IT-Management.

Laut [Rüte06] adressiert CobiT auch das *strategische* Management, wobei ITIL insbesondere in das *taktische* und *operative* Management fällt. Wird die Grafik aus [Rüte06] herangezogen, die in Abbildung 4.2 inhaltlich wiedergegeben wird, so erkennt man, dass IT-Governance sich insbesondere mit den strategischen Belangen auseinandersetzt, wobei auch normative Tätigkeiten zu erkennen sind und IT-Management, wozu vor allem ITIL zählt, sich den taktischen und operativen Belangen widmet.

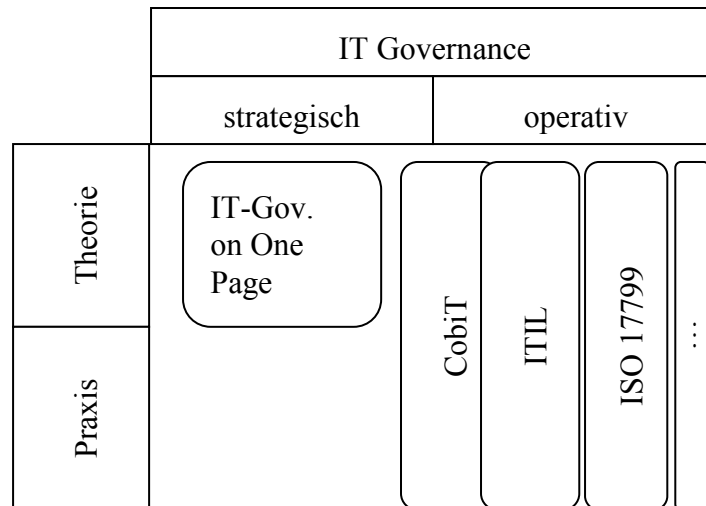


Abbildung 4.2: Zweidimensionale Einordnung unterschiedlicher Frameworks (basierend auf [Rüte06])

Wenn IT-Governance als Teil von IT-Management betrachtet werden soll, so gehört IT-Governance zum strategischen IT-Management. Diese Formulierung spricht implizit von einer strategischen Komponente des IT-Managements, bei welcher es sich nicht um IT-Governance handelt. Diese spiegelt sich insbesondere bei der Gestaltung der IT-Strategie wider.

Aufgrund der strategischen Komponente der IT-Governance wird auch weniger ins *Detail* gegangen; schließlich gibt es noch die taktische und operative Ebene.

Die *Lokalität* ist naturgemäß wiederum bei IT-Management höher und der Wirkungskreis bei IT-Governance tendenziell größer als bei IT-Management, wie Abbildung 4.1 vermuten lässt. Schließlich ist im taktischen/operativen Bereich die Kundennähe (oft) größer als im strategischen. Dies hängt auch von der Aufbauorganisation und vom Zentralisierungsgrad des betrachteten Unternehmens ab. Die notwendige Lokalität wird besonders bei internationalen Konzernen deutlich, die äußerst unterschiedliche Kundengruppen in unterschiedlichen Ländern ansprechen und im Sinne einer Individualisierung flexibel auf lokale Gegebenheiten reagieren müs-

sen. IT-Governance muss aber (vgl. [Weil04]) nicht komplett global sein, IT-Management ist aber dennoch oft etwas lokaler.

Für die *Strategien* sind die oberen Hierarchieebenen verantwortlich, die vor allem von den unteren umgesetzt werden. Es sei an dieser Stelle noch angemerkt, dass die Literatur einerseits den IT-Strategie gestaltenden Charakter der IT-Governance wiedergibt, aber auch die Bestimmung der IT-Governance durch die IT-Strategie (vgl. dazu bspw. [Rüte06], [Goek06], [Grem04]). Dieser Umstand deutet vermutlich auf die wechselseitige Beziehung zwischen IT-Governance und IT-Strategie hin. IT-Governancemechanismen beeinflussen einerseits die IT-Strategie, aber unterschiedliche Elemente der IT-Strategie machen unterschiedliche adäquate IT-Governancemechanismen notwendig. (Das strategische IT-Management ist auch an der Gestaltung der IT-Strategie beteiligt.)

Laut [Goek06] wird in Anlehnung an [Grem04] IT-Management und IT-Governance in die Dimensionen *Geschäfts-* und *Zeitorientierung* - wie in Abbildung 4.3 zu erkennen - eingeordnet.

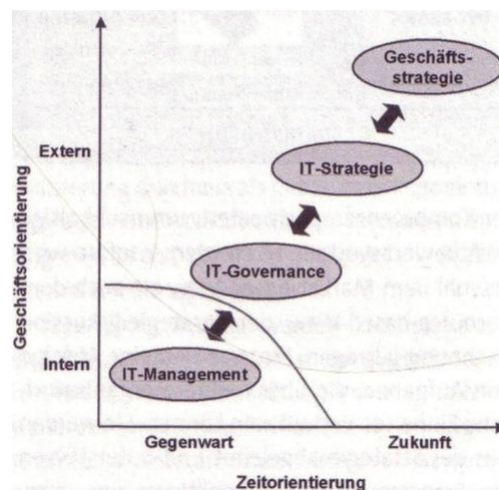


Abbildung 4.3: Einordnung von IT-Management und IT-Governance nach der Geschäftsorientierungs- und Zeitorientierungsdimension ([Goek06] in Anlehnung an [Grem04])

Die *Hebelwirkung* ist bildlich vor allem in Abbildung 4.6 zu erkennen. IT-Governance (und das strategische IT-Management) kann durch eine Handvoll Entscheidungen die IT auf den Unternehmenserfolg ausrichten (und damit auf die Unternehmensziele, vorausgesetzt diese unterstützen den Unternehmenserfolg) oder die Ausrichtung verfehlen. Strategisches IT-Management wurde wie oben angedeutet aufgrund von Erklärungsmaßnahmen des Unterschiedes zwischen IT-Management und IT-Governance nicht mehr extra erwähnt. In Abbildung 4.6 ist strategisches IT-Management etwas mehr links von „IT-Management“ zu sehen. Die IT-Produktion

hingegen kann, vorausgesetzt sie gibt ihr Bestes, nicht mehr allzuviel an der Ausrichtung ändern.

Wie aus dieser Arbeit hervorgeht werden bei IT-Governance insbesondere die oberen Hierarchieebenen adressiert. Ein ähnliches Ergebnis liefert [Hesc05] für CobiT und ITIL.

Da Hierarchien für gewöhnlich einer Pyramide ähneln, ist die *Rollenanzahl* in den mittleren bis unteren Hierarchieebenen höher.

*Gesetze und Regulative* sollten nie punktuell/lokal eingehalten werden; sie betreffen im Allgemeinen das gesamte Unternehmen und müssen daher im Sinne einer adäquaten (IT-)Governance beachtet werden und in den Strategien Eingang finden.

Aufgrund der Vielzahl an unterschiedlichen Tätigkeiten im IT-Managementbereich gibt es noch mehr *Frameworks, Empfehlungen* und *Vorschriften* unterschiedlichem Detaillierungsgrades.

Wie in der Einleitung dieser Arbeit erwähnt, hat die IT im Allgemeinen erst vor (relativ) kurzem einen durchdringenden Status mehr oder weniger unabhängig von der Branche des agierenden Unternehmens erhalten. Vergleicht man den Beginn der Publizierung heute wesentlicher Frameworks, Empfehlungen und Vorschriften, so sind vor allem die 90er Jahre als *Geburtsstunde* des heutigen sich immer weiter entwickelnden Verständnisses der IT zu nennen. Durch die Entwicklung von der technischen Konzentration zur Ausrichtung der IT am Geschäft, hatten am Anfang vor allem die reinen Techniker Kontrolle über das Geschehen, wobei vielfach nicht von ganzheitlichem Management die Rede war, was zu IT-Management und in weiterer Folge zu IT-Governance geführt hat.

## 4.2 Synergien

Gerade aus den Unterschieden zwischen IT-Management und IT-Governance entspringen deren Synergien.

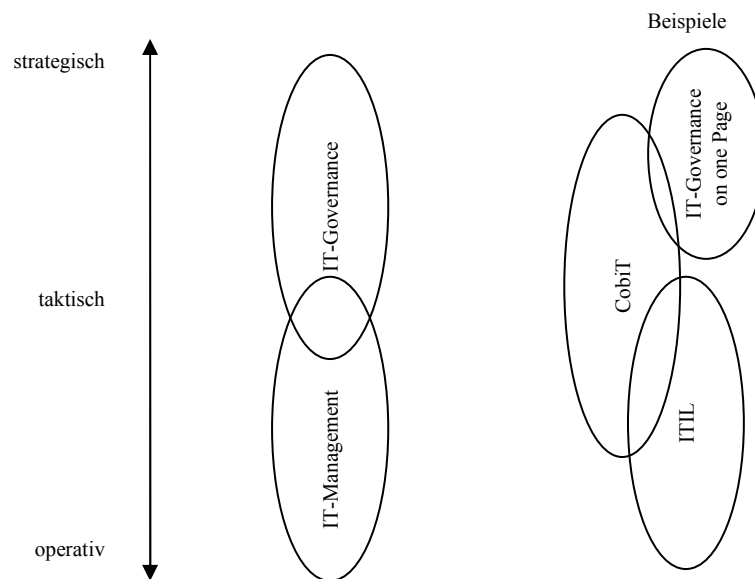


Abbildung 4.4: Einordnung von IT-Management und IT-Governance in der strategisch/taktisch/operativen Dimension (vgl. auch [Rüte06])

Abbildung 4.4 unterstreicht, dass die meisten Frameworks und Empfehlungen sich nicht gegenseitig ersetzen oder behindern [Goek07]. Ebenso ist es möglich, diese nur selektiv einzusetzen, das bedeutet nur Teile unterschiedlicher Frameworks und Empfehlungen zu implementieren. Unbestritten sind die Vorteile einer ganzheitlichen Sicht. Sollten durch die selektive Auswahl von Bereichen, Prozessen und Empfehlungen bestimmte in den Frameworks und Empfehlungen herangetragene Bereiche nicht durch jene behandelt werden, so wird angeraten, jene nicht durch Frameworks und Empfehlungen abgedeckten Bereiche durch andere Maßnahmen zu adressieren oder nur dann nicht näher zu behandeln, wenn diese tatsächlich eine untergeordnete Rolle spielen. Als Beispiel sei angemerkt, dass ITIL oft mit CobiT zum Einsatz kommt [Sox]. Auf [ITIL1] und in [ITGI06] ist deren Zusammenhang dargestellt und ein CobiT-ITIL-Prozessmapping zu finden.

IT-Governance ist eine IT-bezogene Erweiterung der Corporate Governance und damit auch auf diese abgestimmt. IT-Governance bildet den Rahmen um das IT-Management. IT-Management ohne IT-Governance bedeutet die Vernachlässigung eines ganzheitlichen (High-Level-)View und IT-Governance ohne IT-Management kommt einer leeren Hülle ohne Konkretisierungs- und Umsetzungskraft gleich, so dass IT-Governance zu einem Selbstzweck wird – ähnlich einem Staat ohne außerstaatliche unternehmensartige Gebilde.

In Abbildung 4.5 kann man ein weiteres Mal die iterative, prozessartige Verknüpfung von IT-Governance sowie IT-Management erkennen, welche rich-

tungsweisenden Charakter von IT-Governance sowie den umsetzenden des IT-Managements unterstreicht.

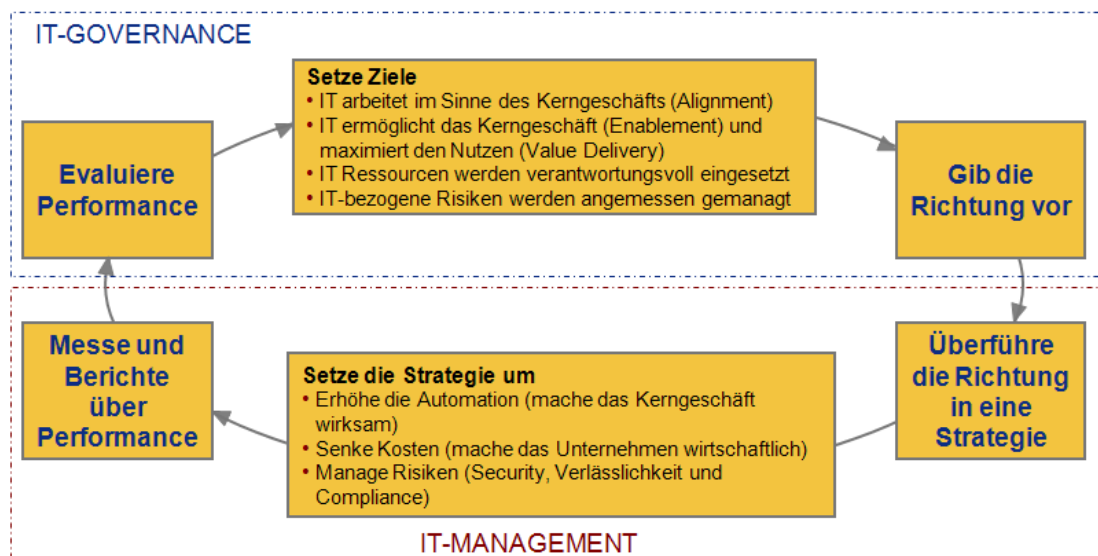


Abbildung 4.5: Synergie von IT-Governance und IT-Management [Hesc07]

Abbildung 4.6 hebt zum Abschluss wesentliche Unterschiede und Synergien in komprimierter Form hervor. Es sei jedoch an dieser Stelle angemerkt, dass diese Abbildung auf IT-bezogene Aspekte und Übersichtlichkeit abgestimmt ist. Es fehlen demnach vor allem Corporate Governance, das Business-Management und der Business-Produktionsbereich. Außerdem müsste der Unternehmenserfolg noch mehrere Andockmöglichkeiten haben, denn einen One-Best-Way gibt es im Allgemeinen nicht.

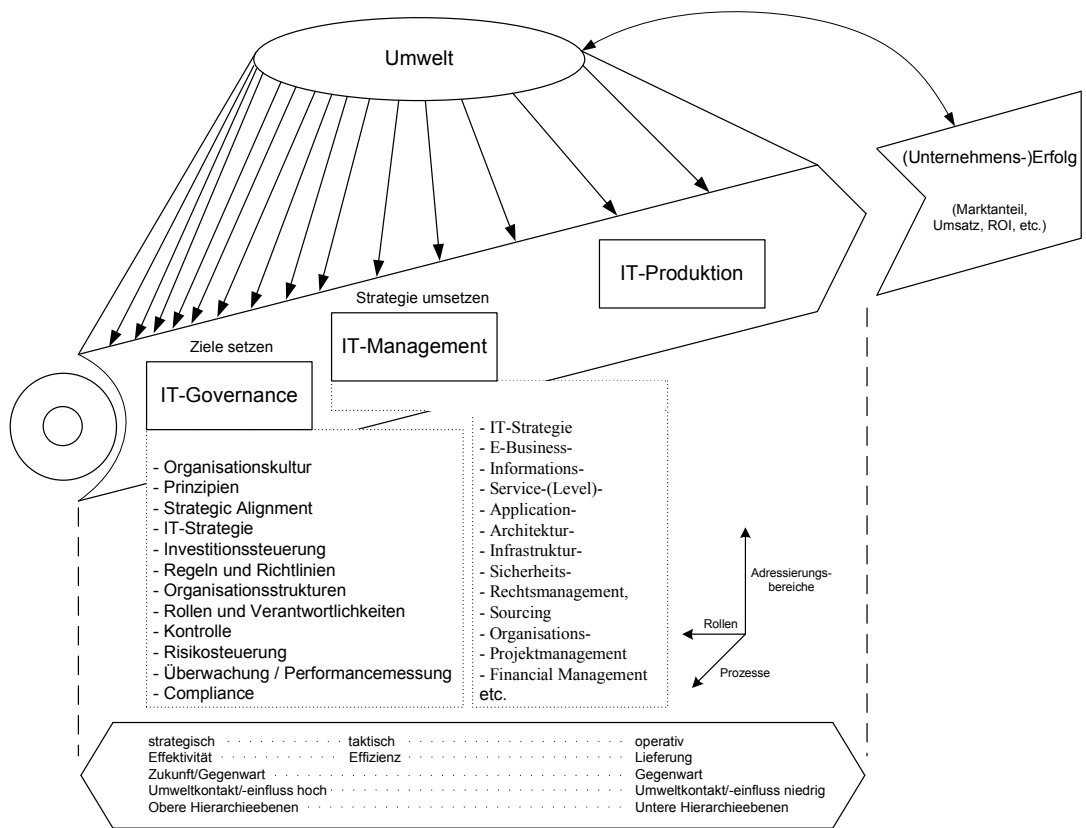


Abbildung 4.6: High-Level-View auf IT-Management und IT-Governance als synergistisches Gebilde  
(basierend auf [Hesc07], [Goek07])

## Kapitel 5

# Zusammenfassung

Die IT hat besonders in den letzten Jahren (wieder) einen Paradigmenwechsel vollzogen. IT wird heute im Umbruch zur Informations- und Wissensgesellschaft weitestgehend nicht nur als Rationalisierungsinstrument gesehen, sondern als Instrument von wertschaffendem Charakter, welches an den Business-Strategien und damit an den Unternehmenszielen und weiters am Unternehmenserfolg ausgerichtet ist.

Ziel dieser Arbeit war es, wesentliche Gegensätze und Gemeinsamkeiten der Themengebiete IT-Management und IT-Governance auf Basis der vorhandenen Literatur herauszuarbeiten und diese über ihre Unterschiede zu einem synergetischen Gebilde zu formen.

Nicht behandelt wurden detaillierte Methoden und Werkzeuge wie die Balanced Scorecard, SWOT, die GAP- oder Portfolioanalyse. Da es sich um eine theoretische Arbeit handelt, wurde auf konkrete Fallstudien und Beispiele verzichtet. Die Messung von IT-Management und IT-Governance, sowie die Standards selbst waren nicht Thema dieser Arbeit, wenngleich Standards dazu verwendet wurden, die Thematik zu durchleuchten. Demnach wurden die einzelnen Modelle und Frameworks auch nicht bewertet. Der/Die LeserIn hat bemerkt, dass der Schwerpunkt auf die unternehmerische Sicht gelegt wurde, was aber kein Hindernis darstellt, den Inhalt auf staatliche Organisationen zu übertragen. Fehler die beispielsweise bei der Umsetzung von IT-Management und IT-Governance auftreten können, sowie konkrete Empfehlungen standen nicht im Mittelpunkt dieser Arbeit.

Die Arbeit hat gezeigt, dass unterschiedliche Sichtweisen auf die behandelten Themengebiete existieren und kein allgemeingültiger Best-Way gefunden werden kann. IT-Governance sowie auch IT-Management müssen auf die Gegebenheiten einer Organisation bzw. Unternehmen abgestimmt werden. Wesentlich ist eine Synergie



---

dieser beiden Gebiete zu erreichen, die bis in die Produktion und alle anderen Bereiche wirkt.

Derzeit finden in Fachkreisen Diskussionen darüber statt, IT-Governance aufgrund starker Überschneidungen mit IT-Management unter dem Begriff „Enterprise Governance over IT“ zu etablieren. Dies soll die allgemeinere Form der Governance hervorheben, wobei der Fokus situativ und kontextbezogen auf die IT gelenkt wird.

Ein weiteres wesentliches Ziel ist nach wie vor „Enterprise Governance over IT“ als auch IT-Management insbesondere in der Geschäftswelt weiter zu integrieren und zu festigen.

# Abbildungsverzeichnis

1.1: Geschichte der IT (basierend auf [Buch05]).....	3
1.2: Wertbeitrag der IT [Buch05].....	4
2.1: Reifegrade des IT-Managements (basierend auf [Buch05]).....	9
2.2: Aufgaben des IT-Managements (basierend auf [Goek06]).....	12
2.3: IT-Managementtreiber im Zeitablauf.....	15
2.4: ITIL-Übersicht (basierend auf [ITIL1]).....	18
3.1: Innen- und Außensicht von Corporate Governance (basierend auf [Rüte06], [ITGI03]).....	28
3.2: IT-Governance-Treiber im Zeitablauf.....	34
3.3: CobiT-Prozesse in der jeweiligen Focus Area und die Adressierung der Focus Areas in den IT-Governance-Domains (basierend auf [ITGI07]).....	41
3.4: IT Governance on One Page [Weil04].....	43
3.5: Rollen, CobiT-Domains nach [ITGI07] und Relevanz der einzelnen Domains für die jeweilige Rolle (y-Achse: absolute Anzahl der Nennungen).....	45
3.6: Rollen, RACI-Eigenschaften, CobiT-Domains nach [ITGI07] und Relevanz der einzelnen Domains für die jeweilige Rolle und RACI-Eigenschaft pro Rolle ...	45
3.7: Rollen und Verantwortlichkeiten (basierend auf [Rüte06]).....	50
4.1: Zwei Sichtweisen über die Einordnung von IT-Management und IT-Governance .....	52
4.2: Zweidimensionale Einordnung unterschiedlicher Frameworks (basierend auf [Rüte06]) .....	55
4.3: Einordnung von IT-Management und IT-Governance nach der Geschäftsorientierungs- und Zeitorientierungsdimension ([Goek06] in Anlehnung an [Grem04]) .....	56
4.4: Einordnung von IT-Management und IT-Governance in der strategisch/taktisch/operativen Dimension (vgl. auch [Rüte06]).....	58
4.5: Synergie von IT-Governance und IT-Management [Hesc07] .....	59
4.6: High-Level-View auf IT-Management und IT-Governance als synergetisches Gebilde (basierend auf [Hesc07], [Goek07]).....	60

---

# Tabellenverzeichnis

1.1: Vokabular der Vergangenheit und Zukunft [Katz06] .....	3
3.1: Übersetzungen von "Governance" und verwandten Wörtern .....	26
3.2: Focus Areas (basierend auf [ITGI07], [ITGI03]) .....	39
3.3: Tätigkeiten nach Kategorien und Rollen (basierend auf [ITGI03]).....	49
4.1: High-Level-Unterschiede zwischen IT-Management und IT-Governance.....	54

# Quellenverzeichnis

## Literatur

- [Agba05] E. Agbaria, PONS Kompaktwörterbuch für alle Fälle: Teil 1 Englisch-Deutsch, 5. Auflage, Klett, 2005
- [BAB05] Basler Ausschuss für Bankenaufsicht, Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen, Bank for International Settlements, Basel, 2004
- [Bon04] Jan van Bon et al., IT Governance: a pocket guide based on CobiT, Van Haren Publishing, Niederlande, 2004
- [Bren06] M. Brenner et al., Requirements Engineering und IT Service Management – Ansatzpunkte einer integrierten Sichtweise, Gesellschaft für Informatik, o. O., 2006
- [Brow05] A. Brown et al., Framing the Frameworks: A Review of IT Governance Research, Communications of the Association for Information Systems, Eric Sprott School of Business an der Carleton University, Ottawa, 2005
- [BSI] BSI, ZuordnungsISO 27001 sowie 17799 und IT-Grundschutz, Bundesamt für Sicherheit und Informationstechnik, Bonn, o. J.
- [Buch05] D. Buchta et al., Strategisches IT-Management: Wert steigern, Leistung steuern, Kosten senken, 2. Auflage, Betriebswirtschaftlicher Verlag Dr. Th. Gabler/GWV Fachverlage GmbH, Wiesbaden, 2005
- [Bund98] Bundestag, Bundesgesetzblatt Teil 1 Ausgegeben zu Bonn am 30. April 1998, Nr. 24, Bonn, 1998
- [Camp05] P. Campbell, A CobiT Primer: Networked Systems Survivability and Assurance Department, Sandia National Laboratories, Albuquerque, 2005
- [CFAC92] The Committee on the Financial Aspects of Corporate Governance, Gee and Co. Ltd., The Financial Aspects of Corporate Governance, Gee and Co. Ltd., London, 1992
- [COSO04] COSO, Enterprise Risk Management Framework (DRAFT), Committee of Sponsoring Organizations of the Treadway Commission, 2004
- [COSO06] COSO, Interne Überwachung der Finanzberichterstattung – Leitfaden für kleinere Aktiengesellschaften (Executive Summary), The Committee of Sponsoring Organizations of the Treadway Commission, USA, 2006
- [COSO92] COSO, Internal Control – Integrated Framework: Executive Summary, The Committee of Sponsoring Organizations of the Treadway Commission, USA, 1992
- [Dahl06] T. Dahlberg et al., An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument, 39<sup>th</sup> Hawaii International Conference on System Sciences, Helsinki, 2006

- 
- [DAkt] Deutsches Aktiengesetz, lt. letzter Änderung durch Art. 11 G v. 16.7.2007 I 1330
- [Dami05] M. Damianides, Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance, Auerbach Publications, Boston, 2005
- [Euro04] Euroforum, Strategisches IT-Management: Das CIO-Dilemma zwischen Mehrwert bringenden Dienstleistungen und Kosteneffizienz, Euroforum HandelsZeitung Konferenz, Zürich, 2004
- [Fran05] V. Frank et al., Optimiertes IT-Management mit ITIL, Vieweg, Wiesbaden, 2005
- [FRC05] The Financial Reporting Council, Internal Control: Revised Guidance for Directors on the Combined Code, The Financial Reporting Council, London, 2005
- [FSA03] FSA, Combined Code on Corporate Governance, Financial Services Authority, London, 2003
- [Gälw90] A. Gälweiler et al., Strategische Unternehmensführung, Campus-Verlag, Frankfurt am Main, 1990
- [Goek06] W. Goeken et al., IT-Governance, Praxis der Wirtschaftsinformatik, 250, 2006
- [Goek07] M. Goeken et al., IT-Governance, Zeitschrift des ISACA Germany Chapter e.V., 1. Jahrgang, 1, 2007
- [Golt06] W. Goltsche, COBIT: kompakt und verständlich, Vieweg, Wiesbaden, 2006
- [Grem04] Van Grembergen et al., Strategies for Information Technology Governance, Idea Group, London, 2004
- [Grüt05] R. Grütter, IT Service Management nach ITIL, Unterschiede zwischen Anbietern und Kunden, Universität Zürich, Zürich, 2005
- [Haes05] S. De Haes et al., IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group, 38<sup>th</sup> Hawaii International Conference on System Sciences, Antwerpen, 2005
- [Hefn02] R. Hefner, Aligning Strategies: Organizational, Project, Individual, IEEE Computer Society, o. O., 2002
- [Helm06] U. Helmbrecht, Leitfaden IT-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2006
- [ICA99] The Institute of Chartered Accountants in England & Wales, Internal Control: Guidance for Directors on the Combined Code, The Institute of Chartered Accountants in England & Wales, London, 1999
- [IMPA05] IMPACT, IT Governance: Developing a successful governance strategy, National Computing Centre, London, 2005
- [ISO05] ISO, IEC, International Standard ISO/IEC 17799, International Organization for Standardization, International Electrotechnical Commission, Genf, 2005
- [ITGI03] ITGI, Board Briefing on IT Governance, IT Governance Institute, Rolling Meadows, 2003

- 
- [ITGI05a] ITGI, CobiT 4.0, IT Governance Institute, Rolling Meadows, 2005
- [ITGI05b] ITGI, OGC, Aligning CobiT, ITIL, and ISO 17799 for Business Benefit: A Management Briefing from ITGI and OGC, IT Governance Institute, Office of Government Commerce, Rolling Meadows, 2005
- [ITGI06] ITGI, CobiT Mapping: Overview of International IT Guidance 2<sup>nd</sup> Edition, IT Governance Institute, Rolling Meadows, 2006
- [ITGI07] ITGI, CobiT 4.1, IT Governance Institute, Rolling Meadows, 2007
- [Köhl06] P. Köhler, ITIL, Springer-Verlag, Heidelberg, 2006
- [Koon55] H. Koontz et al., Principles of Management: An Analysis of Managerial Functions, McGraw Hill, New York, 1955
- [Lipp] P. Lippeck, DIN ISO 17799 – der globale Sicherheitsstandard, Datalog Software AG, München, o. J.
- [Mali02] F. Malik, Die neue Corporate Governance, Frankfurter Allgemeine Buch, Frankfurt am Main, 2002
- [McBr] D. McBride, Successful Deployment of IT Service Management in the Distributed Enterprise, Hewlett-Packard Company, o. O., o. J.
- [Merz02] L. Merz et al., Langenscheidt Routledge: Fachwörterbuch Wirtschaft, Handel und Finanzen Englisch, Langenscheidt, München, 2002
- [MK02] McKinsey, Investor Opinion Survey: Key Findings, McKinsey & Company, London, 2002
- [Nies05] F. Niessink, The IT Service Capability Maturity Model, Vrije Universiteit, Amsterdam, 2005
- [OECD04] OECD, OECD Principles of Corporate Governance, Organisation for Economic Co-operation and Development, Paris, 2004
- [OECD99] OECD, OECD Principles of Corporate Governance, Organisation for Economic Co-operation and Development, Paris, 1999
- [Peter04] R. Peterson, Crafting Information Technology Governance, Auerbach Publications, Boston, 2004
- [Coll04] P. Collin et al., PONS Großes Fachwörterbuch Wirtschaft – Englisch–Deutsch / Deutsch–Englisch, Klett, Stuttgart, 2004
- [PWC07] PWC, ITGI, IT Governance in Practice: Insight from leading CIOs, Price Waterhouse Coopers, IT Governance Institute, South Africa, 2007
- [Ridl04] G. Ridley et al., COBIT and its Utilization: A framework from the literature, 37<sup>th</sup> Hawaii International Conference on System Sciences, Tasmanien, 2004
- [RMG99] Risk Management Group of the Basel Committee on Banking Supervision, Enhancing Corporate Governance for Banking Organisations, Bank for International Settlements, Basel, 1999
- [Rüeg02] J. Rüegg-Sturm, Das neue St. Galler Management-Modell, Haupt Verlag, Bern, 2002
- [Rüte06] A. Rüter et al., IT-Governance in der Praxis, Springer-Verlag, Heidelberg, 2006

- [Sher04] S. Sherer, IS Project Selection: The Role of Strategic Vision and IT Governance, 37<sup>th</sup> Hawaii International Conference on System Sciences, Lehigh, 2004
- [Solm05] B. v. Solms, Information Security governance: COBIT or ISO 17799 or both?, Academy for Information Technology an der University of Johannesburg, Johannesburg, 2005
- [Stei05] H. Steinmann, Management: Grundlagen der Unternehmensführung, Konzepte, Funktionen, Fallstudien, Betriebswirtschaftlicher Verlag Dr. Th. Gabler/GWV Fachverlage GmbH, Wiesbaden, 2005
- [SZF06] Stadt Zürich Finanzkontrolle, Interne Kontrollsysteme in Wirtschafts- und Verwaltungsunternehmen, Stadt Zürich Finanzkontrolle, Zürich, 2006
- [Thom02] J-P. Thommen, Management und Organisation: Konzepte, Instrumente, Umsetzung, Versus-Verlag, Zürich, 2002
- [Tiem06] E. Tiemeyer et al., Handbuch IT-Management, Carl Hanser Verlag, München, 2006
- [Tjoa05] A Min Tjoa et al., IT Governance: Definition, Standards & Zertifizierung, Österreichische Computer Gesellschaft, Wien, 2005
- [Völk05] J. Völker, BS 7799 Von „Best Practice“ zum Standard: Informations-sicherheits-Management nach BS 7799 im Überblick, Secorvo Security Consulting GmbH, Karlsruhe, 2005
- [Weil04] P. Weill et al., IT Governance on One Page, Center for Information Systems Research an der Sloan School of Management des Massachusetts Institute of Technology, Massachusetts, 2004
- [Weill02] P. Weill et al., Don't Just Lead: Govern: Implementing Effective IT Governance, Center for Information Systems Research an der Sloan School of Management des Massachusetts Institute of Technology, Massachusetts, 2002
- [Will91] H. Willman et al., Langenscheidts Großwörterbuch: der englischen und deutschen Sprache, Langenscheidt, München, 1991
- [Wyse02] J. Wyser et al., IT Governance als zentraler Erfolgsfaktor, Ernst & Young, o. O., 2002
- [Zarn03] R. Zarnekow, Strategisches IT-Management, Praxis der Wirtschaftsinformatik, 232, 2003
- [Zuse04] W. Zuser et al., Software Engineering: Mit UML und dem Unified Process, Pearson Studium, München, 2004

## **Onlinequellen (Webseiten)**

- [4Man] 4 Managers Six Sigma, <http://www.4managers.de/themen/six-sigma/>, 03.09.2007
- [Act] Act Management Consulting über IT-Governance, Risk Management und Service Management, <http://www.act-mc.at/themen/it-governance/die-aufgabe>, 08.09.2007

- [CenIT] Central-IT CobiT / ITIL, <http://www.central-it.de/downloads/335/1025/>, 15.09.2007
- [CIO] CIO, <http://www.cio.de/markt/analysen/818673/index3.html>, 01.09.2007
- [CobiT] CobiT, <http://risikomanagement-in-it-projekten.de/03COBIT/seite03.html>, 10.08.2007
- [CobiTF] CobiT Foren, <http://www.controlit.org/>, 15.08.2007
- [CobiTH] CobiT Historie, [http://www.exagon.de/index.php?option=com\\_content&task=view&id=56&Itemid=156](http://www.exagon.de/index.php?option=com_content&task=view&id=56&Itemid=156), 18.08.2007
- [CobiTI] CobiT ISACA Einführung, <http://www.cobit-isaca.de/>, 15.08.2007
- [Comp] Compliance Magazin IT-Governance Institute <http://www.compliancemagazin.de/gesetzstandards/deutschland/standards/itgovernanceinstitute100507.html>, 10.08.2007
- [COSO] COSO, <http://www.coso.org/>, 28.07.2007
- [Cryp] Cryptoshop CobiT, <http://www.cryptoshop.com/index.php>, 15.08.2007
- [CSec] ISO 17799, <http://www.computersecuritynow.com/>, 17.08.2007
- [CWelt] Computerwelt, IT-Governance, <http://www.computerwelt.at/detailArticle.asp?a=109837&n=2>, 08.09.2007
- [CWoa] Computerwoche, IT-Management, [http://www.computerwoche.de/it\\_strategien/it\\_management/](http://www.computerwoche.de/it_strategien/it_management/), 15.09.2007
- [CWob] Computerwoche, IT-Service-Management, [http://www.computerwoche.de/zone/it\\_service\\_management/](http://www.computerwoche.de/zone/it_service_management/), 10.09.2007
- [Gene] Genesiscom IT-Service-Management, [http://www.genesiscom.ch/de/1/solutions/nms/NMS\\_Lo\\_343.asp](http://www.genesiscom.ch/de/1/solutions/nms/NMS_Lo_343.asp), 11.09.2007
- [ISACA] ISACA Cobit, <http://www.isaca.org/Template.cfm?Section=COBIT6&CONTENTID=31096&TEMPLATE=/ContentManagement/ContentDisplay.cfm>, 10.08.2007
- [ISO171] ISO/IEC 17799 im Wikiformat, <http://iso-17799.safemode.org/>, 17.08.2007
- [ISO172] ISO/IEC 17799, <http://www.17799central.com/>, 17.08.2007
- [ISO173] ISO 17799, <http://www.iso-17799.com/>, 17.08.2007
- [ISO174] ISO 17799, <http://www.17799.com/>, 17.08.2007
- [ISO27] ISO 27000 Toolkit, <http://www.27000-toolkit.com/>, 17.08.2007
- [ISO9] ISO 9000 History, [http://www.iso9001help.co.uk/ISO\\_9000\\_history.htm](http://www.iso9001help.co.uk/ISO_9000_history.htm), 05.09.2007
- [ISO900] ISO 9000 Help, [http://www.iso9001help.co.uk/ISO\\_9000\\_history.htm](http://www.iso9001help.co.uk/ISO_9000_history.htm), 03.09.2007



- 
- [ITAud] IT Audit Dokumente, [http://www.it-audit.de/html/ian\\_sch\\_ita\\_th\\_go.html](http://www.it-audit.de/html/ian_sch_ita_th_go.html), 15.08.2007
- [ITG] IT-Governance, <http://www.itgovernance.co.uk/>, 08.09.2007
- [ITIL1] ITIL.org von Glenfis AG, <http://www.itil.org>, 05.09.2007
- [ITIL2] OGC ITIL, [http://www.ogc.gov.uk/guidance\\_itol.asp](http://www.ogc.gov.uk/guidance_itol.asp), 03.09.2007
- [ITIL3] ITIL Official Site, <http://www.itil-officialsite.com/home/home.asp>, 16.08.2007
- [ITIL4] ITIL, <http://www.itsmf.de/bestpractice/index.asp>, 16.08.2007
- [ITIL5] ITIL, <http://www.computerworld.ch/aktuell/itservices/39555/index.html>, 16.08.2007
- [ITIL6] ITIL Open Guide, <http://www.itlibrary.org/>, 16.08.2007
- [ITMan] IT-Service-Management, <http://itmanagement.earthweb.com/netsys/article.php/2195051>, 13.09.2007
- [ITSM] IT-Service-Management, <http://www.itsmportal.net>, 11.09.2007
- [ITWiss] IT Wissen Compliance, [http://www.itwissen.info/definition/lexikon/\\_\\_\\_compliance\\_compliance.html](http://www.itwissen.info/definition/lexikon/___compliance_compliance.html), 15.09.2007
- [IUK] IUK Fraunhofer Zitat Darwin , [http://www.iuk.fraunhofer.de/index2.html?Dok\\_ID=76&Sp=1&MID=1399&PHPSESSID=146ba7b5b46d645e903d9463d7c291b4](http://www.iuk.fraunhofer.de/index2.html?Dok_ID=76&Sp=1&MID=1399&PHPSESSID=146ba7b5b46d645e903d9463d7c291b4), 10.09.2007
- [IWört] Info Wörterbuch, <http://www.woerterbuch.info/>, 14.09.2007
- [LEO] LEO Wörterbuch, <http://dict.leo.org/>, 14.09.2007
- [Merc] Mercury Software für IT-Service-Management, <http://www.mercury.com/de/solutions/itil-itsm/>, 11.09.2007
- [Meyers] Meyers, <http://lexikon.meyers.de/>, 27.08.2007
- [ÖCITG] Österreichische Computergesellschaft IT-Governance, <http://www.ocg.at/ak/governance/index.html>, 08.09.2007
- [Risk] Risknet COSO/ERM, <http://www.risknet.de/COSO-ERM-Framework.143.0.html>, 16.08.2007
- [Sox] Sox-Online COSO/CobiT, [http://www.sox-online.com/coso\\_cobit.html](http://www.sox-online.com/coso_cobit.html), 11.09.2007
- [SSITSM] Silicon Software für IT-Service-Management, [http://www.silicon.de/enid/business\\_software/26967](http://www.silicon.de/enid/business_software/26967), 11.09.2007
- [SSITSM] Softlab Software für IT-Service-Management, <http://www.softlab.com/at/offering/iTServiceManagement/index.html>, 11.09.2007
- [WB] Worldbank, <http://web.worldbank.org/>, 27.08.2007

---

## Präsentationen / Vorträge / Veranstaltungen

- [Altr05] A. Altrhein, ISO 17799 als Informationssicherheitsstrategie, Ansatz- und Methodenpräsentation, Siegen, 2005
- [Berg] J. Bergsmann et al., Analyse nach Cobit und ISO17799, IT Security Lab, Langenstein, o. J.
- [Bitt] P. Bitterli, CobiT-Framework: Eine Einführung in das IT-Governance Modell, Bitterli Consulting, Zürich, o. J.
- [Brun03a] J. Brun, CobiT Framework – Audit Guidelines, Universität Zürich, Zürich, 2003
- [Brun03b] J. Brun, Das CobiT Framework, Universität Zürich, Zürich, 2003
- [Hesc05] J. Heschl, IT Service Management – ITIL, KPMG, Wien, 2005
- [Hesc07] J. Heschl, Personal Communication, KPMG, Wien, 2007.
- [Hübs06] G. Hübsch, IT Governance im Service Management, Energie AG Oberösterreich, Wien, 2006
- [Huis04] M. Huissoud, CobiT der Brückenbauer, Eidgenössische Finanzkontrolle, Bern, 2004
- [Kapp06] G. Kappel, Security, Business Informatics Group an der TU Wien, Wien, 2006
- [Katz06] W. Katzenberger, Systemplanung und Projektmanagement, Institut für Managementwissenschaften an der TU Wien, Wien, 2006
- [Lemk] H. Lemke, Strategisches IT-Management in der Öffentlichen Verwaltung, Land Hessen, Hessen, o. J.
- [Müll06] K. Müller, CobiT als De-facto-Standard der IT-Governance: Praxisbericht über die Einführung von SOX, Telekom Austria, o. O, 2006
- [Plam06] A. Plamberger, IT Service Management: Service Delivery, act Management Consulting, Wien, 2006
- [Strn05] C. Strnadl, IT Governance. Zwischen Hype und Heiligem Gral., Atos Origin Information Technology GmbH, Wien, 2005
- [Stuc04] W. Stucky et al., Betriebliche Informationssysteme, Institut für Angewandte Informatik und Formale Beschreibungsverfahren an der Universität Karlsruhe, Karlsruhe, 2004
- [Stut06] M. Stutz, Grundlagen und Definition: IT-Sourcing Governance, Institut für Wirtschaftsinformatik an der Universität St. Gallen, St. Gallen, 2006
- [Turb06] K. Turbitt, ISO 20000: Was kann ein Unternehmen tun?, BMC Software, Frankfurt, 2006
- [Wojd05] F. Wojda, Organisation & Personal, Institut für Managementwissenschaften an der TU Wien, Wien, 2005
- [Wojd06] F. Wojda, Projektmanagement, Institut für Managementwissenschaften an der TU Wien, Wien, 2006