TECHNISCHE
UNIVERSITÄT
WIEN
Vienna University of Technology

Bachelorarbeit zum Thema

IT-Governance & IT-Compliance

Rechtliche Rahmenbedingungen für Unternehmen

---

ausgeführt zum Zwecke der Erlangung des
akademischen Grades eines Bachelor of Science (BSc.)
unter der Leitung von

Ass.-Prof. Mag.iur. Dr.iur. Markus Haslinger
am Fachbereich Rechtswissenschaften (E 280 / 1)

eingereicht an der Technischen Universität Wien
Fakultät für Informatik von

Thomas Hainzel
Matr.-Nr. 0725657 (033 526)
th.hainzel@gmx.net
Rosaliagasse 16/12, 1120 Wien

Wien, 31. Jänner 2010

Eidesstattliche Erklärung

Hiermit erkläre ich an Eides statt, dass ich die vorliegende Seminararbeit zur Erreichung des akademischen Grades *Bachelor of Science (BSc.)* (kurz Bachelorarbeit) ohne fremde Hilfe und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen eindeutig als solche kenntlich gemacht habe.

Weiters bestätige ich, dass diese Arbeit in gleicher oder ähnlicher Form noch nicht veröffentlicht und auch noch keiner anderen Prüfungsbehörde im In- oder Ausland zur Bewertung vorgelegt wurde.

Wien, 31. Jänner 2010

Thomas Hainzel

Vorwort

Der richtige Einsatz von Informationstechnologie (IT) und der Aufbau umfangreicher Kommunikationsstrukturen stellen für sehr viele Unternehmen - sowohl im nationalen als auch im internationalen Umfeld - entscheidende Erfolgs- und Wettbewerbsfaktoren dar. Ganze Geschäftsprozessketten sind ohne effiziente IT nicht mehr vorstellbar und die Nachvollziehbarkeit bzw. Kontrolle sämtlicher IT-Aktivitäten tritt immer mehr in den Vordergrund.

Die fortschreitende Globalisierung unserer Märkte fordert nun einheitliche, rechtliche Rahmenbedingungen für Unternehmen, die neben der Aufrechterhaltung eines fairen Wettbewerbs und ausreichender IT-Sicherheitsmaßnahmen auch die Vergleichbarkeit und Bewertung der Unternehmensinfrastruktur unterschiedlicher Konzerne anstreben.

Die *IT-Governance* repräsentiert dabei eine klare Management- bzw. Vorstandsaufgabe zur Steuerung der Organisationsstrukturen, der Prozessintegrität sowie der Abstimmung der IT auf die Unternehmensstrategie und die dort verankerten Unternehmensziele. Ein gezieltes Risikomanagement, die Optimierung von ganzen Prozessketten und die Integration von Fachbereichen und IT-Dienstleistungen sind nur einige Kernaufgaben dieser Top-Management-Disziplin.

Die *IT-Compliance* kann als zentraler Einflussfaktor bzw. Teilbereich der IT-Governance verstanden werden und fokussiert die Einhaltung und Kontrolle der gesetzlichen Regelungen auf nationaler oder internationaler Ebene. Dieser rechtliche Rahmen reicht von der Informationssicherheit (IT-Security), über Datenschutz und Datensicherheit bis zum Aufbau und Betrieb eines internen Kontrollsystems (IKS). Sowohl rechtlich verpflichtende Judikate als auch freiwillige Kodizes und Gutachten sollen die internationale Umsetzung vereinheitlichen.

Inhalt dieser Bachelorarbeit soll nun die Aufarbeitung von unternehmensrechtlichen Rahmenbedingungen im Kontext der IT-Governance bzw. IT-Compliance sein. Sowohl die EU-weiten Richtlinien und Verordnungen als auch die österreichische Rechtslage sollen analysiert und dessen Auswirkungen auf Gesellschaft und Wirtschaft untersucht werden.

Leser und Leserinnen dieser Arbeit werden - auch ohne rechtliches oder technisches Vorwissen - für den Themenkomplex *IT-Management* sensibilisiert und sollen die Wichtigkeit von einheitlichen Bestimmungen sowie dessen gesetzlicher Verankerung erkennen. Mehrere nationale und internationale Institutionen haben es sich zur Aufgabe gemacht, einheitliche Rahmenbedingungen zu schaffen und bei der Konzeption von IT-Systemen zu unterstützen.

Standardisierte Rahmenwerke sollen helfen diese Regulative zu implementieren sowie eine direkte Unterstützung für Management und Unternehmensleitung darstellen. Aktuelle Studien zeigen problematische Defizite bei der Implementierung und Umsetzung von IT-Governance/IT-Compliance im internationalen Umfeld auf und geben Denkansätze für die Beseitigung organisatorischer Probleme.

Wien, 31. Jänner 2010

Thomas Hainzel

Preface

Appropriate use of information technology (IT) and building-up large communication structures can be seen as key factors of success and competition for enterprises. Business process chains aren't thinkable without efficient IT and traceability comes into prominence.

The on-going market globalisation demands uniform legal company guidelines which should seek the comparability and evaluation of the infrastructure of different enterprises beside the retention of a fair competetion and sufficient IT security measures.

IT-Governance therefore represents a management or board task to control organisational structure, process integrity and align IT to the business strategy. A specific risk management, optimisation of whole process chains and integration between business departments and IT services are just some key tasks of this top management discipline.

IT-Compliance can be seen as a dominant bottleneck factor or part of IT-Governance and focuses observance of legal regulations on national and international levels. This legal framework reaches from information security (it-security) through data protection/security to construction and maintenance of an internal control system (ICS). Obligate law proceedings as well as voluntary expertises should unify the international implementations.

Content of this paper is the refurbishment of corporate law guidelines in context of IT-Governance and IT-Compliance. European directives as well as Austrian law should be analysed and their consequences on society and economy examined.

Readers of this paper - even without legal or technical knowledge - will be sensitized for *IT management* issues and should render the importance of unified appointments and it's legal anchoring. Several national and international institutions are following the task to develop overall guidelines and to support the conception of IT systems.

Standardised frameworks should help implementing those regulatives as well as providing direct support for management and boards. Current research studies show problematical deficits implementing IT-Governance/IT-Compliance on international levels and made suggestions for the elimination of organisational problems available.

Inhaltsverzeichnis

1 Einleitung & Grundlagen

«Stellen Sie sich vor, der amtierende, amerikanische Präsident[1] würde ermordet werden. Vor 60 Jahren hätte es etwa drei Wochen gedauert, bis auch die letzten Bürger der Industriegesellschaft davon erfahren hätten. Vor 10 Jahren hätte die Verbreitung der Nachricht vielleicht ein oder zwei Tage benötigt. Heute würden wir eine Stunde vorher von einem geplanten Anschlag informiert werden und wären über CNN[2] live dabei...»[3]

Dies ist nur eines von vielen Beispielen, welches die Entwicklung unserer Gesellschaft von einer Agrargesellschaft etwa 8000 v. Chr. über die Industriegesellschaft des 17. Jahrhunderts bis zur heutigen Dienstleistungs-, Informations- und Wissensgesellschaft zeigt. Während sich viele Entwicklungsländer noch im Übergang ins industrielle Zeitalter befinden, ist in den westlichen Industriestaaten bereits eine hochgradige, digitale Vernetzung über insgesamt zwölf Dimensionen[4] erkennbar, welche schlussendlich eine Globalisierung der Technologien, die Entwicklung einer gesättigten Informationsgesellschaft sowie wirtschaftlichen Wandel und Diskontinuität mit sich bringt.[5]

Diese Strukturbrüche, insbesondere die Dimensionen *Technologien*, *Globale Vernetzung* und *Wirtschaftliche Sektoren*, haben in den letzten Jahrzehnten zu mikro- und makroökonomischen Veränderungen geführt. Während in den 80er Jahren überwiegend sequentiellarbeitende Großrechner als zentrales IT-Herzstück international tätiger Unternehmen galten, administrieren Multikonzerne heute dezentrale IT-Infrastrukturen, die weltweit vernetzt, hochverfügbar und um ein Vielfaches leistungsstärker als ihre Vorfahren sind. Parallel dazu steigen Anzahl und Heterogenität der IT-Systeme, die einen wertvollen Beitrag zur Speicherung von Unternehmensdaten leisten oder ganze Geschäftsprozesse abbilden. Die Globalisierung nimmt zusätzlichen Einfluss auf die Distribution der Infrastruktur auf nationale bzw. internationale Standorte und fördert den Einsatz mobiler Endgeräte.[6]

[1] Zum Zeitpunkt des Verfassens dieser Arbeit war dies Barack H. Obama.
[2] Cable News Network, amerikanischer Fernsehsender
[3] Beispielhafte Erklärung des Wandels der Zivilisationsstufen von der Industriegesellschaft zur Informations- und Wissensgesellschaft - Wolfgang E. Katzenberger im Rahmen einer Vorlesungseinheit aus «Systemplanung und Projektmanagement» an der Technischen Universität Wien im Wintersemester 2009/10. vgl. [Katzenberger2009, F. 3]
[4] Sprache, Paradigmen, Axiales System, Wissenschaften, Technologien, Berufsstruktur, Wertvorstellungen, Zukunfsorientierung, Entscheidungsbildung, Differenzierung, Globale Vernetzung und Wirtschaftliche Sektoren. vgl. [Katzenberger2009, F. 4]
[5] vgl. [Katzenberger2009, F. 3-5]
[6] vgl. [Grünendahl2009, Vorwort] bzw. [Grünendahl2009, S. 1-4]

Thomas Popp ergänzt diese technischen Herausforderungen in seiner Masterarbeit[7] um einen heute sehr entscheidenden Wirtschaftsfaktor - die *IT-Kosten*. Heutzutage sind die Kosten einer gut administrierten Informationsstruktur extrem hoch und stehen automatisch mit den aktuell diskutierten Kosteneinsparungen und Aufwandsreduzierungen in allen IT-Bereichen im Widerspruch. Trotzdem entfallen etwa 70 bis 80 Prozent des gesamten IT-Budgets auf die sogenannten «IT-Basiskosten», also den Betrieb und die Wartung der laufenden Systeme und Komponenten.

Für einen solch bedeutenden Kostenfaktor muss jedes Unternehmen entsprechende Vorkehrungen zur finanziellen Absicherung sowie zur Vermeidung und Minimierung technischer oder organisatorischer Zwischenfälle treffen. Ein ausgeprägtes Risikomanagement sowie die ganzheitliche IT-Kontrolle treten dabei zunehmend in den Vordergrund.

Die genannten Aspekte und Beispiele zeigen, dass der Einsatz von Informationstechnologie (IT) und der Aufbau umfangreicher Kommunikationsstrukturen einen entscheidenden, wirtschaftlichen Erfolgs- und Wettbewerbsfaktor darstellt. Branchen, deren Kernwertschöpfung eng an die vorhandene Infrastruktur gekoppelt ist (etwa Banken, Versicherungen oder Telekommunikationsdienstleister), verzeichnen eine hohe IT-Abhängigkeit verbunden mit entsprechend hohem IT-Budget. Andere Branchen weisen derzeit noch eine geringere Technologiebindung auf, werden aber in absehbarer Zeit den sensibleren Geschäftsfeldern folgen.[8]

Durch diese infrastrukturellen Abhängigkeiten und die damit verbundene Steigerung des technologischen und finanziellen Sicherheitsbewusstseins der Unternehmen rückten Themen wie *IT-Security*, *IT-Management* oder *IT-Risikomanagement* immer mehr ins Rampenlicht der Geschäftsführung. Sicherheit in der Informationstechnologie wurde daher zu einer *«unverzichtbaren Unternehmensfunktion, deren Effektivität gegenüber Dritten verpflichtend nachgewiesen werden muss.»*[9] Desweiteren muss dieses Sicherheitsniveau nicht nur initial aufgebaut, sondern auch fortlaufend aufrecht erhalten und dessen Nachhaltigkeit gewährleistet werden.

Umgesetzt werden diese Forderungen der Nachhaltigkeit und Effizienz unter anderem durch zielgerichtetes IT-Risikomanagement, der vordergründigen Betrachtung der Informationssicherheit als Teilaspekt der Gesamtunternehmung aber auch durch die Definition und Standardisierung von ganzen IT-Prozessketten.[10]

[7] vgl. [Popp2007, S. 3-4]
[8] vgl. [Grünendahl2009, Vorwort] bzw. [Grünendahl2009, S. 1-4]
[9] vgl. [Grünendahl2009, Vorwort]
[10] vgl. [Grünendahl2009, Vorwort]

Basierend auf diesen Methoden und Grundsätzen ist es Aufgabe des Vorstandes bzw. der Unternehmensleitung im Zuge einer *IT-Governance* die theoretische Planung durchzuführen bzw. dessen praktische Umsetzung zu überwachen. Durch das *IT-Management* werden zentrale IT-Steuerungsmaßnahmen definiert und von der *IT-Produktion* mess- und kontrollierbar eingesetzt. Das IT-Govenernace-Framework in Abschnitt 1.1.3 setzt diese drei Hauptelemente miteinander in Verbindung und zeigt ein intensives Zusammenspiel mit der *IT-Steuerung* und der *IT-Compliance* auf.

Zusammenfassend kann festgestellt werden, dass sowohl IT-Governance als auch IT-Compliance nur als gemeinsames Konstrukt funktionieren und von einer Vielzahl an Einflussfaktoren aus dem Umfeld des Unternehmens abhängen. Vorstände, Aufsichtsräte und Gesellschafter stehen also vor neuen Herausforderungen, um den rechtlichen Fortbestand sämtlicher, unternehmerischer Aktivitäten im Hinblick auf die Informationstechnologie nachhaltig zu sichern.

1.1 IT-Governance

1.1.1 Corporate Governance

Während die IT-Governance überwiegend im Umfeld der Informationstechnologie angewandt wird, dient die *Corporate Governance* der Steuerung und Kontrolle des gesamten Unternehmens. In gewisser Weise kann Corporate Governance daher als Mutterdisziplin zur IT-Governance verstanden werden und gibt Regulatorien bzw. Grundsätze der Umsetzung vor. Besonders in Abschnitt 1.1.2 wird deutlich sichtbar, dass die Grundprinzipien der Mutterdisziplin auch im IT-Bereich Anwendung finden.

Eine einheitliche Definition von Corporate Governance gibt es bis heute nicht. Adrian Cadbury etwa definiert Corporate Governance als *«System, durch welches Unternehmen gelenkt und gesteuert werden»*[11] und sieht darin eine klare Vorstandsaufgabe. Das Top-Management ist für eine klare Zielsetzung der Unternehmung, die professionelle Führung des Betriebes sowie eine regelmäßige Berichterstattung verantwortlich und hat im Sinne der Gesetze, der Regulatorien und der Aktionäre zu agieren.

Martin Hilb definiert die *New Corporate Governance* basierend auf Cadburys Definition, erweitert diese jedoch um strategische bzw. integrative Tätigkeiten und bringt ganzheitliche bzw. ethische Aspekte ein. Er definiert die neue Corporate Governance als System *«by which companies are strategically directed, integratively managed and holistically controlled in an entrepreneurial and ethical way in accordance with a particular context»*[12]

[11] vgl. [Cadbury1992, S. 14]
[12] vgl. [Hilb2005, S. 10]

All diesen Definitionen ist gemein, dass es einer einheitlichen Regulierung sämtlicher Corporate Governance Aktivitäten bedarf. In Österreich wurde dazu der *Österreichische Arbeitskreis für Corporate Governance*[13] unter der Leitung von Richard Schenz, Regierungsbeauftragter für den Kapitalmarkt, mit der Erstellung eines *Österreichischen Corporate Governance Kodex*[14] (vgl. Abschnitt 2.4.3) beauftragt. Dieses Dokument beinhaltet neben den Verantwortungsbereichen von Aktionären, Aufsichtsrat und Vorstand auch die Regelung von Kompetenzverteilungen und Interessenkonflikten sowie klare Richtlinien für einen transparenten Jahresabschluss und eine vertrauenswürdige Wirtschaftsprüfung.

Auch in anderen EU-Staaten existieren nationale Corporate Governance Kodizes (etwa der Deutsche Corporate Governance Kodex[15]), die einheitliche Strukturen und Vorgaben (teilweise auch auf internationaler Ebene) schaffen sollen. Gemeinsame Eigenschaft dieser Kodizes unterschiedlicher Rechtssysteme ist die Bereitstellung von standardisierten Grundprinzipien und Wertvorstellungen.

1.1.2 Grundprinzipien der Governance

Die einleitend angesprochene Mutter-Kind-Beziehung zwischen der übergeordneten Corporate und der untergeordneten IT-Governance lassen vermuten, dass auch die Basisideen bzw. Primärziele beider Disziplinen ähnlich sind. Martin Fröhlich, Financial-Service- und IT-Governance-Berater im Bereich Process Assurance von PricewaterhouseCoopers WPG AG[16] in Düsseldorf, definiert vier Grundprinzipien[17] zur *«Umsetzung eines wirksamen Steuerung- und Regelungssystems kapitalmarktorientierter Unternehmen im Mittelpunkt einer verantwortungsvollen, transparenten und effizienten Unternehmensführung»*[18]:

- Accountability (Zurechenbarkeit)
- Responsibility (Verantwortung)
- Transparency (Transparenz) und
- Fairness (Fairness)

Accountability (Zurechenbarkeit)

Accountability (Zurechenbarkeit) definiert globale Regeln, um eine Kontrolle des Unternehmens durch Drittorganisationen, Kunden, Lieferanten und Gesellschaft zu ermöglichen. Insbesondere die soziale Verantwortung, der Umgang mit Mitarbeitern sowie die Zertifizierung von Arbeitsplätzen soll die gesellschaftliche Verantwortung repräsentieren.

[13] vgl. `http://www.wienerborse.at/corporate/index.htm`, zuletzt abgerufen am 30.01.2010
[14] vgl. [ÖACG2009a]
[15] vgl. `http://www.corporate-governance-code.de`
[16] vgl. `http://www.pwc.com`, zuletzt abgerufen am 30.01.2010
[17] vgl. [Fröhlich2007, S. 38-42]
[18] vgl. [Fröhlich2007, S. 38]

Responsibility (Verantwortung)

Durch die Produktion von Gütern oder die Bereitstellung von Dienstleistungen bekommen einzelne Unternehmen immer mehr **Verantwortung** - insbesonderen in Bezug auf Qualität, Arbeitssicherheit und Umweltschutz - übertragen. Diese Verantwortlichkeiten gilt es wahrzunehmen und auch durch eine Integration in die Unternehmensstrategie und dessen Ziele schriftlich zu verankern bzw. praktisch umzusetzen.

Transparency (Transparenz)

In den Finanz- und Kapitalbereichen des Unternehmens genießt kontinuierliche und langfristige **Transparenz** in Sachen Kommunikation, Finanzanalysen, Jahresabschlüssen und Offenlegungspflichten hohe Priorität. Dieser anfängliche Aufwand macht sich besonders am Aktienmarkt nachhaltig bezahlt.

Fairness (Fairness)

In letzter Zeit haben vor allem ethische Grundlagen zur Unternehmensführung an Bedeutung gewonnen und sollen den Respekt und die **Fairness** des Unternehmens gegenüber Meinungen von Mitarbeitern, Kunden und Partnern betonen. Der international anerkannte *Code of Conduct*[19] kann dabei als Grundsatz- und Normkatalog - und somit als angemessener Umgangston - verstanden werden.

Diese Prinzipien können zwar inhaltlich als Grundlage der Governance angesehen werden, es wäre jedoch falsch zu glauben, dass die Corporate oder IT-Governance die einzige, beteiligte Komponente ist. Der Erfolg der Umsetzung liegt im Zusammenspiel aller relevanten Kernqualifikationen im strategischen, taktischen und operativen Bereich und soll durch das *IT-Governance-Framework* (vgl. Abschnitt 1.1.3) verdeutlicht werden.

1.1.3 Das IT-Governance-Framework

Es existieren eine Vielzahl an Governance-Frameworks, deren Ziel die Abgrenzung bzw. Eingliederung der Einzelkomponenten und Einflussfaktoren in einen geordneten Rahmen ist. Hauptaugenmerk liegt dabei auf der vereinfachten Darstellung eines komplexen Systems mit unterschiedlichen Differenzierungsmerkmalen.

Martin Fröhlich stellt dazu ein dreistufiges IT-Governance-Framework vor (vgl. Abbildung 1.1)[20].

[19] Der Code of Conduct umfasst einheitliche Regelungen für das Zusammenleben und Kommunizieren innerhalb von Organisationen, Unternehmen oder Teams.

[20] Adaptierte Grafik: Darstellung der drei Elemente des IT-Governance-Framworks nach Andreas Fröhlich [Fröhlich2007, S. 18] in Form einer Pyramide mit eigenständigen Ergänzungen.

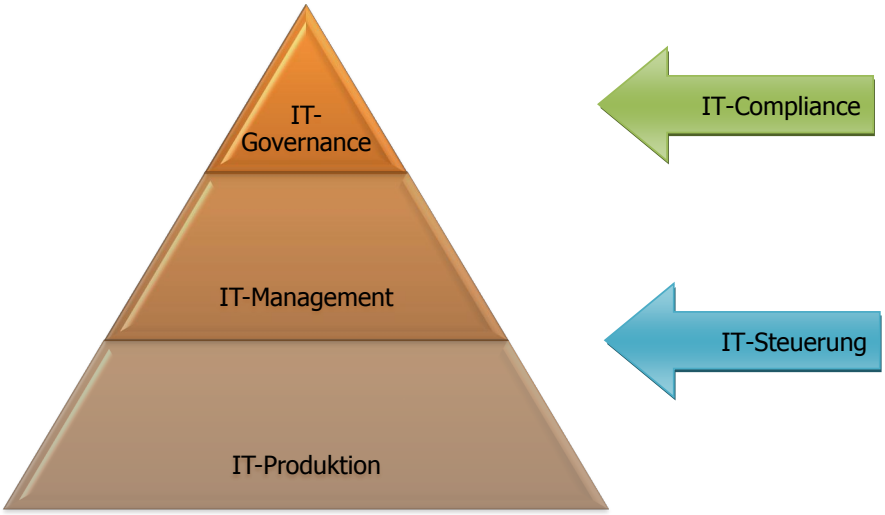

Abbildung 1.1: Darstellung des IT-Governance-Frameworks

Ebene 1: IT-Governance

IT-Governance kann als *«die Organisation, Steuerung und Kontrolle der IT eines Unternehmens zur konsequenten Ausrichtung der IT-Prozesse an der Unternehmensstrategie»* verstanden werden und in weiterer Folge als *«einheitliches Rahmenwerk eingebunden sein, das sich am Geschäftszweck des Unternehmens orientiert und Leitlinien und Standards setzt.»*[21]

Trotz dieses gemeinsamen Grundverständnisses, lässt sich diese Definition auf unterschiedliche Interpretationen in verschiedenen Bereichen der IT zurückführen:[22]

- Die Unternehmensleitung (Vorstand bzw. CIO[23], vgl. Abschnitt 3.2.2) verbindet mit IT-Governance ein strategisches Führungsinstrument zur Steuerung der zentralen und dezentralen IT-Infrastruktur.
- Das operative IT-Management sieht darin ein Rahmenwerk zur Zieldefinition sowie zur Ausstattung der gesamten IT mit den notwendigen Hardware- und Softwarekomponenten.
- Der IT-Betrieb wiederum ist an der formalen Implementierung von internationalen Standards und Frameworks wie zum Beispiel ITIL oder COBIT interessiert (vgl. Abschnitt 3.1.2 bzw. 3.1.3).

[21] vgl. [Fröhlich2007, S. 17]
[22] vgl. [Fröhlich2007, S. 17]
[23] Chief Information Officer - Vorstand für Informations- & Kommunikationstechnologie

Voraussetzung für die Ausformulierung und Gestaltung einer solchen IT-Governance ist die Beachtung der übergeordneten, abstrakteren Komponente - der *Corporate Governance*. Dort verankerte Grundsätze (Zurechenbarkeit, Verantwortlichkeit, Transparenz und Fairness) wurden bereits in Abschnitt 1.1.2 angeführt.

Ebene 2: IT-Management

Während die IT-Governance eine klare Vorstandsaufgabe zur Definition von Entscheidungsrechten, Rollen und Verantwortlichkeiten darstellt, wird der unterhalb der Unternehmensführung liegende Organisationsbereich als **IT-Management** bezeichnet. Aufgabe dieser operativen Managementebene ist die Überführung der strategischen und taktischen Vorgaben des Top-Managements in konkrete Handlungsvorgaben sowie die Anpassung der IT-Zielhierarchie.[24]

Das Arbeitsumfeld des IT-Managements umfasst dabei neben der Aufstellung einer IT-Strategie die Entscheidungsfelder[25]

- Informations- & Kommunikationswesen
- Anwendungen & Applikationsportfolio
- IT-Organisation & -Arbeitsstrutur
- Infrastruktur & Technologien
- In- & Outsourcing
- IT-Sicherheit & Datenschutz und
- IT-Service-Management (vgl. Abschnitt 3.1).

Aufgrund dieser IT-Konzeption können schlussendlich die gesamte IT-Systemarchitektur und die ganzheitlichen IT-Prozesse definiert werden.

Ebene 3: IT-Produktion

Die **IT-Produktion** (auch als *IT-Betrieb* oder *operative IT* bezeichnet) repräsentiert die unterste Ebene des IT-Governance-Frameworks. Sämtliche vom IT-Management und der Unternehmensführung veranlassten Maßnahmen zur Erreichung der IT-Ziele werden von der IT-Produktion in Form von Projekten und Linientätigkeiten operativ umgesetzt sowie Systeme und Messgrößen zur Analyse des Zielerreichungsgrades bereitgestellt.[26]

[24] vgl. [Fröhlich2007, S. 18]
[25] vgl. [Fröhlich2007, S. 20]
[26] vgl. [Fröhlich2007, S. 18]

Besonders bei der Implementierung von IT-Governance-Projekten geht die operative Umsetzung mit der Ausrichtung der IT-Prozesse an gängien Standards - beispielsweise mit Governance-Frameworks wie ITIL oder COBIT (vgl. Abschnitt 3.1.2 bzw. 3.1.3) - und Best Practices einher. Zielführend ist hier eine ausbalancierte Kombination aus standardisierten Vorgehensmodellen und unternehmensspezifischen Erfahrungen aus bisherigen Prüfungen und Beratungsprojekten.[27]

IT-Steuerung als Bindeglied

Die **IT-Steuerung** kann als Bindeglied zwischen dem IT-Management und der darunter liegenden IT-Produktion interpretiert werden. Bereits in der Einleitung wurde ansatzweise auf die IT-Steuerung zur Wahrung der Prozessintegrität sowie zur fortlaufenden Gewährung der Nachhaltigkeit und Effizienz verwiesen. Die in der IT-Strategie verankerten IT-Ziele und Handlungsvorgaben des IT-Managemens müssen nicht nur initial implementiert, sondern auch gesteuert, *«d.h. gemessen und auf ihre Wirksamkeit hin überprüft werden.»*[28]

Im Bereich der IT-Governance werden vor allem zwei Aspekte besonders fokussiert[29]. Einerseits werden alle Steuerungsmechanismen, d.h. Standortbestimmungen, interne und externe Messungen, zeitgleich eingesetzt und andererseits müssen Messgrößen im Hinblick auf die Compliance in einem richtig dimensionierten Kontrollsystem formuliert und dokumentiert werden. Die Beauftragung von externen Servicedienstleistern zur Bewältigung dieser IT-Steuerungsaufgaben stellt praktisch keine Seltenheit dar.

IT-Compliance als rechtliches Rahmenwerk

Die **IT-Compliance** wird im IT-Governance-Framework nach Andreas Fröhlich nur als Randkomponente betrachtet und eigentlich als Bestandteil der obersten Ebene, der IT-Governance, verstanden.

Alexander Teubner und Tom Feller[30] zeigen jedoch einen klaren Unterschied auf, da Compliance als *«Einhaltung von Vorgaben, Normen, Standards oder Gesetzen»*[31] anzusehen ist und dessen Konformität in IT-Audits und Zertifizierungen überprüft wird. *«Transparenz, Sicherheit und Korrektheit technikgestützter Informationsverarbeitung»*[32] stehen dabei im Vordergrund.

[27] vgl. [Fröhlich2007, S. 21]
[28] vgl. [Fröhlich2007, S. 21]
[29] vgl. [Fröhlich2007, S. 21]
[30] Alexander Teubner, Tom Feller, European Research Center for Information Systems, Westfälische Wilhelms-Universität Münster, Institut für Wirtschaftsinformatik, Forschungsgruppe für Informationsmanagement und Unternehmensführung
[31] vgl. [Teubner2008, S. 400]
[32] vgl. [Teubner2008, S. 405]

Auch Günter Müller[33] und Orestis Terzidis[34] unterscheiden Governance und Compliance einerseits durch handelnde und andererseits durch rechtliche Aspekte: *«Während Governance von den Handelnden selbst gesteckte Vorgaben umfasst, handelt es sich bei Compliance um regulatorische oder gesetzliche Auflagen.»*[35]

Zusammengefasst kann unter IT-Compliance also ein internationales und nationales Regelwerk aus Gesetzestexten und Standards verstanden werden, die durch intensive Einwirkung auf die IT-Governance und dessen Maßnahmen die Ebenen *IT-Management* und *IT-Produktion* nachhaltig beeinflussen.

1.1.4 Strategische Informationssysteme

Das erweiterte Modell nach Andreas Fröhlich deckt bereits ein breites Spektrum des Umfeldes der IT-Governance ab und zeigt die Komplexität und das vielfältige Zusammenspiel aller Systeme auf. Phyl Webb sieht zwei Kernkonzepte, welche die Entwicklung der IT-Governance maßgeblich beeinflusst haben (vgl. Abbildung 1.2[36]).

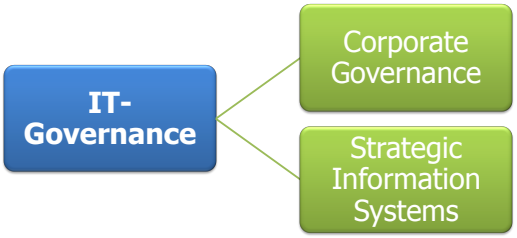

Abbildung 1.2: Entwicklung der IT-Governance nach Webb

Während die Corporate Governance bereits in Abschnitt 1.1.1 betrachtet wurde, unterstreichen die *strategischen Informationssysteme* die bisherigen Aussagen[37] und bringen neue Aspekte ein. Neben den bisher rechtlich verankerten bzw. verpflichtenden Vorgaben durch internationale oder nationale Gesetzgeber, wirft Phyl Webb u.a. folgende Fragestellungen zur strategischen Entwicklung des Unternehmens auf[38]:

- Wie können IT-Systeme für den eigenen Wettbewerbsvorteil genutzt werden?

[33] Günter Müller, Albert-Ludwigs-Universität Freiburg, Institut für Informatik und Gesellschaft, Abteilung Telematik
[34] Orestis Terzidis, SAP Research, Campus Based Engineering Center Deutschland
[35] vgl. [Müller2008, S. 341]
[36] vgl. [Webb2006, S. 2]
[37] Es wird u.a. auf eine effiziente Verwaltung der operativen IT-Ressourcen, die Entwicklung von Standardtechnologien und technischen Architekturen sowie die Abstimmung der IT-Abteilung mit den Endnutzern eingegangen. vgl. [Popp2007, S. 6]
[38] vgl. [Popp2007, S. 6]

- Wie ist es möglich, dass Systeme und Organisationen Bedrohungen erkennen und strategische Möglichkeiten ausnutzen können?
- Wie können zukünftige Entwicklungen für die eigene Strategie und für die anderen Systeme genutzt werden?

Diese besondere, strategische Ausrichtung des Unternehmens und die intensive Auseinandersetzung mit dem Thema *IT-Risikomanagement* (vgl. Abschnitt 1.1.5) zeigen weitere Einflussgrößen im Umfeld der IT-Governance.

1.1.5 Weitere Begriffe & Themenbereiche

IT-Security

Wird in der Literatur von IT-Governance und/oder IT-Compliance gesprochen, so ist meistens auch der Begriff **IT-Security** (oder *IT-Sicherheit*) auffindbar. Durch die dezentralen IT-Infrastukturen und die Mobilität von Daten auf unterschiedlichen Kommunikationskanälen hat die Diskussion um den Schutz von Verfügbarkeit, Vertrauchlichkeit und Integrität unterschiedlichster Daten einen Spitzenplatz eingenommen.[39]

Die Verbindung zur Governance und Compliance liegt damit auf der Hand: Eine zielorientierte, korrekte und vor allem rechtlich nachvollziehbare IT-Unternehmensführung ist nur mit validierten und gesicherten Datenbeständen möglich. Die IT-Security kann also als eines von vielen Teilwerkzeugen zur Implementierung von IT-Governance und IT-Compliance gesehen werden.[40]

IT-Risikomanagement

Maßnahmen des **IT-Risikomanagements** sind Teil der IT-Governance-Umsetzung sowie der IT-Management-Implementierung und müssen kontinuierlich (und nicht nur einmalig) betrieben werden. Michael Klinger[41] und Christian Cuske[42] empfehlen dabei klassische Methoden des Risikomanagements, die nach dem Phasenmodell «Verstehen», «Identifizieren» und «Bewerten» angewandt werden und mit Gegenmaßnahmen sowie einem umfassenden Berichtswesen abschließen.[43]

Besonders wichtig ist dabei eine vollständige Abdeckung aller IT-Risiken unter Zuhilfenahme gängiger Standards wie dem IT-Grundschutzhandbuch des deutschen Bundesamtes

[39] vgl. [Grünendahl2009, S. 1]
[40] Diese Arbeit wird das Gebiet der IT-Security nur am Rande beleuchten bzw. im Zuge der Rahmenwerke und Implementierungsansätze indirekt darauf eingehen. Das gesamte Umfeld der IT-Security würde den Umfang dieser Arbeit sprengen und kann in der einschlägigen Fachliteratur nachgelesen werden.
[41] Michael Klinger, Country Managing Director, Protiviti Deutschland
[42] Christian Cuske, Leiter IT Solutions, Protiviti Deutschland
[43] vgl. [Armin2008, S. 414]

für Sicherheit in der Informationstechnik (BSI)[44] oder dem COBIT-Framework (vgl. Abschnitt 3.1.3). Die gesamte Werkschöpfungskette - und damit verbunden auch das operative Management - soll Problembereiche identifizieren und über Modelle sowie eine einheitliche Sprache ein gemeinsames, methodisches Vorgehen zur Bewältigung dieser Risiken anstreben.[45]

Den Vorteil einer wirkungsvollen IT-Governance sieht Christian Cuske vor allem in der Erkennung und Bewältigung von Risiken. Zwar sind diese dadurch nicht geringer, jedoch kann intensiver bzw. zielgerichtet gegen sie vorgegangen werden. Michael Klinger unterstreicht diese Aussage und sieht die IT-Governance als *«übergeordnetes Rahmenwerk für die Bewältigung von IT-Risiken im Unternehmen.»*[46]

IT-Audits

Im Rahmen von **IT-Audits** (oft auch als *IT-Revisionen* bezeichnet) werden die gesamte IT-Infrastruktur (Hard-, Soft- und Middleware) sowie sämtliche, finanzrelevante Datenbestände des Unternehmens überprüft. Anhand von Strategien und Grundsätzen sollen Effizienz, Effektivität und ökonomisches Verhalten festgestelt und Missinvestitionen, Betrugsfälle oder Falschbuchungen aufgedeckt werden. Die Abhaltung solcher IT-Audits erfolgt regelmäßig und kann durch den Vorstand, ein eigenes Auditing-Commitee, eine staatliche Institution oder durch externe Audit-Dienstleister bzw. Wirtschaftsprüfer durchgeführt werden.[47]

Anna Carlin und Frederick Gallegos[48] sehen das Hauptziel von IT-Audits im Monitoring der Geschäftsaktivitäten sowie im Schutz der Interessen der beteiligten Stakeholder (Manager, Mitarbeiter, Kunden und Investoren). Dazu werden im Rahmen von IT-Audits Sicherheit, Zuverlässigkeit, Integrität und die Privatsphäre von Informationssystemen validiert sowie ein *«Selbstcheck auf Legalität und Angemessenheit»* durchgeführt.[49]

Die vorgestellten Begriffe und Schlagworte zeigen das weitreichende Umfeld des IT-Governance-Frameworks auf und sollen ein Gefühl für dessen Komplexität und Differenzierung geben. Kann *IT-Governance* mit all ihren Facetten somit als Querschnittsmaterie heutiger Unternehmungen verstanden werden?

[44] vgl. `http://www.bsi.bund.de`, zuletzt abgerufen am 30.01.2010
[45] vgl. [Armin2008, S. 414]
[46] vgl. [Armin2008, S. 415]
[47] vgl. [Carlin2007, S. 87]
[48] Anna Carlin, Frederick Gallegos, California State Polytechnic University, Pomona
[49] vgl. [Carlin2007, S. 87]

1.1.6 IT-Governance als Querschnittsmaterie

Die bisherigen Ausführungen haben gezeigt, dass IT-Governance zwar als klare Vorstandsaufgabe des CIO (vgl. Abschnitt 3.2.2) zu verstehen ist, jedoch viele Unternehmensbereiche und Mitarbeiterschichten vom Top-Management über die lokale/regionale Bereichs-/Ressortleitung bis zur ausführenden IT-Produktion beeinflusst. Auch die strategischen Aspekte nach Phyl Webb weisen auf eine solche Abhängigkeit hin.

Die IT-Governance gibt dem Top-Management die Möglichkeit Entscheidungen an nachgelagerte IT-Bereiche des operativen Geschäftes zu delegieren und ihnen die Entscheidungs- und Steuerungsbefugnis zu übertragen. Die Letztentscheidung obliegt jedoch weiterhin dem CIO, um eine einheitliche Entwicklungsrichtung innerhalb des Unternehmens zu gewährleisten.[50] Die dadurch entstehende Entlastung des Managements kann in die strategische Weiterentwicklung des Unternehmens investiert werden.

IT-Governance kann somit eindeutig als Querschnittsmaterie heutiger Unternehmungen betrachtet werden und soll neben der Umsetzung von sozialen und ökonomischen Zielen vor allem die Beachtung der rechtlichen Regulatorien im Rahmen der *IT-Compliance* gewährleisten.

1.2 IT-Compliance

1.2.1 Corporate Compliance

Vergleichbar mit der Corporate Governance als Mutter der IT-Governance existiert auch für die IT-Compliance eine übergeordnete Managementaufgabe - die *Corporate Compliance*. Primitiv formuliert, kann der aus dem anglo-amerikanischen Rechtskreis kommende Begriff, mit der *«Pflicht, die für das Unternehmen geltenden Gesetze einzuhalten»*[51], beschrieben werden. Eigentlich könnte das rechtskonforme Handeln von Unternehmen in der heutigen Wirtschaft als gegeben vorausgesetzt werden. Viel weitreichender ist jedoch die Umsetzung der Corporate Compliance durch die Geschäftsführung bis hin zum Aufbau einer Compliance-Organisation (vgl. Abschnitt 3.2.1).

Ein funktionierendes *Compliance-Management* hat nicht nur den Vorteil von rechtlicher Absicherung, sondern bringt auch wettbewerbstechnische und volkswirtschaftliche Vorteile mit sich, da Kunden und Lieferanten auf eine gesetzeskonforme und risikominimierte Geschäftsbeziehung aufbauen können.[52] Bei einem Rechtsverstoß oder der Miss-

[50] vgl. [Popp2007, S. 7]
[51] vgl. [Wecker2009, S. 33]
[52] vgl. [Wecker2009, S. 33-34]

achtung von Compliance-Vorgaben sind Konsequenzen wie Aufsichtsratseingriffe, Vergabesperren/Blacklisting oder extrem hohe Bußgelder keine Seltenheit.[53]

1.2.2 Eingliederung der Corporate Compliance

Besonders schwierig gestaltet sich die Eingliederung der Corporate Compliance in bestehende Rahmenwerke bzw. die Definition von Über- und Unterordnung zur Corporate Governance.

Referenziert auf das Pyramidenmodell der IT-Governance nach Andreas Fröhlich (vgl. Abbildung 1.1 in Abschnitt 1.1.3) wird die (IT-)Compliance als Einflussfaktor der ganzheitlichen (IT-)Governance interpretiert. Auch Hannes Hausegger verweist auf ein Modell nach Ernst & Young (2005)[54] nach welchem «Gesetze und Regulative» als Umweltbedingungen zu verstehen sind. IT-Governance genießt somit übergeordneten Charakter und die IT-Compliance ist nur eine von vielen, beeinflussenden Komponenten.

Anders sehen dies etwa Alexander Teubner und Tom Feller, welche den Regelungsbereich der Corporate Compliance über den der Corporate Governance stellen: *«Während sich letztere speziell auf das verantwortungsvolle Handeln des Managements bezieht und hier insbesondere die Kompetenzen und Verantwortung der Führungskräfte im Blick hat, bezieht sich erstere auf ein regelkonformes Unternehmenshandeln allgemein. Die Vorgaben, deren Einhaltung im Rahmen der Compliance überprüft wird, richten sich daher nicht nur auf das Handeln des Managements, sondern auf das Handeln der Organisationsmitglieder generell.»*[55]

Besondere Bedeutung kommt dabei den Regelungen in den Risikobereichen des Unternehmens sowie dem Risikomanagement zu. Hinsichtlich einer verantwortlichen und langfristigen Wertschöpfung bedarf es einer auf Corporate Compliance ausgerichteten Unternehmensführung. Dies ist - im Rahmen der Risikoanalyse - eines der fünf Kernelemente der Compliance, die in Abschnitt 1.2.3 Erläuterung finden.

1.2.3 Fünf Elemente der Compliance

Um eine strukturierte Compliance-Vorgehensweise und die damit verbundene aktive Risikovorbeugung im Unternehmen betreiben zu können, stellt Eberhard Vetter ein fünfstufiges Modell[56] vor (vgl. Abbildung 1.3[57]).

[53] vgl. [Wecker2009, S. 38-39]
[54] vgl. [Hausegger2007, S. 7]
[55] vgl. [Teubner2008, S. 400]
[56] vgl. [Wecker2009, S. 42-43]
[57] vgl. [Wecker2009, S. 42-43]

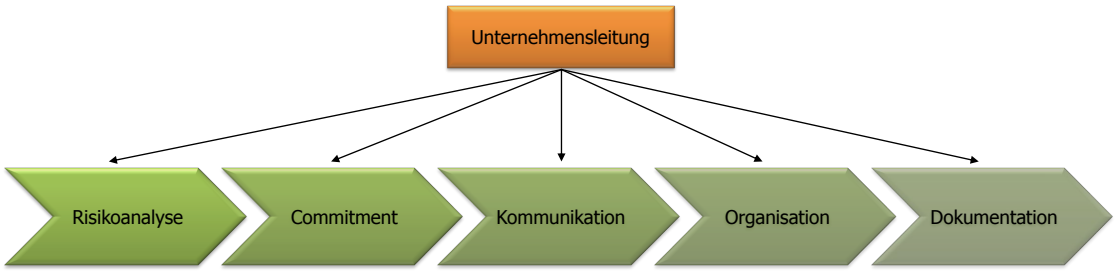

Abbildung 1.3: Fünf Elemente der Compliance

In einer ersten **Risikoanalyse** gilt es die Risiken des jeweiligen Unternehmens zu identifizieren, den möglichen Schadensumfang und dessen Eintrittswahrscheinlichkeit zu ermitteln sowie Schritte zur Risikovorbeugung- und -minimierung abzuleiten.

Als zweites Element muss die gesamte Compliance zur «Chefsache» erklärt und dort auch glaubwürdig und mit Nachdruck betrieben werden. Es gilt die gesamte Belegschaft von einer sinnvollen und korrekten Anwendung der Compliance zu überzeugen und entsprechende Sanktionierungsmaßnahmen im Falle der Nichteinhaltung festzusetzen. Nur so kann es ein gemeinsames **Commitment** zur Umsetzung dieser rechtlichen Regulatorien geben.

Wenn sich die Geschäftsführung nun auf eine Compliance-Strategie geeinigt hat, müssen diese Vorschriften und Regularien zur Prävention und Kontrolle nicht nur an Mitarbeiterinnen und Mitarbeiter, sondern auch an Geschäftspartner weitergegeben werden. Eine offene **Kommunikation** - beispielsweise in Form eines Mission Statements, eines Verhaltenskodex oder regelmäßigen Präsentationen durch Compliance-Beauftragte - ist für die Einhaltung dieser Regelungen auf allen Hierarchieebenen unerlässlich.

Wie auch bei anderen Geschäftsfeldern des Unternehmens muss die Compliance über eine klar definierte **Organisation** verfügen. Von einer ein- oder mehrköpfigen Unternehmensleitung über Ressort- und Bereichsleitung bis zu den ausführenden Stellen des Organigramms muss es klare Verantwortungsbereiche, Zuständigkeiten und Kontrollbefugnisse geben.

Sämtliche die Compliance betreffenden Schritte wie etwa Entscheidungen, Prozesse, Maßnahmen oder Berichtswege des Unternehmens müssen für spätere Audits oder Beweislastregelungen schriftlich festgehalten werden. Die **Dokumentation** beinhaltet beispielsweise Sitzungsprotokolle, Schadens- oder Misstandsberichte aber auch Telefongesprächsmitschriften oder die Betriebs- und Geschäftsordnung.

1.2.4 Aufgaben & Anforderungen der IT-Compliance

Das eigentliche Aufgabengebiet der *IT-Compliance* ist, mit einigen technischen Adaptierungen, ein sehr zentraler Bestandteil der unternehmensweiten Corporate Compliance. Hans-Jürgen Pollirer definiert IT-Compliance als *«Einhaltung und Umsetzung von regulatorischen Anforderungen im weitesten Sinn mit der Zielsetzung einen verantwortungsvollen Umgang mit allen Bereichen der IT zu erreichen»*.[58]

In Verbindung mit den Aufgaben der Mutterdisziplin treten folgende IT-Aufgaben der Compliance zunehmend in den Vordergrund[59]:

- Bildung einer Gesamtheit an organisatorischen Aufsichts-, Schulungs- und Kontrollmaßnahmen der Geschäftsleitung zur Vermeidung von Gesetzesverstößen durch das Management und die untergeordneten IT-Bereiche.
- Sicherstellung der Beherrschung von IT-Risiken durch Risikoidentifikation, Risikoanalyse, Risikobewertung und Risikosteuerung.
- Schutz des Unternehmens vor erkennbaren Gefahren durch gewissenhafte Umsetzung der Sorgfaltspflicht.
- Wahrnehmung der Einflussfaktoren bzw. Bedeutung der Informationstechnologie im eigenen Unternehmen.

Eine der größten Schwierigkeiten der IT-Compliance bzw. gleichzeitige Anforderung an diese ist die übersichtliche Darstellung der Vielzahl an internationalen und nationalen Gesetzestexten, die bei der nachhaltigen Praktizierung der genannten Aufgaben beachtet werden müssen. Neben einschlägigen EU-Verordnungen, EU-Richtlinien und nationalen Gesetzen kommen noch sektorenspezifische Anforderungen (etwa im Bereich der Kapitalgesellschaften) oder Regulatorien aus anderen Fachrichtungen, wie etwa dem Steuerrecht oder der Wirtschaftsprüfung, hinzu. Weltweit wird die Anzahl der Compliance-Anforderungen (im weitesten Sinn) auf etwa 25.000 geschätzt.[60]

Als zweiter Eckpfeiler der IT-Compliance wird von vielen Experten[61] die persönliche Haftung der Unternehmensleitung (Aufsichtsrat, Vorstand oder Gesellschafter und leitende Angestellte) bei der Missachtung regulatorischer Vorgaben genannt. Bestehende Gesetzesgrundlagen (etwa das österreichische Unternehmensgesetzbuch (UGB) - vormals Han-

[58] vgl. [Pollirer2008, F. 4]
[59] vgl. [Wecker2009, S. 119-121]
[60] vgl. [Wecker2009, S. 121]
[61] vgl. [Wecker2009, S. 120] bzw. [Grünendahl2009, S. 2]

delsgesetzbuch (HGB)[62]) werden dahingehend ergänzt, dass risikovorbeugende Entwicklungsmaßnahmen, informationsrelevante Schutzmaßnahmen und angemessene Berichterstattungssysteme umgesetzt bzw. betrieben werden müssen.

Lars Lensdorf und Udo Steger, Heymann & Partner Rechtsanwälte, nennen im Rahmen eines Vortrags der *Deutschen Stiftung für Recht und Informatik*[63] exemplarisch fünf Top-Anforderungen an die IT-Compliance, die ergänzend bzw. teilweise inhaltlich ähnlich den bereits genannten Eckpfeilern nach Gregor Wecker und Ralf-T. Grünendahl sind.[64]

- Datenschutz und Datensicherheit
- Arbeitsrecht
- Unternehmensorganisation
- Buchhaltung, Rechnungslegung, Prüfung
- Banken und Finanzdienstleiter (sektorenspezifisch)

IT-Compliance betrifft somit den unmittelbaren IT-Betrieb sowie sämtliche IT-Systeme und Prozesse im Unternehmen. Von der Buchhaltung und Lohnverrechnung über die Logistikadministration bis hin zum Waren- und Verkaufsmanagement muss der IT-Compliance Rechnung getragen werden. Und bei der heutigen Verknüpfung bereichsübergreifender Geschäftsprozesse ist Compliance ohne funktionierende IT-Compliance nicht mehr zu gewährleisten.[65]

1.2.5 Internes Kontrollsystem (IKS)

Die vorgestellten Elemente, Aufgaben und Anforderungen der IT-Compliance müssen nun im Rahmen eines *internen Kontrollsystems* (IKS) etabliert und in die Unternehmensabläufe integriert werden. Ein IKS besteht somit *«aus den Grundsätzen, Verfahren und Maßnahmen, die der organisatorischen Umsetzung der Managemententscheidung dienen, damit die Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit des Unternehmens gesichert ist, die Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung gewährleistet ist und die maßgeblichen rechtlichen Vorschriften eingehalten werden.»*[66]

[62] dRGBl S 1897/219 idF 2009/71
[63] vgl. `http://www.dsri.de`, zuletzt abgerufen am 30.01.2010
[64] vgl. [Lensdorf2006, F. 12]
[65] vgl. [Lensdorf2006, F. 5]
[66] vgl. [Meyer2009, S. 225]

Primäre Ziele des IKS sind dabei insbesondere[67]

- die Bewahrung des Vermögens des Unternehmens,
- die Gewährleistung der Zuverlässigkeit des Rechnungswesens,
- die Verbesserung der Effizienz unternehmerischer Abläufe und
- die Sicherung der Einhaltung der Geschäftspolitik.

Als Einflussfaktoren eines heute üblichen, internen Kontrollsystems können vor allem[68]

- Größe und Komplexitätsgrad des Unternehmens,
- Rechtsform und Organisation des Unternehmens,
- Diversifikation und Komplexität der Geschäftsfelder,
- regulatorische Anforderungen und
- informationstechnische Prozesse

verstanden werden.

Anhand dieser Indikatoren wird das Design eines IKS gewählt sowie dessen Aufrechterhaltung, Weiterentwicklung und Überwachung durch die Führungsebenen gewährleistet.[69] Nach österreichischem Recht hängt die Dimensionierung des IKS beispielsweise von den Regelungen des §82 Aktiengesetz[70] ab, welcher besagt, dass der Vorstand für die Implementierung eines den Anforderungen des Unternehmens entsprechenden IKS verantwortlich ist.

Während im europäischen Raum überwiegend Kontroll- und Überwachungsaktivitäten den Kern des internen Kontrollsystems darstellen, geht die Definition der amerikanischen Gesellschaft weit über die eigentlichen Kontrolltätigkeiten hinaus. Vielmehr zählt dort auch das Risiko- und Informationsmanagement zu den Komponenten eines modernen IKS.[71]

Zur praktischen Umsetzung eines Kontroll- und Überwachungssystems wurde 1992 vom *Committee of Sponsoring Organisations of the Readway Commission* ein neues Modell vorgestellt - der COSO-Würfel (vgl. Abbildung 2.2). Das damals als de-facto Standard

[67] vgl. [Hausegger2007, S. 16-17]
[68] vgl. [Meyer2009, S. 225-226]
[69] vgl. [Meyer2009, S. 225-226]
[70] BGBl 1965/98 idF BGBl I 2009/71
[71] vgl. [Hausegger2007, S. 16-17]

etablierte Rahmenwerk ist heute von der amerikanischen Börsenaufsicht explizit vorgeschrieben, um ein Compliance konformes IKS zu implementieren (vgl. Abschnitt 2.5.1). Auch im europäischen Raum kommt das mittlerweile 8-stufige Modell immer häufiger zur Anwendung.[72]

1.3 Warum IT-Governance und IT-Compliance?

Nach diesem ersten Abschnitt und einem Überblick über das Umfeld, die Begriffe und Defintionen sowie Modelle und Einsatzmöglichkeiten von Corporate/IT-Governance und Corporate/IT-Compliance fragt sich die bewusste Leserin und der bewusste Leser möglicherweise nach dem Sinn eines solch komplexen Systems. Warum ist IT-Governance ein topaktuelles Thema und warum muss die IT-Compliance rechtliche Sanktionen bei der Nichteinhaltung von eigentlich selbstverständlichen, gesetzlichen Regulatorien definieren?

Die Antwort auf diese Frage und damit verbunden auch der Ursprung des intensiven Aufkommens der IT-Governance und IT-Compliance ist im Jahre 2001 in den USA verankert. Die bislang größten Finanzskandale von Enron und Worldcom, deren Folge unter anderem die Entwicklung des US-Bundesgesetzes *Sarbanes-Oxley Act* (SOX, SOA)[73] war, haben die amerikanische Börsenaufsicht in Aufruhr versetzt. Um solche Bilanzskandale in Zukunft zu vermeiden, soll mit diesem Gesetzestext das Vertrauen der Anleger in die Richtigkeit und Verlässlichkeit der veröffentlichten US-Finanzdaten wiederhergestellt werden.[74]

Etwa drei Jahre später - also 2005 - wurde dieses Governance- und Compliance-Konzept für den europäischen Raum adaptiert und findet seither regelmäßigen Einzug in aktuelle Management- und Wirtschaftsdiskussionen. Da es jedoch enorme Unterschiede zwischen dem anglo-amerikanischen und den europäischen Rechtssystemen gibt, wurden eigene Rechtsakte, Richtlinien und Verordnungen auf EU-Ebene geschaffen. Es ist Aufgabe des nächsten Kapitels einen Überblick über die Rechtslage in Europa zu geben und in weiterer Folge die nationale Rechtssituation in Österreich zu analysieren.

[72] vgl. [Hausegger2007, S. 16-17]
[73] Pub.L. 107-204, 116 Stat. 745
[74] vgl. [Müller2008, S. 341] bzw. [Fröhlich2007, Vorwort]

2 Rechtliche Rahmenbedingungen

IT-Governance und *IT-Compliance* wurden im einleitenden Kapitel in unterschiedliche Teilaspekte zerlegt und in ganzheitlichen Rahmenwerken bzw. strukturellen Gliederungen präsentiert. Dieses sehr komplexe Gebilde - beginnend bei der Corporate Governance über die IT-Governance mit integriertem IT-Management und operativer IT-Produktion bis hin zur IT-Compliance als rechtliches Framework der unternehmensweiten Corporate Compliance - soll nun hinsichtlich der rechtlichen Rahmenbedingungen von bzw. für Unternehmen untersucht werden.

Wie sich anhand der Komplexität bereits vermuten lässt, gibt es eine Vielzahl an internationalem Völkerrecht, EU-weiten Verordnungen/Richtlinien/Kodizes und nationalen Gesetzesgrundlagen, die bei der Umsetzung und Implementierung von IT-Governance- oder -Compliance-Maßnahmen beachtet werden müssen. Insbesondere die differenzierenden Rechtssysteme unterschiedlichster Staaten sowie kulturelle und ökonomische Unterschiede erschweren die Adaption einer gemeinsamen IT-Governance und IT-Compliance.[75] Viele Unternehmen stehen daher - nicht zuletzt aufgrund der raschen Globalisierung und ständigen Expansion in östliche Länder - vor neuen Herausforderungen, die es zu bewältigen gilt. Hinzu kommt noch der erhebliche, finanzielle Aufwand zur Etablierung einer gesetzeskonformen Unternehmensführung mit integrierter Verantwortung.

Ziel dieses Kapitels ist es, nach einer kurzen geschichtlichen Einführung in die Entwicklung der rechtlichen Regulatorien in der letzten Dekade, der Leserin bzw. dem Leser vor allem die europäische Rechtslage sowie die Umsetzung in österreichisches Recht näher zu bringen. Parallel dazu existieren freiwillige Kodizes und Fachgutachten zu Themen der IT-Governance. Abschließend soll ein kurzer Ausblick in die internationale Rechtslage mit besonderem Augenmerk auf die amerikanischen Bundesgesetze *Sarbanes-Oxley Act* (SOX) und *Foreign Corrupt Practices Act* (FCPA)[76] gewährt werden.

[75] vgl. [Hausegger2007, S. 2]
[76] 15 U.S.C. §§ 78dd-1, et seq.

2.1 Wie alles begann...

Gerade in der letzten Dekade haben die Begriffe *IT-Governance* und *IT-Compliance* extrem an Bedeutung gewonnen. Sowohl bei nationalen und internationalen Konferenzen bzw. Institutionen[77], einschlägigen, wissenschaftlichen Fachzeitschriften[78] als auch auf Webportalen von internationalen Konzernen und Unternehmensberatern[79] sind diese Begriffe topaktuell und werden intensiv diskutiert. Doch woher kommt dieser Governance- und Compliance-Hype?

Der Ursprung der heutigen Brisanz dieser Themen stammt aus den Vereinigten Staaten von Amerika (USA) und enstand um die letzte Jahrtausendwende. Als zentrale Auslöser können die größten Finanzskandale in der amerikanischen Wirtschaftsgeschichte der beiden Multikonzerne *Enron* und *Worldcom* gesehen werden.

2.1.1 Enron & Worldcom - Die Hype-Auslöser

Enron war das siebtgrößte Unternehmen der USA und wurde im Jahre 1985 durch die Fusion zweier Gasunternehmen gegründet. Innerhalb nur weniger Monate entwickelte sich ein kleines Startup-Unternehmen unter dem damaligen Enron-CEO Jeff Skilling zu einem Multikonzern der Wall Street und wurde mehrmals als «Innovativstes Unternehmen» mit genialer Unternehmensstrategie ausgezeichnet.[80]

Geschäftsgegenstand von Enron war primär der Handel mit Rohstoffen und Energiequellen über ein Onlineportal und in späteren Geschäftsjahren der Vertrieb von Waren und Vorräten aller Art (beispielsweise Werbeflächen, Breitbandkapazität, verschiedenste Verträge und Termingeschäfte). Während der Energie- und Rohstoffmarkt gut funktionierte, brachten die anderen Geschäftszweige wenig bis gar keine Einnahmen - Tatsachen die jedoch durch das flurierende Primärgeschäft verschleiert wurden.[81]

Im weiteren Verlauf wurden die Geschäftstaktiken von CEO Skilling immer undurchschaubarer und selbst die unternehmenseigenen Finanzexperten hatten keinen völligen Durchblick. Gleichzeitig sackte die Kommunikationspolitik immer weiter zusammen, da

[77] vgl. etwa European Corporate Governance Institute (`http://www.ecgi.org`, zuletzt besucht am 30.01.2010) oder Österreichischer Arbeitskreis für Corporate Governance (`http://www.wienerborse.at/corporate/index.htm`, zuletzt besucht am 30.01.2010)

[78] vgl. etwa Wirtschaftsinformatik (`http://www.wirtschaftsinformatik.de`, zuletzt besucht am 30.01.2010) oder Manager Magazin (`http://www.manager-magazin.de`, zuletzt besucht am 30.01.2010)

[79] vgl. etwa die Konzernwebseite der Telekom Austria Group (`http://www.telekomaustria.com/ir/codex.php`, zuletzt besucht am 30.01.2010) oder die Unternehmenspräsenz der Deloitte Audit Wirtschaftsprüfungs GmbH. (`http://www.deloitte.com/view/en_GX/global/services/enterprise-risk-services/index.htm`, zuletzt besucht am 30.01.2010)

[80] vgl. [Hillenbrand2002]

[81] vgl. [Hillenbrand2002]

die Unternehmensleitung keinerlei Informationen über Finanz- und Ertragslage an die Öffentlichkeit weitergab. Der erste öffentliche Rückschlag fand im November 2001 statt, da Enron seine Gewinne der vergangenen vier Jahre um mehr als 500 Millionen Dollar nach unten korrigieren musste.[82]

Am 4. Dezember 2001 musste Enron nach dem Verfall der eigenen Aktie von einst 90 Dollar auf unter 5 Dollar endgültig Konkurs anmelden. Beispielhaft seien folgende Fakten genannt, die den Enron-Skandal herbeigeführt und schlussendlich den Konkurs erwirkt haben:[83]

- Unter den etwa 1000 an Enron beteiligten Firmen und Institutionen befanden sich 881 Briefkastenfirmen, die Steuerhinterziehungen und Abgabenbefreiungen ermöglichten.
- Der Bösenwert[84] des Unternehmens nahm 1998 um 40%, 1999 um 58% und 2000 um satte 89% zu.
- Enron hatte enormen politischen Einfluss und investierte zwischen 1991 und 2001 etwa 6 Millionen Dollar in Wahlkampfspenden (u.a. von George W. Bush). Als Gegenleistung erhielt Enron das Recht Öl- und Gasfelder in Mosambik, Argentinien, auf den Philippinen oder in Indien auszubeuten.

Die Folgen dieses Börsenskandals hatten nicht nur intensive Auswirkungen auf die amerikanische Wirtschaft, sondern beeinträchtigten auch europäische Institutionen sowie Aktieninhaber und Gläubiger. Doch der nächste Skandal befand sich bereits im Aufbau: Im Sommer 2002, also etwa sechs Monate nach der Enron-Krise, meldete der amerikanische Telekomkonzern Worldcom inklusive aller US-Töchter in New York Konkurs an.

Worldcom war in mehr als 65 Ländern der Erde aktiv und betreute mit rund 60.000 Mitarbeiterinnen und Mitarbeitern Millionen von Telefon- und Tausende von Unternehmenskunden. Die Telekomgesellschaft betrieb das größte Internet-Backbone-Netz der Welt und stellte in den USA 30% der Bandbreite auf den 20 wichtigsten Internetrouten zur Verfügung. Trotz einem Umsatz von etwa 35 Milliarden Dollar sind die unternehmerischen Aktien im Jahre 1999 von knapp 65 Dollar auf nur neun Cent abgestürzt.[85]

Die Dimension des Worldcom-Skandals übertrifft die Insolvenz des Energieriesen Enrons um ein Vielfaches. Aufgrund von Falschbuchungen[86] in der Höhe von 3,85 Milliarden

[82] vgl. [Hillenbrand2002]
[83] vgl. [SoZ2002, S. 13]
[84] auch Shareholder Value genannt
[85] vgl. [Kuri2002]
[86] Worldcoms Finanzchef Scott Sullivan buchte seit 2001 quartalsweise Zahlungen für lokale Anbieter für

Dollar[87] im Jahr 2001 und die Verbuchung von extrem erhöhten Gewinnen, verzeichnete das Unternehmen eine Schuldensumme von mehr als 30 Milliarden Dollar.[88] Später wurde bekannt, dass diese Bilanzfälschungen bis ins Jahr 2000 zurückreichten, da die Zahlen der vergangenen fünf Quartale korrigiert werden mussten.[89]

Wie auch bei Enron stand Worldcom unter großem, politischem Einfluss und zog weitere, beteiligte Telekomanbieter - wie beispielsweise den texanischen Dienstleister EDS - in Mitleidenschaft. Umfangreiche Kooperationen im dreistelligen Millionenbereich sollten den Betrieb der Computer- und Telefonnetze beider Unternehmen gewährleisten. Sowohl die US-Börsenaufsicht als auch das US-Justizministerium wurden in diesem Fall eingeschaltet.[90]

Basierend auf diesen Skandalen mit internationalen Wirtschaftsfolgen wurde in den USA der *Sarbanes-Oxley Act* (SOX, vgl. Abschnitt 2.5.1) verabschiedet. Ziel war dabei die Wiederherstellung des Vertrauens von Kunden, Gläubigern und Eigentümern in die öffentliche Finanzberichtserstattung amerikanischer Konzerne.

2.1.2 Skandale in Europa

Nach den amerikanischen Präsenzfällen wurde die europäische Wirtschaft im Jahr 2003 von vergleichbaren Bilanzierungsskandalen heimgesucht. Als Konsequenz dieser Zwischenfälle bei Ahold und Parmalat hat die Kommission der Europäischen Union den «europäischen Sarbanes-Oxley Act» erlassen - die 8. EU-Richtlinie (Abschlussprüfer-Richtlinie, vgl. Abschnitt 2.2).[91]

Ahold[92], ein niederländischer Einzelhandelskonzern, tätigte Scheinbuchungen bei Umsätzen bzw. Erträgen im dreistelligen Millionenbereich, um die von der US-Tochter Foodservice vorgegebenen Quartalsziele zu erreichen. Die verantwortlichen Manager erhielten ein im Vergleich zu amerikanischen Prozessen geringes Strafausmaß, obwohl der Konzern fast vollständig ruiniert war.[93]

Parmalat[94], ein italienischer Lebensmittelkonzern, wurde Ende 2003 durch einen Finanzskandal erschüttert. Das Unternehmen versuchte durch Fälschungen in der Bilanzierung

die Weiterleitung von Gesprächen - einer der größten Kostenblöcke - fälschlicherweise als Investitionsaufwand statt als operative Kosten ein. (vgl. [Cloer2002])

[87] entspricht etwa der 6-fachen Summe der Gewinnkorrekturen von Enron
[88] vgl. [Kuri2002]
[89] vgl. [Cloer2002]
[90] vgl. [Cloer2002]
[91] vgl. [Beyond2007a]
[92] vgl. `http://www.ahold.com`, zuletzt abgerufen am 30.01.2010
[93] vgl. [Beyond2007a]
[94] vgl. `http://www.parmalat.com`, zuletzt abgerufen am 30.01.2010

nicht vorhandenes Vermögen vorzutäuschen. Bekannt wurde dieses Manöver erst im Rahmen des Jahresabschlusses und führte zu einem Einbruch des Aktienkurses. Der Fehlbetrag von Parmalat wurde in der Höhe von acht Millionen Euro festgestellt. Nach Untersuchungen in den Tochter- und Partnerunternehmen des italienischen Konzerns - darunter Fußballclubs, Banken und Scheinfirmen - deckten Wirtschaftsprüfer Missstände von 23 Millionen Euro auf.[95]

Marco Becht[96], Professor für Finanzen und VWL an der Freien Universität in Brüssel und Geschäftsführer des *European Corporate Governance Instituts*[97], sieht die Problematik solcher Skandale einerseits in ungenügenden Investitionen in gute Unternehmensführung und gezielte Aufsichtsgremien aber auch in den risikobelohnenden Premienmodellen für Top-Manager. Führungskräfte sollen wieder auf den Boden der ökonomischen Realität zurückgeholt werden und ein adäquates Entlohungsmodell auferlegt bekommen.[98]

Ergänzend zeigt Marco Becht Zeichen von Systemversagen auf, da heute Themen der Steuerhinterziehung und des Finanzbetrugs offen diskutiert werden. Hier gilt es durch Reformen und Regulative das System zu stärken, wobei Managementversagen weniger durch strengere Haftungsregelungen, sondern vielmehr durch Konsequenzen im sozialen Umfeld eines Managers und dessen zukünftiger Karriereentwicklung zu setzen sind. Regulative können dabei sowohl verpflichtenden als auch freiwilligen Charakter aufweisen, da Unternehmen heute viel offener und sensibler gegenüber Themen der Corporate Governance sind.[99]

2.2 8. EU-Richtlinie

Die 8. EU-Richtlinie[100] aus dem Jahr 2006 ist laut Beyond Consulting[101] und Hannes Hausegger[102] mit dem Sarbanes-Oxley Act (SOX, vgl. Abschnitt 2.5.1) aus den USA vergleichbar. Sie gibt eine konkrete Aufstellung von Bilanzierungs- und Reportingkennzahlen vor, die das Vertrauen der Öffentlichkeit in die Buch- und Bilanzführung der europäischen Unternehmen stärken und länderübergreifende Finanzskandale vermeiden soll. Der Geschäftsführung wird dabei eine hohe Verantwortung hinsichtlich der Überprüfung und Korrektheit dieser Finanzdaten auferlegt.

[95] vgl. [Beyond2007a]
[96] vgl. [Amann2008]
[97] vgl. http://www.ecgi.org
[98] vgl. [Amann2008]
[99] vgl. [Amann2008]
[100] Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates
[101] vgl. [Beyond2007b]
[102] vgl. [Hausegger2007, S. 2]

Wie für Richtlinien der europäischen Union üblich, muss auch die Richtlinie 2006/43/EG in nationales (in unserem Fall österreichisches) Recht überführt werden und kann weiterführende, länderspezifische Einschränkungen enthalten. Ähnlich wie bei SOX ist auch bei der achten EU-Richtlinie mit hohen Umsetzungskosten und zusätzlichem Implementierungsaufwand für die Unternehmen zu rechnen.[103]

Bereits in der Einleitung wurde auf die vorhandenen IT-Kosten sowie die vollständige Auslastung der verfügbaren IT-Ressourcen hingewiesen. Diese Tatsache bringt den Nachteil mit sich, dass die genannten Neuimplementierungen und strukturellen Umstellungen aufgrund der europaweiten Vorschriften vernachlässigt oder nicht mit entsprechender Sorgfalt umgesetzt werden. Diese Missachtung birgt großes Gefahrenpotenzial in sich und bedarf daher zusätzlicher IT-Sicherheits- und Risikomanagementmaßnahmen.[104]

2.2.1 Komponenten & Addressaten der Richtlinie

Die 8. EU-Richtlinie war bis 29. Juni 2008 in nationales Recht umzusetzen und nimmt regulative Änderungen an bestehenden Richtlinien aus den Jahren 1978, 1983 und 1984 vor. Zusammengefasst werden diese Anpassungen als *EUROSOX* bezeichnet. Im Detail bewirkt sie[105]

- die Änderung der EU-Richtlinie 78/660/EWG[106] (auch als 4. EU-Richtlinie bekannt)
- die Änderung der EU-Richtlinie 83/349/EWG[107] (auch als 7. EU-Richtlinie bekannt)
- die Aufhebung der bisherigen 8. EU-Richtlinie 84/253/EWG[108]

Die rechtlichen Regulative sind für «Unternehmen von öffentlichem Interesse» relevant, d.h. in Österreich für[109]

- Kapitalmarktorientierte Gesellschaften
- Kreditinstitute
- Versicherungsunternehmen

[103] vgl. [Hausegger2007, S. 2]
[104] vgl. [Hausegger2007, S. 2-3]
[105] vgl. [Beyond2007b]
[106] Vierte Richtlinie 78/660/EWG des Rates vom 25. Juli 1978 aufgrund von Artikel 54 Absatz 3 Buchstabe g) des Vertrages über den Jahresabschluß von Gesellschaften bestimmter Rechtsformen
[107] Siebente Richtlinie 83/349/EWG des Rates vom 13. Juni 1983 aufgrund von Artikel 54 Absatz 3 Buchstabe g) des Vertrages über den konsolidierten Abschluß
[108] Achte Richtlinie 84/253/EWG des Rates vom 10. April 1984 aufgrund von Artikel 54 Absatz 3 Buchstabe g) des Vertrages über die Zulassung der mit der Pflichtprüfung der Rechnungslegungsunterlagen beauftragten Personen
[109] Auflistung und gefolgte Erklärungen vgl. [Beyond2007d]

- Abschlussprüfer

Die größte Zielgruppe der EU-Regulative sind **kapitalmarktorientierte Gesellschaften**, also jene Unternehmen, die Aktien oder andere Wertpapiere auf einem geregelten Markt (z.B. der Börse) einem breiten Publikum anbieten und laut OECD[110] zugelassen sind. Neben Kapitalgesellschaften spielen auch Unternehmen im öffentlichen Interesse mit entsprechenden Blianz- und Umsatzgrößen[111] eine wesentliche Rolle.

Kreditinstitute und **Versicherungsunternehmen** unterliegen ebenfalls - unabhängig von ihrer Rechtsform - den EUROSOX-Bestimmungen, wenn deren Bilanzsumme eine Milliarde Euro übersteigt (bei Kreditinstituten) oder wenn die verrechneten Prämien des gesamten Geschäftes 750 Millionen Euro (bei Versicherungsunternehmen) überschreiten. Sind Aktien oder Wertpapiere des jeweiligen Unternehmens im Umlauf haben die Regelungen gemäß Bankwesengesetz[112] bzw. Versicherungsaufsichtsgesetz[113] ebenso Gültigkeit (vgl. Abschnitt 2.2.4 zur Umsetzung in Österreich).

Vierte und letzte Zielgruppe sind die **Abschlussprüfer**, wobei dabei die Unabhängigkeit des Prüfers im Mittelpunkt steht. Besonders auf mögliche Interessenskonflikte zwischen Prüfungstätigkeiten im Rahmen der Regulative und parallel dazu bestehenden Beratungs- oder Dienstleistungsbeziehungen gilt es Rücksicht zu nehmen.

2.2.2 Inhalte & Regulative

Inhaltlich befassen sich die EU-Rechtsvorgaben mit den Jahresabschlüssen sowie den konsolidierten Abschlüssen von Gesellschaften bestimmter Rechtsformen. Um den eingangs erwähnten Finanzskandalen vorzubeugen, wird zusätzlich die öffentliche Aufsicht, die Qualitätssicherung durch externe, unabhängige Dienstleister und Wirtschaftsprüfer sowie die Anwendung internationaler Standards in den Vordergrund gestellt.[114]

Das gesamte EUROSOX-Paket beinhaltet im Wesentlichen folgende Bereiche: [115]

- Zulassung, kontinuierliche Fortbildung und gegenseitige Anerkennung der mitgliedstaatlichen Regelungen

[110] Organisation for Economic Co-Operation and Development, vgl. `http://www.oecd.org`, zuletzt abgerufen am 30.01.2010
[111] Gemäß §221 Abs. 3-6 Unternehmensgesetzbuch (UGB) genießen Unternehmen dann öffentliches Interesse, wenn sie eine Bilanzsumme von mindestens 96,25 Millionen Euro oder im letzten Geschäftsjahr Umsatzerlöse von mindestens 192,5 Millionen Euro erziehlt haben. (vgl. [Beyond2007d])
[112] BGBl 1993/532 idF BGBl I 2009/66
[113] BGBl 1978/569 idF BGBl I 2009/109
[114] vgl. [Beyond2007b]
[115] vgl. [Beyond2007b]

- Registrierung
- Berufsgrundsätze, Unabhängigkeit, Unparteilichkeit, Verschwiegenheit und Berufsgeheimnis (Transparenz der Wirtschaftsprüfungsgesellschaften und Diskretion der Klienteninformation)
- Prüfungsstandards und Bestätigungsvermerk (internationale Prüfstandards)
- Qualitätssicherung der Wirtschaftsprüfung
- Untersuchungen und Sanktionen
- Öffentliche Aufsicht und gegenseitige Anerkennung der mitgliedsstaatlichen Regelungen
- Abschlussprüfung von Unternehmen von öffentlichem Interesse (Prüfungsausschüsse)
- Internationale Aspekte (Zulassung von Wirtschaftsprüfern aus Drittländern)
- Verantwortung des gruppenweiten (Konzern-)Abschlussprüfers

Aus diesen Regulativen lässt sich die dominante Position des Wirtschaftsprüfers in Verbindung mit strengen Bestimmungen über die Einrichtung von nationalen und internationalen Prüfungsausschüssen deutlich erkennen. Getroffen werden diese Vorgaben in Kapitel X des Abschnitts über die «Abschlussprüfung von Unternehmen von öffentlichem Interesse», welches für Unternehmungen direkt anwendbar ist.[116]

2.2.3 Änderungen zur 4. und 7. EU-Richtlinie

Die bereits angesprochenen Änderungen der 4. und 7. EU-Richtlinie sind in der neuen 8. EU-Richtlinie nur in ihren Grundzügen integriert. Detaillierte Ausführungen finden sich in der EU-Richtlinie 2006/46/EG[117], welche bis 5. September 2008 in nationales Recht umzusetzen war. Zielgruppe dieser Änderungsrichtline sind Kapitalgesellschaften, in Österreich also Aktiengesellschaften (AGs) und Gesellschaften mit beschränkter Haftung (GmbHs).[118]

AGs und GmbHs müssen nach österreichischem Recht ihren Jahresabschlüssen - bestehend aus Bilanz bzw. Gewinn- und Verlustrechnung - unter anderem Lageberichte (des Vorstandes bzw. des Aufrichtsrates) beilegen. Seit Umsetzung der EU-Regulative haben

[116] vgl. [Beyond2007b]

[117] Richtlinie 2006/46/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 zur Änderung der Richtlinien des Rates 78/660/EWG über den Jahresabschluss von Gesellschaften bestimmter Rechtsformen, 83/349/EWG über den konsolidierten Abschluss, 86/635/EWG über den Jahresabschluss und den konsolidierten Abschluss von Banken und anderen Finanzinstituten und 91/674/EWG über den Jahresabschluss und den konsolidierten Abschluss von Versicherungsunternehmen

[118] vgl. [Beyond2007b]

diese Berichte auch *«die wesentlichen Merkmale des internen Kontrollsystems und Risikomanagementsystems»*[119] zu enthalten. Desweiteren sind beispielsweise die Erklärung zur Unternehmenführung inklusive näherer Angaben zum Unternehmensführungskodex sowie zu den Unternehmensführungspraktiken aber auch mögliche Sanktionierungsmaßnahmen beizufügen.[120]

2.2.4 Umsetzung in Österreich

Die Umsetzung der beiden EU-Direktiven (2006/43/EG[121], 2006/46/EG[122]) erfolgte in Österreich im Rahmes des Unternehmensrechts-Änderungsgesetzes 2008 (URÄG 2008)[123]. Dieses Gesetz wurde am 7. Mai 2008 im BGBl I 2008/70 kundgemacht und trat mit 1. Juni 2008 in Kraft.

Die fünf Kernthemen des ÜRAG 2008 im Überblick sind[124]

- die Schaffung bzw. Stärkung der Unabhängigkeit des Abschlussprüfers.
- die Festlegung und Kontrollse der Kompetenzen und der Zusammensetzung des Prüfungsausschusses.
- die Einführung eines befristeten Tätigkeitsverbotes für Abschlussprüfer.
- die Unabhängigkeit des Honorars des Abschlussprüfers, da er keine Beratungstätigkeit sondern eine Prüftätigkeit vornimmt.
- die Definition des Umfangs von Management- und Prüfbericht.

Zusätzlich sind seit 1. Jänner 2008 die Änderungen zum Bankwesengesetz und zum Versicherungsaufsichtsgesetz in Kraft, welche sich im wesentlichen in den §63a Abs. 4 Bankwesengesetz und §82b Abs. 4 Versicherungsaufsichtsgesetz niederschlagen.[125]

[119] vgl. EU-Richtlinie 2006/46/EG, Artikel 2 (2), welcher Artikel 36 Absatz 2 der Richtlinie 83/349/EWG ändert
[120] vgl. [Beyond2007b]
[121] auch Abschlussprüfer-Richtlinie
[122] auch Änderungs-Richtlinie
[123] BGBl I 2008/70 - Bundesgesetz, mit dem das Unternehmensgesetzbuch, das Aktiengesetz 1965, das GmbH-Gesetz, das SE-Gesetz, das Genossenschaftsgesetz, das Genossenschaftsrevisionsgesetz, das Spaltungsgesetz, das Luftfahrtgesetz, das Bankwesengesetz und das Versicherungsaufsichtsgesetz geändert werden (Unternehmensrechts-Änderungsgesetz 2008 - URÄG 2008)
[124] vgl. [Beyond2007c]
[125] vgl. [Beyond2007c]

2.3 Basel II

Unter *Basel II* (oft auch als Basel-II-Abkommen bezeichnet) können sämtliche Eigenkapitalvorschriften für Kreditinstitute und Banken verstanden werden, die vom *Basler Ausschuss für Bankenaufsicht* im Jahr 2004 veröffentlicht wurden. Basierend auf dem Basel-I-Rahmenwerk soll die Stabilität des Finanzsystems sichergestellt werden.[126]

2.3.1 Entstehung & Hintergründe

Die thematische Problematik von Basel II liegt in den wirtschaftlichen Eigenschaften von Kredit- und Finanzdienstleistungsunternehmen. Auf der einen Seite verfügen sie über einen entsprechend hohen Fremdkapitalanteil in ihrer Bilanz, welcher sich aus der Natur des Geldvermittlungsgeschäftes ergibt. Die Summe des Eigenkapitals im Vergleich zur Gesamtbilanzsumme (= Eigenkapitalquote) eines Geldinstitutes ist in der Regel wesentlich niedriger.[127]

Auf der anderen Seite besteht zwischen Finanzdienstleistern eine enorme Abhängigkeit durch Kreditvergabe und Bürgschaften, wodurch der Zusammenbruch eines einzelnen Dienstleisters die Stabilität des ganzen Sektors oder sogar der gesamten Wirtschaft beeinflusst. Die Sicherung der Eigenkapitalquote zur Kompensierung etwaiger Verluste aus dem Bankgeschäft genießt daher hohe Priorität.[128]

Im Jahre 1974 wurde, als Reaktion auf große Bankenzusammenbrüche im deutschen Raum, der *Basler Ausschuss für Bankenaufsicht*[129] gegründet, welcher enorme Defizite in den Eigenkapital- und Rechnungslegungsvorschriften von Bankinstituten sichtbar machte. 1988 wurde deshalb der Basler Akkord (Basel I) veröffentlicht, gefolgt vom «Neuen Basler Eigenkapitalakkord» (Basel II) im Juni 2004.

Als Ziele des Basel-II-Abkommens definiert die *Österreichische Finanzmarktaufsicht* (FMA)[130] folgende vier Kernaspekte[131]:

- eine verstärkte Ausrichtung der regulatorischen Eigenmittelunterlegung am ökonomischen Risiko
- eine adäquatere Berücksichtigung von Risiken bei gleichzeitigem Erhalt der bisherigen Eigenkapitalausstattung im Bankwesen insgesamt (d. h. das durchschnittliche Eigenmittelerfordernis des gesamten Bankensektors soll konstant bleiben)

[126] vgl. [FMA2010b]
[127] vgl. [FMA2010b]
[128] vgl. [FMA2010b]
[129] engl. *Basel Committee on Banking Supervision*
[130] vgl. `http://www.fma.gv.at`, zuletzt abgerufen am 30.01.2010
[131] vgl. [FMA2010b]

- eine fortlaufende Verfeinerung der Messverfahren (d.h. eine Erhöhung der Risikosensitivität der Eigenmittelanforderung durch Messverfahren, die den Risikograd von Positionen und Geschäften angemessen berücksichtigen sowie die Schaffung eines Anreizes zur Weiterentwicklung der Messverfahren bzw. zum Übergang zu den fortgeschrittenen Ansätzen)
- eine Vereinheitlichung der internationalen Aufsichtsstandards (Sicherstellung eines «level playing field»)

2.3.2 Inhalt & Architektur

Das Basel-I-Regelwerk beruhte lediglich auf einem inhaltlichen Schwerpunkt, nämlich den Mindestkapitalvorschriften für Banken zur Sicherung der Stabilität des Finanzsystems. Diese Komponente, heute als erste Säule bezeichnet, wurde im Rahmen des Basel-II-Abkommens um zwei weitere Bereiche zur Überprüfung der Bankprozesse sowie intensivierten Veröffentlichungspflichten erweitert. (vgl. Abbildung 2.1[132])

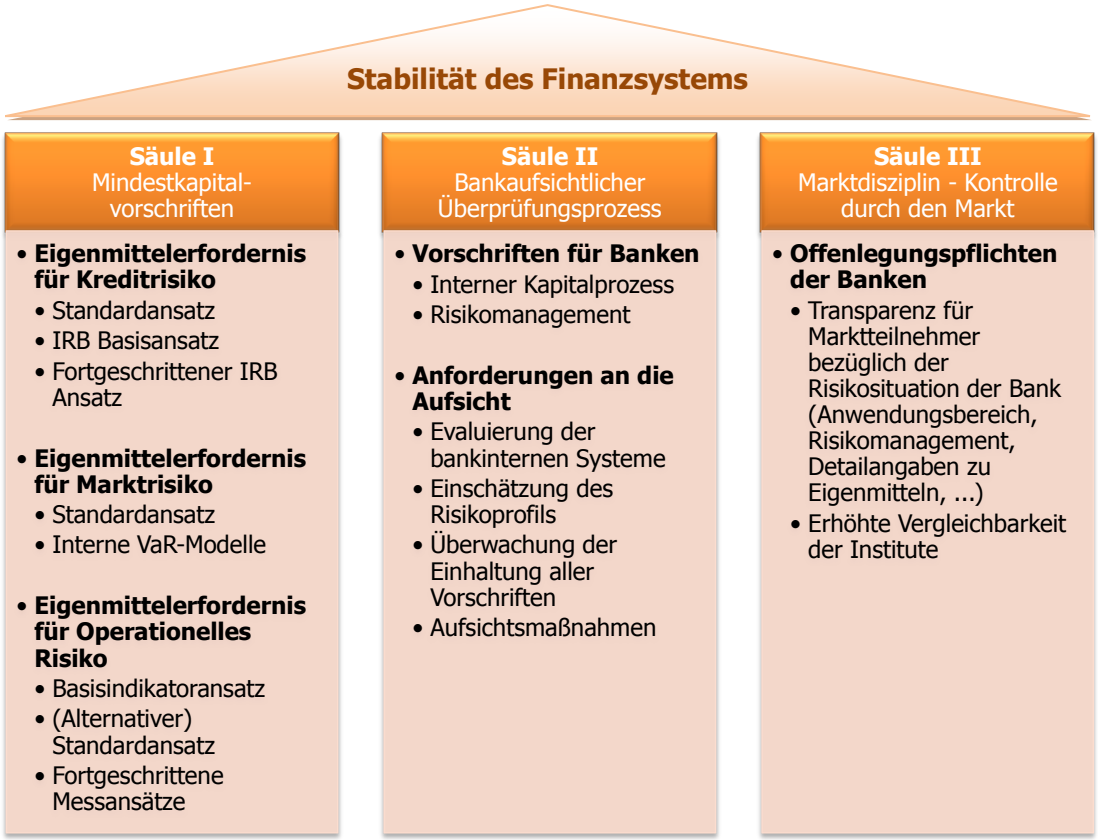

Abbildung 2.1: Basel II - 3-Säulen-Architektur

[132] vgl. [FMA2010a, erste Grafik]

Typische Charakteristika eines stabilen Finanzmarktes nach Basel II können in folgenden drei Säulen dargestellt werden:[133]

- **Säule 1 - Eigenmittelerfordernis**

  Säule 1 beinhaltet bereits die im Basel-I-Rahmenwerk verfügbaren Anforderungen der Eigenmitteladministration und der Risikomessung. Diese wurden weiterentwickelt und insbesondere im Bereich der institutsbezogenen Risikoanalyse sowie der Erfassung operationaler Risikofaktoren modifiziert.

- **Säule 2 - Bankaufsichtlicher Überprüfungsprozess**

  Säule 2 wurde gänzlich neu implementiert und führt erstmals den *Supervisory Review Process* (SRP), jene Anforderung an Kreditinstitute einen umfangreichen Risikomanagementprozess zu etablieren, ein. Ziel der Methoden dieses Bereichs ist der Aufbau einer funktionstüchtigen Gesamtbanksteuerung, aber auch die Umsetzung eines internen Kapitalmanagements.

  In einem zusätzlichen Evaluierungsprozess sollen qualitative Kerngrößen wie Strategie, interne Prozesse oder Managementaufgaben bewertet und gegebenenfalls durch weitere Aufsichtsmaßnahmen regelmäßig kontrolliert werden.

  Letzte Hauptaufgabe der zweiten Säule ist die Behandlung von Zinsänderungs- oder Liquiditätsrisiken, die nicht in das Aufgabenfeld der ersten Säule fallen, sowie die Einbeziehung externer Faktoren der Volkswirtschaft.

- **Säule 3 - Marktdisziplin**

  Säule 3 soll, anlässlich dubioser Offenlegungsmissstände, für Transparenz und mehr Information über Geschäfts- und Risikostrategien einer Bank sorgen. Alle Marktteilnehmer (Investoren, Gläubiger und Kunden) werden einbezogen, wobei deren Reaktionen eine entsprechende Disziplinierung darstellen sollen.

2.3.3 Umsetzung in der Europäischen Union

Die Veröffentlichungen des Basler Ausschusses für Bankenaufsicht waren sehr detailliert, hatten aber lediglich empfehlenden Charakter. Die Europäische Kommission machte es sich daher zur Aufgabe die europäischen Vorschriften zu überarbeiten und somit gleiche Wettbewerbsbedingungen für Finanzdienstleister im europäischen Wirtschaftsraum zu schaffen.[134]

[133] vgl. [FMA2010a]
[134] vgl. [FMA2010b]

Schlussendlich resultierten die zahlreichen Vorschläge des Basel-II-Abkommens in den europäischen Richtlinien 2006/48/EG[135] (Bankenrichtlinie) sowie 2006/49/EG[136] (Kapitaladäquanzrichtlinie), die seit 1. Jänner 2007 für alle Mitgliedsstaaten verbindlich sind.[137]

Besondere Bedeutung bei der internationalen Umsetzung wurde der Berücksichtigung heterogener Bank-, Geld- und Zinssysteme beigemessen, um sowohl weltweit tätigen Multikonzernen als auch kleineren, lokalen Geldinstituten Sicherheit und Zuverlässigkeit zu gewährleisten. Neben der Risikominimierung bzw. -überwachung sollte die Weiterentwicklung gefördert und Wettbewerbsverzerrungen vermieden werden.

EZB[138] Präsident Jean-Claude Trichet verkündete, dass die europäische Implementierung einen *«umfassenden Ansatz für Risikomanagement und Bankenaufsicht darstellt. Basel II wird die Sicherheit und die Zuverlässigkeit der Banken erhöhen, die Stabilität des Finanzsystems stärken und generell die Fähigkeit des Finanzsektors verbessern, als Quelle und Motor eines nachhaltigen Wachstums der gesamten Wirtschaft zu dienen»*[139]

2.3.4 Umsetzung in Österreich

Die *Österreichische Finanzmarktaufsicht* (FMA) beteiligte sich an der Entwicklung der europäischen Regulative und vertrat vor allem lokal relevante Interessen von Banken und Anlegern. Entscheidende Verbesserungen wurden für kleinere Geldinstitute erreicht, da diese nun auch für vergleichsweise geringe Investitionsbeträge die Anforderungen des Schutzsystems erfüllen und auch eine direktere Partizipationsmöglichkeit haben.[140]

Zweiter Erfolgsfaktor für die österreichische Umsetzung war die Betrachtung des zentral- und osteuropäischen Raums. Durch die fortschreitende Expansionspolitik der lokalen Finanzunternehmen in diese Länder wird der Einsatz entsprechender Risikomanagementsysteme notwendig. Gleichzeitig kann trotz geringerer Eigenmittel die Weiterentwicklung des Systems vorangetrieben und somit die Ertragskraft der europäischen Tochterunternehmen gesteigert werden.[141]

Ursprüngliche Befürchtungen, dass das schweizer Komitee zu strenge und unwirtschaftliche Kreditkonditionen verwirklichen wolle, konnten entkräftet werden. Auch bei wirt-

[135] Richtlinie 2006/48/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute
[136] Richtlinie 2006/49/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten
[137] vgl. [Hausegger2007, S. 30]
[138] Europäische Zentralbank
[139] vgl. [FMA2010b, Basel II & Europäische Union, letzter Absatz]
[140] vgl. [FMA2010b]
[141] vgl. [FMA2010b]

schaftlich schwacher Konjunktur funktionieren die Regulatorien angemessen. Lediglich für Kredite mit erhöhtem Ausfallrisiko sind höhere Steuersätze und intensivere Risikomaßnahmen veranschlagt.[142]

2.4 Fachgutachten & Governance Kodizes

Die *8. EU-Richtlinie* sowie *Basel II* können als zwei der umfangreichsten und international übergreifendsten Rahmenwerke im Blickwinkel der Corporate Governance bzw. Compliance gesehen werden. Parallel dazu existiert eine Vielzahl an Fachgutachten diverser Berufssegmente, die darin ihre Erfahrungen, Arbeitsmethoden und Strategien der Öffentlichkeit präsentieren. Tabelle 2.1[143] gibt einen Überblick über Organisationen und deren Fachgutachten im IT-Sektor. Beispielhaft soll anschließend kurz das österreichische Fachgutachten KFS/DV2 vorgestellt werden.

Ähnlichen Ursprungs ist auch die Idee der Governance Kodizes, die in den letzten Jahren vielfältig überarbeitet und strukturiert wurden. Inhalt dieser, meist mit nationalem Bezug abgefassten, Dokumente ist die Festlegung von allgemeinen Grundsätzen guter Unternehmensführung. Exemplarisch wird der österreichische Governance Kodex im Detail untersucht.

Organisation	**Fachgutachten**
IFAC - International Federation of Accountants	ISA 402, ISA 315, ISA 330
AICPA - American Institute of CPAs	SAS/70
KFS - Kammer der Wirtschaftstreuhänder	KFS/DV1, KFS/DV2
IDW - Institut der Wirtschaftsprüfer	FAIT 1, FAIT 2, FAIT 3

Tabelle 2.1: IT-bezogene Organisationen & Fachgutachten

2.4.1 KFS/DV2

Das Fachgutachten zur «Abschlussprüfung bei Einsatz von Informationstechnik» (kurz: KFS/DV2) wurde vom *Fachsenat für Datenverarbeitung* als Teil der *Österreichischen Kammer der Wirtschaftstreuhänder*[144] verabschiedet und beinhaltet nationale und internationale Regelungen für regelmäßige IT-Prüfungen. Da solche IT-Kontrollen Bestandteil ganzheitlicher Unternehmensprüfungen sind, kommt dieses Fachgutachten nach internationalen Prüfungsstandards (ISA) zur Anwendung.[145]

[142] vgl. [FMA2010b]
[143] vgl. [Hausegger2007, S. 26]
[144] vgl. `http://www.kwt.or.at`, zuletzt abgerufen am 30.01.2010
[145] vgl. [Hausegger2007, S. 26]

Ziel und Umfang einer solchen Prüfung in der Informationstechnik ist nach Abschnitt B der Niederschrift die *«Beurteilung der Verlässlichkeit der mit Hilfe von programmgesteuerten Verarbeitungen ermittelten und im Rechnungswesen sowie im Rechnungsabschluss verwendeten Daten.»*[146] Als weiteres Ziel wird die Überprüfung der mit dem technologischen Einsatz verbundenen IT-Risiken, die eine mögliche Gefährdung eines weiteren Bestehens des Unternehmes verhindern sollen, genannt.

In welchem Umfang eine solche IT-Prüfung stattfindet, kann laut Fachgutachten nicht verallgemeinert werden und hängt von insgesamt sechs Umständen ab[147]:

- Größe, Art und Komplexität des Leistungsprogramms des geprüften Unternehmens
- Art und Komplexität der eingesetzten Informationstechnik-Systeme
- Art und Umfang der Integration von unternehmensweiten Anwendungen
- Vorliegen von automatisch generierten Transaktionen, Vernetzungen mit Kunden, Lieferanten oder anderen Dritten
- Maßnahmen des geprüften Unternehmens zur Beseitigung oder Verminderung von Fehlerrisiken
- bei vorangegangenen Prüfungen gewonnene Erkenntnisse

Prüfungsabwicklung & Risikoanalyse

Im Rahmen einer Prüfung der Informationstechnologie muss der Abschlussprüfer die IT-bezogene Prüfung bei der Gesamtplanung berücksichtigen und zeitgerecht entsprechende Mitarbeiterressourcen reservieren oder externe Sachverständige heranziehen. Zur Verschaffung eines Überblicks über die bestehende Systemarchitektur werden Organigramme, IT-Prozesse und -Strategien, Geräte, Programme und Anwendungen genau analysiert.[148]

Angelehnt an den Prüfungsstandard 330 des deutschen Instituts der Wirtschaftsprüfer definiert auch dieses Fachgutachten sowohl anwendungsunabhängige als auch anwendungsabhängige Risiken. Neben dem generellen Vernetzungs- und Komplexitätsgrad der System- und Prozessstruktur werden auch Änderungsfaktoren, fehlgeschlagene Projekte oder Restrukturierungen im Hinblick auf neue Risikofaktoren des Unternehmens untersucht. Das Vorhandensein von qualifizierten Mitarbeitern, ausreichenden IT-Ressourcen sowie die ganzheitliche geschäftliche Ausrichtung der Informatikstechnik auf die Geschäftsstrategie des Unternehmens runden die zu prüfenden Risikofaktoren ab.[149]

[146] vgl. [KammerWTH2004, S. 3]
[147] vgl. [KammerWTH2004, S. 4]
[148] vgl. [KammerWTH2004, S. 5-6]
[149] vgl. [KammerWTH2004, S. 7-8]

Kontrollen & Maßnahmen

Basierend auf diesen vom Abschlussprüfer evaluierten IT-Risiken legt das KFS/DV2 Maßnahmen zur Beseitigung oder Verminderung dieser Risiken fest. Dabei sollen sowohl anwendungsunabhängige Kontrollen der Informationstechnikprozesse (etwa durch das Prozessmodell COBIT, vgl. Abschnitt 3.1.3), als auch anwendungsabhängige Kontrollen der Geschäftsprozesse manuell, semi-automatisch oder vollautomatisch durchgeführt werden.[150]

Die genannten Kontrollen untersuchen etwa die Richtigkeit der Verarbeitungsprozesse (Eingabe - Verarbeitung - Ausgabe), analysieren Programmcode, Konfigurationsparameter bzw. Datenbanken und überprüfen Zugriffschutz, Protokollierung bzw. Schnittstellen zu anderen Systemen. Besondere Aufmerksamkeit erhält die Beurteilung der Rechnungslegung und aller damit verbundenen *«Stammdaten, Schnittstellen, Parameter, Berechtigungskonzepte (Funktionstrennungen) und ähnliche Maßnahmen, durch die Risiken beseitigt oder vermindert werden»*[151] können. Neben der Beurteilung der Wirksamkeit der Systeme gilt es vor allem die Grundsätze ordnungsmäßiger Buchführung sicherzustellen sowie nach Abschluss der Prüfung eine entsprechend ausführliche Dokumentation bzw. Berichterstattung zu erstellen.[152]

IT-Outsourcing

Im letzten Teil (Abschnitt D) des Fachgutachtens wird die Vorgehensweise im Falle von **IT-Outsourcing**, also der Auslagerung von Informationstechnologie an ein anderes Unternehmen, beschrieben. Der Abschlussprüfer ist dabei verpflichtet, sich auch über das beauftragte Dienstleistungsunternehmen Informationen bzgl. Informationstechnik, internes Kontrollsystem und Buchhaltung zu beschaffen, um das Zusammenspiel der Systeme, die wirtschaftliche Lage der Geschäftsbeziehung sowie die Ordnungsmäßigkeit der Buchführung zu überprüfen.[153]

Das KFS/DV2 kann somit nicht nur als Implementierungshilfe für Unternehmen zur Umsetzung risikominimierter IT-Systeme dienen, sondern ist gleichzeitig ein wichtiges Arbeitswerkzeug für Abschlussprüfer, wodurch objektive Prüfungen anhand vorgegebener Richtlinien und Normen stattfinden können.

[150] vgl. [KammerWTH2004, S. 9]
[151] vgl. [KammerWTH2004, S. 10]
[152] vgl. [KammerWTH2004, S. 11]
[153] vgl. [KammerWTH2004, S. 12-13]

2.4.2 Governance Kodizes

Bereits in Abschnitt 1.1.1 wurde kurz auf die Entwicklung diverser Governance Kodizes als Vorgabe allgemeiner Grundsätze zur guten Unternehmensführung eingegangen. Besonders im Bereich der kaptial- oder börsenorientierten Unternehmensformen[154] gewinnt diese Form der Regulative immer mehr an Bedeutung und nicht selten werden Investitions- oder Finanzierungsentscheidungen basierend auf der Umsetzung solcher Vorgaben getätigt.[155]

Eine internationale Norm zur Entwicklung solcher Kodizes gibt es aufgrund unterschiedlicher Rechts- und Wirtschaftssysteme nicht. Trotzdem verfolgen alle Institutionen ein gemeinsames Ziel: Das Vertrauen der Anleger und Investoren durch Transparenz, Kontrollen und strikte Regeln wiederherzustellen und so den Wirtschaftsmarkt langfristig zu stärken.[156]

Hannes Hausegger bezeichnet Governance Kodizes als *«freiwillige Selbstregulierungsmaßnahmen»*[157], wobei die Freiwilligkeit der Anwendung dieser Regelwerke nur begrenzt gegeben ist. Die Börse in New York etwa verlangt von jedem notierten Unternehmen einen «Code of Business Conduct and Ethics» sowie «Corporate Governance Guidelines» aufzustellen und der Öffentlichkeit zu präsentieren. Dabei handelt es sich definitiv um eine zwingend einzuhaltende Vorschrift und keinesfalls um eine lediglich freiwillige Empfehlung.[158]

Ähnlich den nationalen Corporate Governance Kodizes - etwa in Deutschland[159] - hat auch die OECD im Jahre 1999 einige Grundsätze der Corporate Governance[160] herausgegeben und fünf Jahre später nochmals überarbeitet.

Das zweigeteilte Dokument behandelt im ersten Basisabschnitt die Sicherstellung eines effektiven Corporate-Governance-Rahmens sowie Rollen, Rechte und Schlüsselfunktionen aller Unternehmensbeteiligten (Stakeholder). In den Erweiterungen (zweiter Abschnitt) werden diese Regelungen weiter verfeinert sowie insbesondere Offenlung und Transparent aber auch Pflichten der Aufsichtsorgane hervorgehoben.

Im Folgenden soll nun auf den *Österreichischen Corporate Governance Kodex* sowie seine Revision im Jänner 2010 eingegangen werden.

[154] Gesellschaften mit beschränkter Haftung (GmbH.) oder Aktiengesellschaften (AG)
[155] vgl. [Hausegger2007, S. 39-40]
[156] vgl. [Hausegger2007, S. 40]
[157] vgl. [Hausegger2007, S. 40]
[158] vgl. [Hausegger2007, S. 40]
[159] vgl. `http://www.corporate-governance-code.de/index.html`, zuletzt abgerufen am 30.01.2010
[160] vgl. [OECD2004]

2.4.3 Österreichischer Corporate Governance Kodex

Der *Österreichische Arbeitskreis für Corporate Governance*, bestehend aus Mitgliedern zahlreicher Multikonzerne, Investoren und Wirtschaftspartner[161], hat am 1. Oktober 2002 erstmals den *Österreichischen Corporate Governance Kodex* der Öffentlichkeit vorgestellt. Zahlreiche Revisionen, zuletzt im Jänner 2010, haben das knapp 70-seitige Dokument zu einem wirksamen Instrument im österreichischen Wirtschaftsraum gemacht. Der durch das Unternehmensrechts-Änderungsgesetz 2008 (ÜRÄG 2008) verpflichtend aufzustellende Corporate Governance Bericht im Zuge des Jahresabschlusses hat dem Rahmenwerk zusätzliche Bedeutung verliehen.[162]

Ziel & Basis des Kodex

Ziel dieser Regulative ist vor allem das bereits erwähnte Wiederherstellen der Glaubwürdigkeit und des Vertrauens der Anleger in das österreichische Finanzsystem sowie die *«verantwortliche, auf nachhaltige und langfristige Wertschaffung ausgerichtete Leitung und Kontrolle von Gesellschaften und Konzernen»*[163]. Es soll zusätzlich den Interessen aller durch das Wohlergehen des Unternehmens gedient sowie ein hohes Maß an Transparenz für alle Stakeholder erreicht werden.[164]

Als Basis des Kodex werden die international üblichen Standards für gute Unternehmensführung sowie das österreichische Aktien-, Börse- und Kapitalmarktrecht genannt.[165] Ergänzt werden diese durch EU-Empfehlungen zu den Aufgaben der Aufsichtsratsmitglieder, zu der Vergütung von Direktoren sowie den oben erwähnten OECD-Richtlinien für Corporate Governance (vgl. Abschnitt 2.4.2).

Obwohl der Arbeitskreis den Kodex nur als *«freiwillige Selbstverpflichtung der Unternehmen»*[166] definiert, stellt er für österreichische Gesellschaften eine Aufnahmevoraussetzung für die Wiener Börse dar. Weiters wird empfohlen, dass sich Unternehmen öffentlich zur Anwendung dieser Regelungen bekennen und so weiteres Vertrauen und unternehmerische Seriösität gegenüber Anlegern ausstrahlen.[167]

[161] Beteiligte Unternehmen wären etwa das Institut Österreichischer Wirtschaftsprüfer, die Wirtschaftskammer Österreich, die Industriellenvereinigung oder der Investorenbeirat der Wiener Börse aber auch Organisationen wie die Telekom AG, die OMV AG oder die Universität Graz. Eine vollständige Liste der ständigen Mitglieder findet sich unter `http://www.wienerborse.at/corporate/arbeitskreis.htm`, zuletzt besucht am 30.01.2010.
[162] vgl. [ÖACG2009a, S. 5]
[163] vgl. [ÖACG2009a, S. 11]
[164] vgl. [ÖACG2009a, S. 5] bzw. [ÖACG2009a, S. 11]
[165] vgl. [ÖACG2009a, S. 12]
[166] vgl. [ÖACG2009a, S. 12]
[167] vgl. [ÖACG2009a, S. 12]

Regelwerk des Kodex

Die Erläuterungen des Österreichischen Corporate Governance Kodex umfassen drei Regelkategorien, die nähere Details zur Anwendung und Verpflichtung der Unternehmen darlegen (vgl. Tabelle 2.2[168]).

Kürzel	Regelkategorie	Regelanwendung
L	Legal Requirement	Regel beruht auf zwingenden Rechtsvorschriften
C	Comply or Explain	Regel soll eingehalten werden; eine Abweichung muss erklärt und begründet werden, um ein kodexkonformes Verhalten zu erreichen
R	Recommendation	Regel mit Empfehlungscharakter; Nichteinhaltung ist weder offenzulegen noch zu begründen

Tabelle 2.2: Regelwerk des Österreichischen Corporate Governance Kodex

Dieses Regelwerk verdeutlicht nun die zuvor genannte «freiwillige Selbstverpflichtung der Unternehmen». Neben den gesetzlich verpflichtenden Judikaten kann vor allem die Kategorie «Comply or Explain» weit ausgelegt werden, da eine Nicht-Einhaltung zwar keine rechtlichen Folgen hat, aber begründet werden muss. C-Regeln basieren überwiegend auf international anerkannten Vorschriften.

Insgesamt enthält der Kodex in der Fassung vom Jänner 2009 83 Regeln, wovon 33 (40%) als L-Regeln, 45 (54%) als C-Regeln und 5 (6%) als R-Regeln geführt werden. Inhaltlich beschreibt das Dokument Aufgaben, Kompetenzen, Vergütungen und das Zusammenwirken von Vorstand, Aufsichtsrat und Aktionären. Ziel und Zweck der Hauptversammlung sowie die notwendige Transparenz von Rechnungslegung und Abschlussprüfung runden das umfangreiche Regelwerk ab.[169]

Kodex-Revision 2010

Im Dezember 2009 wurde die Kodex-Version vom Jänner des gleichen Jahres überarbeitet. Es enstand eine Kodex-Revision 2010[170], die ab dem 1. Jänner 2010 Gültigkeit hat. Aufgrund des Aktienrechts-Änderungsgesetzes 2009 (AktRÄG 2009)[171] mussten einige bisherige C-Regeln in L-Regeln überführt werden, da diese nun gesetzlich verpflichtend sind.

[168] vgl. [ÖACG2009a, S. 14], Jene L-Regeln, die nur für an der österreichischen Börse notierte Unternehmen gelten, sind für anderwertige Kapitalgesellschaften als C-Regeln zu interpretieren.
[169] vgl. [ÖACG2009a, S. 9]
[170] vgl. [ÖACG2009b]
[171] BGBl I 2009/71 - Bundesgesetz, mit dem das Aktiengesetz 1965, das SE-Gesetz, das Unternehmensgesetzbuch, das Umwandlungsgesetz, das Spaltungsgesetz, das Kapitalberichtigungsgesetz, das Gesellschafter-Ausschlussgesetz, das Übernahmegesetz, das Genossenschaftsrevisionsgesetz und das Grundbuchsgesetz geändert werden (Aktienrechts-Änderungsgesetz 2009 - AktRÄG 2009)

Gleichzeitig wurde der Umsetzung einer EU-Empfehlung zur Managervergütung vom 30. April 2009 Rechnung getragen, die insbesondere Regeln betreffend variable Vergütung, Abfindung, aktienbezogene Vergütung, Vergütungsbericht und Vergütungsausschuss vorsieht.[172]

Richard Schenz, Kapitalmarktbeauftragter und Vorsitzender des Österreichischen Arbeitskreises für Corporate Governance, fasst die Zielsetzung der Revision zusammen: *«Mit den neuen Vergütungsregeln soll das Handeln der Manager noch stärker auf Nachhaltigkeit und Langfristigkeit ausgerichtet werden. Falsche Anreize in der Vergütungsstruktur wie eine unangemessene kurzfristige Erfolgsorientierung oder zu hohe Risikofreudigkeit sollen verhindert werden. Die persönliche Leistung des Vorstandsmitglieds, die wirtschaftliche Lage und die Größe des Unternehmens sollen stärker in der Vergütung berücksichtigt werden. «Goldene Fallschirme» sind nach den neuen Regeln nicht zulässig. Schließlich sollen auch die Vergütungstransparenz und die Professionalität im Vergütungsausschuss des Aufsichtsrats weiter verbessert werden.»*[173]

Der *Österreichische Corporate Governance Kodex* setzt also nicht nur nationales Recht im Bereich der börsennotierten Unternehmen um und integriert EU-weite Regelungen zur Corporate Governance, sondern bildet durch sein flexibles Regelwerk einen dynamischen Umsetzungsrahmen für österreichische Wirtschaftsteilnehmer.

2.4.4 Problematik: Freiwilligkeit & Umsetzung

Ob nun Fachgutachten von österreichischen Expertengruppen, Präferenzen von internationalen Organisationen oder nationale Corporate Governance Kodizes - eines haben alle diese Artefakte gemeinsam: In einem gewissen Grad ist die Anwendung solcher Regulative freiwillig und liegt im jeweiligen Ermessen bzw. der inhaltlichen Auslegung des umsetzenden Unternehmens.

Es zeigt sich deutlich, dass das aus dem Völkerrecht bekannte Problem der internationalen Rechtsdurchsetzung sowie der Definition eines länderübergreifenden Geltungsbereichs aufgrund unterschiedlicher Rechts- und Wirtschaftssysteme auch hier zum Vorschein tritt. Rahmenwerke und Empfehlungen müssen erst durch langwierige Prozesse in nationale, verbindliche Bestimmungen überführt werden und sobald dieser Prozess vollendet ist, wird die nächste Revision bzw. Überarbeitung der internationalen Regulative notwendig.

[172] vgl. [BMF2009]
[173] vgl. [BMF2009]

Deshalb sind die derzeitigen Bemühungen zur Schaffung einer einheitlichen Basis zur Regulierung des internationalen Wirtschaftssystems von großer Bedeutung, damit zukünftig Finanzskanale vermieden, Bilanzfälschungen aufgedeckt und korruptierte Unternehmensgeschäfte weder lokal noch länderübergreifend getätigt werden können.

Einen etwas anderen Ansatz als die freiwillige Umsetzung verschiedenster Richtlinien verfolgt seit 2001 der amerikanische Gesetzgeber. Anlässlich bereits erwähnter Skandale rund um die Multikonzerne Enron und Worldcom wurde in Amerika das Bundesgesetz *Sarbanes-Oxley Act* (SOX) erlassen. Dabei handelt es sich keinesfalls um ledigliche Empfehlungen oder Vorschläge, sondern um nationales Recht mit straf- und zivilrechtlichen Folgen bei Nichtumsetzung.

2.5 Internationale Rechtslage

Basierend auf der Tatsache, dass die größten, bisherigen Finanzskandale ihren Ursprung im amerikanischen Raum haben, existieren auch im Rechtssystem der USA zahlreiche Bestimmungen und Abkommen, die eine fehlerfreie Finanzberichtserstattung sicherstellen sollen und daher den Einsatz eines wirksamen internen Kontrollsystems fordern. Die beiden wohl wichtigsten Vorschriften zur Implementierung sind

- der Sarbanes-Oxley Act (SOX)
- der Foreign Corrupt Practices Act (FCPA)

Anwendbar sind diese Regulative auf alle Unternehmen im In- und Ausland, die bei der US-Börsenaufsicht SEC[174] registriert sind. Daher sind auch viele direkt notierte europäische Unternehmen oder Töchter eines US-Konzerns von dessen Bestimmungen betroffen.[175]

2.5.1 Sarbanes-Oxley Act (SOX)

Der *Sarbanes-Oxley Act* wurde am 30. Juli 2002 in insgesamt 11 Teilen[176] verabschiedet und wird seitdem von der *SEC* bzw. dem *Public Company Accounting Oversight Board* (PCAOB) ergänzt und konkretisiert. Diese beiden Organisationen obliegt auch die Kontrolle über die korrekte Anwendung von SOX. Das über 60-seitige Gesetz ist eines der umfassendsten Bundesgesetze der USA, welches der Betrugsvermeidung und Finanzberichtserstattung gewidmet ist.[177]

[174] U.S. Securities and Exchange Commission, vgl. `http://www.sec.gov`, zuletzt abgerufen am 30.01.2010
[175] vgl. [Menzies2006, S. 15]
[176] Die erste bzw. die ersten beiden Ziffern geben den jeweiligen Teil (engl. Title) und die darauffolgenden Ziffern das jeweilige Kapitel (engl. Section) an.
[177] vgl. [Fröhlich2007, S. 67] bzw. [Hausegger2007, S. 19]

Wichtige Sections des Gesetzes

Die beiden bedeutendsten Sektionen oder Teile des Sarbanes-Oxley Acts sind[178]:

- Section 302 - Disclosure Controls and Procedures
- Section 404 - Internal Control Over Financial Reporting

Section 302 verpflichtet den CEO[179] bzw. CFO[180] eines Unternehmens in einer jährlichen, eidesstattlichen Erklärung zu bestätigen, dass sämtliche Finanzbelange des Unternehmens korrekt dargestellt und alle der Öffentlichkeit präsentierten Berichte jederzeit zugänglich sind, geprüft und gegebenenfalls korrigiert wurden. Der Titel dieser Sektion «Disclosure Controls and Procedures» schreibt außerdem die Einrichtung und Pflege von Kontrollen und Verfahren zur Offenlegung vor.

Section 404, etwas besser bekannt als ihr Vorgänger, beinhaltet die Forderung nach der Einrichtung eines *internen Kontrollsystems* (IKS, vgl. Abschnitt 1.2.5) für die ganzheitliche Finanzberichtserstattung (Internal Control Over Financial Reporting). Wiederum werden CEO und CFO beauftragt einen entsprechenden Prozess einzurichten und zu überwachen, welcher *«die Ordnungsmäßigkeit der Finanzbuchhaltung und damit die Erstellung der Abschlüsse gemäß den Rechnungslegungsvorschriften sicherstellt.»*[181]

Überprüfung & Prüfungsausschuss

Die Überprüfung der Wirksamkeit des internen Kontrollsystems sowie dessen Effektivität muss von einem unabhängigen Abschlussprüfer durchgeführt werden. Unabhängig meint in diesem Kontext, dass die prüfende Organisation keinerlei Dienstleistungen, die nicht mit der direkten Abschlussprüfung zu tun haben, bei dem zu prüfenden Unternehmen durchführen darf.[182] Auch hat der Ablauf einer solchen Prüfung sich an einem international anerkannten Rahmenmodell, wie etwa COSO (vgl. Abbildung 2.2[183]), zu orientieren und bedarf der Integration in die IT-Infrastruktur und vieler IT-Prozesse. Letzteres stellt eine direkte Verknüpfung zur IT-Governance her.[184]

COSO ist ein vom *Committee of Sponsoring Organisations of Treadway Commission* herausgegebenes Rahmenwerk, welches Führungskräften und Top-Managern eine fundierte Möglichkeit des unternehmensweiten Risikomanagements bereitstellt. Der sogenannte

[178] vgl. [Fröhlich2007, S. 67-68]
[179] Chief Executive Officer - Vorstandsvorsitzender
[180] Chief Finance Officer - Finanzvorstand
[181] vgl. [Fröhlich2007, S. 68]
[182] vgl. [Hausegger2007, S. 21]
[183] vgl. [Pfister2006, erste Grafik]
[184] vgl. [Fröhlich2007, S. 68]

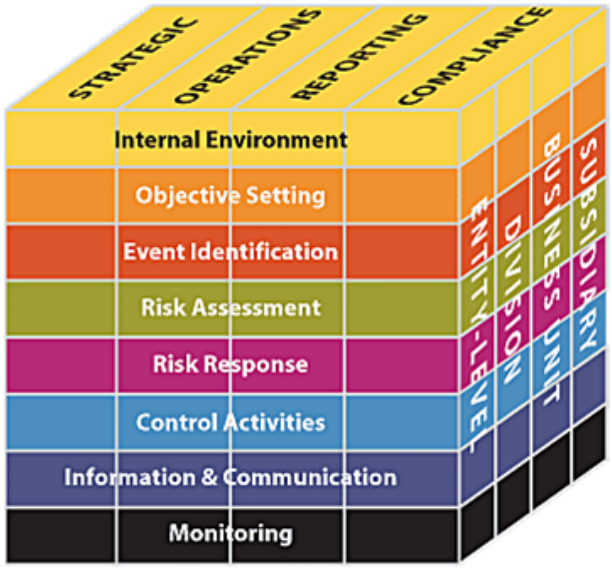

Abbildung 2.2: COSO-Würfel

COSO-Würfel (vgl. Abbildung 2.2) stellt die Basis für die Entwicklung interner Kontrollsysteme dar, dessen Vorschriften, Regeln und Verordnungen im Rahmen von SOX umgesetzt und daher entsprechend dieses 8-Stufen-Modells kontrolliert werden.[185]

Auswirkungen & Aufwand

In den USA wird der Sarbanes-Oxley Act als *«die bedeutendste Regulierungsinitiative in Bezug auf den US-amerikanischen Kapitalmarkt seit 1930»*[186] bezeichnet und berührt die Kernthemen

- Financial Reporting
- Corporate Governance
- Corporate Compliance
- Internal Control und
- Enterprise Risk Management.

Diese Schlagworte sind keineswegs Neuerfindungen, erlangten aber durch die gesetzlichen Regulative zusätzliche Bedeutung und Relevanz. International diskutiert wird etwa der Einfluss der verschärften US-Regeln auf das amerikanische Wirtschafts- und Rechtssystem sowie mögliche Auswirkungen des Kapitalflusses in die USA aus dem Ausland.

[185] vgl. [Pfister2006]
[186] vgl. [Menzies2006, S. 16]

Kritisch hinterfragt wurden vor allem die finanziellen und organisatorischen Aufwände der Umstellung. Vor allem das Erstellen einer normgerechten Dokumentation sowie die vollständige Umsetzung der Section 404 kostete Unternehmen beinahe 0.1% ihres Erlöses. Knapp 20% davon wurden in die Umsetzung der Section 404 investiert.[187] Erschwerend kam hinzu, dass die amerikanische Börsenaufsicht den ursprünglichen Umsetzungstermin vom 15. Juni 2004 mehrmals nach hinten verschoben hat und einige Bestimmungen erst mit 15. Juli 2007 realisiert werden mussten.

In Europa wird SOX weniger als gesetzlicher Rahmen, sondern vielmehl als Initiative des Risikomanagements verstanden und daher in Form einer «light touch» Version angewandt.[188] Best-Practice-Empfehlungen und Anregungen zur Umsetzung nach dem Comply-Or-Explain-Ansatz[189] stellen die europäischen Eckpfeiler dar.

2.5.2 Foreign Corrupt Practices Act (FCPA)

Der **Foreign Corrupt Practices Act** ist ein bereits 1977 vom amerikanischen Kongress verabschiedetes Bundesgesetz und stellte damals eines der ersten Anti-Korruptionsgesetze dar, um Bestechung von ausländischen Regierungsbeamten zur Erlangung von Aufträgen zu verhindern. Oberstes Ziel war die Wiederherstellung des Vertrauens in das amerikanische Geschäftssystem sowie die Beseitigung von Wettbewerbsnachteilen. Im weiteren Verlauf wurde an internationalen Vorschriften (gemeinsam mit der OECD) gearbeitet und bis 2006 36 Anti-Korruptionsgesetze in unterschiedlichsten Staaten erlassen.[190]

Komponenten & Anwendungsbereich

Das Gesetz beinhaltet zwei wesentliche Vorkehrungen[191]:

- Die so genannten **«Anti-Bribery Provisions»** beinhalten Vorschriften und Bestimmungen zur Vermeidung von Bestechung und Korruption.
- Im zweiten Abschnitt, den **«Books and Records Provisions»**, finden sich Regulative zur ordnungsgemäßen Buchführung sowie zum Vorhandensein wirksamer, interner Kontrollsysteme zur Vermeidung von Gesetzesverstößen.

Anwendbar sind diese Normen - wie auch bei SOX - für alle Unternehmen, die an einer amerikanischen Börse mit Eigen- oder Fremdkapital gelistet sind und damit der US-Börsenaufsicht unterliegen. Verstöße gegen den FCPA resultieren in hohen Strafen und

[187] vgl. [Hausegger2007, S. 20]
[188] vgl. [Menzies2006, S. 17]
[189] etwa im Österreichischen Corporate Governance Kodex, vgl. Abschnitt 2.4.3
[190] vgl. [Menzies2006, S. 25]
[191] engl. Provisions, vgl. [Menzies2006, S. 25]

können neben finanziellen und rechtlichen Einbußen auch Rufschädigungen bei ausländischen Partnern oder gar Staaten mitsichbringen.[192]

Anti-Bribery Provisions

Die Antikorruptionsvorschriften sollen verhindern, dass durch Zuwendungen, unlauteren Wettbewerb oder staatlichen Beeinflussungen Aufträge oder Verträge im internationalen Raum abgeschlossen werden. Ein solcher Korruptionsverdacht besteht aus fünf Elementen (vgl. Tabelle 2.3[193]).

Vorschrift	**Beschreibung & Anwendung**
Who - Wen betrifft der FCPA	Neben dem Unternehmen als ganze Einheit ist der FCPA auch auf beteiligte Gesellschafter, Führungskräfte und leitende Angestellte anwendbar.
Corrupt Intent - Die korruptive Absicht	Durch eine geplante bzw. bereits durchgeführte Bestechungshandlung soll ein Vorteil für die bestechende Partei erwirkt werden. Dieses Verhalten (auch wenn es sich um die bloße Bestechungsabsicht handelt) ist gemäß FCPA strafbar.
Payment - Die Zahlung	Der gewährte Vorteil kann sowohl monetären als auch werthaltigen Charakter aufweisen und reicht von Preisnachlässen und Darlehen über die Einladung zu Veranstaltungen oder privaten Dienstleistungen bis hin zu «wohltätigen Spenden».
Recipient - Der Empfänger	Das Empfangen solcher Zuwendungen ist lediglich für «foreign officials», also etwa Staatsführungsorgane (Regierung, Administration, Königshaus), Justiz- & Legislaturmitglieder, Militär oder Angestellte des öffentlichen Sektors verboten.
Business Purpose Test - Geschäftszweck	Korruptionsvorhaben dienen einem konkreten Geschäftszweck und beeinflussen daher ausländische Entscheidungen, Aufträge und Geschäfte. Es muss sich dabei nicht um direkte Geschäftsbeziehungen zu internationalen Regierungsstellen handeln.

Tabelle 2.3: Fünf Elemente der Anti-Bribery Provisions

Books and Records Provisions

Die Buchführungs- und Rechnungslegungsvorschriften gelten für alle Mitarbeiterinnen und Mitarbeiter unabhängig von etwaigen anderen, zusätzlichen Regulativen und beziehen sich auf monetäre sowie materielle Werte. Im Vergleich zu den Antikorruptionsvorschriften ist dieser Gesetzesabschnitt eher allgemein und themenübergreifend formuliert.[194]

[192] vgl. [Menzies2006, S. 25]
[193] vgl. [Menzies2006, S. 26-27]
[194] vgl. [Menzies2006, S. 28]

Im Bereich der ordnungsmäßigen Buchführung fordert der FCPA die transaktionsorientierte Aufzeichnung aller buchhalterischen Bewegungen sowie eine transpartente und korrekte Zusatzdokumentation, die in Einklang mit den Rechnungslegungsvorschriften der SEC stehen muss. Wiederum wird Zahlungen und Spenden ins Ausland mit illegalem Charakter erhöhte Aufmerksamkeit geschenkt.[195]

Die Regelungen zum internen Kontrollsystem sind ähnlich denen der SOX-Section 404 und verlangen autorisiertes Transaktionsmanagement, korrekte Vermögensaufstellungen sowie regelmäßige Inventurprozesse. Interessant ist vor allem die Einführung einer «Whistleblower Hotline», an welche sich alle Mitarbeiterinnen bzw. Mitarbeiter anonym wenden können und auf etwaige Unregelmäßigkeiten oder Betrugsverdächtigungen im Unternehmen hinweisen können. Diese Hotline kann Bestandteil des internen Kontrollsystems sein.[196]

2.6 Implementierung der Rechtsvorschriften

Die im gesamten Kapitel 2 untersuchten Rechtsvorschriften auf nationaler, europäischer und internationaler Ebene - beginnend bei der 8. EU-Richtlinie und dem Basel II Abkommen über das österreichische Comply-Or-Explain-Konzept des nationalen Governance-Kodex bis zur internationalen Regulierung US-börsennotierter Unternehmen durch SOX und FCPA - zeigen einmal mehr den komplexen Aufbau von Wirtschafts- und Rechtssystemen.

Diese Mischform aus freiwilligen Bestimmungen durch Konzepte, Anwendungsmodelle oder Empfehlungen und verpflichtenden Gesetzen stellt viele Unternehmen vor neue Herausforderungen. Es bedarf nicht nur der parallelen Unterwerfung heterogener Rechtssysteme, sondern auch der Straffung interner Strukturen, der Bildung ganzheitlicher Prozessabläufe und der Verantwortungswahrnehmung durch Führungskräfte und Top-Management.

Das folgende Kapitel soll nun die genannten Regulative und Vorschriften praktisch implementieren und damit den direkten Bezug zur IT-Governance bzw. IT-Compliance herstellen. Neben Methoden des IT Service Managements stehen vor allem Fragen der Aufgabenposition des Vorstandes - insbesondere des CIOs - sowie aktuelle Zahlen, Daten und Fakten aus aktuellen Management-Umfragen im Vordergrund.

[195] vgl. [Menzies2006, S. 28-29]
[196] vgl. [Menzies2006, S. 29]

3 Implementierung & Realisierung von IT-Governance/Compliance-Systemen

Die bisherigen Kapitel haben ein Grundverständnis der Begrifflichkeiten *IT-Governance* und *IT-Compliance* vermittelt und in weiterer Folge eine Reihe an rechtlichen Rahmenbedingungen bzw. Regulativen aufgezeigt, die den Einsatz von Informationstechnologie maßgeblich beeinflussen.

Die Umsetzung eines IT-Governance-Systems bedarf in jedem Fall der Unterstützung des Top-Managements und geht mit der Umstrukturierung von Prozessen und Unternehmensstrukturen einher. Es gilt neue Denkansätze zu verfolgen sowie praxisorientierte IT Service Management Methoden anhand standardisierter Frameworks (z.B. ITIL oder COBIT) anzuwenden. Der Chief Information Officer (CIO) eines Unternehmens kann dabei als Steuerungseinheit solcher Modelle angesehen werden, wodurch die Frage nach den Aufgabenbereichen und Verantwortungen des Vorstandes aufgeworfen wird.

Das aktuelle Kapitel verfolgt einen ganzheitlichen Ansatz und stellt Modelle, Frameworks und Best-Practices vor, die eine Implementierung von risikobewussten IT-Systemen ermöglichen. Es stehen dabei die wirtschaftlichen und rechtlichen Aspekte im Vordergrund, d.h. auf technische Details der IT-Sicherheit (beispielsweise Verschlüsselung oder Authentifizierung) bzw. die hardwareorientierte Umsetzung (beispielsweise der System- und Servicearchitektur) wird nicht eingegangen.[197]

3.1 IT Service Management

Im Allgemeinen befasst sich das *IT Service Management* mit Prozessen, Ansätzen und Vorgehensweisen, die zielgerichtete, kundenfreundliche und kostenoptimierte Dienstleistungen der Informationstechnologie ermöglichen sowie gleichnamige planen, steuern und überwachen.[198]

[197] An dieser Stelle darf auf einschlägige Fachliteratur zu den Schlagworten *IT-Sicherheit*, *IT-Betrieb* und *IT-Infrastruktur* verwiesen werden.
[198] vgl. [Olbrich2008, S. 8]

Oberstes Ziel dabei ist die Schaffung von hohen Qualitätsansprüchen, die in weiterer Folge zur Zufriedenheit aller Beteiligten führen sollen. Das IT Service Management greift daher mehrere Aufgabenblöcke, die kreisförmig miteinander in Verbindung stehen, auf (vgl. Abbildung 3.1[199]).

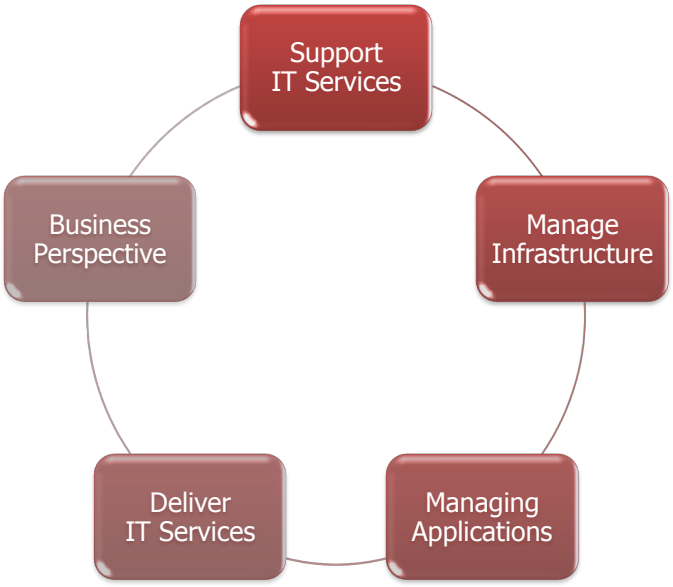

Abbildung 3.1: Aufgaben des IT Service Managements

Diese ganzheitliche Sicht auf alle Ebenen der Informationstechnologie ermöglicht eine effiziente und zielgerichtete Unterstützung der operativen Geschäftsprozesse. Im Rahmen dieser realen Abläufe - beispielsweise wären dies die Transaktionsabwicklung einer Bank oder die Kundenbetreuung eines Telekommunikationsanbieters - müssen nun sämtliche rechtlichen Regulatorien zur Buchführungspflicht, zur Risikominimierung bzw. zur Sicherung des Unternehmensfortbestandes beachtet und umgesetzt werden.

Genau diese Aufgabe erledigt das IT Service Management und bildet damit das Bindeglied zwischen den rechtlichen Regulatorien der IT-Governance bzw. IT-Compliance auf der einen und den realen Geschäftsprozessen auf der anderen Seite. Die Informationstechnologie fungiert somit als Schnittstelle bzw. Dienstleister und versorgt alle Unternehmensbereiche mit IT-Know-How, Infrastruktur, den richtigen Applikationen sowie einer ausgerichteten Geschäftsperspektive.

Alfred Olbrich, seit über 15 Jahren selbständiger Consultant in den Bereichen Projektmanagement, Prozesseinführung und Prozessoptimierung sowie ITIL-Trainer und ITIL IT

[199] vgl. [Olbrich2008, S. 8]

Service Manager[200], zeigt ergänzend die sieben wichtigsten Einflussfaktoren des IT Service Managements auf:

- Mitarbeiter
- Kunden
- Management & Strategie
- Prozesse
- Organisation & Kultur
- Know-How
- Umgebung & Infrastruktur

Neben den technischen Anforderungen spielen auch soziale, politische und kulturelle Belange eine wichtige Rolle. Ziele müssen klar definiert, realistisch sein und in einer allgemein verständlichen Art und Weise dokumentiert werden.[201]

Die juristischen Rahmenbedingungen fordern in vielerlei Hinsicht eine durchgehende Struktur, standardisierte Rahmenwerke sowie interne Kontrollsysteme, die durch ein gezieltes IT Service Management erreicht werden können. Daher haben es sich die beiden internationalen Organisationen ISACA und ITGI zur Aufgabe gemacht, praxisorientierte Rahmenwerke zu entwickeln und diese in Form von international anerkannten Standards zu veröffentlichen.

Im Folgenden sollen sowohl die ISACA bzw. das ITGI kurz vorgestellt werden, sowie die beiden wichtigsten IT-Governance- und IT-Service-Management-Frameworks, nämlich

- Information Technology Infrastructure Library (ITIL) und
- Control Objectives for Information and Related Technology (COBIT)

vorgestellt werden.

3.1.1 ISACA und ITGI

Im internationalen Umfeld gibt es eine Vielzahl an Organisationen, die sich mit dem Themenbereich *IT-Governance* bzw. *IT-Compliance* beschäftigen. Die beiden einflussreichsten Institutionen[202] sind

[200] vgl. [ItServiceManagementForum2010]
[201] vgl. [Olbrich2008, S. 1-2]
[202] vgl. [Fröhlich2007, S. 102]

- die Information Systems Audit and Control Association (ISACA)[203] und
- das IT Governance Institute[204].

Die **ISACA** wurde 1969 gegründet und besteht derzeit aus ca. 61.000 praxisorientierten IT-Experten, die gemeinsam Themen der Sicherheit und Überwachung in der Informationstechnologie bearbeiten. Seit damals gilt diese Vereinigung als eine der treibenden Organisationen im IT-Governance-Umfeld.[205]

1998 nahm das **ITGI** eine weitere Schlüsselrolle in diesem Themenbereich ein und bildete eine nicht-kommerzielle Stiftung zur wirtschaftlichen Weiterentwicklung und praktischen Verbreitung von IT-Governance.[206]

Beide Institutionen verfolgen das Ziel der gemeinschaftlichen Entwicklung eines internationalen Rahmenwerkes zur Implementierung von IT-Governance-Systemen im Gesamtkontext der Unternehmensführung. Sie unterstützen *«somit die für Informationstechnologie in der Verantwortung stehenden Personen mit einem Rahmenwerk, um den ständig steigenden Anforderungen an Transparenz, Flexibilität, Kostendruck, Risikominimierung und Compliance Rechnung zu tragen.»*[207] Ebenso werden beide Vereinigungen von einer zentralen Stelle koordiniert.

3.1.2 Information Technology Infrastructure Library (ITIL)

Bereits im Jahre 1989 wurde die damalige CCTA (Central Computer and Telecommunications Agency) - die heutige OGC (Office of Government Commerce) - damit beauftragt IT-Dienstleiter, Rechenzentren, Kunden und Lieferanten auf aktive Geschäftsprozessunterstützung durch die IT zu untersuchen. Es entstanden umfangreiche Berichte und Zusammenfassungen, die mit dem Namen *IT Infrastructure Library (ITIL)* bezeichnet wurden.[208]

Bestandteile & Kernpublikationen

ITIL 1.0 bestand aus mehr als 40 Büchern über IT Service Management und beinhaltete 26 Module. Zwischen 2000 und 2004 wurden große Teile des bestehenden Frameworks restrukturiert und es entstand ITIL 2.0. Seit dem Frühsommer 2007 ist die Version 3.0 - bestehend aus den Kernpublikationen (ITIL Core), den Ergänzungen (ITIL Complementary Guidance) sowie der Webunterstützung (ITIL Web Support Services) - veröffentlicht.[209]

[203] vgl. `http://www.isaca.org`, zuletzt abgerufen am 30.01.2010
[204] vgl. `http://www.itgi.org`, zuletzt abgerufen am 30.01.2010
[205] vgl. [Fröhlich2007, S. 102]
[206] vgl. [Fröhlich2007, S. 102]
[207] vgl. [Fröhlich2007, S. 103]
[208] vgl. [Olbrich2008, S. 1]
[209] vgl. [Glenfis2010f]

Heute bildet ITIL mit seinen fünf Kernpublikationen (vgl. Tabelle 3.1) einen *«weltweiten De-facto-Standard im Bereich Service Management und beinhaltet eine umfassende und öffentlich verfügbar fachliche Dokumentation zur Planung, Erbringung und Unterstützung von IT Serviceleistungen.»*[210] [211]

Der IT Service Lebenszyklus

Dieser ITIL-Kern bildet den kompletten Lebenszyklus eines Services, beginnend bei der Definition der *Service Strategie*, welche die Richtlinien und Ziele vorgibt, ab. Im Rahmen des *Service Designs*, der *Service Transition* und der *Service Operations* werden diese Planungsvorhaben umgesetzt. Die Phase der *Continual Service Improvements* zielt schlussendlich auf die kontinuierliche Verbesserung und die Fehlervermeidung in zukünftigen Projekten ab.

Abbildung 3.2[212] zeigt, dass die Organisation der vielfältigen Informationen und Verhaltenweisen sehr wichtig für eine zielgerichtete Anwendung des Modells ist. Konkurrierende Ziele müssen strukturiert beseitigt und das wertvolle, vorhandene Wissen voll ausgeschöpft werden.[213]

Anwendungsbereiche

ITIL ist in vielen Branchen und Projekten anwendbar, da die Definitionen sehr allgemein gehalten sind. Es wird vordergründig auf das *WAS* eingegangen, d.h. welche Prozesse, Rollen, Aufgaben und Abhängigkeiten bei dem Aufbau und dem Betrieb einer professionellen IT-Infrastruktur hohen Stellenwert genießen. Die eigentliche Implementierung, also das *WIE* ist abhängig von der Anwendungsdomäne und muss im Einzelfall festgelegt werden. ITIL enthält also keine Formularvorlagen oder Implementierungsvorschriften und empfiehlt auch keine konkreten Softwaretools.[214]

Besonders in den letzten Jahren ist im IT-Sektor ein Wandel von der Selbstrealisierung in Richtung Dienstleistung (Outsourcing, Outtasking) zu beobachten. Zunehmend werden daher Leistungen von externen Dienstleistern (Service Providern) zugekauft, anstatt die eigenen Resourcen mit deren Umsetzung zu belasten. Solche Maßnahmen erfordern eine intensive Interaktion zwischen Kunde (Customer) und Dienstleister (Service Provider) bzw. führen auf der Dienstleistungsseite zu einer ausgeprägten Kundenorientierung.[215]

[210] vgl. [Glenfis2010f]
[211] Beschreibungen der ITIL-Publikationen: Service Strategy ([Glenfis2010d]), Service Design ([Glenfis2010b]), Service Transition ([Glenfis2010e]), Service Operation ([Glenfis2010c]), Continual Service Improvement([Glenfis2010a])
[212] vgl. [Glenfis2010f, erste Grafik]
[213] vgl. [Glenfis2010f]
[214] vgl. [Olbrich2008, S. 1]
[215] vgl. [Olbrich2008, S. 3]

ITIL-Publikation	**Beschreibung & Anwendung**
Service Strategy	Buch eins der Serie beinhaltet Grundprinzipien und Anleitungen, wie die Werte eines Unternehmens strategisch positioniert werden müssen. Zusätzlich definierte Richtlinien und Leitfäden geben Aufschluss über die Anwendung der folgenden vier Phasen des Lifecycles.
Service Design	Dieser Band stellt Leitfäden zur Entwicklung neuer Services zur Verfügung und unterstützt bei der Umsetzung von Service Portfolios und Service Assets. Service Assets sind die nicht greifbaren Werte eines Systems. Beispielsweise wäre das Humankapital (Human Capital) ein Asset einer Organisation (vgl. [Glenfis2010d]). Auch Ansätze zur Leistungsoptimierung und Vereinheitlichung der regulatorischen Anforderungen stellen wertvolle Hinweise dar.
Service Transition	Nach Abschluss der Konzeption finden sich im dritten ITIL-Kern «Betriebsanleitungen» zur Entwicklung und Verbesserung von Services sowie für den IT-Betrieb. In Form von Service-Design-Paketen werden mögliche Fehler und Ausfallrisiken eruriert und mit praktischen Konzepten des Risk-, Programm- und Release-Managements kombiniert. Zusätzlich gilt es Hilfestellungen zu etablieren, die zur Kontrolle des Services zwischen Kunde und Service Provider Anwendung finden.
Service Operation	Klassische Tätigkeiten des IT-Betriebs werden im vierten Abschnitt - der Service Operation - durchgeführt. Effiziente Serviceauslieferungen, gute Supportleistungen sowie die Sicherstellung einer ständigen Kommunikation zwischen Kunde und Service Provider stellen die wesentlichen Eckpfeiler dar. Tätigkeiten des Tagesgeschäfts erfordern zusätzliche Ansätze zur Stabilisierung, zum Erhalt und zur Skalierung bestehender Service Portfolios.
Continual Service Improvement	Als allumfassende Komponente stellt das Continual Service Improvement instrumentalisierte Anleitungen zur Erhaltung des Kundenmehrwerts und zur Optimierung von Design, Betrieb und Wartung zur Verfügung. Prinzipien des Qualitäts-, Prozess- und Änderungsmanagements stehen in direkter Verbindung zu Service Strategie, Service Design, Service Transition und Service Operation.

Tabelle 3.1: ITIL-Kernpublikationen

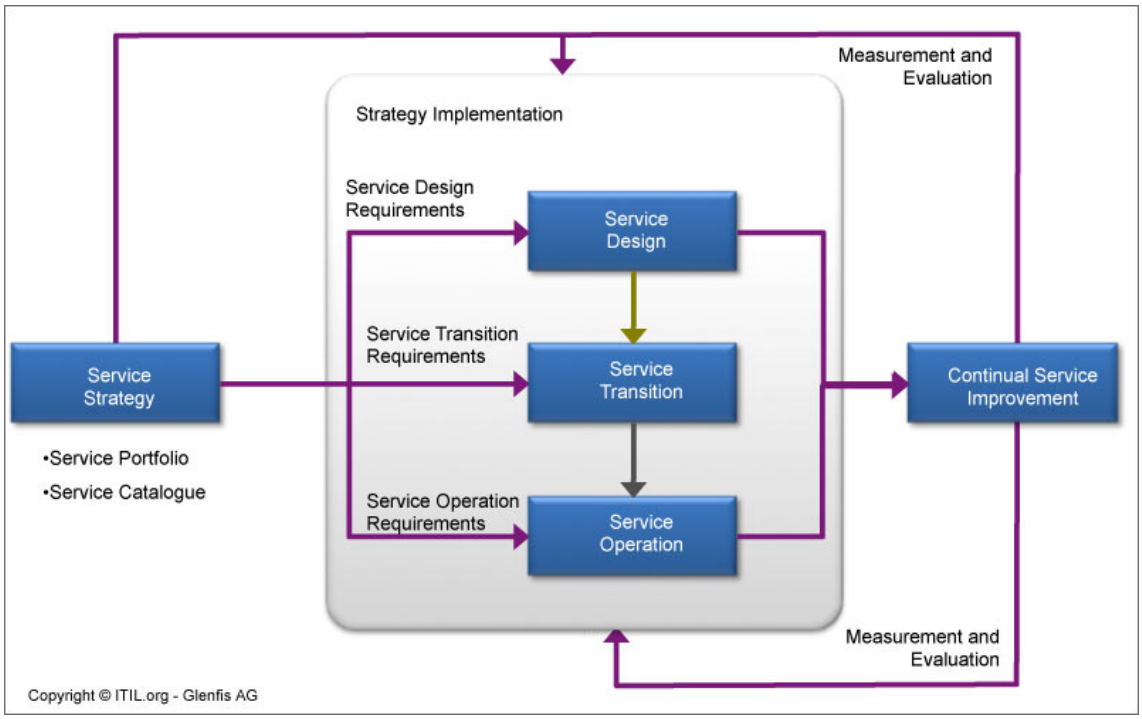

Abbildung 3.2: ITIL Service Lebenszyklus

Dieser «Kulturwandel» wird durch das ITIL-Framework voll und ganz unterstützt, da einerseits ein gemeinsames Verständnis der Materie und andererseits eine strukturierte und abgestimmte Vorgehensweisee in der Abwicklung des gesamten IT Service Managements gewährleistet wird. Eine Dienstleistung bekommt somit einen Mehrwert und steht nicht mehr nur für das bloße Erbringen von Leistung.[216]

ITIL ist ein sehr umfangreiches Framework mit empfehlendem Charakter zum Aufbau einer durchgängigen Kommunikation und führt zu einem erfolgreichen, beständigen Geschäftsbetrieb. Auch für mittelständische und kleine Unternehmen existiert «ITIL in Small Units», welches einfache Ansätze und ein simpleres Anwendungsmodell bereitstellt.[217]

3.1.3 Control Objectives for Information and Related Technology (COBIT)

COBIT ist die wichtigste Publikation des *IT Governance Institutes* (ITGI) und liegt derzeit in Version 4.1 vor. Ins Leben gerufen wurde dieses Framework erstmals im Jahre 1998 und stellt bis heute ein maßgebendes IT-Governance-Werkzeug zur Umsetzung von IT- und Unternehmenszielen dar.[218]

[216] vgl. [Olbrich2008, S. 4]
[217] vgl. [Olbrich2008, S. 5]
[218] vgl. [Popp2007, S. 18-19]

Wie der Name «Control Objectives for Information and Related Technology» bereits vermuten lässt, liegt der zentrale Fokus auf der technologischen Verarbeitung von Informationen innerhalb des Unternehmens. Im Rahmen von COBIT werden wiederum Empfehlungen gemacht und Modelle vorgestellt, die aus der Sicht zahlreicher internationaler Experten positive Auswirkungen auf IT-Aktivitäten, IT- und Unternehmensziele haben.[219]

Zentrale Aussagen des Rahmenmodells sind etwa[220]:

- COBIT ist ausgerichtet auf das Unternehmen.
- COBIT ermöglicht maximale Gewinne.
- COBIT ermöglicht den verantwortungsvollen Einsatz von IT-Ressourcen.
- COBIT ermöglicht ein angemessenes Risikomanagement.
- COBIT verbessert Effektivität und Effizienz.
- COBIT hilft der IT die Anforderungen der Fachbereiche zu verstehen.
- COBIT ist praxisorientiert und jahrelang erprobt.

COBIT-Kernbereiche

Das ITGI legt dem COBIT-Framework eine eigene Defintion von IT-Governance zu Grunde. Diese besteht aus fünf Kernbereichen (*Focus Areas*, vgl. Abbildung 3.3[221]), welche gleichzeitig die Basis des Rahmenwerks zur gewissenhaften Steuerung der IT durch entsprechende Maßnahmen darstellen.

Diese fünf Kernbereiche der IT-Governance nehmen die in Tabelle 3.2 beschriebenen Hauptaufgaben bzw. Aspekte war.[222]

Informationskriterien

Als zentrales COBIT-Element wurde bereits eingangs eine strukturierte Menge an Informationen vorgestellt. Diese Informationen müssen festgelegten Kriterien entsprechen, um ein gleiches Verständnis und eine zielgerichtete Anwendung in allen Prozesschritten des COBIT-Frameworks zu gewährleisten.

[219] vgl. [Popp2007, S. 20]
[220] vgl. [ISACA2009a, S. 2-3] bzw. [Popp2007, S. 22]
[221] vgl. [ISACA2009b, F. 8]
[222] vgl. [ISACA2009a, S. 3] bzw. [Popp2007, S. 21-22]

Abbildung 3.3: IT-Governance Kernbereiche nach ITGI

Diese Informationskriterien (*Information Criteria*) sind[223]:

- Wirksamkeit (Effectiveness)
- Wirtschaftlichkeit (Efficiency)
- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)
- Compliance (Compliance)
- Verlässlichkeit (Reliability)

Vollständiges COBIT-Framework

Die IT-Governance-Basisdefinition bzw. die soeben konkretisierten Informationskriterien können bei Betrachtung des gesamten Frameworks (vgl. Abbildung 3.4[224]) als äußere Hülle (Ring eins und zwei) verstanden werden. Eigentliche Aufgabe des prozessorientierten Rahmenmodells ist die Umsetzung von 34 Prozessen in den vier COBIT-Domänen, die in der inneren Kreisfläche dargestellt sind.[225]

Abbildung 3.4 lässt weiters erkennen, dass es eine Vielzahl von Einflüssen und Rahmenbedingungen im COBIT-Framework gibt und das gewünschte Ziel genau im Mittelpunkt aller Prozesse - also die direkte Kontrolle (*Direct Control*) aller IT-Aktivitäten - platziert wird.

[223] vgl. [Popp2007, S. 23-24]
[224] vgl. [ISACA2009b, F. 11]
[225] vgl. [Popp2007, S. 26]

Kernbereich	**Beschreibung & Anwendung**
Strategic Alignment	fokussiert die Verbindung zwischen Fachbereichen und IT-Plänen und definiert, verbessert bzw. validiert IT-Werte und den IT-Betrieb. Es sollen die IT-Ziele auf die Unternehmensziele ausgerichtet sowie der IT-Wertbeitrag sichergestellt werden.
Value Delivery	stellt sicher, dass IT-Aktivitäten den veranschlagten Nutzen bringen und kostenoptimiert umgesetzt werden. Auch die nachhaltige Administration der IT-Lieferkette (*Delivery Cycle*) darf nicht außer Acht gelassen werden.
Resource Management	optimiert Investitionen in kritische IT-Ressourcen wie Prozesse, Mitarbeiter, Applikationen, Infrastruktur und Informationen (vgl. auch Abbildung 3.4). Gleichzeitig werden Know-How und Entwicklung optimiert.
Risk Management	erfordert risikobewusstes Verhalten des Top-Managements sowie ein klares Verständnis möglicher Risikoauswirkungen, um so Probleme transparent zu machen und entsprechende Verantwortlichkeiten und Prozesse zur Vermeidung derselbigen im Unternehmen zu etablieren.
Performance Measurement	überwacht und verfolgt Strategieimplementierungen, Projektverläufe, Ressourcenverwendung, Prozessperformance und Servicegrade. Daraus abgeleitet werden Balanced Scorecards (BSCs), die mögliche Strategien in realistische und vor allem messbare Ziele umwandeln.

Tabelle 3.2: IT-Governance Hauptaufgaben nach ITGI

Prozessablauf im COBIT-Framework

Beginnend mit der Planung und Formulierung der gewünschten Ziele werden im ersten Prozesschritt **«Plan and Organise»** notwendige Schritte zur Ausrichtung und Erreichung dieser IT-Aktivitäten definiert. Die entwickelte Vision gilt es anschließend zu kommunizieren sowie die Übereinstimmung dieser *IT-Strategie* mit den Ressourcen, der Qualität und dem vorhandenen Risikomanagement sicherzustellen.[226]

Aufbauend auf der Planung kann mit der Umsetzung, also dem **«Acquire and Implement»**, begonnen werden. *«Mögliche IT-Lösungen müssen gefunden, evaluiert und in die bestehenden (Geschäfts-)Prozesse integriert werden.»*[227] Desweiteren finden sich Kontroll-,

[226] vgl. [Popp2007, S. 27-28]
[227] vgl. [Popp2007, S. 28]

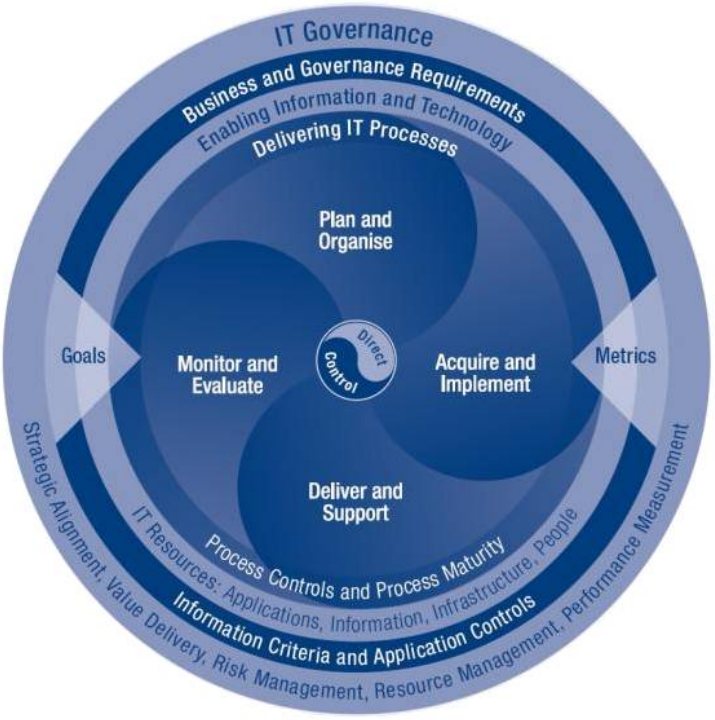

Abbildung 3.4: COBIT-Framework

Warnungs- und Änderungsmaßnahmen zur Adaptierung an die Unternehmensanforderungen in dieser Domäne.

Sobald die Implementierung abgeschlossen ist, kann die Auslieferung und der Support («**Deliver and Support**») initiiert werden. Dieser Prozessschritt beinhaltet neben der eigentlichen Serviceerbringung - und dem damit generierten Wertbeitrag der IT für das Unternehmen - auch die Administration der Sicherheit und Kontinuität des Services, die Unterstützung der Benutzer sowie Effizienz und Effektivität im Umgang mit den beteiligten Systemen (IT-Kosten, Produktivität). Dieser Teil des Rahmenwerks ist daher der öffentlichkeitswirksamste, da intensive Schnittstellen zu anderen Abteilungen und externen Partnern bestehen.[228]

Zum Vergleich der erbrachten Serviceleistung mit den ursprünglich definierten Vorgaben wird eine Monitoring- bzw. Evaluierungsphase («**Monitor and Evaluate**») installiert. Diese Überwachung achtet auf definierte Kontroll- bzw. Prozessziele und gewährleistet die adäquate Umsetzung von notwendigen Regulativen, Performancemessungen und Berichtserstattungen.[229]

[228] vgl. [Popp2007, S. 27-28]
[229] vgl. [Popp2007, S. 28]

Messung der Ziele

Der Prozessschritt *Monitor and Evaluate* setzt voraus, dass die zuvor definierten Ziele mess- und darstellbar sind. COBIT implementiert dazu sogenannte *Controls* (Messpunkte), die regelmäßige IT-Werte erheben. Die zu erreichenden Zielwerte werden in *Control Objectives* (Kontrollzielen) definiert, die sich wiederum aus der Hierarchie der Unternehmens- bzw. IT-Ziele ergeben.[230]

Als Messtechniken definiert COBIT die Anwendung von sogenannten Reifegradmodellen aber auch Performancemessungen. In beiden Fällen ist es unerlässlich, dass die Controls in die jeweiligen IT-Aktivitäten eingebunden werden und so ein konsistenter Zusammenhang von der IT-Governance über die IT-Prozessdefinitionen bis zu den Messwerten der einzelnen Controls hergestellt werden kann.[231]

Das Reifegradmodell wird auf Einzelprozessebene angewandt und bestimmt die Entwicklungsstufe eines kritischen Prozesses auf einer sechsstufigen Skala (vgl. Tabelle 3.3[232])

Reifegrad	**Bezeichnung**	**Beschreibung**
0	Nicht existent	Kein Prozess erkennbar und daher keine Behandlung erforderlich.
1	Initial	Ein situationsbezogener Ad-Hoc-Prozess ist vorhanden, jedoch noch nicht standardisiert.
2	Wiederholbar	Verschiedene Prozesse wenden gleichartige Verfahren an, jedoch gibt es kaum Wissen und Informationen über den Prozess, wodurch Fehler auftreten.
3	Definiert	Der Prozess wurde als formales Abbild der Realität standardisiert, wird unregelmäßig überprüft und ist nicht automatisiert.
4	Gemanaged	Eine Messung und Überwachung des Prozesses findet statt, Schwachstellen werden behoben und Best-Practices verbessert, jedoch liegt eine eingeschränkte Automatisierung vor.
5	Optimiert	Prozesse werden in einem ganzheitlichen Kontext integiert und mittels IT-Unterstützung mit anderen Organisationen verglichen, um Verbesserungen in Qualität und Wirksamkeit durch flexible Prozessanpassungen zu erwirken.

Tabelle 3.3: Reifegradmodell nach COBIT

[230] vgl. [Popp2007, S. 29]
[231] vgl. [Popp2007, S. 29-30]
[232] vgl. [Popp2007, S. 31]

Zur Durchführung von Performancemessungen sieht das COBIT-Rahmenwerk zwei unterschiedliche Metriken vor[233]:

- **Key Goal Indicators (KGI)**

  KGIs messen, ob eine IT-Aktivität das zuvor definierte Ziel überhaupt erreicht hat. Wichtige Kenngröße dabei ist der Output nach der Ausführung einer Aktivität in Zusammenspiel mit den Informationskriterien (Waren alle benötigten Informationen verfügbar? Gab es Mängel bei der Integrität bzw. Vertraulichkeit? Wurde kosteneffizient gewirtschaftet?)

- **Key Performance Indicators (KPI)**

  KPIs messen die Performance eines IT-Prozesses während dessen Ausführung. Dadurch soll ermittelt werden, wie wahrscheinlich ein Ziel erreicht wird und welches Potenzial, welche Praktiken und welche Fähigkeiten zur Implementierung einer wirksamen Prozessperformance notwendig sind.

Die genannten Indikatoren sind aber keinesfalls unabhängig voneinander zu betrachten. Sobald ein Key Goal Indicator ermittelt und das korrespondierende Aktivitätsziel erreicht wurde, treibt das Ergebnis den übergeordneten Key Performance Indicator an, um auch dort eine optimale Performance zu erwirken.[234]

Anwendungsbereiche

Wie auch bei ITIL stellt COBIT ein allgemeines Rahmenwerk, definiert in vier Domänen und mehreren Prozessen bzw. Rahmenbedingungen, zur Verfügung. Durch die Ableitung der IT-Ziele und dessen Kontrollkennzahlen aus den übergeordneten Unternehmenszielen bildet COBIT ein branchenunabhängiges Modell zur Steuerung ganzheitlicher IT-Prozesse.[235]

Die zur Messung von Output und Performance vorgeschlagenen Indikatoren sowie das Reifegradmodell wirken ebenenübergreifend und unterstreichen das COBIT Mission Statement. *«To research, develop, publish and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.»*[236]

[233] vgl. [Popp2007, S. 32-34]
[234] vgl. [Popp2007, S. 34] bzw. die linken und rechten Einflussfaktoren «Goals» bzw. «Metrics» in Abbildung 3.4
[235] vgl. [Popp2007, S. 36]
[236] vgl. [Fröhlich2007, S. 77]

3.1.4 Risk IT & Val IT

ITIL und COBIT stellen die wohl umfangreichsten und am häufigsten eingesetzten Frameworks zur Implementierung von IT-Governance bzw. IT-Compliance dar. Die eingangs erwähnten Institutionen (ISACA, ITGI) haben jedoch das COBIT-Modell um zwei Spezialisierungsansätze - nämlich Risk IT und Val IT - erweitert, die zusätzliche Aufgaben einer ganzheitlichen IT-Governance umsetzen sollen.

Abbildung 3.5[237] zeigt die Schnittstellen sowie den Zyklus der drei Systeme COBIT, Risk IT und Val IT.

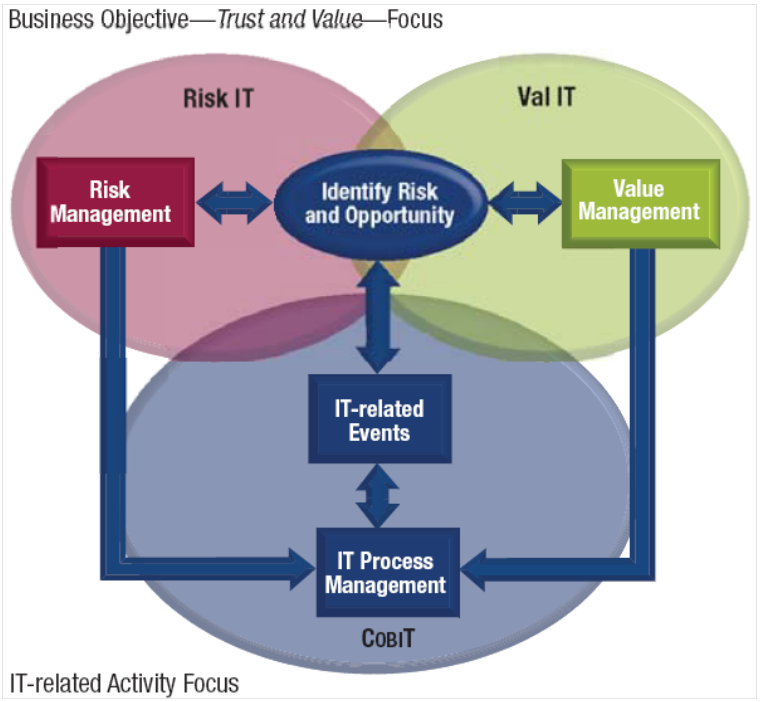

Abbildung 3.5: COBIT-Erweiterung durch Risk IT und Val IT

Risk IT

IT-Risiken sind heute stärker präsent denn je, werden jedoch von Vorständen und Managern meistens übersehen. Diese konzentrieren sich gezielt auf Markt-, Finanz- und operative Risiken und lassen die Herausforderungen der Informationstechnologie völlig außer Acht.[238]

Risk IT ist ein Framework, welches genau an dieser Schwachstelle ansetzt und angemessene, risikobewusste Entscheidungen unterstützen soll. Als Erweiterung zum bestehenden COBIT-Framework, welches primär versucht IT-Risiken zu mildern, hat Risk IT die Auf-

[237] vgl. [ISACA2009d, F. 8]
[238] vgl. [ISACA2009c, S. 2]

gabe unternehmensweite IT-Risiken zu identifzieren, zu beeinflussen und zu administrieren.[239]

Wie auch bei den vorhergehenden Frameworks handelt es sich bei Risk IT um Empfehlungen und Best-Practice-Ansätze zur Etablierung entsprechender Prozesse. Das Risk-IT-Modell besteht dabei aus drei Domänen[240]:

- Risk Governance
- Risk Evaluation
- Risk Response

Val IT

Val IT kann als drittes Element neben COBIT und Risk IT zum Einsatz kommen und somit den Kreislauf schließen. Oberstes Ziel dieser Erweiterung ist der Aufbau bzw. die Festigung der innerbetrieblichen Beziehungen zwischen der IT und den operativen Geschäftsbereichen. Entscheidungen des Managements sollen Innovationen im IT-Bereich fördern und so einen höheren ROI[241] für das gesamte Unternehmen erwirken.[242]

Ergänzend zu COBIT stellt Val IT sicher, dass die richtigen Entscheidungen bzw. Investitionen, am richtigen Weg und mit den richtigen Methoden umgesetzt werden, um einen maximalen Nutzen daraus zu ziehen. *«Val IT hat für alle Managementebenen der IT bzw. anderer Geschäftsbereiche Relevanz, beginnend beim CEO und seinem Management bis zu jenen Mitarbeitern, die direkt in Auswahl-, Beschafftungs-, Entwicklungs-, Produktions-, Auslieferungs- und Abrechnungsprozessen involviert sind.»*[243]

Das Framework - in der Version 2.0 - gibt insgesamt *22 Key Management Prozesse* vor, die in den drei Anwendungsdomänen

- Value Governance (6 Key Management Prozesse)
- Portfolio Management (6 Key Management Prozesse)
- Investment Management (10 Key Management Prozesse)

zusammengefasst sind.

[239] vgl. [ISACA2009c, S. 2]
[240] vgl. [ISACA2009c, S. 3]
[241] Return on Investment = Rendite des eingesetzten Kapitals
[242] vgl. [ISACA2009e, S. 2]
[243] vgl. [ISACA2009e, S. 2]

3.2 IT-Governance/IT-Compliance als Aufgabe des Managements

Die rechtlichen Rahmenbedingungen, aber auch die bisher besprochenen Implementierungsansätze haben einen zentralen Aspekt der IT-Governance- bzw. Compliance-Umsetzung gemein: *Sie alle fordern die vollständige, dauerhafte und zielgerichtete Unterstützung und Verantwortung des Top-Managements bzw. der Unternehmensleitung.*

Besonders die Rahmenmodelle ITIL bzw. COBIT zeigen alternative Denkansätze, strukturierte und vor allem ganzheitliche Prozessabläufe und optimierte, aufeinander abgestimmte Unternehmensziele auf. Zur Durchsetzung dieser Maßnahmen und nicht zuletzt zur Erreichung der vorgeschlagenen Ziele muss die gesamte Unternehmensstruktur - beginnend bei der kleinen Mitarbeiterin und dem kleinen Mitarbeiter bis hin zum Top-Management - an einem Strang ziehen.

Konsolidiert mit den rechtlichen Rahmenbedingungen stellt sich daher die Frage, welche Aufgaben, Verpflichtungen und Verantwortungen von der oberen Management-Elite eines Konzerns zu tragen sind, um eine entsprechende IT-Governance- bzw. IT-Compliance-Kultur im Unternehmen zu etablieren. Besonders der CIO als Vorstand für technische Belange nimmt dabei eine entscheidende Schlüsselrolle ein.

3.2.1 Aufbau einer Compliance-Organisation

Als Gegenpol zu der Vielzahl an freiwilligen Empfehlungen und Initiativen zum Aufbau einer Compliance-Organisation existieren in manchen Wirtschaftsbereichen - insbesondere für Kapitalgesellschaften - bereits einschlägige Rechtspflichten für die Geschäftsleitung. Exemplarisch seien an dieser Stelle die Allgemeine Sorgfalts- & Treuepflicht, die Überwachungs- & Risikokontrollpflicht sowie die Buchführungs- & Bilanzierungspflicht[244] genannt.

Allgemeine Sorgfalts- & Treuepflicht

Vertretungsbefugte Organe von Aktiengesellschaften oder Gesellschaften mit beschränkter Haftung müssen bereits grundlegend die Allgemeine Sorgfalts- und Treuepflicht einhalten. Diese ergibt sich aus den in Gesetz, Satzung und Anstellungsvertrag festgelegten Grenzen, wobei primär sämtliche Geschäfte, die nicht im Interesse bzw. zum Unwohle des Unternehmens getätigt werden, zu unterlassen sind.[245]

[244] vgl. [Wecker2009, S. 54-57]
[245] vgl. [Wecker2009, S. 55]

Auch Geheimhaltungspflichten und die Prinzipien des fairen Wettbewerbs gilt es zu wahren sowie der für unternehmerische Entscheidungen vorgeschriebenen Pflicht zur Informationseinholung nachzukommen. Etwa beim Aufkauf eines Unternehmens oder der Vergabe von Aufträgen müssen Informationen über den Geschäftspartner eingeholt und nach bestem Wissen und Gewissen verarbeitet werden. Bei der Nichteinhaltung dieser Regulative wären Unterlassungsansprüche bzw. Schadensersatzansprüche geltend zu machen.[246]

Überwachungs- & Risikokontrollpflichten

Ab einer bestimmten Unternehmensdimension ist es für die Geschäftsleitung quasi unmöglich alle Aufgabengebiete selbst zu überwachen. Diese Verantwortlichkeit wird daher an untergeordnete Mitarbeiterinnen und Mitarbeiter delegiert, wobei diese in die korrekte und vollständige Anwendung der notwendigen Überwachungs- und Kontrollmaßnahmen eingewiesen werden müssen. Nach einer Überprüfung der Fähigkeiten und persönlichen Eignung des/der Angestellten muss die Geschäftsleitung die benötigten Sachmittel und Ressourcen zur Verfügung stellen, bevor die eigentliche Delegation erfolgen kann.[247]

Die Geschäftsführung ist dadurch aber keinesfalls von ihren Pflichten befreit, da sie nun die Aufgabe hat, die Kontrolltätigkeiten des soeben bestimmten Aufsichtsorgans ständig zu überwachen. Auch bei der Aufteilung des Vorstandes in mehrere Ressorts, bleiben ressortfremde Geschäftsführer für die Überwachung ihnen nicht zugeteilter Unternehmensbereiche verantwortlich und müssen bei Missständen den Geschäftsbereich in die Gesamtgeschäftsführung zurückholen.[248]

Buchführungs- & Bilanzierungspflicht

Die Buchführungs- bzw. Bilanzierungspflicht besagt, dass Unternehmen mindestens jährliche Jahresabschlüsse (Bilanz, Gewinn- und Verlustrechnung) aufstellen müssen, wobei Kapitalgesellschaften zusätzlich Anhänge und Lageberichte beizufügen haben. Auch wenn diese Tätigkeiten von externen Dienstleitern oder untergeordneten Finanzabteilungen durchgeführt werden, bleibt der Vorstand für die ordnungsgemäße Erfüllung dieser Verpflichtungen voll haftbar.[249]

Diese beispielhaften Verantwortungen zeigen, dass die Installation einer Compliance Organisation nicht nur zur zukunftsorientierten Entwicklung des Unternehmens beiträgt, sondern bereits frühzeitig auf rechtliche Fehlerquellen oder Zwischenfälle durch Rechtsverstöße hinweist. Eine strukturierte Compliance-Organisation verbessert somit den internen Informationsfluss, adaptiert Kontrollmaßnahmen zur frühzeitigen Entdeckung von Fehlern und

[246] vgl. [Wecker2009, S. 55]
[247] vgl. [Wecker2009, S. 56]
[248] vgl. [Wecker2009, S. 56]
[249] vgl. [Wecker2009, S. 57]

liefert schlussendlich eine Imageverbesserung durch eine optimale Außendarstellung gegenüber Kunden und Lieferanten.[250]

Der Bogen zur IT-Governance bzw. IT-Compliance kann wieder über die weitreichende Unterstützung bzw. Serviceorientierung der Informationstechnologie gezogen werden. Bilanzierungs-, Abrechnungs-, Kontroll- und Administrationsprozesse laufen heute weitgehend automatisiert bzw. mit intensiver Unterstützung durch technische Infrastruktur ab. Somit müssen diese Grundsätze guter Unternehmensführung auch im IT-Bereich etabliert werden - eine Aufgabe, die vom CIO im Rahmen ganzheitlicher IT-Prozessadministration wahrgenommen werden sollte.

3.2.2 Der CIO als Schlüsselfigur der IT-Governance

In den letzten Jahren hat der Begriff *«Informationstechnolgie»* einen stetigen Wandel durchlebt. Während anfänglich von einer schlichten EDV-Abteilung, mit der Aufgabe die bestehende Hardware zu betreiben, die Rede war, finden wir heute abteilungsübergreifende IT-Prozesse, heterogene IT-Infrastrukturen und neuartige Systemlandschaften vor. Die einst operativen Tätigkeiten eines EDV-Leiters haben sich somit zu einer allumfassenden Managementaufgabe entwickelt, die von einer Vorstandsstelle bekleidet wird - dem Chief Information Officer (CIO).[251]

Eingliederung des CIO

Durch diese Restrukturierung der IT und die steigende Bedeutung von IT-Systemen im Wettbewerb erhalten immer mehr IT-Themen sogenannte *Board Attention* (oder *Management Attention*), werden also auf oberster Vorstandsebene diskutiert und entschieden. Durch die ganzheitlichen Ansätze bei der Implementierung von IT-Governance- bzw. IT-Compliance-Maßnahmen und die dafür notwendigen Entscheidungskompetenzen ist der CIO genau jene Schnittstelle zum Top-Management, die eine effiziente IT-Organisation benötigt.[252]

Der CIO kann entweder direkt im Vorstand sitzen oder eine Ebene darunter eingegliedert werden. Einzige Bedingung dabei ist, dass die Aufgaben des operativen IT-Managements nicht mit jenen des CIOs vermischt werden und die Kompetenzen, Verantwortungen und Entscheidungen bezüglich IT-Governance- und Compliance-Anliegen eindeutig dem CIO zugeordnet sind.[253]

[250] vgl. [Wecker2009, S. 59]
[251] vgl. [Kuhlin2004, S. 376]
[252] vgl. [Kuhlin2004, S. 376]
[253] vgl. [Armin2008, S. 416]

Einige Experten[254] weiten die Aufgabenfelder eines CIOs weiter aus, da ein reines «Verwalten von Technologien» in der heutigen Zeit nicht mehr ausreicht, um wettbewerbsfähig zu bleiben. Vielmehr wird der CIO zu einem CPO - einem Chief Process Officer. Die einzelnen Fachbereiche stellen zunehmend komplexere Anforderungen, die aus einer reinen IT-Position nicht vollständig erfasst werden können. Es bedarf eines 360-Grad-Blickwinkels, der sogar über die Unternehmensgrenzen hinweg geht, um die Wechselwirkungen zwischen IT und Geschäftsprozessen einzuschätzen. Genau das ist die Aufgabe eines CPO.[255]

Andere Ansätze[256] sehen den CIO auch als CRO (Chief Risk Officer), der eine zentrale Rolle im Vorstand einnimmt und für die gesamte IT-Landschaft eines Unternehmens (und somit auch deren Governance bzw. Compliance) verantwortlich ist.

Kompetenzen eines CIOs bzw. CPOs

Eine Mischung aus betrieblichem, marktrelevantem und technischem Know-How in Verbindung mit einem geschulten Auge für Umstrukturierungen und Innovationsmöglichkeiten wird das zukünftige Berufsbild eines CIOs/CPOs prägen. Diese C-Management-Position[257] wird somit zum «Change Agent»[258] und benötigt vor allem vier Kernkompetenzen (vgl. Tabelle 3.4[259]).

Dieses neue Anforderungsprofil an CIOs bzw. CPOs verlangt nicht nur nach Änderungen in der Ausbildung, sondern auch nach einem Umdenkprozess in den Fachabteilungen. Ausgefeilte Fähigkeiten im Netzwerk- oder Servermanagement sind heute nicht mehr gefordert. *«Entscheidend ist sein betriebswirtschaftliches Verständnis und die Fähigkeit, das Innovationspotenzial der IT für die Geschäftsprozesse zu erkennen und zu erschließen.»*[260]

3.3 Aktuelle Zahlen, Daten & Fakten

Die bislang präsentierten Konzepte, Methoden und Rahmenwerke setzen ein sehr ausgeprägtes IT-Governance- bzw. IT-Compliance-Management voraus. Optimierte Prozessabläufe, keine Verschwendung von Ressourcen, vollständige Unterstützung durch das Top-Management und die strikte Einhaltung nationaler und internationaler Rechtsnormen definieren dabei den Soll-Zustand, indem sich ein IT-orientiertes Unternehmen des 21. Jahrhunderts befinden sollte.

[254] vgl. [Kuhlin2004, S. 377]
[255] vgl. [Kuhlin2004, S. 376-377]
[256] vgl. [Armin2008, S. 416]
[257] Als C-Management-Positionen werden jene Vorstandposten bezeichnet, deren englische Abkürzungen mit dem Buchstaben *C* beginnen (z.B. CEO, CFO, CIO).
[258] vgl. [Kuhlin2004, S. 379]
[259] vgl. [Kuhlin2004, S. 380]
[260] vgl. [Kuhlin2004, S. 380]

Kompetenz	**Beschreibung**
Kommunikationsfähigkeit	Sowohl für interne als auch für externe Prozesse bedarf es unkomplizierter Informations- und Kommunikationsstrukturen. Gespräche mit Geschäftspartnern und Mitarbeitern sollen dabei im Vordergrund stehen.
Prozessdenken	Die gesamte Supply-Chain (Wertschöpfungskette) ist mit technischem, betriebswirtschaftlichem und organisatorischem Know-How zu betrachten und als Ganzes zu verstehen.
Sozialkompetenz	Der soziale Umgang im Team ist besonders bei dem zu praktizierenden Change Management, der Restrukturierung von ganzen Prozessketten und für die Bildung und den Einsatz neuer Teams und Prozesseigentümer (Process Owners) unerlässlich.
Motivation & Innovation	CIOs/CPOs arbeiten zukunftsorientiert, d.h. die Analyse von neuen Ideen in Produktion, Vertrieb oder Marketing sowie die permanente Optimierung bestehender Prozesslandschaften sind Aufgaben dieser Position.

Tabelle 3.4: Managementfähigkeiten eines CIOs bzw. CPOs

Nur einige wenige Unternehmen haben in mühsamer und kostenintensiver Arbeit eine Compliance gerechte Governance-Struktur aufgebaut. Eine Vielzahl an Organisationen und Managern haben den wahren Wert der IT sowie die damit verbundenen Risiken, Chancen und Potenziale noch nicht vollständig erkannt.

Insbesonders Unternehmensberater, Consulting Agenturen und Wirtschaftsprüfer haben es sich daher zur Aufgabe gemacht, in umfangreichen Marktstudien und Analysen den derzeitigen IT-Markt hinsichtlich der Umsetzung, Implementierung und nachhaltigen Nutzung von IT-Strukturen zu untersuchen. Exemplarisch sollen an dieser Stelle zwei aktuelle Studien vorgestellt werden:

- **Deloitte** - ein weltweit tätiges Unternehmen im Bereich der Steuerberatung, Wirtschaftsprüfung und Unternehmensberatung - präsentiert eine Studie zur IT-Nutzung in Unternehmen und zeigt, inwieweit die IT an heutige Geschäftserfordernisse angepasst ist und wie effizient die Erreichung des Unternehmenserfolges unterstützt wird.
- **PricewaterhouseCoopers** - ebenso ein Dienstleistungsunternehmen spezialisiert auf Wirtschaftsprüfung, Steuerberatung und Corporate Finance - untersuchte gemeinsam mit dem **IT Governance Institute (ITGI)** den Einsatz, die Effizienz

und die Ergebnisse von IT-Governance und fasst gängige IT-Governance-Praktiken von über 250 C-Level-Führungskräften in 22 Ländern zusammen.

3.3.1 Deloitte: Survey on IT-Business Balance

Die 2009 veröffentlichte Studie von Deloitte - durchgeführt von Consulting Spezialisten und Mitarbeitern des Bereichs «Enterprise Risk Management» - hinterfragt das strategische Potenzial IT-relevanter Fragestellungen und zeigt internationale Problemfelder des Zusammenspiels zwischen Business und IT auf. Befragt wurden über 500 IT-Manager, Unternehmens- bzw. Bereichsleiter aus 28 verschiedenen Ländern.[261]

Die Studie orientiert sich an der IT-Governance-Definition des ITGI, welche diese als integralen Bestandteil der unternehmensweiten Corporate Governance versteht. Obwohl sich daraus ableiten lässt, dass Unternehmensstrategie und IT-Strategie vollständig harmonieren müssten, haben viele Manager das Potenzial einer integrierten IT noch nicht erkannt. Die in Fachkreisen als «Business-IT-Alignment» bezeichnete Ausrichtung der IT auf die Unternehmensziele ist noch nicht vollständig implementiert und zeigt immer wieder Lücken auf.[262]

IT-Themen im Vorstand & IT Steering Committees

Abbildung 3.6[263] zeigt, dass nur etwa die Hälfte der Unternehmen IT-Themen auf oberster Management-Ebene diskutieren und die andere Hälfte dies nur selten bis gar nicht tut. Auch glauben 19% der Top-Manager, dass IT-Themen im Rahmen von Vorstandssitzungen immer zur Sprache kommen, aber lediglich 13% der IT-Fachspezialisten sind dieser Ansicht.

Die Frequenz, wie oft IT-Themen im Vorstand besprochen werden, und die Formalisierung diverser Anliegen in Form eines *IT Steering Committees*, liegt in den asiatischen bzw. kanadischen Regionen deutlich höher, als im europäischen bzw. amerikanischen Raum. 72% der asiatischen Führungskräfte arbeiten aktiv an IT-Problemen und 9 von 10 Organisationen besitzen funktioniere IT Steering Committees. Trotz dieser scheinbaren Abhängigkeit bestätigt die Studie, dass kein direkter Zusammenhang zwischen der Existenz eines IT Steering Committees und der Diskussion von IT-Themen auf Vorstandsebene besteht.[264]

Ausrichtung der Unternehmens- und IT-Strategie

Als zweiten Schwerpunkt im Abschnitt «IT-Governance» widmet sich die Deloitte-Studie der Frage, wie oft die IT-Ziele bzw. die IT-Strategien mit den übergeordneten Unterneh-

[261] vgl. [Deloitte2009a]
[262] vgl. [Deloitte2009b, S. 19]
[263] vgl. [Deloitte2009b, S. 20]
[264] vgl. [Deloitte2009b, S. 22-23]

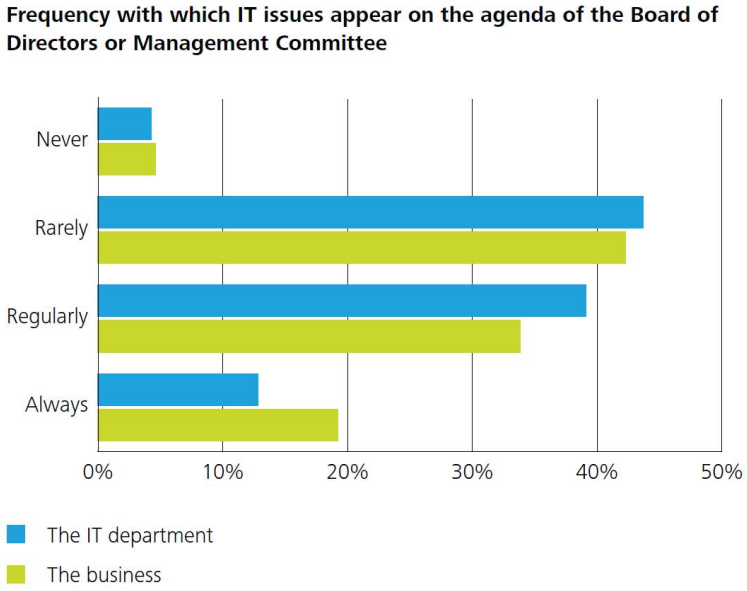

Abbildung 3.6: IT-Fokus des Top-Managements

menszielen abgeglichen werden. Abbildung 3.7[265] verdeutlicht, dass wiederum fast 50% der Organisationen nur jährlich - meistens im Zuge des betriebswirtschaftlichen Jahresabschlusses - die IT-Strategie mit der Unternehmensstrategie abgleichen. Es scheint weiters, dass auch dieser einmalige Abgleich nur durch die verpflichtende Abrechnung des IT-Budgets erzwungen wird. Wäre diese «Budgetierungsmaßnahme» nicht vorhanden, würde gar nie ein Abgleich stattfinden.[266]

Der bereits im ersten Schwerpunkt besprochene Vorzug Asiens bestätigt sich auch in der Ausrichtung von Unternehmens- und IT-Strategie. Amerika und der europäische Raum sind hier deutlich schlechter aufgestellt. *«Es scheint so, als ob IT-Governance im asiatisch-parzifischen Raum eher strukturiert abläuft, als in den anderen beiden Regionen, die immer noch nachhinkend versuchen IT- und Geschäftsstrategie aufeinander abzustimmen.»*[267]

3.3.2 PWC & ITGI: An Executive View of IT Governance

Im Rahmen dieser Studie wurde erhoben, für wie wichtig Vorstandsmitglieder und Manager eine funktionierende IT erachten, inwiefern diese zur Erreichung der Unternehmensziele beiträgt und ob das derzeit noch nicht vollständig ausgeschöpfte IT-Potenzial vollwertig in Unternehmenswerte übergehen kann.[268]

[265] vgl. [Deloitte2009b, S. 25]
[266] vgl. [Deloitte2009b, S. 25]
[267] vgl. [Deloitte2009b, S. 26]
[268] vgl. [PricewaterhouseCoopers2009, S. 6]

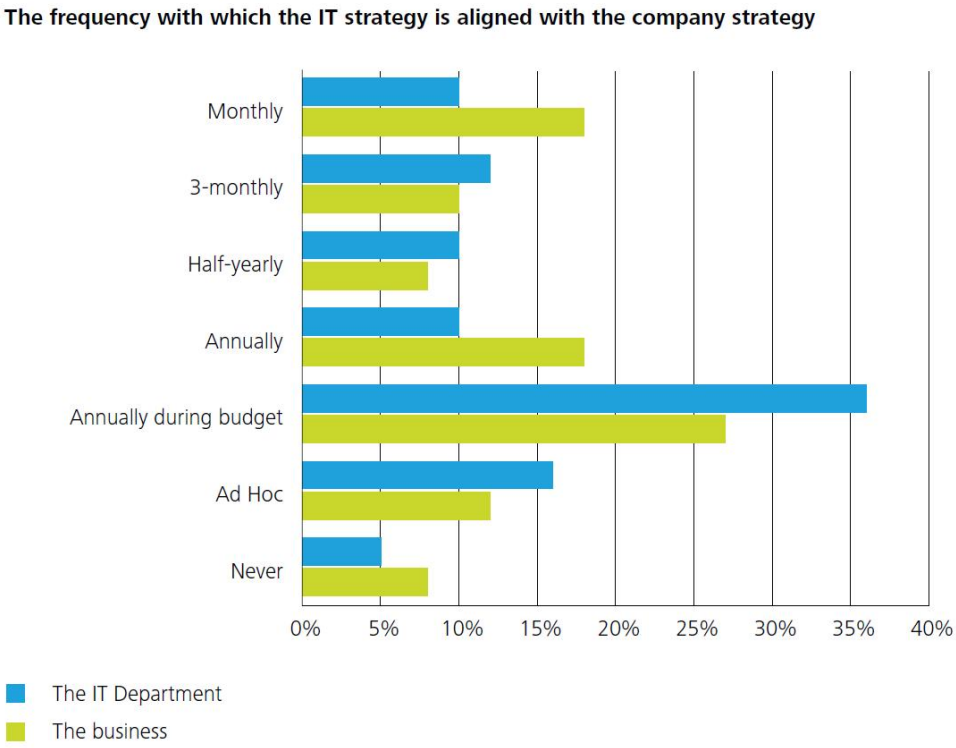

Abbildung 3.7: Abstimmung zwischen IT- und Unternehmensstrategie

Das Consultingunternehmen *PricewaterhouseCoopers Belgien/International* (PwC) und das *IT Governance Institute* (ITGI) führten dazu zwischen Mai und August 2008 mehr als 250 Interviews in 22 Ländern durch. Befragt wurden Vorstände und Geschäftsführer ohne IT-Hintergrund bzw. IT-Verantwortung aus großen und kleinen Betrieben unterschiedlicher Branchen.[269]

Hauptthemen der Studie

PWC/ITGI definierten Fragen, welche die vier Hauptthemen

- Wichtigkeit der IT,
- IT Performance,
- IT Verantwortlichkeit und
- Effektivität von IT-Governance

abdecken sollen (vgl. Tabelle 3.5[270]).

[269] vgl. [PricewaterhouseCoopers2009, S. 6]
[270] vgl. [PricewaterhouseCoopers2009, S. 8]

Thema	Fragestellungen
Wichtigkeit der IT	Wie wichtig ist IT für Ihre Unternehmung, und warum? Welchen Beitrag zur Unternehmung erwarten Sie sich von der IT?
IT Performance	Wie zufrieden sind Sie mit dem aktuellen Beitrag der IT zu Ihrer Unternehmung?
IT Verantwortlichkeit	Welche Rolle spielen die unterschiedlichen Beteiligten (Stakeholder) - geschäftlich und IT-mäßig - bei der Leitung der Informationstechnologie? Wo positioniert der CEO die IT Führung (oder die Führung der Informationstechnologie)? Sind die Verantwortlichkeiten wirklich definiert und akzeptabel?
Effektivität von IT-Governance	Sind die Bestrebungen der IT Governance integriert mit den unternehmensweiten Governance Regelungen Ihres Unternehmens? Wie effektiv sind IT Governance Regelungen innerhalb Ihres Unternehmens?

Tabelle 3.5: Hauptthemen der PWC/ITGI-Studie

Wichtigkeit der IT

Mehr als die Hälfte der befragten Vorstände ist der Meinung, dass die IT einen wesentlichen Beitrag zur Erreichung der Unternehmens- bzw. Geschäftsstrategie leistet. Weitere 36% befinden die IT in «irgendeiner Art und Weise» für wichtig zur Etablierung der Geschäftsziele (vgl. Abbildung 3.8[271]). Im Detail wurden die IT-Beiträge zu Innovation, Effizienz bzw. Effektivität hinterfragt, wobei die Innovationsleistung der IT am niedrigsten - mit nur 59% beziffert wurde.[272]

Abbildung 3.9[273] zeigt jedoch, dass der Informationsfluss in Bezug auf neue Technologien und Möglichkeiten durch Innovationsansätze zwischen der IT und den Fachbereichen nur sehr rudimentär vorhanden ist. Lediglich ein Drittel der IT-Abteilungen informieren die Fachbereiche regelmäßig über Neuerungen ihres Sektors oder alternative Geschäftsmöglichkeiten. Die beiden anderen Drittel verteilen sich etwa gleichmäßig auf mittelmäßig und vollständig informierte Unternehmensressorts.[274]

[271] vgl. [PricewaterhouseCoopers2009, S. 10]
[272] vgl. [PricewaterhouseCoopers2009, S. 10-11]
[273] vgl. [PricewaterhouseCoopers2009, S. 11]
[274] vgl. [PricewaterhouseCoopers2009, S. 11]

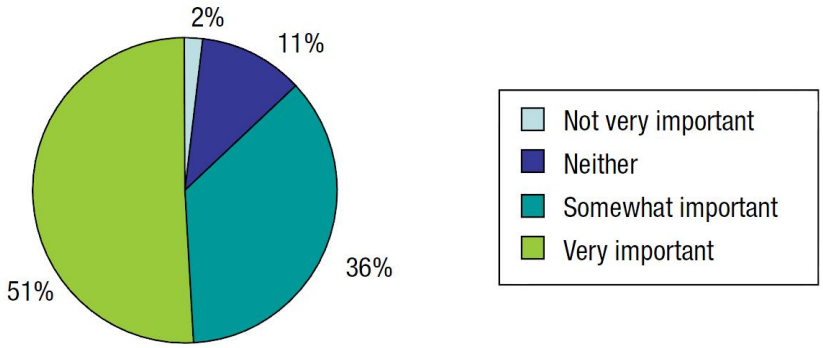

Abbildung 3.8: Beitrag der IT zum Unternehmenserfolg

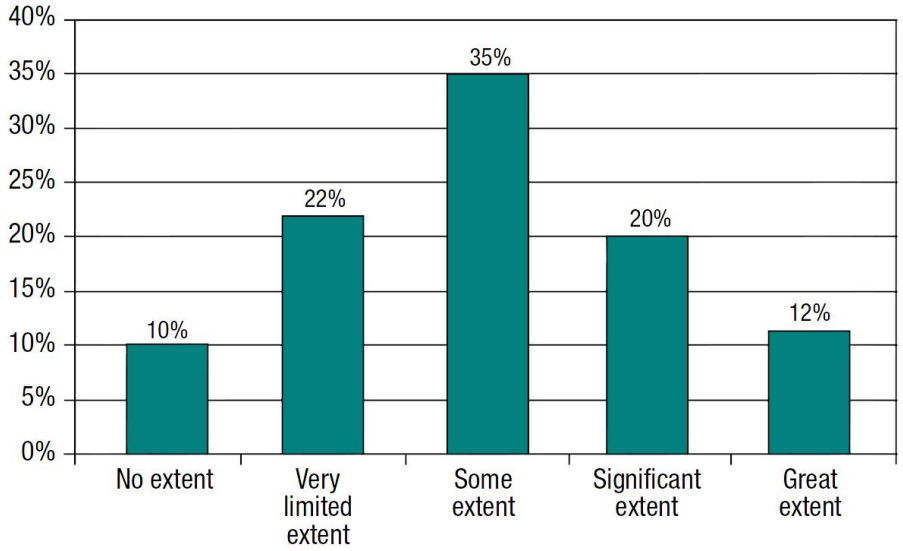

Abbildung 3.9: Informationsfrequenz zwischen IT und Fachbereich

IT Performance

Die Aussage, dass Investitionen in Informationstechnolgie einen Mehrwert für das gesamte Unternehmen bringt, wurde von über 75% der Befragten bestätigt. Erschreckend ist jedoch, dass 22% keine Informationen über die Leistungen und den Input ihrer IT-Abteilungen haben und daher keine konkrete Aussage treffen konnten. (vgl. Abbildung 3.10[275]) Nur die Hälfte der Unternehmungen (56%) messen ihre IT-Ziele, weitgehend jedoch nur mittels Einnahmen-/Ausgabenrechnung.[276]

Obwohl ein hoher Prozentsatz des Managements den Wertbeitrag der IT wahrnimmt und auch schätzt, scheint es nicht in der Lage zu sein, die vorhandenen Barrieren zu beseitigen

[275] vgl. [PricewaterhouseCoopers2009, S. 12]
[276] vgl. [PricewaterhouseCoopers2009, S. 12]

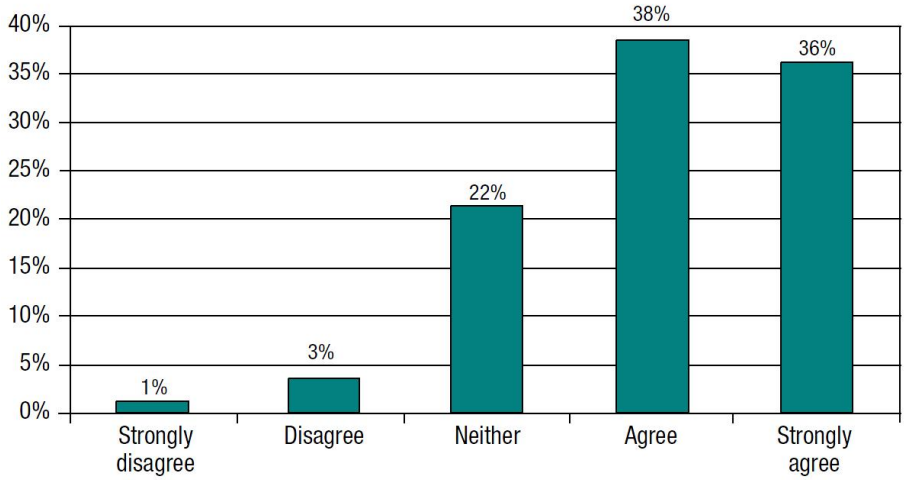

Abbildung 3.10: Wertbeitrag der IT-Investitionen

Barriere	**Prozentwert**
Schwierigkeiten bei der Implementierung von Applikationen	37%
Organisationskultur	20%
Zu geringe Fähigkeiten	16%
Angst vor Veränderungen	7%
Zu wenig Zeit	7%
Ungenügende Ausbildung/Trainings	5%
Andere	4%
Unbekannte Barrieren	18%
Keine Angabe	1%

Tabelle 3.6: Barrieren bei IT-Investitionen

(vgl. Tabelle 3.6[277]). Gerade das Management hat die Aufgabe Zeit für Ausbildung und Trainings der Mitarbeiterinnen und Mitarbeiter bereitzustellen sowie eine IT-orientierte Unternehmenskultur zu etablieren. Die Vorbildfunktion des Managements sollte in diesem Bereich intensiviert werden.[278]

IT Verantwortlichkeiten

Das dritte Kernthema geht der Frage nach, wer im Unternehmen für IT-Governance verantwortlich ist und wo die sogenannten «Key Champions for IT-Governance» sitzen. IT-Governance wird mit über 70% als Vorstandsaufgabe gesehen (vgl. Abbildung 3.11[279]). Die wirklichen Spezialisten sitzen jedoch nur zu 55% in den Vorstandsebenen - die verbleibenden 45% des IT-Governance-Know-Hows kommen aus dem mittleren Management.

[277] vgl. [PricewaterhouseCoopers2009, S. 13]
[278] vgl. [PricewaterhouseCoopers2009, S. 13]
[279] vgl. [PricewaterhouseCoopers2009, S. 15]

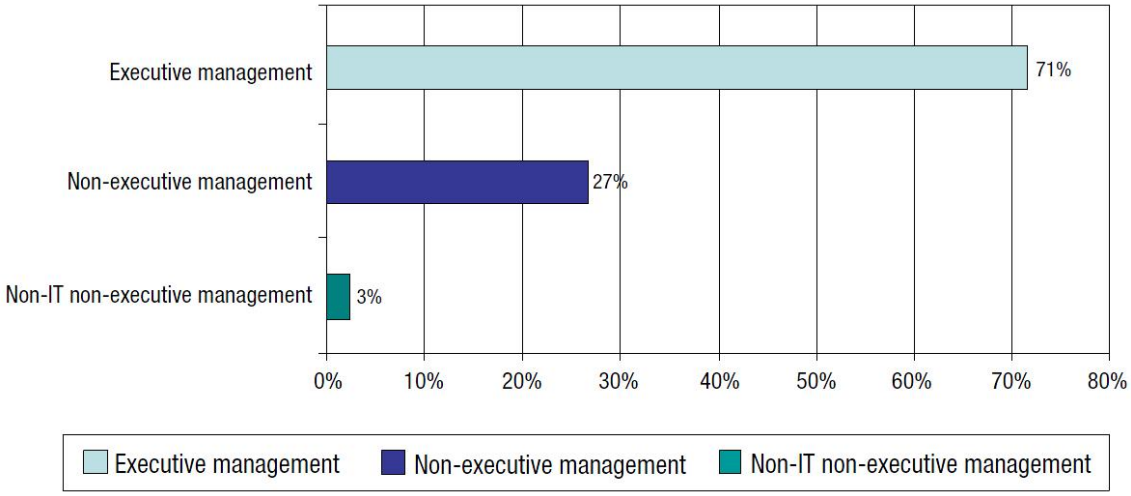

Abbildung 3.11: Verantwortlichkeiten für IT-Governance

Interessant zeigt sich auch die Integration des CIOs in das Management Board. In 58% der Unternehmen ist der CIO vollwertiges Mitglied des Vorstandes im Gegensatz zu 27% ohne CIO-Positionierung im Top-Management. 13% der Teilnehmer haben keinen CIO.[280]

In knapp der Hälfte aller Unternehmen wird der CIO dem Finanzbereich unterstellt und berichtet somit dem CFO. Nur in 23% der Unternehmen wird das gesamte Board über Statements und Entscheidungen des CIOs informiert und 12% berichten direkt dem Vorstandsvorsitzenden (CEO).[281]

Effektivität von IT-Governance

Der umfangreichste, vierte Teil der Studie beschäftigt sich mit der Effektivität von IT-Governance im Unternehmen sowie der Diskussion und Handhabung von IT-Themen auf Vorstandsebene. Besonders hervorzuheben sind die Ergebnisse zweier Fragen:

- Wie oft befinden sich IT-Themen auf der Tagesordnung von Vorstandssitzungen und welchen Fokus haben Vorstandsdiskussionen über IT? (vgl. Abbildung 3.12[282])
- Versucht Ihr Unternehmen Geschäfts- und IT-Strategie aneinander auszurichten und wenn ja, wie? (vgl. Abbildung 3.13[283])

Nur etwa 5% der Vorstände behandeln keinerlei IT-Themen in ihren Sitzungen. 95% besprechen technische Angelegenheiten, jedoch nur 37% tun dies wirklich regelmäßig. Die

[280] vgl. [PricewaterhouseCoopers2009, S. 17]
[281] vgl. [PricewaterhouseCoopers2009, S. 17]
[282] vgl. [PricewaterhouseCoopers2009, S. 20]
[283] vgl. [PricewaterhouseCoopers2009, S. 21]

restlichen CEOs behandeln IT-Thematiken im Rahmen von Ad-Hoc-Anfragen, also sobald eine Diskussion zu einem ganz konkreten Fall notwendig wird.[284]

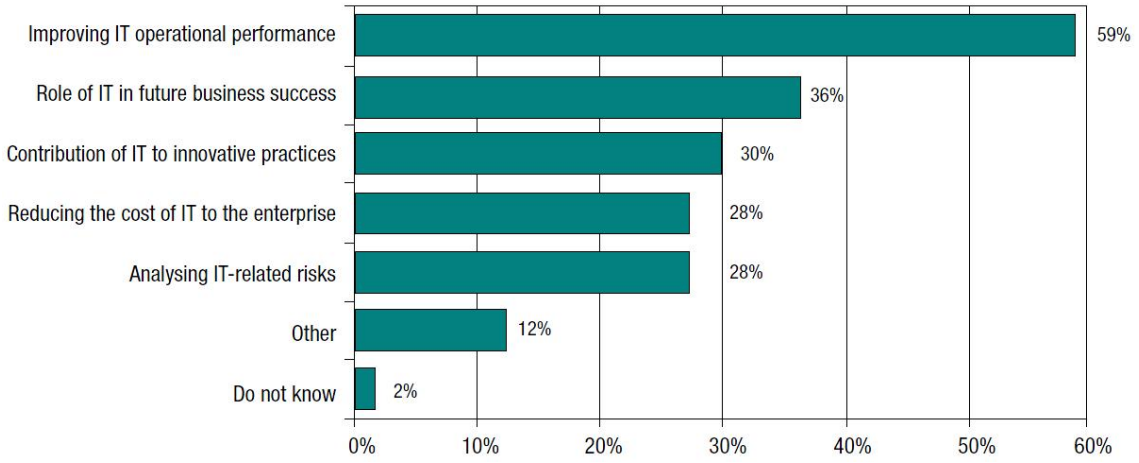

Abbildung 3.12: IT-Themen in Vorstandssitzungen

Abbildung 3.12 zeigt konkrete IT-Themenbereiche, die auf Vorstandsebene diskutiert werden. Klarer Spitzenreiter sind Gespräche über die Verbesserung der operativen IT-Performance gefolgt von der zukunftsorientierten Ausrichtung der Informationstechnologie sowie dem Innovationsbeitrag der IT.[285]

Die Ausrichtung der IT-Strategie auf die unternehmensweite Geschäftsstrategie orientiert sich an den Zahlen der Verantwortlichkeiten für IT-Governance-Themen. Fast 75% der Unternehmen stimmen ihre IT-Strategie regelmäßig mit der Unternehmensstrategie ab und lediglich 25% unterlassen derartige Maßnahmen.[286]

Die Methoden der Ausrichtung zwischen IT- und Unternehmensstrategie sind in Abbildung 3.13[287] dargestellt. Etwa die Hälfte der Befragten treffen IT-Entscheidungen gemeinsam mit der Geschäftsführung (52%) oder berufen regelmäßige IT-Management-Meetings ein (43%).

Obwohl für viele IT-Dienstleistungen im Umfeld der IT-Governance externe Berater hinzugezogen werden (55%), erfolgt die Abstimmung zwischen IT- und Geschäftsstrategie meist intern. Lediglich 25% der Unternehmen beanspruchen dabei regelmäßige Leistungen von externen Review- und Consultinganbietern.[288]

[284] vgl. [PricewaterhouseCoopers2009, S. 19]
[285] vgl. [PricewaterhouseCoopers2009, S. 19-20]
[286] vgl. [PricewaterhouseCoopers2009, S. 20]
[287] vgl. [PricewaterhouseCoopers2009, S. 21]
[288] vgl. [PricewaterhouseCoopers2009, S. 21]

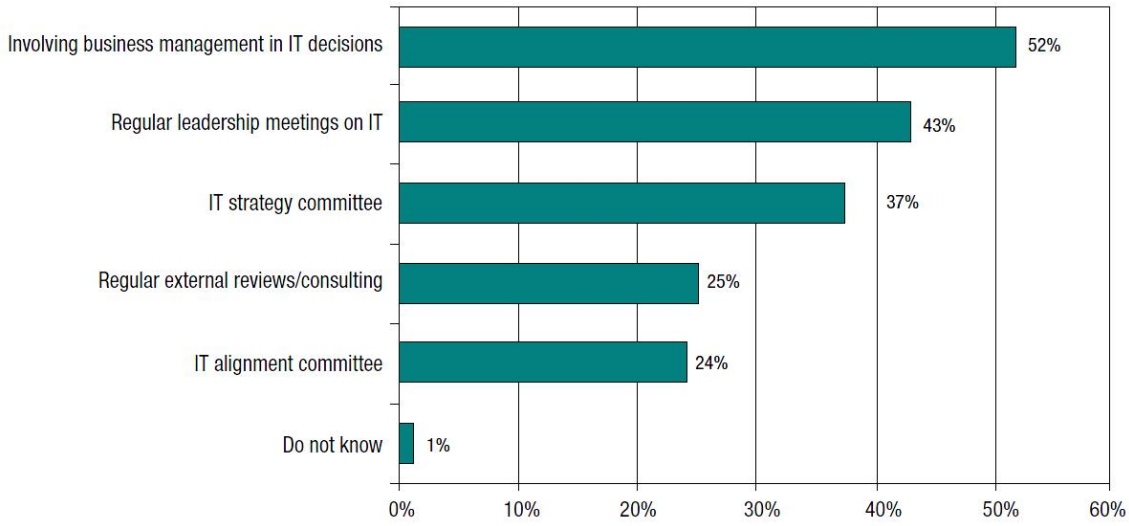

Abbildung 3.13: Ausrichtung von Unternehmens- und IT-Strategie

Die beiden letzten Analyseergebnisse stehen inhaltlich in einem direkten Zusammenhang mit den Ergebnissen der in Abschnitt 3.3.1 besprochenen Deloitte-Umfrage. Beide Consulting-Unternehmen zeigen, dass sich Vorstandssitzungen zwar mit IT-Themen beschäftigen, dies aber nicht regelmäßig sondern nur in konkreten Anwendungsszenarien oder im Zuge des Jahresabschlusses tun.

3.3.3 Kernaussagen der Studien

Beide Analysen wurden weltweit durchgeführt und haben gezeigt, dass die IT zwar immer weiter in die Vorstandsebene vordringt und der Beitrag zur unternehmensweiten Entwicklung gesehen wird, die Umsetzung entsprechender Maßnahmen sowie die Verantwortungsdelegation aber noch auszuschöpfendes Potenzial aufweist.

Deloitte hat daher fünf Highlights ihrer Umfrage herausgearbeitet und sieht Vorstände, CIOs und Organisationen vor allem fünf Aufgabenstellungen gegenüber. Diese reichen von der Entwicklung der IT-Governance und des IT-Managements bis zum sinnvollen IT-Outsourcing (vgl. Tabelle 3.7[289]).

[289] vgl. [Deloitte2009b, S. 5-6]

Thematik	**Problematik & Aufgabe**
Entwicklung & Trends	Von der IT wird nicht nur Automatisierung und Effizienz, sondern auch ein Beitrag zum Unternehmenswert erwartet.
IT-Governance	Die IT hat noch nicht vollen «Management-Fokus» und kann daher nur teilweise korrekt ausgerichtet werden.
IT-Management	Die IT ist noch keine treibende Kraft, obwohl sie es zwecks Entscheidungsunterstützung sein sollte.
IT-(Out)Sourcing	Outsourcing von IT-Bereichen ist zwar immer noch eine Möglichkeit, aber am heutigen Markt kritisch zu betrachten.
IT-Sicherheit	Die Bereiche IT-Sicherheit, Privatsphäre und Betrugsvorbeugung werden noch nicht mit dem notwendigen Bewusstsein wahrgenommen.

Tabelle 3.7: Highlights der Deloitte-Studie

Auch PricewaterhouseCoopers (PWC) und das IT Governance Institute (ITGI) sehen Handlungsbedarf durch derzeitige und zukünftige Top-Manager und präsentieren vergleichbare Verbesserungsansätze[290]:

- Take ownership of IT governance and assume overall accountability over IT.
- Make the CIO reporting line as direct as possible to the top executive decision body.
- Pay more attention to the potential for innovation IT can offer.
- Start measuring the value IT brings (or does not bring) to the enterprise.
- Use external advisors as the most effective source of knowledge and guidance in relation to IT governance.

[290] vgl. [PricewaterhouseCoopers2009, S. 6]

4 Zusammenfassung & Ausblick

4.1 Zusammenfassung

In den letzten Jahren konnte eine rasante Entwicklung der Informationstechnologie sowie ein Wandel der Zivilisation zu einer Informations- und Wissensgesellschaft beobachtet werden. Einfache EDV-Systeme zur Datenverarbeitung wurden durch komplexe, heterogene IT-Infrastrukturen ersetzt, die eine weltweite Vernetzung multikultureller Konzerne und den Einsatz mobiler Kommunikation ermöglichen.

Gleichzeitig schaffte diese Modernisierung intensive IT-Abhängigkeiten vieler Branchen, die in weiterer Folge zur Restrukturierung von Organisationen, Wirtschafts- und Rechtssystemen führte. Die anfänglich eigenständige IT integrierte sich mehr und mehr in Geschäftsprozesse und ist heute aus keinem Unternehmensressort mehr wegzudenken.

Es ist daher Aufgabe der *IT-Governance* den wirtschaftlichen, risikobewussten und gezielten Einsatz von Informationstechnologie im gesamten Unternehmen und nach außen sicherzustellen sowie eine durchgängige IT-Strategie - beginnend beim Top-Management und endend bei der IT-Produktion bzw. dem IT-Betrieb - aufzubauen, zu administrieren und anzupassen.

Die *IT-Compliance* liefert das dazu notwendige Rahmenwerk in Form von internationalen Empfehlungen und Best Practices (Fachgutachten, Governance Kodizes) aber auch gesetzlichen Regulativen (EU-Richtlinien, Basel II), die es in nationales Recht umzusetzen gilt. Basis dieser Rahmenbedingungen stellt u.a. das amerikanische Bundesgesetz *Sarbanes-Oxley Act* dar, welches um die Jahrtausendwende zur Verhinderung milliardenschwerer Finanzskandale veröffentlicht wurde.

Um die auf internationaler Ebene sehr vielseitigen Rechts- und Wirtschaftssysteme zu unterstützen, machten es sich internationale Organisationen wie etwa die OECD, die ISACA oder das ITGI zur Aufgabe einheitliche Rahmenwerke und Standards zur Umsetzung der komplexen Anforderungen aus IT-Governance und IT-Compliance zu entwickeln. Neben ITIL stellt auch COBIT einen solchen Werkzeugkasten bereit und kann durch individuelle Erweiterungen (Risk IT, Val IT) auf die Anwendungsdomäne spezialisiert werden.

Sowohl die rechtlichen Rahmenbedingungen als auch die unterstützenden Frameworks setzen die Aufmerksamkeit des Top-Managements voraus. Die Rolle des CIOs soll den Aufbau einer strukturierten Compliance-Organisation überwachen und unternehmensweite IT- und Prozessoptimierungen initiieren. Erst durch entsprechende Maßnahmen auf oberster Ebene können IT- und Unternehmensstrategie aneinander ausgerichtet und der wertvolle Beitrag der IT zum Geschäftserfolg vollständig realisiert werden.

4.2 Ausblick

Aktuelle Studien von Deloitte, PricewaterhouseCoopers und dem ITGI zeigen jedoch, dass IT-Themen zwar intensiveren Einzug in Management-Diskussionen und Vorstandssitzungen finden, aber immer noch unvollständig, unstrukturiert oder unregelmäßig zur Sprache kommen. Es obliegt daher dem heutigen und zukünftigen IT- bzw. Prozessmanagement diese Rückstände zu erkennen und durch geeignete Maßnahmen vorhandene Verbesserungspotenziale auszuschöpfen.

Die Informationstechnolgie darf zukünftig nicht mehr als reine «Automatisierungsabteilung» verstanden werden, sondern soll durch den Erhalt der notwendigen *Management Attention* einen zusätzlichen Mehrwert für das Unternehmen erzielen. Die IT als treibende Kraft von Innovation, Effektivität und Effizienz in Verbindung mit Optimierung, Entscheidungsunterstützung und Risikoreduktion über Unternehmensgrenzen hinweg stellen die anzustrebenden Ziele der nächsten *IT-Management-Generation* dar.

Unternehmen werden auch zukünftig permanenten Konjunkturschwankungen, rasanten Technologiefortschritten und einem stetig wachsenden, rechtlichen Rahmenwerk ausgesetzt sein. Die bestehenden Modelle liefern einen guten Ausgangspunkt zur weiterführenden Implementierung von IT-Governance- und IT-Compliance-Strukturen. Ganzheitliche Optimierungsansätze, transparente Methoden und vor allem ein umfangreiches Verständnis der Notwendigkeit einer IT-Restrukturierung werden die zukünftigen Entwicklungen in der Informationstechnologie nachhaltig beeinflussen.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[Amann2008] Amann, Susanne: *Corporate Governance - Deutschland lügt sich etwas vor.* Online-Artikel, http://www.spiegel.de/wirtschaft/0,1518,566178,00.html, zuletzt abgerufen am 30.01.2010, Juli 2008.

[Armin2008] Armin, Prof. Dr.: *Interview mit Michael Klinger und Christian Cuske zum Thema «IT-Governance und Compliance».* Wirtschaftsinformatik, Seiten 413–417, Oktober 2008.

[Beyond2007a] Beyond Consulting GmbH: *Eurosox - Entstehung & Geschichte.* Online-Artikel, http://www.eurosox.at/index_new.php?menuid=9, zuletzt abgerufen am 30.01.2010, Februar 2007.

[Beyond2007b] Beyond Consulting GmbH: *Richtlinien.* Online-Artikel, http://www.eurosox.at/index_print.php?lang=de&mid=2&cid=1&directURI=, zuletzt abgerufen am 30.01.2010, Februar 2007.

[Beyond2007c] Beyond Consulting GmbH: *Umsetzung in Österreich.* Online-Artikel, http://www.eurosox.at/index_new.php?menuid=10, zuletzt abgerufen am 30.01.2010, Februar 2007.

[Beyond2007d] Beyond Consulting GmbH: *Wer sind die Adressaten?* Online-Artikel, http://www.eurosox.at/index_new.php?menuid=11, zuletzt abgerufen am 30.01.2010, Februar 2007.

[BMF2009] Bundesministerium für Finanzen (BMF): *Corporate Governance Kodex für 2010 beschlossen.* http://www.ots.at/presseaussendung/OTS_20091218_OTS0098, zuletzt abgerufen am 30.01.2010, Dezember 2009.

[Cadbury1992] Cadbury, Adrian: *The Financial Aspects of Corporate Governance.* The Committee on the Financial Aspects of Corporate Governance and Gee and Co. Ltd., Dezember 1992.

[Carlin2007] Carlin, Anna und Frederick Gallegos: *IT Audit: A Critical Business Process.* Computer, Seiten 87–89, Juli 2007.

[Cloer2002] Cloer, Thomas: *Worldcom-Skandal: Die Hintergründe, die Folgen.* Online-Artikel, http://www.computerwoche.de/nachrichtenarchiv/531070/, zuletzt abgerufen am 30.01.2010, Juni 2002.

[Deloitte2009a] Deloitte Touche Tohmatsu: *IT Business Balance Survey 2009 - Studie zur IT-Nutzung im Unternehmen.* Online-Artikel, http://www.deloitte.com/view/de_DE/de/dienstleistungen/wirtschaftspruefung/enterprise-risk-services/security-privacy/article/bf81bf29bfff0210VgnVCM100000ba42f00aRCRD.htm, zuletzt abgerufen am 30.01.2010, März 2009.

[Deloitte2009b] Deloitte Touche Tohmatsu (Chris Verdonck & Christian Combes): *Deloitte 2009 Survey on IT-business balance - Shaping the relationship between business and IT for the future.* IT Business Balance Survey, Dezember 2009.

[Fröhlich2007] Fröhlich, Martin und Kurt Glasner: *IT Governance.* Gabler, GWV Fachverlage GmbH, Wiesbaden, 1. Auflage, April 2007.

[FMA2010a] FMA - Österreichische Finanzmarktaufsicht: *Die Architektur von Basel II - Das 3 Säulen-Modell.* Online-Portal, http://www.fma.gv.at/cms/basel2/DE/einzel.html?channel=CH0272, zuletzt abgerufen am 30.01.2010, Jänner 2010.

[FMA2010b] FMA - Österreichische Finanzmarktaufsicht: *Grundlagen Basel II.* Online-Portal, http://www.fma.gv.at/cms/basel2/DE/einzel.html?channel=CH0258, zuletzt abgerufen am 30.01.2010, Jänner 2010.

[Glenfis2010a] Glenfis AG: *Continual Service Improvement.* Online-Artikel, http://www.itil.org/de/vomkennen/itil/serviceimprovement/index.php, zuletzt abgerufen am 30.01.2010, Jänner 2010.

[Glenfis2010b] Glenfis AG: *Service Design.* Online-Artikel, http://www.itil.org/de/vomkennen/itil/servicedesign/index.php, zuletzt abgerufen am 30.01.2010, Jänner 2010.

[Glenfis2010c] Glenfis AG: *Service Operation.* Online-Artikel, http://www.itil.org/de/vomkennen/itil/serviceoperation/index.php, zuletzt abgerufen am 30.01.2010, Jänner 2010.

[Glenfis2010d] Glenfis AG: *Service Strategy.* Online-Artikel, http://www.itil.org/de/vomkennen/itil/servicestrategy/index.php, zuletzt abgerufen am 30.01.2010, Jänner 2010.

[Glenfis2010e] Glenfis AG: *Service Transition.* Online-Artikel, http://www.itil.org/de/vomkennen/itil/servicetransition/index.php, zuletzt abgerufen am 30.01.2010, Jänner 2010.

[Glenfis2010f] Glenfis AG: *Was ist ITIL?* Online-Artikel, http://www.itil.org/de/vomkennen/itil/ueberblick/index.php, zuletzt abgerufen am 30.01.2010, Jänner 2010.

[Grünendahl2009] Grünendahl, Ralf-T., Andreas F. Steinbacher und Peter H.L. Will: *Das IT-Gesetz: Compliance in der IT-Sicherheit.* Vieweg+Teubner, GWV Fachverlage GmbH, Wiesbaden, 1 Auflage, 2009.

[Hausegger2007] Hausegger, Hannes: *Auswirkungen von Compliance Änderungen auf IT Governance im Hinblick auf das interne Kontrollsystem.* Masterarbeit, Technische Universität Wien, November 2007.

[Hillenbrand2002] Hillenbrand, Thomas: *Das führende Unternehmen der Welt.* Online-Artikel, http://www.spiegel.de/wirtschaft/0,1518,176509,00.html, zuletzt abgerufen am 30.01.2010, Jänner 2002.

[Hilb2005] Hilb, Martin: *New Corporate Governance - Successful Board Management Tools.* Springer-Verlag Berlin Heidelberg New York, 2005.

[ISACA2009a] Information Systems Audit And Control Association (ISACA): *COBIT 4.1 - The Newest Evolution Of Control Objectives For Information And Related Technology, The World's Leading IT Control And Governance Framework.* Broschüre, http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/CobiT4.1_Brochure.pdf, zuletzt abgerufen am 30.01.2010, 2009.

[ISACA2009b] Information Systems Audit And Control Association (ISACA): *COBIT Overview.* Präsentation, http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=54922, zuletzt abgerufen am 30.01.2010, 2009.

[ISACA2009c] Information Systems Audit And Control Association (ISACA): *Risk IT based on COBIT.* Broschüre, http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=52519, zuletzt abgerufen am 30.01.2010, 2009.

[ISACA2009d] Information Systems Audit And Control Association (ISACA): *Risk IT Overview.* Präsentation, http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=54918, zuletzt abgerufen am 30.01.2010, 2009.

[ISACA2009e] Information Systems Audit And Control Association (ISACA): *Val IT 2.0 based on COBIT.* Broschüre, http://www.isaca.org/

ContentManagement/ContentDisplay.cfm?ContentID=44532, zuletzt abgerufen am 30.01.2010, 2009.

[ItServiceManagementForum2010] IT Service Management Forum: *Alfred Olbrich - wibas IT Maturity Services GmbH.* Kurzbeschreibung CV, http://www.itsmf.de/154.html, zuletzt abgerufen am 30.01.2010, Jänner 2010.

[KammerWTH2004] Kammer der Wirtschaftstreuhänder: *Fachgutachten der Fachsenate für Datenverarbeitung und für Handelsrecht und Revision des Instituts für Betriebswirtschaftslehre, Steuerrecht und Organisation der Kammer der Wirtschaftstreuhänder über Abschlussprüfung bei Einsatz von Informationstechnik.* Fachgutachten, Juni/Oktober 2004.

[Katzenberger2009] Katzenberger, Wolfgang E.: *Vorlesung «Systemplanung und Projektmanagement».* Vorlesungsbesuch, Mitschriften, Skriptum (Ausgabe September 2009), Wintersemester 2009/10.

[Kuhlin2004] Kuhlin, Bernd und Heinz Thielmann: *Real-Time Enterprise in der Praxis - Fakten und Ausblick.* Springer-Verlag Berlin Heidelberg New York, 1. Auflage, Oktober 2004.

[Kuri2002] Kuri, Jürgen: *US-Telecomriese WorldCom meldet Konkurs an.* Online-Artikel, http://www.heise.de/newsticker/meldung/US-Telecomriese-WorldCom-meldet-Konkurs-an-64882.html, zuletzt abgerufen am 30.01.2010, Juli 2002.

[Lensdorf2006] Lensdorf, Lars und Udo Steger: *IT-Compliance im Unternehmen.* Foliensatz, http://www.dsri.de/downloads/ha2006/19-Lensdorf-Steger.pdf, zuletzt abgerufen am 30.01.2010, September 2006.

[Menzies2006] Menzies, Christof: *Sarbanes-Oxley und Corporate Compliance - Nachhaltigkeit, Optimierung, Integration.* Schäffer-Poeschl Verlag für Wirtschaft, Steuern, Recht GmbH, 1. Auflage, September 2006.

[Meyer2009] Meyer, Marco, Rüdiger Loitz, Jerome-Oliver Quella und Peter Zerwas: *Latente Steuern - Bewertung, Bilanzierung, Beratung.* Gabler, GWV Fachverlage GmbH, Wiesbaden, 2. Auflage, Februar 2009.

[Müller2008] Müller, Günter und Orestis Terzidis: *IT-Compliance und IT-Governance.* Wirtschaftsinformatik, Seiten 341–342, Mai 2008.

[OECD2004] OECD - Organisation for Economic Co-operation and Development: *OECD-Grundsätze der Corporate Governance.* http://www.oecd.org/dataoecd/57/19/32159487.pdf, zuletzt abgerufen am 30.01.2010, 2004.

[Olbrich2008] Olbrich, Alfred: *ITIL kompakt und verständlich - Effizientes IT Service Management - Den Standard für IT-Prozesse kennenlernen, verstehen und erfolgreich in der Praxis umsetzen.* Vieweg+Teubner, GWV Fachverlage GmbH, Wiesbaden, 4. Auflage, Februar 2008.

[Pfister2006] Pfister, Thomas: *Unternehmensweites Risikomanagement (COSO).* Abbildung des COSO-Würfels, `http://www.revision24.de/index.php?option=com_content&task=view&id=52&Itemid=22`, zuletzt abgerufen am 30.01.2010, Jänner 2010.

[Pollirer2008] Pollirer, Hans-Jürgen: *TrendTalk IT und Recht 2 - Datenschutz als integraler Bestandteil der IT-Compliance.* Foliensatz, `http://www.isaca.at/Ressourcen/TrendTalk_IT&Recht%2008052008.pdf`, zuletzt abgerufen am 30.01.2010, Mai 2008.

[Popp2007] Popp, Thomas: *IT-Governance-Modelle.* Masterarbeit, Technische Universität Wien, Oktober 2007.

[PricewaterhouseCoopers2009] PricewaterhouseCoopers & IT Governance Institute: *An Executive View of IT Governance.* ITGI Surveys, 2009.

[SoZ2002] SoZ - Sozialistische Zeitung: *Der Fall Enron - Die Normalität eines Global Player.* Online-Artikel, `http://www.vsp-vernetzt.de/soz/020813.htm`, zuletzt abgerufen am 30.01.2010, August 2002.

[ÖACG2009a] Österreichischer Arbeitskreis für Corporate Governance (Richard Schenz): *Österreichischer Corporate Governance Kodex.* Österreichischer Arbeitskreis für Corporate Governance, Jänner 2009.

[ÖACG2009b] Österreichischer Arbeitskreis für Corporate Governance (Richard Schenz): *Österreichischer Corporate Governance Kodex - Kodex-Revision 2010.* Österreichischer Arbeitskreis für Corporate Governance, November 2009.

[Teubner2008] Teubner, Alexander und Tom Feller: *Informationstechnologie, Governance und Compliance.* Wirtschaftsinformatik, Seiten 400–407, Oktober 2008.

[Webb2006] Webb, Phyl, Carol Pollard und Gail Ridley: *Attempting to Define IT Governance: Wisdom or Folly?* Proceedings of the 39th Hawaii International Conference on System Sciences, Jänner 2006.

[Wecker2009] Wecker, Gregor und Hendrik van Laak: *Compliance in der Unternehmerpraxis.* Gabler, GWV Fachverlage GmbH, Wiesbaden, 2. Auflage, Juni 2009.