Achtung,
diese Diplomarbeit ist vollkommen überarbeitet und ergänzt als Buch herausgegeben. Sie können dieses Buch

hier bei Amazon

beziehen.

Das Buch enthält natürlich auch die Tabelle mit einer Zuordnung von Anforderungen der unterschiedlichen Standards zu CobiT.

Sie erhalten folglich das aktuellste und umfassendste CobiT Mapping.

lg Jimmy Heschl

IT Governance

Diplomarbeit
(leicht modifiziert)

zur Erlangung des akademischen Grades eines Magisters
der Sozial- und Wirtschaftswissenschaften

eingereicht beim
WIN - Institut für Wirtschaftsinformatik
Schwerpunkt Information Engineering

Betreuer: o. Univ.-Prof. Dipl.-Ing. Dr. L. J. Heinrich

von cand. Mag. rer. soc. oec. Jimmy Heschl

Matrikelnummer: 9255956

Studienadresse: Pramergasse 29/8, 1090 Wien

Heimatadresse: Pramergasse 29/8, 1090 Wien

E-mail Adresse: jimmy@heschl.at

Wien, 13. August 2002

I Eidesstattliche Erklärung

Ich erkläre an Eides Statt, dass ich die Diplomarbeit mit dem Titel „IT Governance“ selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und alle den benutzten Quellen wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Wien, 25. Oktober 2005 Jimmy Heschl

II Danksagung

Entgegen den Vorschriften des WIN - Institut für Wirtschaftsinformatik, Schwerpunkt Information Engineering möchte ich an dieser Stelle meinen herzlichen Dank an meine Eltern, Geschwister, Freundinnen, Freunden und Kollegen (wobei sämtliche genannte Personengruppen Doppelfunktionen einnehmen) aussprechen, die mir nicht nur die Zeit während des Studiums unheimlich erleichterten, sondern mich auch nach meinem eigentlichen Studium noch mit sanften Druck dazu gebracht haben, diese vorliegende Arbeit abzuschließen. Ich hoffe, dass ich mit Euch noch viele weitere Stunden verbringen kann.

Danke für alles

Jimmy

III Inhaltsverzeichnis

IV Abbildungsverzeichnis

V Tabellenverzeichnis

VI Akronyme

AICPA	American Institute of Certified Public Accountants
AktG	Aktiengesetz
BAO	Bundesabgabenordnung
BKA	Bundeskanzleramt
BCM	Business Continuity Management
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik British Standards Institute
BWG	Bankwesengesetz
CCIMB	Common Criteria Interpretations Management Board
CICA	Canadian Institute of Chartered Accountants
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
CSF	Critical Success Factor
DSG	Datenschutzgesetz
ECV	„Verordnung der Bundes-Wertpapieraufsicht (BWA) über Grundsätze für die Informationsweitergabe im Unternehmen sowie betreffend organisatorische Maßnahmen zur Vermeidung von Insiderinformationsmissbrauch für Emittenten“ (Emittenten-Compliance-Verordnung – ECV)
ERP	Enterprise Resource Planning
EnSEC	Enterprise Security Management
FAMA	Fachausschuss für moderne Abrechnungssysteme beim Institut der Wirtschaftsprüfer Deutschland eV
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	GmbH-Gesetz
GoB	Grundsätze ordnungsmäßiger Buchführung
GoDS	Grundsätze ordnungsmäßigen Datenschutzes
GoDV	Grundsätze ordnungsmäßiger Datenverarbeitung
GoS	Grundsätze ordnungsmäßiger Speicherbuchführung
HGB	Handelsgesetzbuch
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
IFAC	International Federation of Accountants
IRÄG	Insolvenzrechtsänderungsgesetzes
ISA	International Standards on Auditing
ISACA	Information Systems Audit and Controls Association

ISACF	Information Systems Audit and Controls Foundation
ISO	International Organisation for Standardisation
IT	Informationstechnologie, auch Information and Related Technology
IWP	Institut österreichischer Wirtschaftsprüfer
KGI	Key Goal Indicator
KonTraG	Kontroll- und Transparenzgesetz
KPI	Key Performance Indicator
OECD	Organisation for Economic Cooperation and Development (UN-Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
ÖNORM	Österreichische Norm
ORM	Operational Risk Management
ÖVFA	Österreichische Vereinigung für Finanzanalyse und Asset Management
RIS	Rechtsinformationssystem
TOE	Target of Evaluation (Evaluierungsziel)
TÜV	Technischer Überwachungsverein
WTC	World Trade Center

Tabelle 1: Akronyme

1 Überblick

Die immer höher werdende Durchdringung von Organisationen durch Informationstechnologien bedingt, dass Organisationen im immer höheren Maß von deren Verfügbarkeit und deren Verlässlichkeit abhängig sind. Derzeit steht jedoch kein umfassendes Modell zur Verfügung, um den Prozess der Informationsverarbeitung derart zu modellieren, dass die Verfügbarkeit der aus diesem Prozess entstehenden Outputs und deren Verlässlichkeit kontrolliert und gesteuert ablaufen. Neben dieser geschäftsgetriebenen Forderung zeigt auch die nationale und internationale Gesetzgebung, dass die Kontrolle des IT Prozesses in Form eines internen Kontrollsystems abzubilden ist.

Ein oft gezogener Vergleich von der Kontrolle über die Ressource Kapital mit jener über die Ressource Information zeigt, dass auf Seite der Kapitalkontrolle neben Verantwortlichkeiten in den höchsten Führungsgremien der Organisationen auch anerkannte Bewertungsmodelle verfügbar sind, die Kontrolle der Informationsverarbeitung obliegt jedoch bei einer Vielzahl österreichischer Unternehmen den Managern der zweiten oder dritten Führungsebene. Umfangreiche und aussagekräftige Modelle und Kontrollen, die im IT Prozess zu integrieren sind, stehen nicht – oder nur auf Teilaufgaben beschränkt – zur Verfügung.

Aus der Kombination der immer größer werdenden Abhängigkeit mit der Nichtverfügbarkeit von Systemen zur Kontrolle ergibt sich die Forderung, ein Modell zur umfassenden Kontrolle des IT Prozesse zu entwerfen. Die vorliegende Arbeit zeigt einen Versuch, die derzeit verfügbaren Modelle in ein umfassendes Modell zu integrieren, damit bei einer Modellierung des IT Prozesses die derzeit verfügbaren Standards berücksichtigt werden können.

Ausgehend von der Darstellung der gesetzlichen Lage und der Forderung von Organisationen werden die wichtigsten Standards vorgestellt und auf ein Modell zugeordnet.

Das Ergebnis ist eine Liste von Kontrollen, die bei der Modellierung des IT Prozesses zu berücksichtigen sind. Durch diese Kontrollen – in Verbindung mit einem Ziel- und Messsystem – wird IT Governance, also die Steuerung des IT Prozesses, ermöglicht.

2 Grundlagen

In den 1990er Jahren hatte die Debatte um Corporate Governance ihren Ausgangspunkt, die das Auseinanderdriften der Interessen von Aktionären und Geschäftsführern zum Inhalt hatte. Der Gruppe der Aktionäre wurde unterstellt, dass sie das Unternehmen nicht selbst leiten können, andererseits jedoch stets in Gefahr seien, dass ihre Interessen, von den Geschäftsführern nicht verfolgt würden. Dies weckte den Bedarf nach angemessenen Kontrollsystemen in börsennotierenden Unternehmen zum Schutz der Interessen der Aktionäre.

In Anlehnung an die Internationalen Prüfungsgrundsätze [vgl. ISA01] wird in der gesamten Arbeit unter einem Kontrollsystem eine systematische Anordnung von Kontrollen verstanden, wobei an dieser Stelle keine Unterscheidung gemacht wird, ob die Kontrollen in ein (IT)-System eingebunden sind es ist vielmehr die Systematik der Kontrollen maßgeblich. Eine Kontrolle ist, wie von Heinrich [vgl. HEI98, S 310] beschrieben, ein Teil der betrieblichen Aufgabe Überwachung.

Unangemessene Standards im Bereich von Buchführung und Offenlegung haben im Jahr 2002 auch einen Teil zum Niedergang von Enron, einem der größten Konzerne in den USA, beigetragen [vgl. FIN02]. Offensichtlich und in der Presse kommentiert war hier allerdings auch, dass die Sorgfalts- und Überwachungspflichten von Vorständen, und Aufsichtsräten, aber auch von Abschlussprüfern und Überwachungsbehörden nicht in angemessenem Umfang wahrgenommen wurden [vgl. STA02-1]. Die Erkenntnisse aus diesem Fall werden national als auch international erhebliche Auswirkungen auf Gesetze und Standards, insbesondere für jene im Bereich der Corporate Governance, mit sich bringen.

Die Terroranschläge vom 11. September haben gravierende Auswirkungen für zahlreiche Unternehmen und Organisationen mit sich gebracht, die im World Trade Center in New York City angesiedelt waren. Es hat sich aber gezeigt, dass Unternehmen, die über ein angemessenes Risikomanagement und daraus abgeleiteter Krisenplanung verfügten, mit den unvorhersehbaren, aufgetretenen Widrigkeiten wesentlich besser zu Rande gekommen sind, als die Unternehmen ohne derartige Instrumentarien, und innerhalb von 4-24 Stunden nach dem Einsturz des WTC einen nahezu uneingeschränkten Geschäftsbetrieb wieder aufnehmen konnten. [vgl. TED01, ROB01]

Hieraus ist zu erkennen, dass durch ein methodisch unterstütztes Vorgehen im Bereich der Corporate Governance und des Risikomanagements nicht nur die Bewältigung einer Krise erleichtert wird, sondern mit einem definierten Risikomanagement auch der Fortbestand von Unternehmen gesichert werden kann.

Für die Disziplin der Wirtschaftsinformatik ergibt sich daraus die Forderung, nach geeigneten Methoden und Modellen zu suchen, die im Rahmen des Einflussbereichs der Wirtschaftsinformatik, also im Bereich der Information und der damit in Zusammenhang stehenden Technologie, eine Unterstützung für die Einführung von IT Governance sind und diese in ein Gesamtmodell zu integrieren. Mit Hilfe eines derartigen Modells ist nicht nur die Implementierung einer IT Governance in Unternehmen, sondern auch die Möglichkeit zur Überprüfung der Funktionsfähigkeit der IT Governance anzustreben.

Die Corporate Governance umfasst im weiteren Sinne alle Organisations- und Strukturfragen der Unternehmen, die die Aktionäre direkt oder indirekt beeinflussen können. In einem engeren Sinne sind die Agenden der obersten Führungsebene – also zumeist des Aufsichtsrats – neben der Richtungsgebung hauptsächlich die Kontrolle der Organisationen und Organisationseinheiten, ob die getätigten Aktionen der Erreichung der gesetzten Ziele entsprechen. In der heutigen Diskussion umfasst die Corporate Governance aber nicht nur die Aktionäre („shareholder“), sondern auch andere Gruppen mit Ansprüchen gegenüber dem Unternehmen („stakeholder“), wie Kunden, Mitarbeiter, Interessensverbände, Finanzdienstleister etc. Hier wird vom Paradigmenwandel vom Shareholder-Value zum Stakeholder-Value gesprochen.

Die Begriffe Corporate Governance und IT Governance möchte ich, nach dem sie bereits mehrmals aufgetreten sind und in der weiteren Arbeit eine zentrale Bedeutung haben werden, an dieser Stelle definieren.

Aus dem englischen wird der Begriff „governance“ mit *„Regieren, Herrschaft, Regierung, Regierungsgewalt, Staatsführung oder Steuerung“* [LEO02] übersetzt. Letzteres (Steuerung) entspricht der lateinischen Wurzel des Wortes, „GUBERNARE“. GUBERNARE ist die lateinische Entsprechung vom griechischen KYBERNÂN, von dem der Begriff „Kybernetik“ abstammt, beide Begriffe bedeuten *„Steuern eines Schiffes“*. [vgl. SCH96, S. 10]

Als Definition des Begriffs Corporate Governance möchte ich jene des Cadbury Report anführen: *„Corporate Governance is the system by which companies are directed and controlled.*“ [FAC92, S 14], sie umfasst die meines Erachtens wichtigen Aspekte:

- **System:** die Corporate Governance eine umfassende und hoch integrierte Einrichtung, nach Heinrich ist ein System *„Der ganzheitliche Zusammenhang von Objekten oder Vorgängen, die voneinander abhängig sind, ineinandergreifen oder zusammenwirken, also miteinander in Beziehung stehen. [...]“* [HEI98, S 513]
- **Directed:** Unternehmen werden mit Hilfe des Systems gelenkt und geführt
- **Controlled:** Unternehmen werden mit Hilfe des Systems kontrolliert, also sind im System Kontrollen vorhanden, wobei eine Kontrolle als *„Im Sinne der Betriebswirtschafslehre der Teil der betrieblichen Aufgabe Überwachung, welcher der Beobachtung des tatsächlichen Verhaltens und seiner Beurteilung anhand von Verhaltenserwartungen (z.B. in Form von Maßstabs- oder Normgrößen) [...] dient. [...]“* [HEI02, S 310] definiert ist.

Nach dem IT Governance Institute, das durch die „Information Systems Audit and Control Association“ (ISACA), der weltweiten Vereinigung von IT-Prüfern und der Stiftung „Information Systems and Audit and Control Foundation“ (ISACF) gegründet wurde, ist IT Governance wie folgt definiert:
„IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives.“ [ISA01, S 9]

Die wichtigen Punkte aus dieser Definition sind:

- Nicht nur das mittlere Management (vor allem die Informationsmanager oder, wie im anglikanischen Raum üblich, als „CIO“ bezeichnet), sondern auch und vor allem die Geschäftsleitung trägt die Verantwortung, diese Aufgabe wahrzunehmen *(„responsibility of the board of directors and executive management“*)
- IT Governance ist nicht isoliert und als Projekt sondern als integraler Bestandteil der Führungs- und Kontrollaufgabe zu betrachten. *(„integral part of enterprise governance“)*
- Die Ziele der Organisation sind mit Hilfe von Informationstechnologie zu unterstützen oder auszubauen. *(“sustains or extends […] strategies and objectives”*)

Robert S. Roussey, derzeitiger Vorsitzende der ISACA erläutert den Begriff folgendermaßen: *“IT governance is the term used to describe how those persons entrusted with governance of an entity will consider IT in their supervision,*

monitoring, control and direction of the entity. How IT is applied within the entity will have an immense impact on whether the entity will attain its vision, mission or strategic goals." [ISA01, S 1].

Die Gesetzgeber - sowohl auf europäischer Ebene, als auch auf Ebene der Einzelstaaten – verlangen von Unternehmen die Schaffung und Aufrechterhaltung eines *„internen Kontrollsystems*", wie dies im § 82 Abs. 1 AktG bzw. im § 22 GmbHG bezeichnet wird. In Deutschland existiert das KonTraG, das noch weitere diesbezügliche Forderungen - vor allem im Bereich der Offenlegung - stellt. Weiters sind derzeit verschiedenartige nationale und internationale Standards, Normen und Empfehlungen (z.B. BS7799, BSI-Grundschutzhandbuch, Common Criteria, Basel-II, ÖNORM-17799, ISO/IEC-17799, Fachgutachten FAMA, Fachgutachten KFS/DV1 der Kammer der Wirtschaftstreuhänder, EnSEC, IT-Monitoring der IFAC etc.) in Kraft beziehungsweise in Begutachtung, die sich unter anderem mit den Anforderungen für eine Steuerung und Kontrolle des Unterstützungsprozesses IT beschäftigen.

Die IT innerhalb eines Unternehmens wird im Prozessmodell nach Porter [vgl. POR98] als „Unterstützungsprozess" im Rahmen der Geschäftsprozesskette gesehen, der eine Schnittstelle zu den anderen Prozessen (Kernprozesse und Unterstützungsprozesse) in Form von Information für diese Prozesse hat.

Die Prozesse benötigen Informationen, die einerseits unterschiedlichen Kriterien entsprechen müssen (z.B. Integrität, Verfügbarkeit, Verlässlichkeit, etc.), und die andererseits durch unterschiedliche Ressourcen (z.B. Daten, Applikationen, Geräte, etc.) repräsentiert werden. In der Folge wird von IT Prozess in der Form des Unterstützungsprozesses nach Porter gesprochen; es ist evident, dass unter diesem Begriff mehrere einzelne und unterschiedlich ausgestaltete Prozesse subsummiert werden.

Nach Heinrich ist ein Prozess *„Eine Menge von Operationen, die durch einen Input in ein System, interne Funktionen im System und einen Output aus dem System beschrieben wird [...]"* [HEI98, S 434]. Diese Definition ist mit der obigen Darstellung insofern konsistent, dass sowohl beim IT Prozess als Gesamtheit, als auch bei den Einzelprozessen jeweils interne Funktionen durch einen Input angestoßen einen Output ergeben, jedoch in unterschiedlicher Granularität.

EU-weit und weltweit sind Bestrebungen zur Umsetzung von Corporate Governance zu erkennen, die neben dem Kern der Corporate Governance auch mit Anforderungen an die IT mit sich bringen werden. Insbesondere werden Anfor-

derungen an Sicherheit (Sicherheit im engeren Sinne, Verfügbarkeit, Vertraulichkeit) und Verlässlichkeit (Einhaltung externer Anforderungen, Integrität) der Informationen steigen und in der Folge neue und umfassende Anforderungen an das Management des Unterstützungsprozesses IT mit sich bringen. Die Kategorisierung der Anforderungen ist an jener des COBIT Modells angelehnt und weiter unten genauer erläutert.

Nicht nur das Unternehmen als Ganzes will gesteuert werden (Corporate Governance), auch die IT als ein wichtiges Element im Unternehmen im Hinblick auf die Zielerreichung bedarf einer regelmäßigen Neuausrichtung. Durch die steigende Durchdringung (z.B. Automatisierung und Integration von Kerngeschäftsprozessen), das Zusammenwachsen von Unternehmen (z.B. durch verstärkten und automatisierten Austausch von Informationen) sowie auch durch die Anforderungen der Stakeholder wird eine erhöhte Transparenz und eine aktive Steuerung des Unterstützungsprozesses IT gefordert. Im Allgemeinen wird hier von IT Governance gesprochen.

IT Governance beschäftigt sich mit der Steuerung (im Sinne einer Zielvorgabe), Messung, Kontrolle (im Sinne der Zielerreichung) und Überwachung (im Sinne einer Abweichungsanalyse) der IT (Prozesse) in einer Unternehmung durch jene Personen, die auch mit der Unternehmenssteuerung (Corporate Governance) betraut sind. Dieser Regelkreis ist in der folgenden Abbildung dargestellt:

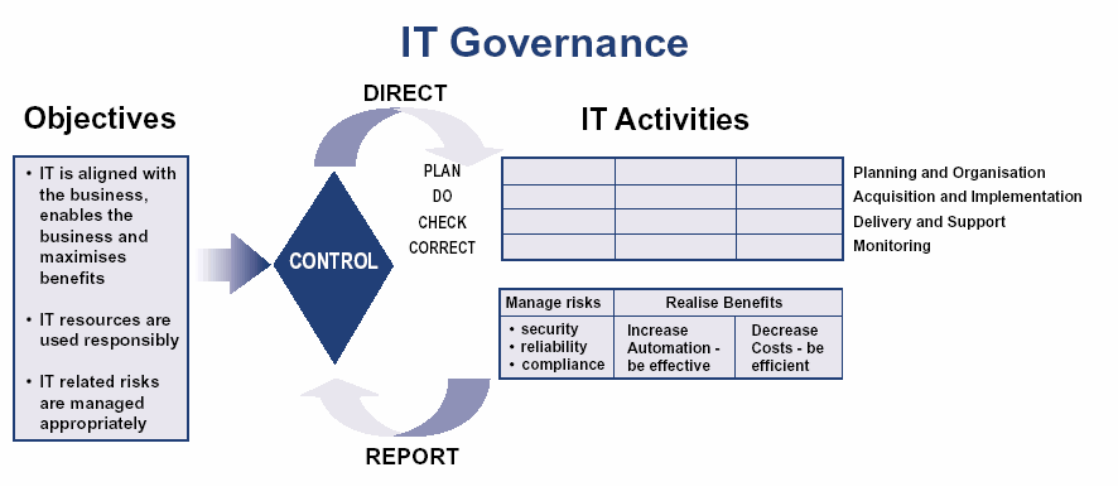


Abb 1: IT Governance Regelkreis [ISA00-1, S 10]

Obwohl in Österreich noch relativ unbekannt, gibt es international schon zahlreiche Bestrebungen und Gruppierungen, die sich mit IT Governance beschäftigen sowie auch diesbezügliche Stellungnahmen und Arbeitspapiere. Die Organisation, die sich bisher am eingehendsten mit IT Governance beschäftigt, ist das

IT Governance Institute, eine Tochterorganisation der ISACA (Information Systems Audit Control Association).

Derzeit ist kein umfassendes Modell verfügbar, mit Hilfe dessen die IT Prozesse gestaltet und gemessen werden könnten, lediglich das COBIT Prozessmodell kann als diesbezüglicher Ansatz gesehen werden. Im Rahmen dieser Arbeit soll das COBIT Modell um unterschiedliche Standards erweitert werden, um sowohl horizontal als auch vertikal ein angemessenes Modell für IT Governance zu erstellen.

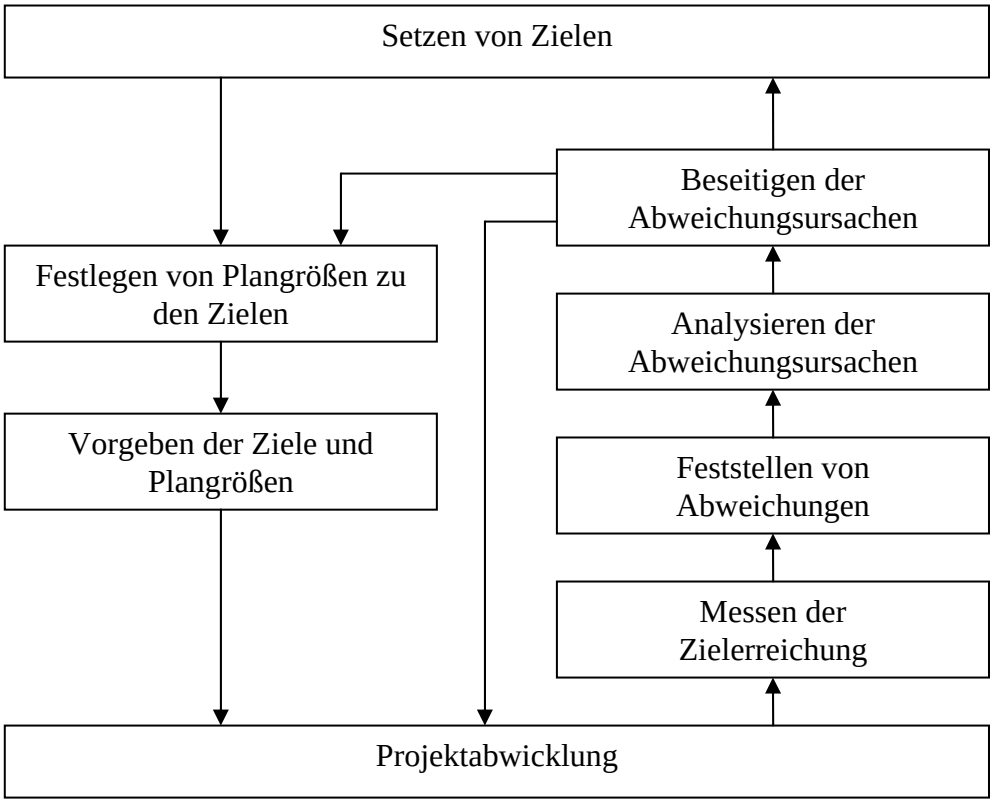


Abb 2: Wirkungskreislauf der Controlling-Teilfunktionen [HEI02, S 169]

Nach der Darstellung der rechtlichen Rahmenbedingungen in Österreich, Deutschland und den USA, und den internationalen gesetzlichen und gesetzesähnlichen Regelungen zur Schaffung und Aufrechterhaltung des internen Kontrollsystems und dessen Auswirkungen auf die IT, möchte ich die entsprechenden Standards, Normen und Richtlinien auflisten und erörtern. Weiters möchte ich die in Literatur und Praxis verfügbaren Mess- und Steuerungsmöglichkeiten für IT Prozesse darstellen, sowie auch die jeweiligen Verantwortlichen für die Durchführung von Überwachungsmaßnahmen herausarbeiten.

In einem Praxisteil werden mit Hilfe des Prozessmodells COBIT die diversen Regularien strukturiert, und ein Modell entwickelt, das die Einführung eines Kontrollsystems aber auch dessen Überprüfung auf Einhaltung und Vollständigkeit ermöglicht.

Ein derartiges Modell beinhaltet jedoch nicht nur die beschriebenen Regularien, sondern muss meines Erachtens auch messbare Größen für die unterschiedlichen Prozesse beinhalten, um den Anforderungen der IT Governance zu genügen. Dies kann ähnlich dem Wirkungskreislauf der Controlling-Teilfunktionen gesehen werden, der sich angefangen beim Setzen von messbaren Zielen bis hin zur Analyse und Beseitigung der Abweichungsursachen zieht, wie dies aus Abbildung 2 ersichtlich ist.

Das Ergebnis der Arbeit ist ein Modell zur Überprüfung der Einhaltung von Standards, Normen und Richtlinien beim Unterstützungsprozess IT, das die lokalen gesetzlichen Anforderungen, die international anerkannten Best Practices sowie messbare Größen inkludiert. Mit Hilfe dieses Modell wird den Stakeholder die Möglichkeit gegeben, die Vollständigkeit des Prozesses bewerten zu können. Durch eine permanente Messung und Abweichungsanalyse und durch eine transparente Gestaltung ist der Prozess für die Stakeholder rasch zu bewerten.

Der Begriff *„Best Practices“* ist als “optimales Verfahren” übersetzt [vgl. LEO02], darunter ist ein allgemein akzeptiertes, als vorbildlich zu bezeichnendes Verfahren zu verstehen.

2.1 Nationale und internationale Regulative

Der Bedarf für Corporate Governance und demzufolge IT Governance ist international sehr uneinheitlich geregelt. Laut einer Studie der EU [vgl. HOL02] ist Österreich auf dem Gebiet der Corporate Governance weitgehend unerforscht: *„In 1997, a report by the European Corporate Governance Network („ECGN") observed that ‚the structure of Austrian corporate governance has remained largely unexplored."* [Hol02, Annex IV, Seite 1].

Dies wird auf die Eigentümerstruktur österreichischer Unternehmen zurückgeführt – eine Vielzahl der Unternehmen ist entweder im Staatsbesitz oder unter Kontrolle eines Eigners. Als weiteres Argument für das Fehlen einer entsprechenden Richtlinie wird der Einfluss von Banken und deren enge Verflechtung in die Geschäftsführungsgremien der Unternehmen angeführt.

Dennoch finden sich in einigen österreichischen Gesetzen Vorgaben für die Schaffung von Corporate sowie von IT Governance.

2.1.1 Aktiengesetz und GmbH-Gesetz

Bezüglich der Corporate Governance sind im Aktiengesetz unter anderem die beiden §§ 81 (Bericht an den Aufsichtsrat) und 92 (Innere Ordnung des Aufsichtsrats) maßgeblich.

§ 81 (1) AktG: *„Der Vorstand hat dem Aufsichtsrat mindestens einmal jährlich über grundsätzliche Fragen der künftigen Geschäftspolitik des Unternehmens zu berichten sowie die künftige Entwicklung der Vermögens-, Finanz- und Ertragslage anhand einer Vorschaurechnung darzustellen (Jahresbericht). Der Vorstand hat weiters dem Aufsichtsrat regelmäßig, mindestens vierteljährlich, über den Gang der Geschäfte und die Lage des Unternehmens im Vergleich zur Vorschaurechnung unter Berücksichtigung der künftigen Entwicklung zu berichten (Quartalsbericht). Bei wichtigem Anlaß ist dem Vorsitzenden des Aufsichtsrats unverzüglich zu berichten; ferner ist über Umstände, die für die Rentabilität oder Liquidität der Gesellschaft von erheblicher Bedeutung sind, dem Aufsichtsrat unverzüglich zu berichten (Sonderbericht).*
(2) Der Jahresbericht und die Quartalsberichte sind schriftlich zu erstatten und auf Verlangen des Aufsichtsrats mündlich zu erläutern; sie sind jedem Aufsichtsratsmitglied auszuhändigen. Die Sonderberichte sind schriftlich oder mündlich zu erstatten." [vgl. RIS02]

§ 92 (4) AktG: *„[...] Besteht der Aufsichtsrat aus mehr als fünf Mitgliedern, so ist zur Prüfung und Vorbereitung der Feststellung des Jahresabschlusses jedenfalls ein Ausschuß zu bestellen. [...]“ [vgl. RIS02]*

Aus diesen Paragraphen ist die Aufgabe des Vorstandes zur – regelmäßigen und unregelmäßigen – Prüfung der Geschäftstätigkeit und der Zielerreichung sowie auch die diese Aufgaben ausführenden Organe ersichtlich. Jedenfalls sei an dieser Stelle festgehalten, dass die Verpflichtung normiert ist, für die Prüfung der Feststellung des Jahresabschlusses einen Ausschuss im Vorstand zu bilden, der an den Aufsichtsrat einen entsprechenden Bericht zu liefern hat.

Im GmbHG ist keine diesbezügliche Regelung getroffen, bei großen GmbHs gelten jedoch die Bestimmungen des AktG sinngemäß. Die Unterscheidung ist im § 221 HGB erläutert. Demzufolge hat eine GmbH entsprechend den Forderungen des AktG zu handeln, falls mindestens zwei der drei Kriterien

- Bilanzsumme von mehr als 12,5 Millionen Euro,
- mehr als 25 Millionen Euro Umsatzerlöse und
- mehr als 250 Arbeitnehmer im Jahresdurchschnitt

erfüllt werden.

Bis 1997 waren in Österreich noch keinerlei gesetzliche Vorschriften verfügbar, wie und durch wen Unternehmen zu steuern sind, geschweigen denn eine Gesetzgebung bezüglich der Führung eines internen Kontrollsystems, das – wie bereits oben erwähnt – immer mehr in der IT abgebildet ist. Erst im Zuge des Insolvenzrechtsänderungsgesetzes (IRÄG) 1997 wurde die Verantwortung für die Erstellung und Aufrechterhaltung eines angemessenen internen Kontrollsystems in den Unternehmen durch die Änderung der §§ 82 AktG und 22 GmbHG dem Vorstand beziehungsweise den Geschäftsführern zugewiesen.

Die Trennung in die beiden Verantwortlichen rührt aus den unterschiedlichen Organen der Kapitalgesellschaftsformen, für Aktiengesellschaften ist der Vorstand (§ 82 AktG: *„Der Vorstand hat dafür zu sorgen, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen.“* [RIS02]), in der Gesellschaft mit beschränkter Haftung sind die Geschäftsführer (§ 22 (1) GmbHG: *„Die Geschäftsführer haben dafür zu sorgen, [...].“*[RIS02]) für die Führung eines internen Kontrollsystems verantwortlich.

Werden die drei oben genannten Vorgaben (Führung eines internen Kontrollsystems, Prüfung des Jahresabschlusses und der Geschäftstätigkeit sowie die

hierfür definierte Verantwortung in den jeweiligen Organen) mit der sich stetig erhöhenden Durchdringung der entsprechenden Aufgabenbereiche mit IT und dem daraus folgenden erhöhten Automationsgrad zusammengeführt, ist die Verpflichtung der leitenden Organe zur Schaffung und zur regelmäßigen Prüfung eines Kontrollsystems in der IT evident. Eine derartige Systematik wird in der Folge als IT Governance bezeichnet.

Der Bedarf für die Verbesserung von Kontrollen in der IT wurde bereits 1976 von Fischer konstatiert, der folgendes veröffentlichte: „Die Umstellung eines konventionellen Buchführungssystems auf EDV verändert das herkömmliche Kontrollgefüge in einer Unternehmung grundlegend. Die Ursache liegt darin, dass mit der Einführung der EDV nicht lediglich manuelle oder halbmaschinelle Verarbeitungsprozesse auf EDV-Anlagen übertragen werden. Vielmehr erfolgt eine Konzentration der gesamten Informationsverarbeitung, wovon das Rechnungswesen und somit auch die Buchführung nur ein kleiner, wenn auch wichtiger Teil sind, in der zentralen Datenverarbeitungsabteilung. Dies bedeutet, dass einerseits traditionelle Kontrollen, welche auf der Aufteilung von Aufgaben und der Trennung von Funktionen beruhen, weitgehend entfallen.“ [vgl. FIS76, S 16]

Ein weiterer Aspekt ist die Verpflichtung der Gesellschaften, den Jahresabschluss nicht nur durch die internen Organe Vorstand und Aufsichtsrat zu überprüfen, sondern denselben durch einen unabhängigen Abschlussprüfer kontrollieren lassen zu müssen, wie dies im § 93 Abs. 1 AktG geregelt ist. Der Abschlussprüfer, der nach § 275 HGB verpflichtet ist, die Prüfung gewissenhaft vorzunehmen, bedient sich bei der Überprüfung der Angemessenheit des internen Kontrollsystems der Internationalen Prüfungsgrundsätze (ISA), die vorsehen, dass der Abschlussprüfer den Einfluss der IT auf die Prüfung zu berücksichtigen hat [WIR00, S 221]. Für die Unternehmen bedingt diese Verpflichtung jedenfalls, dass das Kontrollsystem derart transparent zu gestalten ist, dass sie – wie im § 189 HGB geregelt – einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln können. Dies bezieht sich nicht nur auf die Buchführung, sondern auch auf die Verfolgbarkeit der Entstehung (Geschäftsfall) und Abwicklung (Verbuchung).

2.1.2 Bundesabgabenordung

Im § 131 Abs. 3 BAO sind Kriterien der Ordnungsmäßigkeit bei Einsatz von automationsunterstützter Verarbeitung geregelt:
„Zur Führung von Büchern und Aufzeichnungen können Datenträger verwendet werden, wenn die inhaltsgleiche, vollständige und geordnete Wiedergabe bis zum Ablauf der gesetzlichen Aufbewahrungsfrist jederzeit gewährleistet ist; die vollständige und richtige Erfassung aller Geschäftsvorfälle soll durch entsprechende Einrichtungen gesichert werden. [...]“ [vgl. RIS02]

Folglich ist das Unternehmen – im Falle der BAO wird dieses als Abgabepflichtiger bezeichnet – verpflichtet, nicht nur sämtliche Geschäftsvorfälle zu erfassen, sondern auch zu gewährleisten, dass diese Aufzeichnungen für die gesetzliche Aufbewahrungsdauer, die derzeit in Österreich sieben Jahre beträgt, vollständig und richtig zu halten, also entsprechend zu schützen. In Verbindung mit dem im § 131 Abs. 1 Z6 definierten Radierverbot, das die Unveränderbarkeit der Aufzeichnungen definiert, entsteht für Buchführungssysteme ein hoher Schutzbedarf gegen nachträgliche Veränderung.

2.1.3 Bankwesengesetz

Im Bankwesengesetz sind, ähnlich wie im GmbHG und im AktG, keine exakten Vorkehrungen für die Schaffung einer IT Governance gefordert.

Die Sorgfaltspflicht ist im § 39 BWG normiert, der besagt, dass sich die Geschäftsleiter eines Kreditinstitutes über die bankgeschäftlichen und bankbetrieblichen Risiken zu informieren haben, und die Risiken angemessen begrenzen müssen. Im Originaltext lautet der Absatz 2*: „Die Kreditinstitute haben jene Verwaltungs-, Rechnungs- und Kontrollverfahren einzurichten, die für die Erfassung und Beurteilung der bankgeschäftlichen und bankbetrieblichen Risiken des Kreditinstitutes, die weitestmögliche Erfassung und Beurteilung der sich aus neuartigen Geschäften möglicherweise ergebenden Risiken sowie von Risikogleichläufen erforderlich sind. Die Zweckmäßigkeit dieser Verfahren und deren Anwendung ist von der internen Revision mindestens einmal jährlich zu prüfen.“* [vgl. RIS02] Zusammengefasst wird dies allgemein unter dem Begriff „*Risikomanagement*“, oder mit dem vom Basel Komitee on Banking Supervision geprägten Begriff „*Operational Risk Management“*. Für weitere Einzelheiten bezüglich Basel und ORM sei auf das entsprechende Kapitel weiter unten verwiesen; in diesem Rahmen möchte ich

lediglich die Forderung der österreichischen Gesetzgebung nach der Schaffung eines Instrumentariums zur Bewertung und Begrenzung von Risiken aufzeigen. Ausdrücklich sind sowohl die internen Risiken der Bank als auch die Risiken, die sich aus Kundengeschäften ergeben, angeführt.

Im § 39 BWG ist ebenfalls gefordert, dass das Verfahren zur Risikoerfassung und Beurteilung durch eine interne Revision zu erfolgen hat. Die Verpflichtung zur Einrichtung einer internen Revision ist im § 42 BWG festgehalten, der auch die Aufgaben der internen Revision als *„laufende und umfassende Prüfung der Gesetzmäßigkeit, Ordnungsmäßigkeit und Zweckmäßigkeit des gesamten Unternehmens ...“* [vgl. RIS02] beschreibt, die auf Basis eines jährlichen Revisionsplans wahrzunehmen sind.

Besonderes Augenmerk hat der Gesetzgeber auch auf die Verhinderung von Geldwäscherei gelegt, beispielsweise sei der § 44 Abs. 4 Z1 BWG erwähnt, nach dem die Kredit- und Finanzinstitute geeignete Kontroll- und Mitteilungsverfahren einzuführen haben, um Transaktionen vorzubeugen, die der Geldwäscherei dienen.

Im Bereich der Informationssicherheit ist der § 38 BWG (Bankgeheimnis) als maßgeblich anzusehen, in dessen Abs. 1 geregelt ist, dass in Kreditinstituten beschäftigte Personen, deren Organe, Organmitglieder sowie sonstige für das Institut tätige Personen Informationen, die Ihnen ausschließlich auf Grund ihrer Tätigkeit zugänglich sind, nicht offenbaren oder verwerten dürfen. Ausgenommen sind hier lediglich die im § 38 Abs. 2 BWG aufgeführten Möglichkeiten.

Für die IT von Kreditinstituten führt dies dazu, dass sie – vor allem aber nicht ausschließlich in den Kommunikationssystemen – Vorkehrungen treffen müssen, damit Tatsachen, die dem Bankgeheimnis unterliegen, nicht offenbart werden.

Dies umfasst jedenfalls den Aufbau und das Management eines Systems zur Sicherstellung der Informationssicherheit, wie dies beispielsweise in der Norm ISO/IEC BS 17799:2000 definiert ist.

Die Forderung nach internem sowie externem Risikomanagement sollte ebenfalls in ein umfassendes System eingebunden werden, das meines Erachtens jedenfalls die Aufgaben der Verbrechensverhinderung (z.B. Geldwäscherei) und die Agenden der Revision umfassen soll.

Das im Kapitel AktG und GmbHG erwähnte interne Kontrollsystem ist hier in zwei Bereichen von Interesse: Einerseits können bei großzügiger Betrachtung des § 39 BWG Kreditinstitute bei einer Kreditgewährung vom Antragsteller die Offenlegung seines internen Kontrollsystems verlangen, um das Risiko der Bank im Rahmen der Kreditvergabe einschätzen zu können, folglich müsste das interne Kontrollsystem des Antragstellers externen Anforderungen genügen können und transparent sein. Auf der anderen Seite ist das interne Kontrollsystem des Kreditinstitutes analog dem System gem. AktG zu etablieren, jedoch mit der Erweiterung, dass im BWG ausdrücklich Informationen und die Abwendung von diversen Straftaten gefordert sind.

2.1.4 Datenschutzgesetz

Das Datenschutzgesetz 2000, das mit 1.1.2000 nach einer Anpassung an die EU-Datenschutzrichtlinie neu in Kraft gesetzt wurde, hat einen maßgeblichen Einfluss auf IT Governance, da dieses Gesetz konkrete Forderungen an den Auftraggeber der Datenverarbeitung stellt.

Nach diesem Gesetz hat jeder ein Grundrecht auf Datenschutz und einen Anspruch auf Geheimhaltung der personenbezogenen Daten, sofern daran ein schutzwürdiges Interesse besteht. (§ 1 DSG)

Die Einhaltung der Bestimmungen liegen laut § 6 Abs. 2 DSG im Verantwortungsbereich des Auftraggebers, selbst dann, wenn Dienstleister herangezogen werden. Nach § 4 Abs. 4 DSG gilt als Auftraggeber, wer die Entscheidung getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten, folglich im Zweifel die Geschäftsführung eines Unternehmens.

Im Gesetz werden umfangreiche neue Protokollierungsvorschriften für den Fall von Zugriffen auf Daten definiert. Im § 14 DSG werden umfangreiche Datensicherheitsmaßnahmen definiert. So ist

- eine Aufgabenverteilung ausdrücklich festzulegen.
- die Verwendung von Daten an das Vorliegen gültiger Aufträge (Stellenbeschreibung etc.) zu binden.
- eine Belehrung der Mitarbeiter durchzuführen.
- die Zutrittsberechtigung zu den Räumlichkeiten zu regeln.
- Geräte gegen unbefugte Inbetriebnahme zu sichern.
- Protokoll über die Verwendung zu führen, damit sämtliche Zugriffe nachvollziehbar sind, wobei ich darauf hinweisen möchte, dass nicht nur verändernde, sondern auch lesende Zugriffe zu protokollieren sind.

- die Dokumentation der Regelungen so zu erstellen und zur Verfügung zu stellen, dass sie für Mitarbeiter jederzeit einsichtig sind.

Nach § 52 Abs. 4 Z 4 DSG (Verwaltungsstrafbestimmung) besteht eine Verwaltungsübertretung, wenn die gemäß § 14 DSG notwendigen Sicherheitsmaßnahmen gröblich außer Acht gelassen werden.

Die Übermittlung von Daten (insbesondere auch E-Mail Verkehr etc.) ist laut § 15 DSG an eine ausdrückliche Anordnung des Arbeitgebers gebunden, weiters besteht die Verpflichtung zur Wahrung des Datengeheimnisses.

Erfolgt die Datenverwendung unrechtmäßig nach § 51 DSG in Gewinn- oder Schädigungsabsicht, so sind auf Ermächtigung des Verletzten die Täter zu verfolgen und mit einer Freiheitsstrafe von bis zu einem Jahr zu bestrafen, sofern nicht strengere Normen zur Anwendung kommen.

2.1.5 Emittenten-Compliance-Verordnung – ECV

Die ECV trat mit 1. April 2002 in Kraft und umfasst Bestimmungen, die den Insiderhandel verhindern oder zumindest reduzieren sollen. Somit gilt diese Verordnung zwar nur für börsennotierte Unternehmen, für diese hat es jedoch erhebliche Auswirkungen für die IT und fordert somit, in dieser Arbeit dargestellt zu werden.

Neben zahlreichen organisatorischen Bestimmungen sind auch einige relevante Bestimmungen für IT Governance enthalten.

So wird z.B. angeordnet, dass

- Compliance Verantwortliche definiert werden, die praktischerweise eventuell mit der Funktion eines Sicherheitsverantwortlichen kombiniert werden können,
- eine Compliance-Richtlinie zu erstellen ist, die die Einhaltung der Vorschriften bezüglich der Weitergabe von Insiderinformationen beschreibt,
- Vertraulichkeitsbereiche definiert werden müssen und diese in geeigneter Weise – inklusive EDV-Zugriffsbeschränkungen – zur Verhinderung missbräuchlicher Verwendung oder Weitergabe von Insiderinformationen abzugrenzen,
- Schriftstücke und Datenträger derart aufzubewahren sind, dass sie Unberechtigten nicht zugänglich sind sowie dass

- Elektronisch gespeicherte Daten, inklusive E-Mails, die Insiderinformationen enthalten, vor unberechtigten Zugriff geschützt werden müssen.

2.1.6 Corporate Governance Codex

Am 25. April 2002 wurde in Österreich der erste Entwurf des *„Österreichischen Corporate Governance Codex“* [vgl. ÖAC02] vorgestellt. Er wurde von Vertretern vom ÖVFA, dem IWP und von wissenschaftlichen Beiräten verschiedener Universitätsinstitute sowie dem Regierungsbeauftragten für den Kapitalmarkt erstellt. Die Möglichkeit zur Stellungnahme zu diesem Entwurf bestand bis zum 30. Juni 2002. Eine endgültige Version dieses Code of Corporate Governance für Österreich wird im Herbst 2002 vom österreichischem Arbeitskreis für Corporate Governance der Öffentlichkeit vorgestellt werden.

Ihre Geltung erhalten die Standards durch freiwillige Selbstbindung von Unternehmen, konkret wird dies vor allem börsennotierende Unternehmen umfassen, jedoch ist die Ausdehnung dieser Verordnung auf andere Eigentumsformen denkbar. Die Zielsetzung liegt einerseits in der Verbesserung der Leitung und Kontrolle und andererseits in einem höheren Maß an Transparenz für die qualitative Analyse von Unternehmen.

In der Präambel des Entwurfs wird die Zielsetzung wie folgt zusammengefasst: *„Mit dem österreichischen Corporate Governance Kodex wird österreichischen Gesellschaften ein Ordnungsrahmen für die Leitung und Überwachung des Unternehmens zur Verfügung gestellt, der die international üblichen Standards für gute Unternehmensführung enthält, aber auch die in diesem Zusammenhang bedeutsamen Regelungen des österreichischen Aktienrechts darstellt.“* [ÖAC02, S 5]

Die im Rahmen der Corporate Governance in Zusammenhang mit Risikomanagement und IT Governance relevanten Passagen möchte ich in der Folge anführen:

- **Punkt 14:** *„Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle relevanten Fragen der Geschäftsentwicklung, der Risikolage und des Risikomanagements in der Gesellschaft und in den wesentlichen Konzernunternehmen.“*
- **Punkt 26:** *„Der Vorstand [...] hat sich ferner von der Funktionsfähigkeit der Kontrollsysteme [...] ein eigenes Bild zu machen.“*

- **Punkt 27:** *"In Abhängigkeit von der Größe des Unternehmens ist [...] eine interne Revision als eigene Stabsstelle des Vorstands einzurichten."*
- **Punkt 95:** *„Die Gesellschaft macht im Anhang des Konzernabschlusses detaillierte Aussagen über mögliche Risiken [...] und beschreibt die eingesetzten Risikomanagement-Instrumente im Unternehmen."*
- **Punkt 109:** *„Der Abschlussprüfer hat auch die Funktionsfähigkeit des Risikomanagements zu beurteilen und darüber gesondert Bericht zu erstatten."*

Folglich hat im Rahmen der IT Governance der Vorstand die Aufgaben:

- Sich über die Funktionsfähigkeit der Kontrollsysteme, insbesondere jene im Bereich der IT zu informieren
- Den Aufsichtsrat unter anderem im Bereich der Risikolage und des Risikomanagements zu informieren.
- Durch eine interne Revision sowie durch einen Abschlussprüfer das Risikomanagement prüfen zu lassen.

Für den Bereich der IT im Unternehmen ergibt sich aus diesem Entwurf die Forderung, ein funktionierendes Kontrollsystem zu etablieren und dies derart zu gestalten, dass die das System überwachenden Organe (Vorstand, interne Revision und Abschlussprüfer) über dessen Funktionsfähigkeit urteilen können.

Weiters wird bei einer Analyse der wirtschaftlichen und rechtlichen Rahmenbedingungen für Investitionen künftig von Investoren verstärkt Wert auf die Einhaltung dieses Code of Corporate Governance gelegt werden. Die Nichteinhaltung einer Verpflichtung wird nach meiner Auffassung zum Nachteil für Unternehmen ausgelegt werden. Das gilt nicht nur für Unternehmen, deren Aktien an einer Börse notieren, sondern wird meines Erachtens auch für Gesellschaften angewandt werden, die über einen geschlossenen Eigentümerkreis verfügen, die international und vor allem mit kotierten Unternehmen tätig sind beziehungsweise mit industriellen Partnern, Finanzinvestoren und Kreditgebern kooperieren.

2.1.7 KonTraG

Als ersten Vertreter internationaler Gesetzgebungen möchte ich das deutsche Kontroll- und Transparenzgesetz im Unternehmensbereich erwähnen, das, ähnlich dem Insolvenzrechtsänderungsgesetz in Österreich, im wesentlichen das deutsche Aktiengesetz und das deutsche HGB mit dem Ziel ändert, die Unternehmenskontrolle zu verbessern. Das KonTraG muss ergänzend zum § 91 II des

deutschen Aktiengesetzes gesehen werden, in dem definiert wird, dass es zu den Sorgfaltspflichten eines Vorstands gehört, ein angemessenes Risikomanagement sowie ein interne Überwachungssystem zu etablieren.

Das KonTraG gilt insbesonders für alle Kapitalgesellschaften, börsennotierte AGs, Gesellschaften, die einen Aufsichtsrat haben und nach überwiegender Auffassung auch für GmbHs, aber auch für andere Rechtsformen.

Die Grundlagen eines Risikomanagements sollten in einem Handbuch oder in entsprechenden – eventuell datenbankgestützten – Richtlinien erfasst sein. Ergebnisse der Risikobewertung sollten in einem entsprechenden Inventar dokumentiert sein. [vlg. ROM00]

Die wichtigsten Bestimmungen sind (so weit für diese Arbeit in Zusammenhang stehend) in Kürze [vgl. DÖR99]:

- Der Pflichtbericht des Vorstandes an den Aufsichtsrat hat auch grundsätzliche Fragen der Unternehmensplanung zu umfassen, wobei insbesondere die Finanz-, Investitions- und Personalplanung einzuschließen sind.
- Der Vorstand hat geeignete Maßnahmen zu treffen, um frühzeitig Entwicklungen erkennen zu können, die den Fortbestand der Gesellschaft gefährden könnten. Dies wird im Regelfall mit einem internen Risikomanagement gleichgesetzt.
- Im Bericht ist bei der Darstellung des Geschäftsverlaufs und der Lage der Gesellschaft künftig auch auf die Risiken der künftigen Entwicklung einzugehen, folglich sind bestandsgefährdende Risiken bzw. Risiken mit wesentlichem Einfluss berichtspflichtig.
- Die Prüfung durch den Abschlussprüfer ist so anzulegen, dass Unrichtigkeiten und Verstöße gegen gesetzliche Vorschriften, die sich in der Bilanz niederschlagen könnten, erkannt werden.
- Die Prüfung hat sich auch darauf zu erstrecken, ob die Risiken der künftigen Entwicklung im Lagebericht zutreffend dargestellt sind.
- Es ist – bei Prüfung des Risikofrüherkennungssystems – darauf einzugehen, ob Maßnahmen erforderlich sind, um das interne Überwachungssystem zu verbessern.

Aus diesen Punkten ist ersichtlich, dass im Gegensatz zur österreichischen Legislatur – neben den begrifflichen Unterschieden – ein hohes Augenmerk auf die Erstellung eines Früherkennungssystems gelegt wird. Dies wird im Prüfungsstandard des Risikofrüherkennungssystems nach § 317 HGB, in dem folgendes definiert wird, deutlich: *„Die Reaktionen des Vorstands auf erfasste*

und kommunizierte Risiken selbst sind nicht Gegenstand der Maßnahmen i.S.d § 91 Abs. 2 AktG und damit auch nicht Gegenstand der Prüfung nach § 317 Abs. 4 HGB. Ebenso gehört die Beurteilung, ob die von den nachgeordneten Entscheidungsträgern eingeleiteten oder durchgeführten Handlungen zur Risikobewältigung bzw. der Verzicht auf solche, sachgerecht oder wirtschaftlich sinnvoll sind, nicht zum Risikofrüherkennungssystem.“ (Anmerkung: der § 91 AktG normiert die Erfordernis, ein Überwachungssystem einzurichten, damit der Fortbestand der Gesellschaft früh erkannt wird; der § 317 HGB definiert, dass vom Vorstand Maßnahmen in geeigneter Form getroffen werden müssen, damit das Überwachungssystem seine Aufgaben erfüllen kann.). [vgl. IDW99]

Weiters definiert dieser Standard, dass die Einhaltung der eingerichteten Maßnahmen zur Erfassung und Kommunikation bestandsgefährdender Risiken und ihrer Veränderung durch ein geeignetes Überwachungssystem abzusichern ist. Ein Teil der Maßnahmen sind in die Abläufe fest eingebaute Kontrollen, z.B. die IT gestützte Überwachung der Einhaltung von Terminen, die Genehmigung und Kontrolle der Risikoberichterstattung oder der Vergleich interner Daten mit externen Quellen. [vgl. IDW99]

Zusammengefasst kann gesagt werden, dass durch die Einführung des KonTraG im Gegensatz zur österreichischen Rechtssprechung detaillierte Forderungen bezüglich der Schaffung und Aufrechterhaltung eines internen Kontrollsystems gestellt werden, die entsprechend von Abschlussprüfern zu prüfen sind. In der österreichischen Gesetzgebung ist dies im Ansatz lediglich im Bankwesengesetz enthalten, eine Anleitung zur Implementierung eines Kontrollsystems und die Offenlegung der Kontrollen ist im Gegensatz zum deutschen KonTraG aus österreichischen Gesetzen nicht erkennbar.

2.1.8 Health Insurance Portability and Accountability Act

Das US-amerikanische Gesetz *“Health Insurance Portability and Accountability Act of 1996”* (HIPAA) regelt über Vorgaben bezüglich der Sicherstellung des Schutzes der Privatsphäre, insbesondere von Gesundheitsinformationen. Ich habe dieses Gesetz als internationalen Vertreter von gesetzlichen Regelungen außerhalb der Europäischen Union gewählt, da im Gesetz konkrete Anforderungen an die Absicherung der IT gestellt werden, die über Protokollierungsvorschriften (wie im österreichischen DSG geregelt) hinausgehen. Im Rahmen

des HIPAA werden sowohl der Bedarf für Strategien und strategische Planung, als auch die Einbindung von Drittparteien in der Form von Dienstleistern und/oder Lieferanten, als auch Überwachungsmaßnahmen definiert.

Zweck des HIPAA war, in den amerikanischen Unternehmen des Gesundheitswesens Kosten zu sparen, in dem die Agenden weitgehend standardisiert und reglementiert wurden.

Als wesentlich im Rahmen dieser Arbeit ist jedoch die Verfügbarkeit von Grundsätzen und umfangreichen Leitfäden (Policies und Guidelines), die für den praktischen Teil relevant sind. An dieser Stelle sei festgehalten, dass in der amerikanischen Gesetzgebung konkrete Maßnahmen enthalten sind, die umfangreichen Schutz von Informationen reglementieren.

2.1.9 Combined Code

Der Combined Code ist kein Gesetz, sondern eine Richtlinie, die Anforderungen an ein Risikomanagement definiert, welche eingehalten werden müssen, wenn Aktien des Unternehmens an der Londoner Stock Exchange gelistet werden sollen.

Der Turnbull Report aus dem Jahr 1999 ist nach dem Vorsitzenden einer Arbeitsgruppe zum Thema Risikomanagement der Londoner Börse Nigel Turnbull benannt und ist der bekannteste aus einer Reihe diesbezüglicher Reports. Er baut auf den Reports anderer Ausschüsse wie Cadbury (1992), Greenburry (1995) und Hampel (1995) auf und wurde im Jahr 2000 als *„Combined Code“* der Londoner Stock Exchange als Mindeststandard für in London kotierte Gesellschaften definiert.

Der Turnbull-Report widmet sich dem Thema der internen Kontrollen und weist dem Vorstand die Verantwortung zu: *„The board of directors is responsible for the company’s internal control. It should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning effectively. The board must further ensure that the system of internal control is effective in managing risks in the manner which it has approved.“* [ACC99, S 9]

Auch der Hampel-Report, der logische Vorläufer des Turnbull-Report, nimmt zu den internen Kontrollen bereits Stellung, in dem angewiesen wird, dass durch den Vorstand ein intaktes System interner Kontrollen einzurichten ist, um die

Investitionen der Aktionäre und den Bestand des Unternehmens zu sichern (*„The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.“*, [ACC99, S 9].)

Des weiteren wird vom Cadbury Committee das interne Kontrollsystem als *„key aspect of the efficient management of a company“* [ACC99, S 26] angesehen und dem Vorstand angeraten, ein Statement zur Effektivität des internen Kontrollsystems im Rahmen des Jahresberichts abzugeben. Eine maßgebliche Rolle wird der internen Revision zugesprochen, die die Unternehmensabläufe kennt, die Kontrollsysteme überprüft und beurteilt, sowie die Ergebnisse dem Vorstand berichtet. [vgl. FAC92]

Der Report fordert im wesentlichen die Einführung eines risikobasierten Ansatzes zur Etablierung eines effektiven internen Kontrollsystems und betont auch die Notwendigkeit, dessen Effektivität laufend zu kontrollieren.

Der Ansatz geht von den Geschäftszielen aus und verbindet diese mit einzelnen Risiken. In einem nächsten Schritt werden den Risiken Kontrollen zugeordnet, um die Risiken in einem erforderlichen Ausmaß kontrollieren zu können.

2.1.10 OECD Principles of Corporate Governance

Wie der bereits oben erwähnte Combined Code sind die Grundsätze der Corporate Governance, die von der OECD herausgegeben wurden, kein Gesetz, sondern verstehen sich als Richtlinie. Sie wurden von der OECD publiziert. Die Prinzipien erschienen im Jahr 1999 und sind auf sehr hohem und abstraktem Niveau.

Der grundsätzlichen Richtung der Corporate Governance folgend, konzentrieren sich die Prinzipien an der Lenkung von Unternehmen, oder wie dies von Mitgliedern der Weltbank ausgedrückt wurde: *„Corporate Governance-Grundsätze dienen der Verwirklichung einer verantwortlichen, auf Wertschöpfung ausgerichteten Leitung und Kontrolle von Unternehmen und Konzernen.“* [WOR00, S 2]

Die Grundsätze des ersten Teiles sind in 5 Bereiche unterteilt

I. Die Rechte der Aktionäre
II. Die Gleichbehandlung der Aktionäre
III. Die Rolle der Stakeholder
IV. Veröffentlichungen und Transparenz

V. Verantwortung der Geschäftsführung

Im Rahmen dieser Arbeit erscheinen die letzten drei Punkte als zentral.

- Es wird festgelegt, dass, sobald Stakeholder am Governance Prozess beteiligt sind, eine aktive Kooperation erforderlich ist, um Vermögen, Arbeitsplätze und die Zukunft von finanziell gesunden Unternehmen zu ermöglichen. Dies wird durch die Zusicherung von Rechten und Rechtsmitteln zur Durchsetzung dieser Rechte, aber auch durch die Verpflichtung der Unternehmen, Informationen weiterzugeben, ermöglicht.
- Die zeitnahe Veröffentlichung der finanziellen Situation, der Leistungsfähigkeit, Eigentümerschaft und Geschäftsführung ist im Prinzip IV gefordert. Ausdrücklich erwähnt ist auch die Veröffentlichung von Information über vorhersehbare Risiken. Die Veröffentlichung der Informationen muss entsprechend hoher Qualitätsstandards erfolgen *(„[...] disclosed in accordance with high quality standards of accounting, financial and non-financial disclosure, and audit.“* [OEC99, S 8]. Jährlich ist auch die Art und Weise, wie die veröffentlichten Statements entstanden sind und wie diese veröffentlicht werden, durch einen unabhängigen Prüfer zu prüfen.
- Die Aufgaben der strategischen Leitung des Unternehmens beinhaltet das laufende Monitoring der Geschäftsführung und die Verantwortung gegenüber dem Unternehmen und den Aktionären. In den durch die Geschäftsführung zu erfüllenden Funktionen sind unter anderem die folgenden beschrieben:
  - Erstellung und Überwachung einer Risikorichtlinie
  - Setzen von Performancezielen
  - Sicherstellung der Integrität des Reportingsystems durch das Einbeziehen einer unabhängiger Revision und der Prüfung der Angemessenheit von Kontrollen, vor allem im Bereich von Risikoüberwachung, Kontrolle der Finanzmittel und der Einhaltung von Gesetzen
  - Übersicht über Veröffentlichung und Kommunikation. Zur Erfüllung der Aufgaben sollen die Geschäftsführer über Zugang zu richtiger relevanter und zeitgerechter Information verfügen. [vgl. OEC99], dies fordert die Verfügbarkeit von angemessenen Managementinformationen.

2.1.11 Grundsätze ordnungsgemäßer Buchführung, Datenverarbeitung, Speicherbuchführung und Daten-

schutz

Nach dem § 189 HGB ist ein Kaufmann verpflichtet, eine Buchführung zu führen und diese nach den Grundsätzen ordnungsmäßiger Buchführung (GoB) darzulegen: § 189. (1) HGB *„Der Kaufmann hat Bücher zu führen und in diesen seine Handelsgeschäfte und die Lage seines Vermögens nach den Grundsätzen ordnungsmäßiger Buchführung ersichtlich zu machen. [...]“* [vgl. RIS02]

Die Grundsätze der ordnungsgemäßer Buchführung umfassen folgende wesentliche Teile:

- **Inventur**
  - Lückenlose Erfassung
  - Einzelbewertung
  - Anschaffungskosten
  - Herstellungskosten
- **Bilanzierung**
  - Materialität
  - Going-Concern-Conzept
  - Vorsicht
  - Vergleichbarkeit
  - Klarheit
  - Wahrheit, Richtigkeit
  - Vollständigkeit
- **Erfolgsrechnung**
  - Periodenabgrenzung
  - Realisationsprinzip
  - Imparitätsprinzip, nach dem negative Erfolgskomponenten in der Periode zu verbuchen sind, in dem sie bekannt werden.
- **Abschlussprüfung**
  - Prüfungsgrundsätze
  - Berichterstattung
  - Bestätigungsvermerk
- **Offenlegung**
  - Dokumentation
  - Jahresabschluss
  - Anhang
  - Lagebericht [vgl. HOF93, S 166]

Aus der obigen Auflistung ist erkennbar, dass die Verpflichtung zur Buchführung durch die Zuhilfenahme eines IT-Systems der Forderung nach Vollständigkeit, Richtigkeit, Klarheit, Zuordenbarkeit sowie Transparenz nachzukommen hat. Die exakten Anforderungen an die IT ergeben sich aus den Grundsätzen ordnungsmäßiger Datenverarbeitung, Speicherbuchführung und Datenschutz:

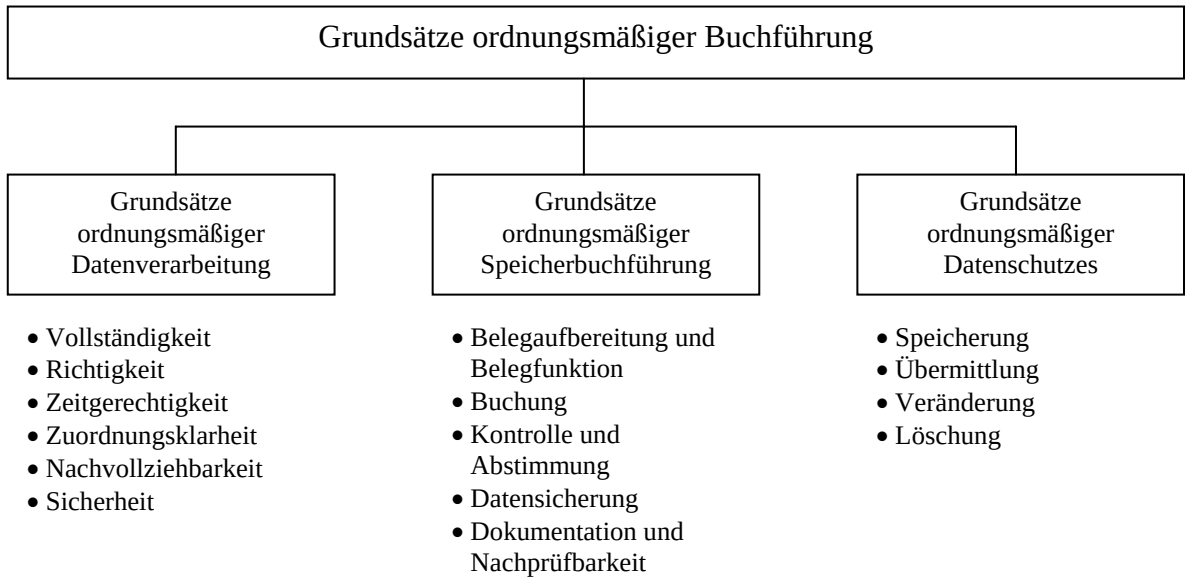


Abb 3: Weiterentwicklung der GoB in Anpassung an die wirtschaftlichen und technischen Veränderungen im Zeitablauf [HOF93, S 172]

Die Grundsätze ordnungsgemäßer Datenverarbeitung (GoDV) ergeben sich im wesentlichen aus einer Veröffentlichung des deutschen Fachausschusses für moderne Abrechnungssysteme (FAMA) des Instituts der Wirtschaftsprüfer (IDW) aus dem Jahr 1987 [vgl. IDW87]. Das in Österreich derzeit gültige Fachgutachten Nr. 58 der Kammer der Wirtschaftstreuhänder [vgl. KDW77] aus Österreich beschäftigt sich mit der selben Thematik, stammt jedoch aus dem Jahr 1977 und ist darob gegenüber der deutschen Publikation als obsolet anzusehen. Nach Auskunft der Kammer ist geplant, noch in diesem Jahr ein neues Fachgutachten zu erstellen.

Nach einer Definition von Schuppenhauer sind die Grundsätze ordnungsmäßiger Datenverarbeitung (GoDV):

- *„Grundsatz der Auftragsbindung an den Auftraggeber der EDV und an die für den Auftraggeber geltenden Vorschriften,*
- *Grundsatz der Kontrollierbarkeit der EDV-Arbeitsabwicklung,*
- *Grundsatz der Transparenz durch EDV-Dokumentation,*

- *Grundsatz der Funktionssicherheit des EDV-Systems.“* [vgl. SCH98, S 48]

Das Fachgutachten KFS/DV1 der Kammer der Wirtschaftstreuhänder definiert als GoB, wobei eingeschränkt werden muss, dass in diesem Fachgutachten (KFS/DV1) keine taxative Aufstellung der GoB angestrebt wurde. Das Fachgutachten behandelt die Ordnungsmäßigkeitskriterien einer EDV gestützten Buchführung, folglich sind lediglich die dafür relevanten Grundsätze enthalten:

- **Grundsatz der Auftragsbindung**: Die IT ist an die Weisungen und Vorschriften des Kaufmanns gebunden. Dies bedingt meines Erachtens, dass der Kaufmann die Steuerung und Kontrolle des IT Prozesses zu übernehmen hat.
- **Grundsatz der Transparenz**: Nicht nur die Verfolgbarkeit der Buchungen muss gewährleistet sein, sondern das Buchführungssystem ist so zu gestalten, dass ein sachverständiger Dritter in angemessener Zeit die Lage des Unternehmens beurteilen können muss.
- **Grundsatz der Kontrollierbarkeit**: Die Buchungen müssen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden. Um dies zu gewährleisten, müssen Verfahren mit ausreichenden Kontrollen eingerichtet sein, für dessen Ausübung der Kaufmann verantwortlich ist.
- **Grundsatz der Funktionssicherheit**: Die mit der IT verbundenen Risiken von Datenverlust oder Datenmanipulation sind durch den Kaufmann durch entsprechende Mittel zu sichern. [vgl. KDW99, S 7f]

Im Rahmen der Grundsätze der ordnungsgemäßen Speicherbuchführung (GoS) [vlg. BMF78] sind die folgenden Punkte zu beachten:

- Belegaufbereitung und Belegfunktion
- Buchung
- Kontrolle und Abstimmung
- Datensicherung
- Dokumentation

Die Grundsätze ordnungsmäßigen Datenschutzes (GoDS) behandeln die Verarbeitung personengeschützter Daten, die – zusammengefasst – nur dann zulässig ist, wenn dies durch eine Rechtsvorschrift wie etwa dem Datenschutzgesetz erlaubt ist.

Die Ordnungsmässigkeit einer Buchführung ist in Österreich durch das oben bereits erwähnte Fachgutachten KFS/DV1 definiert und wird an Hand der folgenden Kriterien überprüft:

- **Die Prüfbarkeit:** Nach der jeder Geschäftsfall nachvollziehbar sein muss (durch Journal-, Beleg- und Kontenfunktionen)

- **Das interne Kontrollsystem:** Maßnahmen, die Eingabe, Verarbeitung und Ausgabe betreffen. Diese Maßnahmen behandeln:
  - Systemeinführung und Weiterentwicklung (Dokumentationspflichten von Angemessenheitsüberprüfungen und Freigaben)
  - Aufbauorganisation (Funktionstrennung, Zugriffsberechtigung, Unabhängigkeit der Organisation von einzelnen Personen)
  - Ablauforganisation (Einhaltung der Bedienungsvorschriften, Datensicherung, Betriebsbereitschaft, Zugriff auf Datenträger, Sicherstellung der vollständigen und richtigen Erfassung, etc.)
  - Dokumentation (zur Programmanwendung, von Zugriffsberechtigungen, ungewöhnlicher Vorkommnise) [vgl. KDW99, S 10 ff]

2.1.12 Basel II

Der Baseler Ausschuss für Bankenaufsicht (Basel Committee on Banking Supervision) hat im Jänner 2001 einen Vorschlag zur Neuregelung der internationalen Regelungen zur Eigenkapitalanforderungen von Banken vorgestellt, der unter der Bezeichnung Basel II bekannt ist. In diesem Papier, das derzeit in der dritten Runde konsultiert wird [vgl. BAS01-1] ist geregelt, dass die Höhe der derzeit mindestens von den Banken zu haltenden Eigenkapitalreserven nach Risikogesichtspunkten neu zu berechnen ist. Die Risiken umfassen unter anderem auch operationelle Risiken. Nach dem Ausschuss wird das operationelle Risiko (als Übersetzung von „operational Risk“) als *„Die Gefahr von unmittelbaren oder mittelbaren Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder von externen Ereignisse eintreten.“* definiert [BAS01-1, S 34]. Die Diskussionspapiere behandeln auch Kredit-, Zins- und Marktrisiken und unterschiedlichen betriebswirtschaftliche Ansätze zur quantitativen Risikobewertung, im Rahmen der Arbeit werden jedoch lediglich die Implikationen auf IT Governance diskutiert. Die erwähnten internen Verfahren, Menschen und Systeme werden in der Originalausgabe unter „Operational Risk Management“ subsummiert.

Nach der Veröffentlichung des Standards, mit dem bis Ende 2003 zu rechnen ist [vgl. STA02-2], treten die Regelungen in Stufen bis Ende 2006 in Kraft. Anfangs sind die operativen Risiken innerhalb der Banken, später die operativen Risiken aus Großkrediten und in der letzten Phase auch die operativen Risiken für Kredite ab einer Höhe von einer Million Euro bzw. Kredite an Unternehmen von mehr als 50 Millionen Euro Jahresumsatz durch die Banken zu bewerten, wie dies vom Ausschuss am 11. Juli 2002 im Rahmen einer Pressekonferenz bekannt gegeben wurde [vgl. STA02-2]. Dies wird mit an Sicherheit grenzender

Wahrscheinlichkeit dazu führen, dass von den Banken, diverse Kennzahlen und Offenlegungen von den Unternehmen gefordert werden, die über das heutige Maß (z.B. Business-Pläne, Kennzahlen wie Cashflow etc.) weit hinausgehen, die aber den Banken helfen werden, die Risiken aus dem Kredit an das Unternehmen bewerten zu können.

Die Risiken werden unter Zuhilfenahme der vom Ausschuss derzeit diskutierten „Sound Practices“ [vgl. BAS01-2] bewertet. Diese stellen eine Anleitung zur Einführung und Aufrechterhaltung sowie einen Mindeststandard für Operational Risk Management dar. Diese Mindeststandards sind jedoch sehr abstrakt gehalten.

2.1.13 Schlussfolgerung

Aus der Darstellung der Regulative ist der Bedarf für die Führung eines Risiko- und Kontrollsystems ersichtlich. Die Verantwortung für die Etablierung eines derartigen Systems liegt bei jenen Organen der Unternehmen, die die Geschäftsführung innehaben.

Eine dezidierte Forderung aus Gesetzen, Erlässen oder Verordnungen zur Etablierung des internen Kontrollsystems im Bereich der IT ist – mit Ausnahme von Regelungen zur Speicherbuchführung in der BAO und den Anforderungen des DSG – derzeit zwar nicht vorhanden, kann jedoch aus den Regulativen klar abgeleitet werden.

2.2 Standards, Normen und Modelle

2.2.1 Allgemein

Wie bereits in der Einleitung erwähnt, existieren zahlreiche Anleitungen zur Etablierung einer IT Governance in Form von Standards, Richtlinien, Normen, Kriterienkatalogen oder Modellen, die in der Folge dargestellt werden sollen. Ich möchte keinen Anspruch auf Vollständigkeit erheben; vor allem Regelwerke, die sehr stark technische Aspekte betrachten (z.B. X.509, dem Standard für digitale Zertifikate) habe ich bewusst vernachlässigt, ebenso wie Standards der Softwareentwicklung und des Projektmanagements. Jedoch habe ich versucht, sämtliche zur Verfügung stehende Regelwerke, die einen wesentlichen Einfluss auf den IT Prozess besitzen, zu berücksichtigen.

In der Erläuterung der Werke möchte ich folgenden Punkte analysieren, bevor der Inhalt des jeweiligen Werkes dargestellt wird. Dies hauptsächlich mit der Zielsetzung, nicht nur einen Überblick über den Inhalt des Werks zu geben, sondern auch um die Zielsetzung des herausgebenden Organisation und die Eignung zur Unterstützung der Implementierung von IT Governance darzulegen.

- **Art:** Ist das Werk eine Norm, ein Standard, etc.?
- **Zielsetzung:** Was ist der Zweck des Kriterienwerks?
- **Herausgeber:** Welche Organisation ist bzw. welche Organisationen sind Herausgeber des Werks?
- **Zielgruppe:** An welche Gruppe richtet sich das Werk?
- **Aktualität:** Entspricht das Werk dem Stand der Technik? Ist das Werk sehr technisch und damit schwer aktualisierbar? Wie oft erfolgt die Aktualisierung und seit wann ist das Werk verfügbar?
- **Vollständigkeit:** Wie umfassend ist das Werk? Dies als Basis für den späteren Abgleich der Werke, wobei auf die horizontale (Aufgabenumfang im Rahmen des IT Prozesses) und auf die vertikale (Detaillierungsgrad der Anforderungen) Vollständigkeit Bedacht genommen wird
- **Internationalität:** Ist das Werk auch außerhalb seines ursprünglichen Gebietes anerkannt bzw. etabliert?
- **Möglichkeit einer Zertifizierung:** Ist eine Zertifizierung nach dem Werk möglich?

2.2.2 Informationstechnik – Leitfaden zum Management von Informationssicherheit, BS ISO/IEC 17799:2000 [vgl. ISO00]

Art

Internationale Norm, wobei nach Heinrich eine Norm als „Eine durch eine dazu befugte Institution festgelegte Vorschrift für Größen, Qualitäten, Methoden, Begriffe usw., die – i.d.R. durch Publikationen – allg. zugänglich gemacht ist.“ definiert ist. [HEI98, S 376]

Zielsetzung

Die Norm stellt eine umfassende Sammlung von Maßnahmen zur Erreichung von Informationssicherheit dar.

Herausgeber

Das Werk wird gemeinsam von ISO (Internationale Organisation für Standardisierung) und IEC (Internationale Elektrotechnische Kommission) herausgegeben.

Zielgruppe

Die Zielgruppe teilt sich in zwei Bereiche, einerseits Unternehmen oder Organisationen, die ein System zur Informationssicherheit einführen wollen, auf der anderen Seite ist diese Norm für Prüfer und/oder Zertifizierende als Referenzwerk von hoher Relevanz.

Zielansprechpartner sind für die Umsetzung im wesentlichen Sicherheitsbeauftragte und IT Manager.

Aktualität

Die Norm ist derzeit in der Erstausgabe verfügbar. Die Sammlung stellt aus derzeitiger Sicht „Best Practice“ in der Informationssicherheit dar, die laufende Aktualisierung ist seitens der ISO/IEC zu erwarten, ein verbindlicher Aktualisierungszyklus ist jedoch nicht erwähnt.

Vollständigkeit

Die Norm gibt sehr generische Maßnahmen vor, die die Informationssicherheit in sehr umfangreicher Weise beschreiben, weiters wird die Einhaltung von Gesetzten gefordert.

Im Vergleich zu seinem Vorgänger, dem BS 7799, fehlt dem Standard der Katalog an Kontrollen, er ist horizontal als relativ breit, vertikal als umfassend zu bezeichnen.

Internationalität

Die Norm ist als ISO-Norm als international verbreitet zu bezeichnen, in Österreich wird derzeit an der Einführung der Norm als ÖNORM A 7799 gearbeitet [vgl. OEN02]. Inhaltlich wird dem Vernehmen nach die lokale Norm der internationalen weitestgehend entsprechen.

Möglichkeit einer Zertifizierung

Derzeit ist in Österreich noch keine Zertifizierung nach dieser Norm möglich, da noch kein Zertifizierungsdienstleister akkreditiert ist, es ist jedoch ein Akkreditierungsverfahren im Laufen.

Inhalt

Die Norm basiert im Wesentlichen auf dem British Standard 7799-1:2000 und definiert die Leitprinzipien („*Guiding-Principles*“), die – wie in der Norm ausgeführt ist– für die meisten Organisationen anwendbar sind [ISO00, S X].

Die Leitprinzipien stellen einen Ausgangspunkt für die Implementierung von Informationssicherheit dar und beruhen entweder auf gesetzlichen Anforderungen oder auf allgemein anerkannte Best Practices.

Als Maßnahmen auf Grund von gesetzlichen Anforderungen werden

- Schutz und Geheimhaltung personenbezogener Informationen,
- Schutz der Aufzeichnungen (Daten) der Organisation und
- Schutz des geistigen Eigentums

gezählt, die Best Practices werden als

- Informationssicherheitsrichtlinie ,
- Zuweisung von Verantwortung für Informationssicherheit,
- Schulung zur Informationssicherheit,
- Problemmeldewesen und
- Management des kontinuierlichen Betriebs (Business Continuity Management – BCM)

angeführt.

In der Einleitung der Norm werden kritische Erfolgsfaktoren für die erfolgreiche Umsetzung von Informationssicherheit im Unternehmen genannt:

- Sicherheitspolitik, -ziele und -aktivitäten spiegeln die Geschäftsziele wider
- Die Implementierung erfolgt unter Beachtung der Organisationskultur
- Offene Unterstützung und Einsatz der Geschäftsleitung
- Umfassende Kenntnis von Sicherheitsanforderungen, Risikobewertung und Risikomanagement
- Effektives Marketing von Sicherheit gegenüber allen Mitarbeitern, inklusive dem Management
- Kommunikation der Regelungen der Sicherheitspolitik und –richtlinien an alle Mitarbeiter und durch Verträge gebundene Organisationen. In der Norm wird der Begriff „contractor“ verwandt, da im anglikanischen Raum üblicherweise ein Vertrag mit Organisationen geschlossen wird, wurde als Übersetzung „durch Verträge gebundene Organisationen“ verwendet
- Angemessene Ausbildungs- und Schulungsangebote sowohl für Mitarbeiter der IT Abteilung als auch für Endanwender
- Ein ausgewogenes und umfassendes Messsystem zur Leistungsbeurteilung des Informationssicherheitsmanagements und zur Verbesserung desselben durch Feedback und Anregungen

Nach diesen Rahmenbedingungen wird in den Kern der Norm vorgedrungen, der Entwicklung eines organisationsspezifischen Managementsystems zur Informationssicherheit.

Ein derartiges System soll laut der Norm aus den unten angeführten Bestandteilen bestehen, die um die Zieldefinition des jeweiligen Teils erweitert wurde. Aus Gründen der Durchgängigkeit habe ich die englische Bezeichnung der Teile beibehalten, und lediglich die Zieldefinition zur Erläuterung in der deutschen Übersetzung angeführt. Die Nummerierung der Teile beginnt mit 3, da die Kapitel 1 („*Scope*“) und 2 („*Terms and Definitions*“) nicht unbedingt Teile eines Informationssicherheitssystems darstellen, sondern im Rahmen der Norm Verwendung finden.

3 Security policy

3.1 Information security policy

Richtungsvorgabe durch das Management, sowie die notwendige Unterstützung für die Informationssicherheit.

4 Organizational security

4.1 Information security infrastructure

Herstellung der Infrastrukturmaßnahmen für das Management von

Informationssicherheit innerhalb der Organisation.

4.2 Security of third party access

Erhaltung der Sicherheit von Geräten und sonstigen Anlagen der Organisation (bzw. des Unternehmens) im Bereich der IT, die im Zugriff von fremden Organisationen stehen.

4.3 Outsourcing

Aufrechterhaltung der Sicherheit der Informationsverarbeitung, falls diese in ein anderes Unternehmen im Rahmen von Outsourcing ausgelagert wurde.

5 Asset classification and control

5.1 Accountability for assets

Beibehaltung eines angemessenen Schutzes für die Anlagen der Organisation.

5.2 Information classification

Sicherstellen, dass die Informationen und die Anlagen der Informationsverarbeitung ein angemessenes Schutzniveau erhalten.

6 Personnel security

6.1 Security in job definition and resourcing

Reduktion von Risiken, die Schäden die auf Grund menschlichen Irrtum, Diebstahl, Betrug, Missbrauchs von Einrichtungen oder ähnlichem verursachen.

6.2 User training

Gewährleistung, dass sich Benutzer der Bedrohung von Informationssicherheit und deren Wichtigkeit bewusst sind, und dass ihnen bei ihrer täglichen Arbeit Mittel zur Verfügung stehen, mit denen sie organisationseigene Sicherheitspolitik verfolgen können.

6.3 Responding to security incidents and malfunctions

Die Schäden zu minimieren, die in der Folge von Sicherheitsvorfällen und Fehlfunktionen entstehen könnten, um derartige Vorfälle beobachten zu können und aus ihnen lernen zu können.

7 Physical and environmental security

7.1 Secure areas

Unberechtigten Zugang, Beschädigung oder Störung von Geschäftsräumen und Informationen zu verhindern.

7.2 Equipment security

Verhinderung von Verlust, Beschädigung oder Kompromittierung von Werten und der Unterbrechung von Geschäftsaktivitäten.

7.3 General controls

Schutz vor Beeinträchtigung und vor Diebstahl von Informationen und Anlagen der Informationsverarbeitung.

8 Communications and operations management

8.1 Operational procedures and responsibilities

Gewährleisten, dass die Geräte der Informationsverarbeitung korrekt und sicher arbeiten.

8.2 System planning and acceptance

Minimierung des Risikos von Systemausfällen.

8.3 Protection against malicious software

Schutz der Integrität von Software und Informationen.

8.4 Housekeeping

Erhalt der Integrität und Verfügbarkeit von Informationsverarbeitungs- und Kommunikationsdiensten. Der Begriff Housekeeping (mit Haushaltsführung, Ordnung und Sauberkeit übersetzt [vgl. LEO02]) ist meines Erachtens irreführend, in diesem Kapitel ist Informationssicherung (Information back-up) und Protokollierung von administrativen Tätigkeiten (Operator logs) und Fehlern (Fault logging) zusammengefasst.

8.5 Network management

Den Schutz von Information in Netzwerken und der Netzwerkinfrastruktur gewährleisten.

8.6 Media handling and security

Schäden an Anlagen verhindern, die die Geschäftstätigkeit unterbrechen könnten. Physischer Schutz und Kontrolle von Medien.

8.7 Exchanges of information and software

Den Verlust, die Modifikation und den Missbrauch von Informationen, die zwischen Organisation ausgetauscht werden, verhindern.

9 Access control

9.1 Business requirement for access control

Kontrolle über den Zugang zu Informationen.

9.2 User access management

Verhindern von unberechtigtem Zugriff auf Informationssysteme.

9.3 User responsibilities

Unberechtigten Benutzerzugriff verhindern.

9.4 Network access control

Schutz vernetzter Dienste.

9.5 Operating system access control

Verhindern von unberechtigten Zugriffen auf Computer.

9.6 Application access control

Verhinderung des unberechtigten Zugriffs auf Informationen, die sich in Informationssystemen befinden.

9.7 Monitoring system access and use

Unautorisierte Vorgänge entdecken.

9.8 Mobile computing and teleworking

Informationssicherheit bei mobilen Geräten und bei Telearbeit gewährleisten.

10 Systems development and maintenance

10.1 Security requirements of systems

Sicherheit in Informationssysteme zu integrieren.

10.2 Security in application systems

Verlust, Änderung oder Missbrauch von Benutzerdaten in Anwendungssystemen verhindern.

10.3 Cryptographic controls

Vertraulichkeit, Authentizität und Integrität von Informationen zu schützen.

10.4 Security of system files
Sicherstellen, dass IT Projekte und operative Aktivitäten auf sichere Weise durchgeführt werden.

10.5 Security in development and support processes
Die Sicherheit von Anwendungssoftware und deren Informationen erhalten.

11 Business continuity management

11.1 Aspects of business continuity management
Unterbrechungen der Geschäftstätigkeit entgegenwirken und kritische Geschäftsprozesse vor den Auswirkungen von maßgeblichen Fehlern oder Desastern zu bewahren.

12 Compliance

12.1 Compliance with legal requirements
Die Verletzung von Gesetzen des Straf- und Zivilrechts sowie gesetzlicher, behördlicher oder vertraglicher Verpflichtungen oder sonstiger Sicherheitsanforderungen verhindern.

12.2 Reviews of security policy and technical compliance
Sicherstellen, dass die Systeme die eigenen Sicherheitspolitiken und Normen einhalten.

12.3 System audit considerations
Die Effektivität des Systemaudits maximieren und gleichzeitig die Störung desselben minimieren.

2.2.3 BS 7799-1:1999 [vgl. BSI99-1] und BS 7799-2:1999 [vgl. BSI99-2]

Art

British Standard, der nach österreichischer Nomenklatur einer nationalen Norm gleichkommt. Die Übersetzung des englischen Ausdrucks „Standard“ mit „Norm“ ist nach Heinrich [HEI98] gültig, wenn er auch als Übersetzung „Standard“ im Sinne eines allgemein akzeptierten Niveaus, das als vorbildlich angesehen wird, anführt [vgl. HEI98, S 499]. Maßgeblich für die Unterscheidung zwischen Standard und Norm (jeweils der deutschsprachige Ausdruck) liegt

darin, dass eine Norm von einer anerkannten Institution veröffentlicht wird, diese Institution kann national (z.B. Österreichisches Normungsinstitut) oder auch international (z.B. ISO) sein, privatwirtschaftliche Institutionen, Berufsvereinigungen etc. können demzufolge lediglich Standards veröffentlichen. Zusammengefasst kann eine Norm als Standard (in der Praxis wird oft von „Best Practice“ oder „Leading Practice“ gesprochen) angesehen werden, ein Standard jedoch nicht als Norm gelten.

Zielsetzung

Der British Standard ist einerseits eine umfassende Sammlung von Maßnahmen zur Erreichung von Informationssicherheit (Teil 1[vgl. BSI99-1]), andererseits bietet er eine Anleitung zur Implementierung eines Informationssicherheitsmanagementsystems (Teil 2 [vgl. BSI99-2]) und umfasst zahlreiche Kontrollen.

Herausgeber

Das Werk wurde erstmals 1995 vom BSI (British Standards Institute) herausgegeben, die derzeit aktuelle Fassung stammt aus dem Jahr 1999.

Zielgruppe

Die Zielgruppe sind Organisationen, die ein System zur Informationssicherheit einführen oder prüfen wollen.

Als weitere Zielgruppe sind Standardisierungsorganisationen zu nennen, da wie oben erwähnt der Teil 1 des BS 7799 im wesentlichen in den ISO/IEC 17799:2000 eingegangen ist.

Aktualität

Das Werk liegt in seiner zweiten Fassung vor, inhaltlich sind sowohl Teil 1 als auch Teil 2 als aktuell anzusehen. Es liegen keine Informationen vor, ob das BSI die Aktualisierung des British Standard vornimmt oder ob die Aktualisierung durch den Übergang in die ISO-Norm abgedeckt werden wird.

Vollständigkeit

Neben dem umfangreichen Katalog des Teil-1 spricht die Verfügbarkeit von Kontrollen für die vertikale Vollständigkeit des British Standard, wenngleich er inhaltlich nicht die Breite von COBIT aufweist.

Internationalität
Das Werk scheint als nationaler British Standard regional begrenzt, dennoch ist es international vor allem im englischsprachigen Raum (USA, Australien, etc.) weit verbreitet. Im deutschsprachigen Raum ist das Werk wenig bekannt.

Möglichkeit einer Zertifizierung
Mit Hilfe des zweiten Teils (Kontrollen) ist eine Zertifizierung möglich, jedoch ist in Österreich derzeit kein Unternehmen entsprechend akkreditiert, um Zertifizierungen durchführen zu können.

Inhalt
Auf Grund der umfangreichen Darstellung des Inhalts der Norm ISO/IEC 17799:2000 wird auf eine neuerliche Auflistung des nahezu inhaltsgleichen BS 7799-1:1999 verzichtet, lediglich die Unterschiede zur oben genannten Norm und die Darstellung des BS 7799-2:1999 möchte ich hier anführen.

Im Gegensatz zur Norm ISO/IEC 17799:2000 ist die Reihenfolge der Maßnahmen die sich aus gesetzlichen Anforderungen ergeben, anders. Im British Standard ist der Schutz des geistigen Eigentums an erster, der Schutz und die Geheimhaltung personenbezogener Daten an dritter Stelle gereiht.

Der zweite Teil des British Standard listet nach einem Vorgehensmodell zur Einführung eines Sicherheitsmanagementmodells detaillierte Kontrollziele („*control objectives*“) auf, schränkt jedoch ein, dass die Auflistung nicht erschöpfend ist und bei Bedarf erweitert werden kann, falls die Organisation der Ansicht ist, dass zusätzliche Ziele und Maßnahmen notwendig wären. [BSI99-2, S ii]

Im dritten Kapitel des Werks wird die Vorgehensweise für die Einführung eines Systems zum Management von Informationssicherheit dargestellt, eine Diskussion des Vorgehensmodells würde jedoch den Rahmen dieser Arbeit sprengen. Im vierten Kapitel werden die detaillierten Kontrollen aufgelistet, die in zehn Unterkapitel eingeteilt werden, die identisch mit den Kapiteln 3 bis 12 des ersten Teils des Werks und folglich mit den Kapiteln 3 bis 12 des oben beschriebenen ISO/IEC 17799:2000 sind, aus Gründen der Vollständigkeit möchte ich die Kapitel anführen, auf eine weitere Erklärung jedoch verzichten.

- Detailed controls
- 4.1 Security policy
- 4.2 Security organization

- 4.3 Asset classification and control
- 4.4 Personnel security
- 4.5 Physical and environmental security
- 4.6 Communications and operations management
- 4.7 Access control
- 4.8 Systems development and maintenance
- 4.9 Business continuity management
- 4.10 Compliance

2.2.4 IT-Grundschutzhandbuch [vgl. BSI00]

Art

Handbuch, das Empfehlungen für Standardsicherheitsmaßnahmen für typische IT-Systeme enthält.

Zielsetzung

„Das Ziel dieser IT-Grundschutz-Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann.“ [BSI00, Kapitel 1.1]

Herausgeber

Das Handbuch wird vom deutschen Bundesamt für Sicherheit in der Informationstechnik herausgegeben und halbjährlich aktualisiert. Es ist in Form einer Loseblattsammlung mit halbjährlichen Ergänzungsblättern, in elektronischer Form sowie im World-Wide-Web online verfügbar.

Zielgruppe

Das Grundschutzhandbuch richtet sich primär an Behörden und Unternehmen [vgl. BSI00, Kapitel 3.6], die IT-Sicherheitskonzepte realisieren wollen. Auf Grund der sehr technischen Ausrichtung eignet sich das Handbuch auch für Hersteller von Hard- und/oder Softwareprodukten. Nachdem auf Basis des Grundschutzhandbuches auch eine Zertifizierung möglich ist, sind Zertifizierungsdienstleister ebenfalls als Zielgruppe zu erwähnen. Herauszuheben ist, dass im Maßnahmenkatalog die Verantwortung für die Initiierung und die Verantwortung für die Durchführung ausgewiesen ist.

Das Handbuch eignet sich für (vgl. [BSI00, Kapitel 1.3]

- IT-Sicherheitsprozess und IT-Sicherheitsmanagement
- IT-Strukturanalyse
- Schutzbedarfsfeststellung
- Sicherheitskonzeption
- Basis-Sicherheitscheck
- IT-Sicherheitsrevision
- Umsetzung von IT-Sicherheitskonzepten
- Qualifizierung nach IT-Grundschutz

Aktualität

Das gedruckte Werk wird laut Publikation mindestens halbjährlich aktualisiert, die letzte Aktualisierung erfolgte jedoch am 13. August 2001, die online Version wird laufend aktualisiert; die letzte Aktualisierung erfolgte in Form der Korrektur am 6. Dezember 2001.

Die Fortschreibung erfolgt in Reaktion auf Umfragen, nach denen die Baustein-Themen priorisiert und entsprechend umgesetzt werden.

Vollständigkeit

Das Grundschutzhandbuch hat in der derzeitigen Fassung mehr als 1700 Seiten, es ist jedoch sehr technisch ausgerichtet und enthält detaillierte technische Anleitungen und Erklärungen.

Es enthält neben einem Gefährdungskatalog auch einen Maßnahmenkatalog mit Maßnahmen, Verantwortlichkeiten und Kontrollfragen. Die Maßnahmen sind jedoch nicht den einzelnen Gefährdungen zugeordnet oder umgekehrt, eine diesbezügliche Zuordnung erfolgt lediglich über die Bausteine in den Kapiteln drei bis neun, in denen jeder Komponente die Gefährdungslage und die entsprechenden Maßnahmenempfehlungen zugeordnet werden.

Das Handbuch ist folglich für eine technische Anleitung als sehr umfangreich und ausgesprochen detailliert anzusehen. Der Softwareentwicklungsprozess ist jedoch nicht Teil des Handbuchs und wurde von diesem ausdrücklich nicht behandelt. Im Rahmen der IT-Governance ist das Vorhandensein von Applikationskontrollen, die im Rahmen einer Entwicklung und oder Änderung eingerichtet werden, als wesentlich anzusehen, die reine Betrachtung des IT-Grundschutzes ist nicht ausreichend, er kann folglich als tief, jedoch nicht als breit bezeichnet werden.

Internationalität

Das Werk hat als Handbuch eines deutschen Bundesamtes ursprünglich lediglich regionale Bedeutung, auf Grund der Verfügbarkeit einer englischen Übersetzung ist es auch international verbreitet, nach der Initiative D21 waren per Dezember 2001 600 europäische und etwa 350 nicht europäische Anwender registriert [vgl. INI01, S 33].

Möglichkeit einer Zertifizierung

Nach Angaben auf der Website des BSI [vgl. BSI02-1] wird an einem Qualifizierungsschema gearbeitet, um Behörden und Unternehmen die Möglichkeit zu geben, deren Bemühen um IT-Sicherheit zu dokumentieren. Ein derartiges Prüfschema ist seit 30. Jänner 2002 verfügbar.

Inhalt

Das Grundschutzhandbuch enthält nach der Einleitung und Verwendungshinweisen eine Anleitung zur Einführung eines angemessenen Sicherheitsniveaus, bevor die Bausteine vorgestellt werden und der Gefährdungs- und Maßnahmenkatalog aufgelistet wird.

Die Vorgehensweise zur Etablierung eines angemessenen Sicherheitsniveaus und der damit zusammenhängenden Feststellung der Angemessenheit des Schutzniveaus wird laut dem IT-Grundschutzhandbuch wie in der Abbildung 4 dargestellt.

Die Schutzbedarfsfeststellung ist im Kontext der IT Governance jener Zeitpunkt, zu dem die Anforderungen an ein Kontrollsystem definiert werden; dessen geforderte Funktionsfähigkeit ist in der Realisierungsplanung abgebildet.

Im Kapitel der Schutzbedarfsfeststellung sind Schutzbedarfskategorien *(„niedrig bis mittel“, „hoch“ und „sehr hoch“)* definiert, zu denen mit Hilfe einer Tabelle die IT-Strukturelemente (als Ergebnis der IT-Strukturanalyse) zugeordnet werden und ausdrücklich darauf hingewiesen wird, dass Folgeschäden zu bewerten sind, folglich Strukturelemente in eine höhere Klasse einzustufen sind, falls von ihnen abhängige Elemente in diese höhere Klasse fallen. Die Ergebnisse sind zu dokumentieren und in der Folge wird wie aus Abbildung 4 ersichtlich weiter verfahren.

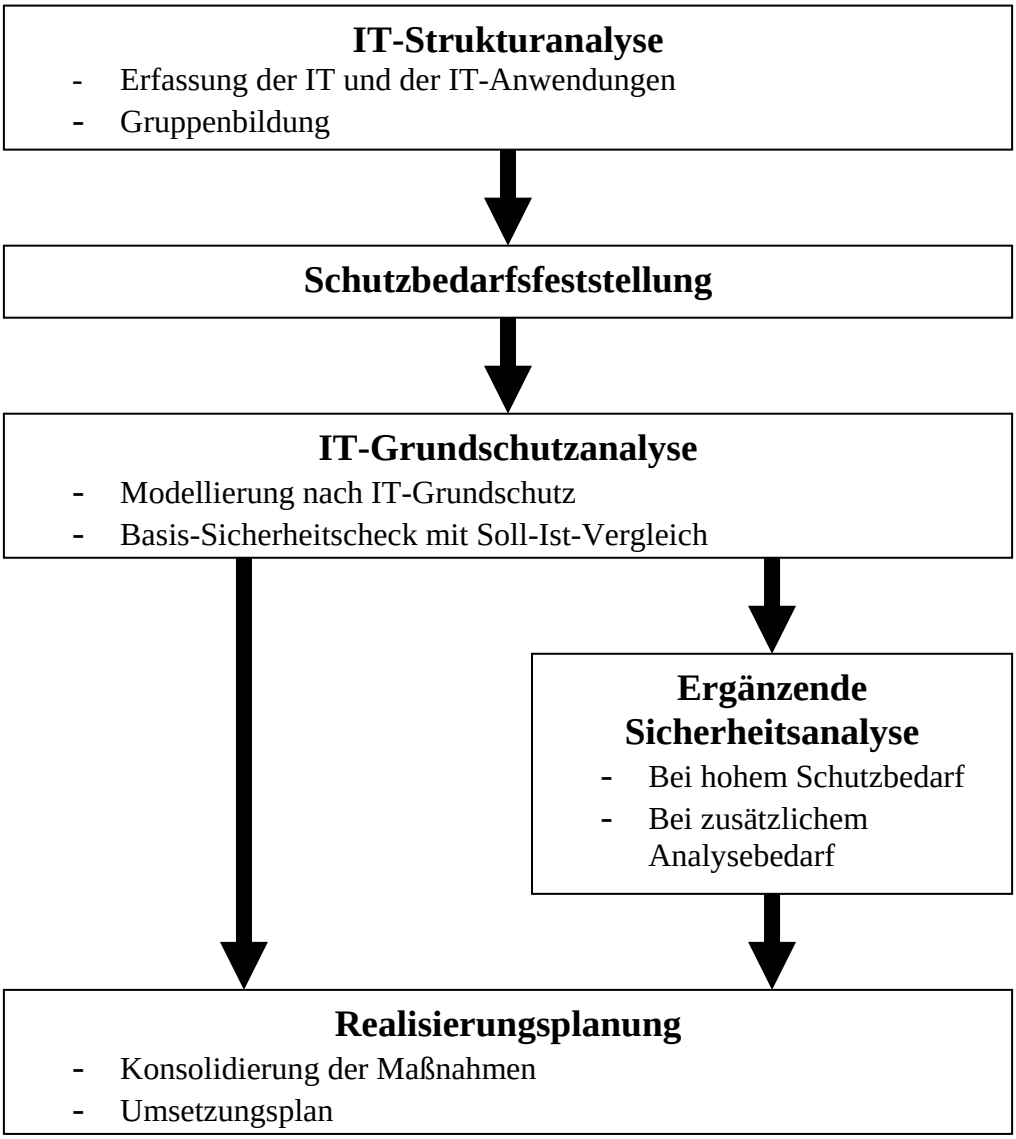


Abb 4: Erstellung eines IT-Sicherheitskonzeptes [BSI00, Kapitel 2]

Die Bausteine gliedern sich wie folgt, wobei die nicht eindeutigen Komponenten erklärt werden:

IT-Grundschutz übergeordnete Komponenten

IT-Sicherheitsmanagement

Als Voraussetzung für die sinnvolle Umsetzung und Kontrolle von IT-Sicherheitsmaßnahmen ist ein durchdachter und gesteuerter IT-sicherheits-prozess zu unterhalten, die diesbezügliche Planungs- und Lenkungsaufgabe ist als IT-Sicherheitsmanagement bezeichnet.

Organisation

Sammlung der allgemeinen und übergreifenden organisatorischen

Maßnahmen zur Erreichung eines Mindestschutzniveaus.

Personal

Die standardmäßig durchzuführenden Grundschutzmaßnahmen im Personalbereich, wie z.B. Einschulung neuer Mitarbeiter, Vertretungsregelungen etc.

Notfallvorsorge-Konzept

Maßnahmen zur Wiederherstellung der Betriebsfähigkeit nach dem Ausfall eines IT-Systems. Erläuternd wird ein vierstufiger Phasenplan angegeben, von der Planung der Notfallvorsorge, Umsetzung der Notfallvorsorgemaßnahmen, Durchführung von Notfallübungen bis zur Umsetzung der geplanten Maßnahmen nach Eintritt eines Notfalls.

Datensicherungs-Konzept

Erstellung eines Konzepts zur angemessenen und funktionstüchtigen Datensicherung, um korrektive Maßnahmen bei technischem Versagen, versehentlichem Löschen oder bei Manipulation treffen zu können.

Datenschutz

Schutz personenbezogener Daten vor Beeinträchtigung.

Computer-Virenschutzkonzept

Maßnahmen zur Verhinderung bzw. Früherkennung von Computer-Viren sowie zur Begrenzung von Schäden durch Computer-Viren.

Kryptokonzept

Beschreibung der Vorgehensweise, wie in heterogenen Umgebungen lokal gespeicherte Daten aber auch zu übertragende Daten durch kryptographische Verfahren und Techniken geschützt werden.

Behandlung von Sicherheitsvorfällen

Zur Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb soll die Behandlung von Sicherheitsvorfällen konzipiert und trainiert werden.

IT-Grundschutz im Bereich Infrastruktur

Gebäude

Verkabelung

Räume

Büroraum

Serverraum

Datenträgerarchiv

Raum für technische Infrastruktur

Schutzschränke

Häuslicher Arbeitsplatz

Nicht vernetzte IT-Systeme / Clients

DOS-PC (ein Benutzer)

PCs mit wechselnden Benutzern
Tragbarer PC
Unix-System
Windows NT - PC
Windows 95 - PC
Allgemeines nicht vernetztes IT-System

Vernetzte IT-Systeme
Servergestütztes Netz
Unix-Server
Peer-to-Peer-Netz
Windows NT Netz
Novell Netware 3.x
Novell Netware 4.x
Heterogene Netze
Topologie, Auswahl und Konfiguration von aktiven Netzwerkkomponenten (Bridges, Switches, Router, Gateways), Auswahl von Übertragungsprotokollen und des Netzwerkmanagement.
Netz- und Systemmanagement
Gesamtheit der Vorkehrungen sowie der Aktivitäten zur Sicherstellung der Funktionsfähigkeit des Netzes, beispielsweise das Monitoring der Performance oder die zentrale Konfiguration der Komponenten.

Datenübertragungseinrichtungen
Datenträgeraustausch
Der Austausch von Datenträgern zur Übertragung in nicht vernetzten Systemen mittels Diskette, Wechselplatte, CD-ROM, Magnetband oder Kassetten.
Modem
Firewall
E-Mail
WWW-Server
Remote-Access

Telekommunikation
TK-Anlage
Faxgerät
Anrufbeantworter
LAN-Anbindung eines IT-Systems über ISDN
Faxserver
Mobiltelefon

Sonstige IT-Komponenten

Standardsoftware
Vorgehensweise für den Umgang mit Standardsoftware (Anforderungskatalog, Vorauswahl, Test, Freigabe, Installation, Lizenzenverwaltung bis zur Deinstallation)
Datenbanken
Telearbeit

Der umfangreiche Gefährdungskatalog wird eingeteilt in die Kategorien; die nach der Kategorienbezeichnung in Klammern gesetzte Zahl gibt die Anzahl der in diese Kategorie subsumierten Gefährdungsbeschreibungen wieder:

- Höhere Gewalt (13)
- Organisatorische Mängel (67)
- Menschliche Fehlhandlungen (47)
- Technisches Versagen (43, inklusive zwei gestrichener Gefährdungen)
- Vorsätzliche Handlungen (102)

Der sehr detaillierte – und mit 608 Einzelmaßnahmen sehr umfangreiche – Maßnahmenkatalog ist wie folgt eingeteilt:

- Infrastruktur (58)
- Organisation (226)
- Personal (26)
- Hardware/Software (135)
- Kommunikation (88)
- Notfallvorsorge (75)

Im IT-Grundschutzhandbuch ist jedoch nicht angeführt, welche Maßnahme zu treffen ist, um eine Gefährdung aus dem Gefährdungskatalog angemessen abwenden zu können. Die einzige Verbindung aus Gefährdung und Maßnahme ist über die Komponenten, wobei eine exakte Verbindung von Maßnahme zu Gefährdung und umgekehrt auch dort nicht möglich ist. Auch das vom Bundesamt vertriebene GSTOOL (einem Anwendungsprogramm zur Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten [vgl. BSI02-1]) hat als zentralen Ansatzpunkt die im Rahmen der oben beschriebenen Vorgehensweise erfassten und modellierten Komponenten. Mit diesem Tool ist ebenfalls die Verbindung von Gefährdung und der daraus folgenden Maßnahmen lediglich über die Komponenten möglich, nicht jedoch direkt.

In der Zusammenführung der Regelwerke werde ich mich bezüglich des Grundschutzhandbuches auf die im Handbuch aufgelisteten Maßnahmen konzent-

rieren, da diese mit den in anderen Standards angeführten Kontrollzielen gleichzusetzen sind.

2.2.5 Information Technology Security Evaluation Criteria – ITSEC

Art

Kriterienkatalog zur Evaluierung von Sicherheit von IT-Systemen

Zielsetzung

Der Kriterienkatalog wurde herausgegeben, um eine international einheitliche Grundlage für die Zertifizierung zu geben [vgl. CEC91, S 3], wobei angemerkt werden muss, dass sich die Zertifizierung nicht auf den weiter oben beschriebenen IT Prozess beziehungsweise einen Sicherheitsprozess im Bereich der IT bezieht, sondern auf Hard- und/oder Softwareprodukte, die an Hand des Kriterienkatalogs zertifiziert werden sollten.

Herausgeber

Das Werk wurde im Jahre 1991 von der Europäischen Kommission herausgegeben und stellt das Ergebnis der Zusammenarbeit des französischen *„Service Central de la Sécurité des Systèmes d'Information“*, des deutschen *„Bundesamt für Sicherheit in der Informationstechnik“*, des niederländischen *„National Comsec Agency“* und des britischen *„Head of the Certification Body of the UK IT Security Evaluation and Certification Scheme“* dar.

Zielgruppe

Das Werk richtet sich an Hersteller von Hard- und Softwareprodukten (im selben als System oder Produkt bezeichnet, wobei ein IT-System eine spezielle IT-Installation mit einem definierten Zweck und einer bekannten Einsatzumgebung ist, ein IT-Produkt jedoch ein Hardware- und/oder Softwarepaket, das "von der Stange" gekauft und in eine Vielzahl von Systemen eingebaut werden kann), die bei der Herstellung ihrer Produkte auf die für Dritte nachvollziehbare und an Hand des Katalogs ausgerichtete Vorgehensweise zurückgreifen wollen, dies vor allem auf Grund der in der Vorgehensweise definierten Sicherheitseigenschaften.

Weitere Zielgruppe sind Anwender in sicherheitsrelevanten Bereichen, die Informationen über die sicherheitstechnische Qualität der eingesetzten IT-

Systeme benötigen und die auf eine Prüfung der Systeme durch unabhängige, kompetente Stellen zurückgreifen wollen oder müssen. [vgl. INI01, S 11]

Aktualität

Die aktuelle Version des Katalogs ist die Version 1.2, die seit 1991 verfügbar ist. Auf Grund der Tatsache, dass die im Katalog angeführten Kriterien als sehr stabil angesehen werden können, ist das Werk immer noch aktuell. Es ist anzumerken, dass eine Aktualisierung nicht mehr vorgesehen ist, da das Werk durch die Common Criteria abgelöst werden sollen, die seit 1999 verfügbar sind.

Vollständigkeit

Die Kriterien sind auf beliebige IT-Systeme und IT-Produkte anwendbar und in diesem Bereich als erschöpfend zu bezeichnen. Die Prüftiefe reicht von einer Black-Box Prüfung bis hin zur Detailprüfung an Hand von mathematischen Modellen. Die Vollständigkeit in der Breite muss jedoch eingeschränkt werden, da lediglich zertifizierbare Produkte behandelt werden.

Internationalität

Der Katalog ist als international zu bezeichnen, er ist jedoch vor allem im europäischen Raum verbreitet.

Möglichkeit einer Zertifizierung

Die Zertifizierung war ausdrücklich Bestandteil des Erstellungsvorhabens und ist somit zentraler Bestandteil des gesamten Werks.

Inhalt

Den Inhalt möchte ich nur darstellen, da wie erwähnt die Common Criteria als Nachfolger des Werks gelten. Der Einfluss des Werks auf die Common Criteria ist für das Gesamtverständnis der Kriterien von Belang.

Im Kapitel 1 wird in Form einer kurzen Darstellung des Umfangs der Anwendungsbereich der Kriterien dargestellt. In diesem Kapitel sind auch die wichtigsten verwendeten Betriffe definiert, es wird ebenfalls das Evaluationsverfahren und der Zertifizierungsprozess kurz beschrieben.

Im Kapitel 2 werden die Sicherheitsanforderungen definiert und beschrieben, das Kapitel 3 definiert jene Kriterien, nach denen Vertrauen in die Wirksamkeit eines Evaluationsziel (Target of Evaluation, weiterhin wie im Werk als TOE abgekürzt), bewertet werden, wobei folgende Aspekte betrachtet werden:

- Eignung der sicherheitsrelevanten Funktionen des TOE.

- Fähigkeit der einzelnen Funktionen und der Mechanismen des TOE, sich gegenseitig zu unterstützen und eine integrierte, wirksame Gesamtheit zu bilden.
- Fähigkeit, einem Angriff zu widerstehen.
- Können bekannte Schwachstellen in der Konstruktion des TOE zu einer Beeinträchtigung der Sicherheit führen.
- Das TOE kann nicht dergestalt konfiguriert werden, dass es Lücken in der Sicherheit aufweist aber für Administratoren oder Endbenutzer als sicher erscheint.
- Ob bekannte Sicherheitslücken im Betrieb des TOE zur Beeinträchtigung der Sicherheit führen können.

Das Kapitel 4 erweitert den Betrachtungshorizont um die Korrektheit der Lösung und behandelt die detaillierten Kriterien, die in jeder Evaluierungsebene E1 bis E6 erfüllt werden müssen. Die Ebenen unterscheiden sich hauptsächlich in zusätzlichen Anforderungen an den Entwicklungsprozess.
Das Kapitel 5 listet die möglichen Zertifizierungsergebnisse auf, das Kapitel 6 ergänzt das Werk um ein Glossar der in den Kriterien verwendeten Begriffe.

2.2.6 The Common Criteria for Information Technology Security Evaluation [vgl. CCI99]

Art
Kriterienkatalog zur Evaluierung von Sicherheit in IT-Systemen

Zielsetzung
Der Kriterienkatalog ist der Nachfolger des oben beschriebenen Katalogs ITSEC mit der Zielsetzung einer größeren Verbreitung als der Vorgänger. Wie sein Vorgänger dient der Katalog zur Zertifizierung der Sicherheit von IT-Systemen und –Komponenten.

Herausgeber
Die aktuelle Version 2.1 Werk wurde im Jahre 1999 vom CCIMB, dem Common Criteria Interpretations Management Board herausgegeben. Im herausgebenden Gremium waren und sind die folgenden internationale Institutionen vertreten:

- Communications Security Establishment, Kanada
- Service Central de la Sécurité des Systèmes d'Information, Frankreich
- Bundesamt für Sicherheit in der Informationstechnik, Deutschland

- Netherlands National Communications Security Agency, Niederlande
- Communications-Electronics Security Group, Großbritannien
- National Institute of Standards and Technology, Vereinigte Staaten von Amerika
- National Security Agency, Vereinigte Staaten von Amerika [vgl. CCI99-1, S ii]

Die historische Entwicklung des Werkes und dessen Beeinflussung durch andere Kriterienwerke ist in der folgenden Abbildung dargestellt:

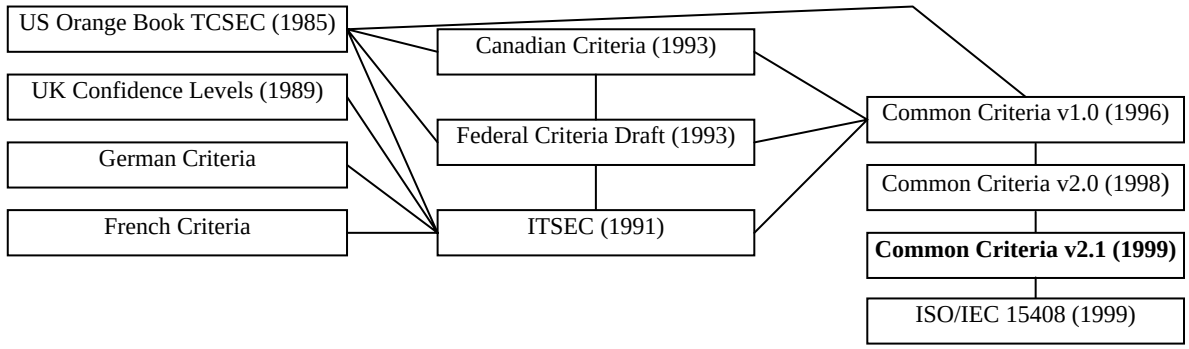


Abb 5: Zusammenhang der Kriterienkataloge

Zielgruppe

Als Zielgruppe kommen – wie bei dem oben beschriebenen ITSEC – Hersteller von Produkten und Systemen sowie Anwender in sicherheitsrelevanten Bereichen in Frage.
Ausdrücklich erwähnt sind Konsumenten, deren Bedürfnisse eine wichtige Rolle für den Evaluierungsprozess sind [vgl. CCI99-1, S 8]

Aktualität

Die aktuelle Version des Katalogs ist die Version 2.1, die seit 1999 verfügbar ist. Die im Katalog angeführten Kriterien sind als sehr stabil zu bezeichnen, bedürfen daher keiner sehr häufigen Überarbeitung, folglich ist der Standard bis heute aktuell. Die Überarbeitung der Version 2 mit dem Ergebnis der Version 2.1 rührt aus der Aufnahme von Formulierungen, die aus dem Standard ISO/IEC 15408 übernommen wurden. Diese Formulierungen sind lediglich qualitativer Natur und rühren aus Vorgaben der ISO, der wesentliche Inhalt wurde nicht abgeändert.

Vollständigkeit
Die Vollständigkeit ist wie oben bereits beschrieben aus Sicht der IT-Governance in der Breite eingeschränkt, da von den Common Criteria lediglich zertifizierbare Produkte und Systeme behandelt werden, wenngleich diese sehr detailliert ausgearbeitet sind.

Internationalität
Der Katalog ist als international zu bezeichnen, er ist jedoch sowohl im europäischen, als auch im amerikanischen und australischen Raum verbreitet.

Möglichkeit einer Zertifizierung
Die Zertifizierung war ausdrücklich Bestandteil des Erstellungsvorhabens und ist somit zentraler Bestandteil des gesamten Werks.

Inhalt
Das Werk ist vom Umfang her mit dem oben beschriebenen ITSEC stark vergleichbar, es ist lediglich anders gegliedert.

Der Teil 1 [vgl. CCI99-1] entspricht den Kapiteln 1 und 2 von ITSEC, es werden nach der Definition der wichtigsten Begriffe das allgemeine Modell und die allgemeinen Kriterien, also die Sicherheitsanforderungen erläutert.

Der Teil 2 [vgl. CCI99-2] ist dem ITSEC Kapitel 3 gleichzusetzen, er behandelt die funktionalen Anforderungen, der Teil 3 [vgl. CCI99-3] befasst sich mit der Korrektheit, entspricht also dem Kapitel 4 der ITSEC.

2.2.7 ISO/IEC 15408

Die drei Teile der ISO-Standard 15408 kommen denen der Version 2.1 der oben beschriebenen Common Criteria gleich, auf eine detaillierte Darstellung wird darob verzichtet. Es sei jedoch vermerkt, dass der Inhalt der Common Criteria auch als allgemein gültige ISO-Norm veröffentlicht ist, eine Zertifizierung nach diesem Standard ist möglich.

2.2.8 IT Infrastructure Library [vgl. ITI02]

Art
Sammlung von Dokumenten, die als Best Practice des IT-Service-Management bezeichnet werden [vgl. ITI02], meines Erachtens ist IT-Service-Management mit Aufgaben zur Sicherstellung des laufenden Betriebs gleichzusetzen, von ITIL wird IT-Service-Management jedoch mit „*Management of Services to meet the Customer's requirements*" beschrieben.

Zielsetzung
„The ethos behind the development of ITIL is the recognition that organisations are becoming increasingly dependent on IT in order to satisfy their corporate aims and meet their business needs. This growing dependency leads to a growing requirement for high quality IT services." [vgl. ITI02]

ITIL konzentriert sich auf die Bereitstellung von Informationen zum Aufbau und Betrieb von Dienstleistungen im Rahmen der IT, um den Anforderungen auf Grund der hohen Abhängigkeit der Unternehmen von der IT gerecht zu werden.

Herausgeber
Der Aufbau der ITIL wurde im Jahre 2000 vom britischen *„Office of Government Commerce"* begonnen. Derzeit umfasst die Sammlung nach Angabe auf der Webseite 39 Bücher, es sind jedoch lediglich zwei davon verfügbar.

Zielgruppe
Als Zielgruppe werden Organisationen unterschiedlicher Größenordnung genannt.

Aktualität
Durch die laufende Weiterentwicklung der Sammlung kann das Gesamtwerk als aktuell angesehen werden, wenngleich eingeräumt werden muss, dass einzelne Publikationen auf Grund der teilweise hohen technischen Detaillierung einem schnellen Alterungsprozess unterliegen.

Vollständigkeit
Das Werk kann als relativ vollständig hinsichtlich der Spezialisierung angesehen werden, bezüglich der Breite sind im Vergleich zu COBIT Mängel vorhanden.

Internationalität
Die Sammlung umfasst lediglich Werke in englischer Sprache und die Verbreitung ist folglich leicht eingeschränkt, wenngleich die Verwendung der englischen Sprache im IT-Bereich mittlerweile als Standard angesehen werden kann.

Nach Angaben auf der Website verwenden weltweit hunderte Unternehmen die Library.

Möglichkeit einer Zertifizierung

Derzeit existieren drei unterschiedliche Zertifikate, mit denen jedoch nicht ein Kontrollsystem oder Teile einesselben zertifiziert werden, sondern es handelt sich um die Zertifizierung von Personen.

- Foundation Certificate als Einstiegsqualifikation in dem die grundlegenden Prinzipien und Konzepte der ITIL gefordert sind.
- Practitioners Certificates für spezifische Bestandteile (z.B. Virenschutz) aus der Grundgesamtheit der Library
- Managers Certificate als umfassende Zertifizierung

Inhalt

Der Inhalt wurde nach Rücksprache mit Service Management Organisationen und ITIL Benutzergruppen vor kurzem strukturiert und enthält seither sechs Kernelemente, die jedoch nicht öffentlich verfügbar sind.

- „**Service Support**“, in dem hauptsächlich Helpdesk, Problemmanagement, und Änderungswesen behandelt werden.
- "**Service Delivery**", das Service Level Management, Budgetplanung und Kostenverrechnung, Kontinuitäts- und Verfügbarkeitsmanagement umfasst.
- „**Planning to Implement Service Management**“ als Anleitung zur Einführung von ITIL Informationsquelle über den Nutzen von ITIL
- „**IT Infrastructure Management**“ in dem Netzwerke, Rechenzentrumsbetrieb, Installation und Update sowie Systemmanagement erläutert werden.
- „**Applications Management**“ der Softwareentwicklung umfasst, wobei ein Software Development Lifecycle mit Test neben notwendigen Änderungen auf Grund von veränderten Anforderungen des Geschäftsbetriebs in Form klarer Anforderungsdefinition bis hin zur Implementierung behandelt werden.
- „**The Business Perspective**“, das Business Continuity Management, langfristige Partnerschaften im Rahmen von Outsourcing und Change Management behandelt werden.

Generell ist anzumerken, dass die ITIL zwar sehr umfangreich ist, jedoch auf Grund einer mangelnden Strukturierung, die auch durch Bemühungen in der

jüngeren Vergangenheit nicht verbessert werden konnte, unübersichtlich und nicht anwendungsfreundlich ist.

2.2.9 IFAC International IT Guidelines [vgl. IFA02]

Art
Sammlung von Richtlinien

Zielsetzung
Mit Hilfe der Richtlinien wird versucht, das Verständnis der Geschäftsführung für die wichtigsten Anliegen des IT-Managements zu fördern. [vgl. IFA02, S 2]

Herausgeber
Die Richtlinien werden vom Information Technology Committee der International Federation of Accountants herausgegeben und umfassen mittlerweile 6 Veröffentlichungen. Die erste wurde im Jahr 1998 herausgegeben, die letzte im April 2002.

Zielgruppe
Als Zielgruppe wird das Management genannt, realistischerweise ist die primäre Zielgruppe die Berufsgruppe von Wirtschaftsprüfern, im speziellen IT-Prüfer.

Aktualität
Das Werk kann als aktuell bezeichnet werden, die Veröffentlichung fand im April des laufenden Jahres statt, außerdem sind die veröffentlichten Kriterien auf hohem Niveau und damit keiner sehr raschen Veralterung unterworfen.

Vollständigkeit
Die Richtlinien befassen sich auf sehr breiter Basis mit Aufgaben der IT Governance, sie sind jedoch auf sehr hohem Niveau und folglich nicht ausgeprägt vertikal.

Internationalität
Die Dokumente sind lediglich in englischer Sprache vorhanden, außerdem realistisch betrachtet lediglich einer relativ kleinen Berufsgruppe zugänglich, weshalb die Verbreitung international begrenzt ist.

Möglichkeit einer Zertifizierung
Es existiert keine Möglichkeit einer Zertifizierung.

Inhalt

Es sind bis dato sechs Richtlinien veröffentlicht worden, die Inhalte dieser Dokumente sind wie folgt:

- **"Managing Security of Information" (1998):** Die Bedeutung von Informationssicherheit, die Prinzipien von Informationssicherheit und ein Vorgehensmodell zur Umsetzung von Informationssicherheit wird ausgeführt. Die Prinzipien sind:
  - Accountability — Verantwortung und Zurechenbarkeit müssen offenkundig sein.
  - Awareness — Bewusstsein von Risiken und Sicherheitsinitiativen muss verbreitet sein.
  - Multidisciplinary — Der Sicherheitsansatz muss sowohl technische als auch nichttechnische Belange berücksichtigen
  - Cost Effectiveness — Sicherheit muss kosteneffektiv hergestellt werden.
  - Integration — Sicherheit muss koordiniert und integriert sein.
  - Reassessment — Sicherheit muss periodisch neu bewertet werden.
  - Timeliness — Sicherheitsvorkehrungen müssen für Vorkehrungen eine zeitlich nahe Überwachung und rechtzeitige Reaktion besitzen. [vgl. IFA98, S 8ff]

- **"Planning for Business Impact"** (1999): Die Bedeutung einer IT Planung, Wesen der Planung, Grundprinzipien in der Entwicklung eines IT Plans, Vorgehen im Rahmen der Planung. [vgl. IFA99]
- **„Acquisition of Information Technology"** (2000): Die Grundprinzipien werden dargestellt und ein Ansatz für die Beschaffung von IT wird angeführt. [vgl. IFA00-1]
- **„Implementation of Information Technology Solutions"** (2000): Softwareentwicklungsprozess, Ansätze für die Implementierung, beteiligte Personen an einem Implementierungsprojekt, Kommunikationsplanung. In den Anhängen werden Vorgehensweisen für die Implementierung von ERP-Paketen, Groupware Systeme, Data-Warehouse Systemen sowie für andere gegeben. [vgl. IFA00-2]
- **„IT Service Delivery and Support"** (2000): Service Level Management, Management der Leistung von Drittparteien, Kostenverrechnung, Kontinuitätsmanagement, Rechenzentrumsbetrieb, Aus- und Weiterbildung von Benutzern, Helpdesk, Problemmanagement, Datenmanagement und Umgang mit Informationen, Facility Management, Änderungswesen, Konfigurationsmanagement und Richtlinienerstellung. [vgl. IFA00-3]

- **„Monitoring“** (2002): Was ist Monitoring (Überwachung), wie kann die Geschäftsführung die IT überwachen, Werkzeuge zur Überwachung, Ansatz für die Einführung von Monitoring, Zeitpunkt für das Monitoring, Verantwortung für die Durchführung. [vgl. IFA02]

2.2.10 Enterprise Security Management - EnSEC [vgl. TÜV01-1]

Art
Zertifizierungsstandard

Zielsetzung
Mit Hilfe eines Framework sollen Unternehmen „ganzheitlich durchleuchtet“ werden, wobei sich die Ganzheitlichkeit auf bestehende Sicherheitssysteme, IT-Komponenten, die IT-Organisation, bautechnische Infrastruktur, Daten-Backups, PC-Arbeitsplätze usw. beschränkt [vgl. TÜV01-1].

Herausgeber
Der Standard wurde erstmals 1997 vom deutschen TÜV Rheinland Berlin Brandenburg, genauer von dessen Unterorganisation TÜV Secure iT GmbH herausgegeben. Im Dokument wird zwischen Name (TÜV Rheinland Berlin Brandenburg) und Funktion (TÜV Secure iT GmbH) unterschieden, als Kontakt ist auf den Veröffentlichungen jeweils die TÜV Secure iT GmbH angegeben. Die aktuelle Version des Anforderungskataloges ist 1.12, sie ist mit 17. Jänner 2001 datiert. [vgl. TÜV01-2]

Zielgruppe
Zielgruppe sind Unternehmen, die an Hand des Standards zertifiziert werden sollten, nach Informationen des Herausgebers ist lediglich dieser befugt, ein Zertifikat nach diesem Standard auszustellen.

Aktualität
Der Standard kann als aktuell bezeichnet werden, die veröffentlichten Kriterien sind auf hohem Niveau und damit keiner sehr raschen Veralterung unterworfen.

Vollständigkeit
Die Richtlinien befassen sich sehr umfangreich mit Sicherheit, sie sind auf sehr hohem Niveau, referenzieren jedoch für Detailmaßnahmen auf das IT-Grundschutzhandbuch des BSI.

Für unterschiedliche Branchen (z.B. System- und Entwicklungs-Partner der Automobilindustrie) werden ergänzende Anforderungen [vgl. TÜV00] entwickelt. Sie sind folglich als relativ breit und relativ tief einzustufen.

Internationalität

Der Anforderungskatalog ist in deutscher und englischer Sprache verfügbar, durch die internationale Verbreitung des TÜV ist auch der Standard international, wenn auch noch nicht viele Unternehmen danach zertifiziert wurden. Der Katalog lag jedoch lediglich in deutscher Sprache vor, vom TÜV Rheinland wurde mir trotz Anfragen keine englischsprachige Version zur Verfügung gestellt.

Möglichkeit einer Zertifizierung

Die Zertifizierung ist zentraler Bestandteil von EnSEC.

Inhalt

Der Anforderungskatalog ist wie folgt gegliedert:

1 IT-Sicherheitsmanagement

1.1 Sicherheitspolitik

Eine Sicherheitspolitik ist durch die Unternehmensleitung festgelegt und dokumentiert, Sicherheitsziele, der Geltungsbereich, und die Verhaltensregeln sind ebenso enthalten, wie die Verpflichtung zur Aufrechterhaltung des Sicherheitsprozesses

1.2 Ressourcenmanagement

Von der Unternehmensleitung sind ausreichend angemessene Mittel und Personal, sowohl für leitende als auch für ausführende Tätigkeiten im Rahmen der Sicherstellung der Sicherheit zur Verfügung gestellt.

1.3 Sicherheitsprozess

Ein Sicherheitsprozess ist im Sicherheitshandbuch dokumentiert und die Aufrechterhaltung des Sicherheitsprozesses ist Teil des Handbuches.

Der Sicherheitsprozess umfasst folgende Schritte:

- **Feststellung des Schutzbedarfs** der Geschäftsprozesse und Unternehmensdaten;
- **Analyse der Bedrohungen/Risiken** für schutzbedürftige IT-Systeme, Anwendungen und Daten;
- Planung, Realisierung und Aufrechterhaltung von **Sicherheitsmaßnahmen** zur Reduktion festgestellter Bedrohungen/Risiken;
- **Schulung** von Management und Mitarbeitern, insbesondere bei Einführung neuer Systeme;

- kontinuierliche **Überprüfung der Angemessenheit** der Ressourcen,
- Planung, Durchführung und Dokumentation interner **Audits** zur Prüfung, ob die sicherheitsbezogenen Tätigkeiten und Systemkonfigurationen den geplanten Festlegungen entsprechen und ob der Sicherheitsprozess wirksam ist;

Entwicklung und Training von Notfallsmaßnahmen, die Aufzeichnung und Verfolgung von Sicherheitsverstößen und die Systematik einer Risikoanalyse bei hohem Schutzbedarf / Schadenspotential sind ebenfalls im Sicherheitshandbuch zu dokumentieren.

1.4 Aufzeichnung von Vorfällen

Beschwerden, sicherheitsrelevante Vor- und Notfälle werden aufgezeichnet und dem Management zur Kenntnis gebracht.

2 Organisation und Personal

2.1 Personal

Die Verantwortung, Kompetenz, Befugnis, Vertretung und die gegenseitige Beziehung von Personal - besonders jenem, das die Verantwortung für Vorbeugungsmaßnahmen gegen mögliche Sicherheitslücken in der IT oder in der Organisation bearbeitet - ist festgelegt und bekannt

2.2 Sicherheitsbeauftragter

Ein Sicherheitsbeauftragter ist ernannt, der über ausreichende Befugnisse verfügt, den Sicherheitsprozess festzulegen, zu verwirklichen und aufrecht zu erhalten, außerdem ist er verpflichtet, der Unternehmensleitung über die Wirksamkeit des Sicherheitsprozesses zu berichten.

2.3 Information

Mitarbeiter, Führungskräfte und externe Mitarbeiter sind nachweislich über den Umgang mit vertraulichen Informationen und mit den entsprechenden Konsequenzen von Zuwiderhandlungen informiert.

2.4 Personalauswahl

Es werden angemessene Kriterien bei der Auswahl von Mitarbeitern (aber auch bei der Auswahl externer Dienstleister) angewandt und technische Systeme dürfen nur von entsprechend unterwiesenem und autorisiertem Personal verwaltet werden.

3 Informations- und kommunikationstechnische Infrastruktur

3.1 Auslegung der kritischen Systeme

Die Systeme sind dergestalt ausgelegt, dass die von den Geschäftsprozessen angemessene Verfügbarkeit, Vertraulichkeit und Integrität der Daten

sichergestellt ist.

3.2 Betrieb der kritischen Systeme

Die kritischen Systeme (Systeme zum Schutz der Daten, Authentisierungssysteme, Firewall, Backup-Einrichtung, Verschlüsselungseinrichtung, ...) werden dem Schutzbedarf entsprechend nur durch berechtigtes und geschultes Personal betrieben.

3.3 Inventar

Ein Netzwerkplan und ein Inventurregister der Hard- und Software ist vorhanden.

4 Bautechnische Infrastruktur

4.1 Versorgungseinrichtungen

Die Versorgungseinrichtungen (Strom, Telekommunikationsverbindungen, ...) entsprechen der geplanten Beanspruchung, der notwendigen Verfügbarkeit und der den Schutzbedarf notwendigen Sicherheit.

4.2 Angemessene Zugangskontrollen

Es werden angemessene Zugangskontrollen betrieben, die sicherstellen, dass lediglich befugtes Personal Zugang zum Unternehmen, zu Daten und zu IT-Systemen erhält. In abgestuften Schutzzonen wird über Regelungen zur persönlichen Kontrolle, technische Zugangseinrichtungen und durch geeignete bauliche und organisatorische Maßnahmen angemessener Zugangsschutz sichergestellt.

4.3 Physische Schutzeinrichtungen

Gegen ein mögliches Abhören von Leitungen und Geräten, Stromausfall, Brand, Wasserschaden und Zerstörung oder terroristische Attacken sind entsprechende physische Schutzmaßnahmen vorhanden.

5 Systemverwaltung

Es existieren angemessene Regelungen und Verantwortlichkeiten bezüglich der Administration der sicherheitsrelevanten Systeme, die nach unterschiedlichen Betriebssystemen gegliedert sind und die Netzinfrastrukturen berücksichtigen. Ebenso ist die Einrichtung von Arbeitsplatzrechnern, die Zugriffskontrolle, Vernichtung von Datenträgern, der Betrieb von RAS-Zugängen, Datensicherung, Wartung, Konfiguration etc. durch entsprechende Richtlinien geregelt.

6 Arbeitsplätze / Mitarbeiterverantwortung

6.1 Verhaltensweisen

Den Mitarbeitern sind die festgelegten Verhaltensweisen im Umgang mit IT und den verbundenen Risiken und Maßnahmen (Internetpolicy, Verhalten bei Virenattacken, Weitergabe von Informationen, Installation von Software etc.) bekannt und die Verhaltensweisen werden überwacht.

2.2.11 WebTrust [vgl. AIC01-1, AIC01-2, AIC01-3 und AIC01-4]

Art

Sammlung von Zertifizierungsstandards, von WebTrust als „Programm“ bezeichnet.

Zielsetzung

Sicherheitslücken im Bereich von E-Commerce Systemen schaffen ein Vertrauensdefizit bei prospektiven Kunden. Da dies ein Handelshemmnis darstellt, sollten im Interesse von Verbrauchern, Anbietern und Gesamtwirtschaft, die Geschäfts- und Sicherheitspraktiken im Internet angegeben werden, die Angemessenheit sowie die Einhaltung dieser Praktiken einer unabhängigen Prüfung unterzogen und das E-Commerce System zertifiziert werden.

Aus diesem Grund wurden Prinzipien und Kriterien entwickelt, an Hand derer eine Zertifizierung eines E-Commerce Systems durchgeführt werden kann, die Zertifizierung selbst ist in den Werken nicht beschrieben.

Herausgeber

Die „WebTrust Principle and Criteria“ wurden von der AICPA - der amerikanischen Vereinigung der Wirtschaftstreuhänder - gemeinsam mit ihrem kanadischen Pendant, der CICA, ausgearbeitet.

Zielgruppe

Zielgruppe sind Unternehmen, die E-Commerce Systeme betreiben und sich dem jeweiligen Prinzip unterwerfen sowie sich an Hand der jeweiligen Kriterien zertifizieren lassen wollen, wobei ein einzelnes Programm oder gleichzeitig mehrere Programme zertifiziert werden können.

Eine Ausgabe der Principle and Criteria ist zur Zertifizierung von Herausgebern digitaler Zertifikate, sogenannten Certification Authorities, anzuwenden, dieser Standard ist jedoch noch im Entwurfsstadium und wird voraussichtlich im Herbst 2002 veröffentlicht.

Aktualität
Der Standard ist inhaltlich aktuell, die Prinzipien und Kriterien sind auf hohem Niveau und damit keiner sehr raschen Veralterung unterworfen. Eines der Programme (Online Privacy) der derzeit gültigen Version 3.0 ist seit 2000 verfügbar, die anderen verfügbaren Programme stammen aus dem Jahr 2001.

Derzeit ist ein Entwurf eines Nachfolgestandards [vgl. AIC02-3] in der ersten Fassung veröffentlicht, der sowohl WebTrust, als auch das weiter unten beschriebene SysTrust ablösen soll. Inhaltlich ist dieser Standard eine Zusammenführung der unterschiedlichen Ansätze von WebTrust, das für Systeme des E-Commerce zutreffend ist, und SysTrust, das allgemein für Systeme angewandt werden soll. Zur klaren Darstellung des Begriffs System sei auf das Kapitel 2.2.12 SysTrust verwiesen. Weiters ist eine Vereinheitlichung in der Strukturierung der Kriterien und eine einheitliche Nomenklatur zu erkennen; inhaltlich sind jedoch keine Ergänzungen in Form von zusätzlichen oder abgeänderten Kriterien festzustellen. Als Exkurs ist die Gliederung des Entwurfs nach der Beschreibung des Inhalts von SysTrust angeführt.

Vollständigkeit
Die Richtlinien beinhalten nicht nur technische Anforderungen, die erfüllt werden müssen, sondern auch Anforderungen an organisatorische Abläufe und Überwachungsmaßnahmen, sie sind folglich horizontal breit, vertikal sind sie auf Grund des hohen Abstraktionsniveaus flach. Hervorzuheben ist, dass zu den Kriterien Beispiele gegeben werden, mit denen die Kriterien erfüllt werden können.

Internationalität
Der Standard aus dem amerikanischen Raum ist international verbreitet.

Möglichkeit einer Zertifizierung
Die Zertifizierung ist zentraler Bestandteil des Standards.

Inhalt
Das gültige WebTrust Programm besteht aus fünf Einzelprogrammen, die jeweils eine Erläuterung des Prinzips und einen Kriterienkatalog enthalten. Die Kriterien sind durchgängig in vier Bereiche unterteilt:

- **Disclosures**: Veröffentlichungen, etwa in Form von Allgemeinen Geschäftsbedingungen

- **Policies**: Im Unternehmen vorhandene und zu befolgende Richtlinien und Vorschriften
- **Procedures**: Im Unternehmen eingesetzte Methoden und Werkzeuge
- **Monitoring**: Überwachungsfunktionen, sowohl technischer Natur (z.B. Prüfprogramme wie z.B. SATAN oder änliches) als auch in Form von Berichten für das Management und dessen Stellungnahmen zu den Berichten

Zu jedem Kriterium sind Beispiele angeführt, mit denen Business-to-Business, Business-to-Consumer und Serviceprovider das jeweilige Kriterium erfüllen können.

Die einzelnen Programme sind in der Folge ausgehend vom jeweiligen Prinzip dargestellt, die deutsche Übersetzung stammt von der österreichischen Internet-seite über WebTrust [vgl. EUR01] und ist in Klammern angegeben:

On-Line Privacy (Privatsphäre)
"The entity discloses its privacy practices, complies with such privacy practices, and maintains effective controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce is protected in conformity with its disclosed privacy practices." [AIC00-1, S 19]

Folglich schützt das Unternehmen Daten – die auf Grund einer E-Commerce Transaktion gespeichert werden – auf eine Art und Weise, dass die agierende Person (in der Regel prospektiver Kunde) nicht identifizierbar ist.

Nach diesem Programm wird beispielsweise geprüft, welche Informationen gesammelt werden, wie die gesammelten Informationen verwendet und verwaltet werden, an wen diese Informationen auf welche Weise weitergegeben werden etc.

Confidentiality (Vertraulichkeit)
"The entity discloses its confidentiality practices, complies with such confidentiality practices, and maintains effective controls to provide reasonable assurance that access to information obtained as a result of electronic commerce and designated as confidential is restricted to authorized individuals, groups of individuals, or entities in conformity with its disclosed confidentiality practices." [AIC01-1, S 6]

Der Zugriff auf Informationen, die im Zuge einer E-Commerce Transaktion erhoben wurden und die als vertraulich gelten, ist auf autorisierte Personen, Gruppen und Unternehmen eingeschränkt.

Geprüft wird unter anderem, ob die Sicherheitssysteme die Übertragung der Informationen angemessen schützen, ob die Sammlung der vertraulichen Informationen den Geschäftszielen entspricht oder ob Daten gesammelt werden, die mit dem ursprünglichen Geschäft nicht in direktem Zusammenhang stehen, Vorgehensweisen bei einer vermuteten Verletzung der Vertraulichkeit, etc.

Security (Datensicherheit)
"The entity discloses its key security practices, complies with such security practices, and maintains effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to authorized individuals in conformity with its disclosed security practices." [AIC01-2, S 5]

Der Zugang zu den E-Commerce Systemen ist durch effektive Kontrollen auf autorisierte Personen beschränkt, wobei eingeschränkt wird, dass eine angemessene Absicherung erfolgt.

Hierbei wird geprüft, ob die Vorgehensweise nach einer Sicherheitsverletzung definiert wurde, ob Verschlüsselungstechnologien angemessen eingesetzt werden, ob angemessene Kontrollen im Umgang mit Benutzerkonten im Einsatz sind etc.

Business Practices/Transaction Integrity (Vereinbarungsgemäße Geschäftsabwicklung)
"The entity discloses its business practices for electronic commerce, executes transactions in conformity with such practices, and maintains effective controls to provide reasonable assurance that electronic commerce transactions are processed completely, accurately, and in conformity with its disclosed business practices." [AIC01-3, S 5]

Es sind Kontrollen im Einsatz, die mit hoher Sicherheit gewährleisten, dass die Geschäfte vollständig und sorgfältig ausgeführt werden.

Die Kriterien umfassen Bereiche wie vorhandene Informationen über die angebotenen Produkte, Lieferzeiten, Zahlungsbedingungen, Stornierungsmöglichkeiten, etc.

Availability (Verfügbarkeit)
The entity discloses its availability practices, complies with such availability practices, and maintains effective controls to provide reasonable assurance that

electronic commerce systems and data are available in conformity with its disclosed availability practices." [vgl. AIC01-4, S 6]

Die Verfügbarkeit der E-Commerce Systeme und Daten wird sichergestellt.

Im Rahmen dieses Programms wird geprüft, ob der Zugriff auf die Systeme angemessen erfolgt, die physische Absicherung und Redundanz der Systeme, die Verfügbarkeit von Kontinuitätsplänen und Wiederanlaufplänen, Tests und Dokumentation von Hard- und Software oder ob Wartungszeiten angemessen geplant und kommuniziert sind.

2.2.12 SysTrust [vgl. AIC02-01]

Art
Zertifizierungsstandard

Zielsetzung
Auf Grund der Tatsache, dass Organisationen in immer stärkerem Maß in Geschäftsführung, der Produktion aber auch in der Kommunikation mit Kunden und Geschäftspartnern von Informationstechnologie abhängig sind, ist die Sicherheit, Verfügbarkeit der Systeme und die Verlässlichkeit der Information als kritisch anzusehen. Darum wurde SysTrust eingeführt, mit Hilfe dessen Wirtschaftsprüfer die Zuverlässigkeit der Systeme zertifizieren können. [vgl. AIC02-01]

Herausgeber
Der Standard wurde von der AICPA und CICA ausgearbeitet.

Zielgruppe
Zielgruppe sind Betreiber von Systemen, also im wesentlichen Rechenzentren, sowohl unternehmensinterne als auch Rechenzentrumsbetreiber, die diese Dienstleistung ihren Kunden anbieten, welche die Funktionsfähigkeit des internen Kontrollsystems in ihrem Bereich an Hand der Prinzipien und Kriterien [vgl. AIC00-2] von SysTrust durch unabhängige Dritte akkreditieren lassen wollen.

Aktualität
Der Standard ist, obwohl auf sehr hohem Niveau, nicht mehr ganz aktuell, die derzeit gültige Version 2.0 stammt aus dem Jahr 2000. Nach Auskunft der

AICPA wird derzeit an einer Überarbeitung des Standard gearbeitet, der weiter unten beschrieben wird.

Vollständigkeit
Die Richtlinien beinhalten neben technischen auch organisatorische Anforderungen und Überwachungskriterien, die erfüllt werden müssen. Sie sind folglich horizontal breit, vertikal sind sie auf Grund des hohen Abstraktionsniveaus flach.

Internationalität
Der Standard aus dem amerikanischen Raum ist international verbreitet.

Möglichkeit einer Zertifizierung
Die Zertifizierung ist zentraler Bestandteil des Standards.

Inhalt
Der wesentliche Unterschied zu dem weiter oben erläuterten Standard WebTrust ist jener, dass er sich nicht auf E-Commerce Systeme beschränkt, sondern allgemein von Systemen spricht, die wie folgt definiert werden: *„A System is an organized collection of software, infrastructure, people, procedures and data that, together within a business context, produces information.“* [AIC02-2, Folie 22]. Im Entwurf des Standards „Trust Services“ wird System wie folgt definiert: *„A ‘system’ consists of 5 key components organized to achieve a specified objective.”* [AIC02-3, S 5] Die Komponenten sind Infrastruktur (Facilities, Netzwerk und Ausrüstung), Software (Betriebssysteme, Anwendungen und Dienstprogramme), Personal (Entwickler, Anlagenbediener (Nach Heinrich die Übersetzung von „operator“ [vgl. HEI98, S 49]), Benutzer und Management), Abläufe (automatisiert und manuell) und Daten (Dateien, Datenbanken, Tabellen, Transaktionen).

Die Principles sind [vgl. AIC02-1]:

- **Availability** (Verfügbarkeit): Das System ist zu den in Service-Level-Agreement vereinbarten Zeiten in Betrieb und bereit zur Benützung.
- **Security** (Sicherheit): Das System ist gegen unberechtigten phyischen oder logischen Zugriff geschützt.
- **Integrity** (Integrität): Die Verarbeitung durch das System erfolgt vollständig, akkurat, zeitgerecht und autorisiert.
- **Maintainability** (Wartbarkeit): Das System kann bei Bedarf in einer Weise erneuert werden, in der Verfügbarkeit, Sicherheit und Integrität gesichert sind.

Die Kriterien sind jeweils in die folgenden Bereiche unterteilt [vgl. AIC02-1]:

- Es wurden Performancevorgaben, Richtlinien und Standards für das System definiert und kommuniziert.
- Es stehen angemessene Prozeduren, Personal, Software, Daten und Infrastruktur zur Verfügung, um die Ziele in den Richtlinien und Standards erreichen zu können.
- Die Systeme werden überwacht und es werden Aktionen gesetzt, um die Richtlinien und Standards einzuhalten und die gesetzten Ziele zu erreichen.

Exkurs: Struktur des nachfolgenden Standard „Trust Services“

Wie oben beschrieben, ist von den Herausgebern des Standard geplant, diesen und den unten beschriebenen SysTrust durch sogenannte „Trust Services“ abzulösen, aus Grund der Vollständigkeit und der Aktualität möchte ich die Strukturierung darstellen.

Nach einer kurzen Einleitung sind die Prinzipien aufgelistet:

- Security (Sicherheit)
- Availability (Verfügbarkeit)
- Processing Integrity (Integrität)
- Online Privacy (Privatsphäre)
- Confidentiality (Vertraulichkeit)

Die Kriterien sind wie in den WebTrust Programmen in vier Kapitel gegliedert, jedoch wird nicht mehr von *„Disclosures“* (Veröffentlichungen), sondern von *„Communications“* (Nachrichtenwesen, Kommunikationen [vgl. LEO02]) gesprochen.

- **Policies:** Es wurden schriftlich Policies erstellt. Der Begriff „policies“ wird als schriftliche Stellungnahmen („written statements“) des Management beschrieben, die die Intention, die Ziele, Anforderungen, Verantwortlichkeiten und/oder Standards zu einem bestimmten Thema enthalten. Diese Stellungnahmen können explizit als „policies“ (hier würde ich den Begriff mit „Grundsätze“ oder „Anweisungen“ übersetzen) oder auch implizit (als Kommunikation mit Benutzern oder Ablaufbeschreibungen) vorliegen, dies jedoch allenfalls schriftlich. [vgl. AIC02-3, S 6]
    - Erstellung und Freigabe von Policies
    - Anforderungen an die Policies
    - Verantwortung für Änderungen

- **Communications:** Die Kommunikation der Policies an autorisierte Personen ist geregelt
  - Beschreibung des Systems
  - Kommunikation an Benutzer, an Programmierer etc.
- **Procedures:** Es werden Verfahren verwendet, um die Ziele in Übereinstimmung mit den Policies zu erreichen
  - Sicherheitskriterien wie logischer und physischer Zugriffsschutz, Virenschutz, Verschlüsselung, Korrekturverfahren etc.
  - Erstellung und Verwaltung des Systems und erforderliche Qualifikation des Personals
  - Wartung des Systems inklusive der entsprechenden Autorisierungserfordernisse und Testverfahren bei Änderungen
  - Verfügbarkeitskriterien mit präventiven (z.B. Datensicherung, pyhsischer Schutz) und korrektiven Maßnahmen (z.B. Wiederanlaufpläne)
- **Monitoring:** Das System wird überwacht und bei Bedarf werden angemessene Maßnahmen zur Sicherstellung der Einhaltung der Policies getroffen
  - Art und Umfang der Leistungsmessung (Performance-Monitoring) sowohl technischer Natur als auch organisatorischer Leistungsindikatoren
  - Identifikation von Schwächen und Ergreifung entsprechender Maßnahmen
  - Überwachung von technologischen Veränderungen und deren Einflüsse auf die Prinzipien.

Zu jedem Prinzip sind die detaillierten Kriterien mit beispielhaften Kontrollen angeführt.

2.2.13 COBIT [vgl. ISA00-1, ISA00-2, ISA00-3, ISA00-4, ISA00-5, ISA00-6]

Art

Ursprünglich war COBIT eine Sammlung von Kontrollzielen als Unterstützung im Rahmen von IT-Revisionen. Heute stellt COBIT eine Sammlung von Veröffentlichungen dar, die als allgemein akzeptierter Standard für IT-Sicherheit und IT-Kontrolle bezeichnet werden können, und die ein Modell ergeben, das von Mitgliedern des Managements, Anwendern, Auditoren und Sicherheitsfachleuten angewandt werden kann. In COBIT wird von einem „*framework*“ gesprochen, das laut Heinrich mit „*Rahmenvorschlag*“ [vgl.

HEI98, S 447 übersetzt wird und das einer Grundkonzeption im Rahmen eines Systementwurfes Anwendung findet, im Gegensatz dazu verwende ich den deutschsprachigen Begriff eines Modells, das nach Heinrich als „*Im allg. S. jede vereinfachende Abbildung eines Ausschnitts der Wirklichkeit oder eines Vorbilds für die Wirklichkeit (Beschreibungsmodell), [...]*“ definiert wird [HEI98, S 359], was der Bedeutung des Begriffs „*framework*“ im Rahmen von COBIT meines Erachtens näher kommt. [vgl. ISA02-1]

Zielsetzung

“The COBIT Mission: To research, develop, publicise 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.” [ISA00-2, S 1]

Herausgeber

Der Standard wurde ursprünglich von der ISACF publiziert, die aktuelle Version ist gemeinsam mit dem „IT Governance Institute“ veröffentlicht.

Zielgruppe

Als Zielgruppe sind sowohl Unternehmen, als auch Prüfungseinrichtungen wie z.B. Wirtschaftsprüfuer, Rechnungshöfe etc. relevant.

Aktualität

COBIT ist auf sehr hohem Niveau und aktuell, derzeit wird an einer Erweiterung, gearbeitet. Das Modell an sich und die derzeit gültigen Komponenten werden jedoch nicht geändert, sondern lediglich um andere Aspekte erweitert (z.B. sind Benchmarks vorgesehen, um Branchenvergleiche durchführen zu können, eine Variante „COBIT-Light“ ist in Planung etc.).

Vollständigkeit

COBIT ist von der Breite als der umfangreichste Standard im Rahmen der IT Governance anzusehen, die Tiefe ist – obwohl keine technischen Details angegeben werden – als relativ groß anzusehen, da aus den Kontrollzielen ähnlich dem ISO/IEC 17799:2000 sehr leicht die notwendigen Maßnahmen abzuleiten sind.

Internationalität

COBIT ist international weit verbreitet, in Österreich jedoch noch wenig bekannt.

Möglichkeit einer Zertifizierung

Es besteht derzeit keine Möglichkeit, nach COBIT zertifiziert zu werden.

Inhalt

Der IT Governance Ansatz von COBIT

Enterprise Governance (Die oben diskutierte Corporate Governance wird in Rahmen von COBIT als Enterprise Governance bezeichnet.) und IT Governance sind interdependent und dürfen nicht isoliert betrachtet werden. Die IT wurde lange als unterstützender, abgeschlossener Teil der strategischen Unternehmensführung gesehen, sie muss jedoch integraler Bestandteil derselben sein. [vgl. ISA00-3, S 8].

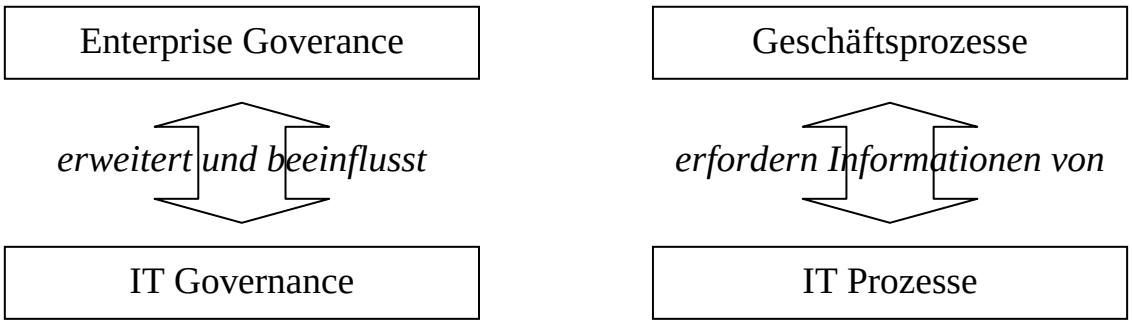


Abb 6: Zusammenhang zwischen IT und Kerngeschäft [vgl. ISA02-3, S 9]

Aus diesem Ansatz heraus sind die IT Prozesse nicht Selbstzweck, sondern liefern an die Geschäftsprozesse die geforderten Informationen, die den definierten Informationskriterien entsprechen.

Aus diesem Grund ist es Aufgabe der Unternehmensleitung – um die gesetzten Ziele im Unternehmen zu erreichen – die IT zu steuern, mit anderen Worten: IT Governance zu betreiben.

Der historische Kern von COBIT und auch der Namensgeber des Modells liegt in den Kontrollzielen. Aus diesen ist ersichtlich, dass COBIT ursprünglich ein Modell zu ex-post Überprüfung der IT war, das hauptsächlich von Wirtschaftsprüfern und Revisoren in Verwendung war. Seit der Version 3 ist COBIT durch die Verfügbarkeit der Management Guidelines ein Modell zur Steuerung der IT Prozesse, also ein Modell, mit Hilfe dessen IT Governance betrieben werden kann.

Geschichte und Bestandteile

Die Bestandteile der Version 3 sind aus der auf der nächsten Seite abgebildeten Abb 7. dargestellt. COBIT hat seinen Ursprung in einer Sammlung von 318

Kontrollzielen („Control Objectives“), die nach 34 Prozessen in 4 Domänen strukturiert sind.

Die Strukturierung der einzelnen IT Prozesse nach Domänen und diese wiederum als IT Prozess ist im Framework enthalten. Ebenfalls Bestandteil des Framework (das inhaltsgleich auch in den Control Objectives ist) sind 34 High-Level Kontrollziele, die nach einem Wasserfallmodell aufgebaut sind. Die Details sind weiter unten beschrieben.

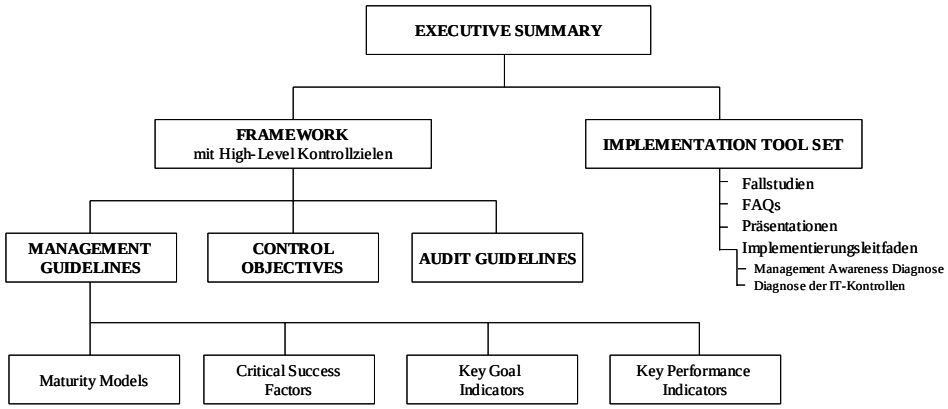


Abb 7: Bestandteile von COBIT 3rd Edition [vgl. ISA00-5, S 19]

Die Kurzfassung („Management Summary“) richtet sich an Geschäftsführer und enthält eine kurze Beschreibung der Ansätze von COBIT, sowie eine Beschreibung des Prozesses „*Governance over information technology and its processes*“ in der Form der Management Guidelines.

Die „Audit Guidelines“ beinhalten eine Anleitung zur Überprüfung der IT Governance. Als diesbezügliches, allgemeines Modell für die Vorgehensweise eines Audits ist die folgende angegeben, aus der ersichtlich ist, dass aus den geschäftsgetriebenen Ereignissen über die Ressourcen Informationen nach unterschiedlichen Kriterien zur Verfügung gestellt werden:

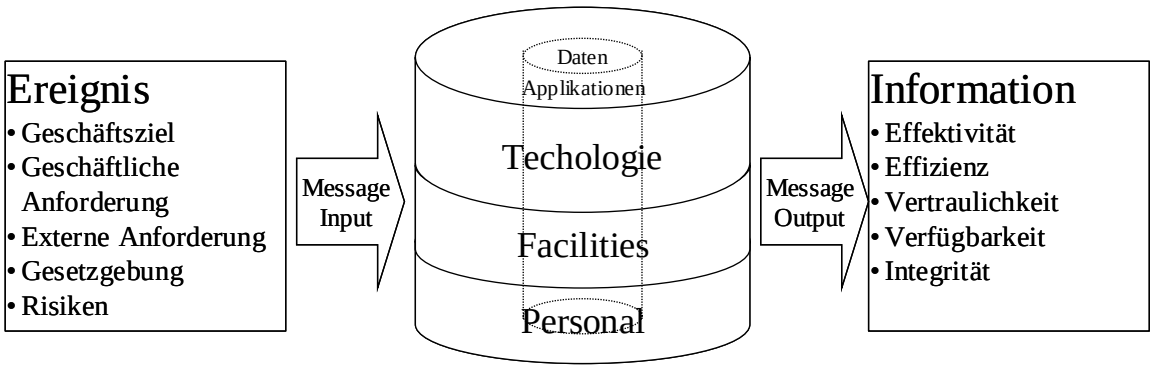


Abb 8: Vorgehensweise bei einem Audit nach COBIT [vgl. ISA00-6, S 15]

Die „Management Guidelines“ (der eigentliche Kern des IT Governance Ansatzes im Sinne der Steuerung der IT in Unternehmen) enthalten neben dem High-Level Kontrollziel die kritischen Erfolgsfaktoren („*Critical Success Factors*“), die Zielerreichungsindikatoren („*Key Goal Indicators*“), die Leistungsindikatoren („*Key Performance Indicators*“) und eine Beschreibung der unterschiedlichen Reifegrade der 34 IT Prozesse und des IT Governance Prozesses aus den „Management Guidelines“ an Hand des Reifegradmodells („*Maturity Model*“).

Das „Implementation Tool Set“ enthält Fallstudien zur Einführung von COBIT, einen Fragen- und Antwortkatalog (Frequently Asked Questions), Präsentationen zur Bewusstseinsbildung, einen Fragebogen zur Feststellung des Bewusstseins der Geschäftsleitung und Fragebögen zur Diagnose der bestehenden Risiken und Kontrollen.

Die Geschichte von COBIT ist wie folgt

1996: Erste Version der Control Objectives for Information and related Technology, herausgegeben von der Information Systems Audit and Control Foundation (ISACF)

1998: Version 2 der Kontrollziele, deren Anzahl durch Aufnahme von neuen Kontrollzielen erhöht wurde, Veröffentlichung des „*Implementation Tool Set*“

2000: Veröffentlichung der Version 3, die jedoch nicht nur durch die Stiftung ISACF sondern durch das 1998 durch ISACF und ISACA gegründete IT Governance Institute.

2002: Für Herbst des Jahres 2002 ist die Version 4 zu erwarten.

IT Prozess nach CobiT

Der IT Prozess wird in COBIT in vier Domänen (Domains) unterteilt und ist in der Abbildung 9 dargestellt, wobei dies die Sichtweise einer einzelnen Leistung (wobei der Begriff der Leistung als Übersetzung des englischen Begriffs „Service“ ist, also beispielsweise in der Zur-Verfügung-Stellung einer Applikation für eine funktionale Abteilung zu verstehen ist) und nicht des Gesamtprozesses IT ist.

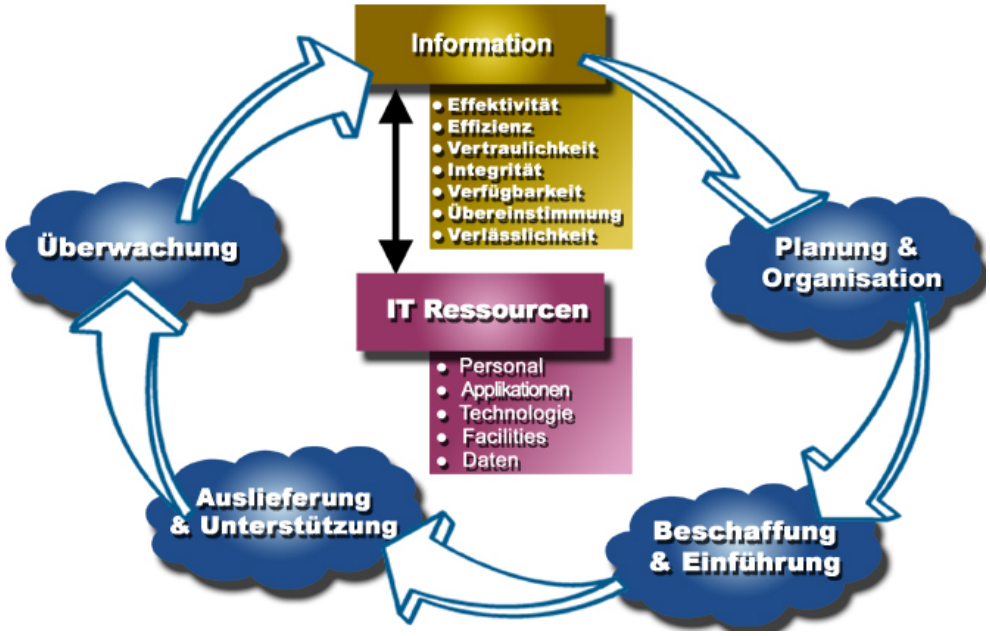


Abb 9: Der COBIT IT Prozess in 4 Domänen (blaue Wolken) mit den Informationskriterien und den IT Ressourcen [vgl. ISA00-3, S 7]

Nach dieser Darstellung ist jede Einzelleistung zu planen, beziehungsweise mit dem bestehenden Plänen und Strukturen abzustimmen, in der Folge zu beschaffen und einzuführen und danach auszuliefern sowie für die laufende Unterstützung zu sorgen und die entsprechenden Überwachungsmaßnahmen zu setzen, die bei Abweichungen in einen neuerlichen Durchlauf münden.

Aus Sicht des Gesamtprozesses bevorzuge ich die folgende Darstellung in Abbildung 10, die den übergeordneten Charakter der Domäne Überwachung darstellt. Ebenso wird die Beeinflussung von Neueinführung und laufenden Betrieb durch die Domäne Planung und Organisation verdeutlicht und nicht von einer einzelnen Leistung ausgegangen, sondern von der Gesamtheit der Aufgaben der IT aus der Sichtweise der IT Governance. IT Governance betrachtet die Aufgaben der IT nicht nur auf Basis des Top-Down-Ansatzes (Vergleiche hierzu die Abbildung 11), sondern aus der abstrahierten Sicht der Übergreifenden Aufgabe der IT, also der Unterstützung der Geschäftsprozesse, verdeutlicht.

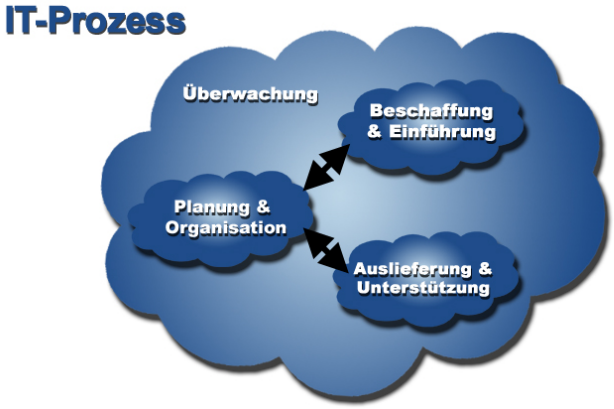


Abb 10: Der IT Prozess, und die übergeordnete Domäne der Überwachung

Die Hauptaufgaben der einzelnen Prozesse in den Domänen sind zusammengefasst:

- **PO – Planning and Organisation** (Planung und Organisation)
  - Strategische und taktische Vorgaben für die IT
  - Sicherstellung der Einhaltung der Geschäftsziele
  - Adäquate Planung, Kommunikation und Management
  - Geeignete organisatorische und technische Strukturen und Regelungen
- **AI – Aquisistion and Implementation** (Beschaffung und Einführung)
  - Umsetzung der Strategie
  - Lösungen, die identifiziert, entwickelt oder gekauft und implementiert werden
  - Lösungen, die in den Geschäftsprozess integriert werden
  - Änderungswesen und Wartung
- **DS – Delivery and Support** (Auslieferung und Unterstützung)
  - Zeitgerechte Leistung von benötigten Leistungen
  - Effektive Sicherheit inklusive Training
  - Sicherstellung der Supportprozesse
  - Verarbeitung der Daten
- **M – Monitoring** (Überwachung)
  - Regelmäßige Bewertung der IT Prozesse
  - Einhaltung und Qualität der Kontrollen
  - Unabhängige Informations- und Zertifizierungseinholung

Diese Domänen sind wiederum in Prozesse unterteilt:

- Planung und Organisation
  - **PO 1 – Define a strategic IT plan** (Definition des strategischen IT-Plans)

  - **PO 2 – Define the information architecture** (Definition der Informationsarchitektur)
  - **PO 3 – Determine technological direction** (Bestimmung der technologischen Richtung)
  - **PO 4 – Define the IT organisation and relationships** (Definition der IT-Organisation und ihrer Beziehungen)
  - **PO 5 – Manage the IT investment** (Verwaltung der IT-Investitionen)
  - **PO 6 – Communicate management aims and direction** (Kommunikation von Unternehmenszielen und –richtung)
  - **PO 7 – Manage human resources** (Personalwesen)
  - **PO 8 – Ensure compliance with external requirements** (Sicherstellung der Einhaltung externer Anforderungen)
  - **PO 9 – Assess risks** (Risikobeurteilung)
  - **PO 10 – Manage projects** (Projektmanagement)
  - **PO 11 – Manage quality** (Qualitätsmanagement)
- Beschaffung und Einführung
  - **AI 1 – Identify automated solutions** (Identifikation von Lösungen)
  - **AI 2 – Acquire and maintain application software** (Beschaffung und Unterhalt von Anwendungssoftware)
  - **AI 3 – Develop and maintain procedures** (Beschaffung und Unterhalt der technischen Architektur)
  - **AI 4 – Acquire and maintain technology** infrastructure (Entwicklung und Unterhalt von IT-Verfahren)
  - **AI 5 – Install and accredit systems** (Installation und Akkreditierung von Systemen)
  - **AI 6 – Manage changes** (Änderungswesen)
- Auslieferung und Unterstützung
  - **DS 1 – Define and manage service levels** (Definition von Dienstleistungsgraden (SLAs))
  - **DS 2 – Manage third-party services** (Handhabung der Leistungen von Drittparteien)
  - **DS 3 – Manage performance and capacity** (Leistungs- und Kapazitätsmanagement)
  - **DS 4 – Ensure continuous service** (Sicherstellung der kontinuierlichen Dienstleistung)
  - **DS 5 – Ensure systems security** (Sicherstellung der Systemsicherheit)
  - **DS 6 – Identify and allocate costs** (Identifikation und Zuordnung von Kosten)

- **DS 7 – Educate and train users** (Aus- und Weiterbildung der Benutzer)
- **DS 8 – Assist and advise customers** (Unterstützung und Beratung von IT-Kunden)
- **DS 9 – Manage the configuration** (Konfigurationsmanagement)
- **DS 10 – Manage problems and incidents** (Umgang mit Problemen und Vorfällen)
- **DS 11 – Manage data** (Verwaltung von Daten)
- **DS 12 – Manage facilities** (Verwaltung von Einrichtungen)
- **DS 13 – Manage operations** (Management des Operating)

- Monitoring
  - **M 1 – Monitor the processes** (Überwachung der Prozesse)
  - **M 2 – Assess internal control adequacy** (Beurteilung der Angemessenheit der internen Kontrollen)
  - **M 3 – Obtain independent assurance** (Einholung einer unabhängigen Bestätigung)
  - **M 4 – Provide for independent audit** (Für unabhängige Revision sorgen)

Abstrahiert ist der Top-Down Ansatz wie folgt zusammengefasst:

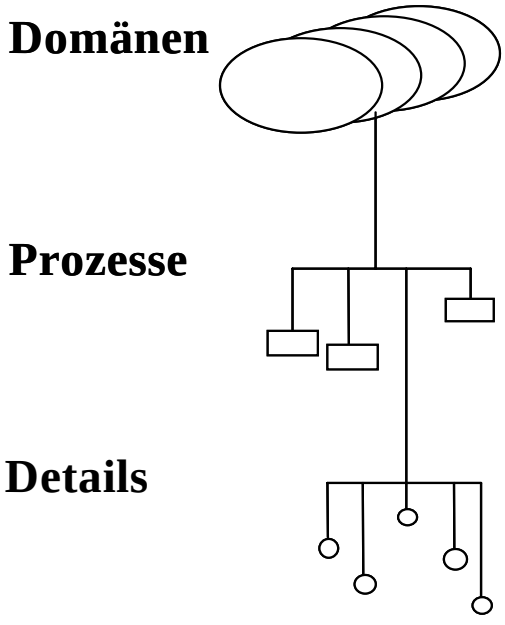


Abb 11: Top-Down Ansatz des IT Prozesses nach COBIT [vgl. ISA00-3, S 16]

Eine weitere Unterteilung erfolgt durch die Angabe von:

- High-Level Kontrollziel
- Detaillierte Kontrollziele

- Informationskriterien die durch den Prozess beeinflusst werden
- IT-Ressourcen, die verwendet werden
- Typische Ausprägung nach Reifegrad
- Kritische Erfolgsfaktoren
- Key Performance Indicators
- Key Goal Indicators

Informationskriterien
Die Informationskriterien (Information Criteria) sind wie folgt strukturiert:

- **Qualitätsanforderungen**
  - Effektivität – Information ist für den Geschäftsprozess relevant und angemessen und steht rechtzeitig, korrekt, konsistent und benutzbar zur Verfügung.
  - Effizienz – Die Bereitstellung der Information erfolgt durch die optimale Verwendung von Ressourcen, sowohl aus Sicht der Nutzenbetrachtung als auch aus ökonomischer Sicht.
- **Sicherheitsanforderungen**
  - Vertraulichkeit – Schutz vertraulicher Information vor unautorisierter Offenlegung.
  - Integrität – Information ist vollständig und akkurat sowie entsprechend der Erwartungen stichhaltig.
  - Verfügbarkeit – Die Information ist bei Bedarf des Geschäftsprozesses und auch künftig verfügbar. Verfügbarkeit umfasst auch die Absicherung notwendiger Ressourcen und die Sicherung der Verfügbarkeit notwendiger Ressourcen.
- **Ordnungsmäßigkeitskriterien**
  - Übereinstimmung – die Information stimmt mit Gesetzen, Verträgen und sonstigen Verpflichtungen überein.
  - Verlässlichkeit – Die Vorhaltung von angemessenen Informationen für das Management zur Führung des Unternehmens und um den Informations- und Offenlegungsverpflichtungen nachkommen zu können. [vgl. ISA00-3, S 24]

IT-Ressourcen
Die IT-Ressourcen sind laut COBIT:

- Daten – Objekte im weitesten Sinne (z.B. intern und extern, strukturiert und unstrukturiert, Grafiken, Töne, etc.).
- Applikationen: Die Summe manueller und programmierter Arbeitsschritte
- Technologien – Umfasst Hardware, Beriebssysteme, Datenbankmanagementsysteme, Netzwerk etc.

- Facilities – Die beherbergenden Ressourcen (z.B. Gebäude) und Infrastruktureinrichtungen (z.B. Strom, Telekommunikationseinrichtungen).
- Personal – Personal, Fähigkeiten, Bewusstsein und Fähigkeit. Informationssysteme zu planen, zu organisieren, zu beschaffen, zu unterstützen, zu bedienen und zu überwachen. [vgl. ISA00-3, S 24]

Würfel

Die Zusammenstellung der oben beschriebenen Komponenten IT Prozesse, Informationskriterien und IT-Ressourcen erfolgt wie COBIT mit COBIT Würfel, der aus Abbildung 12 ersichtlich ist.

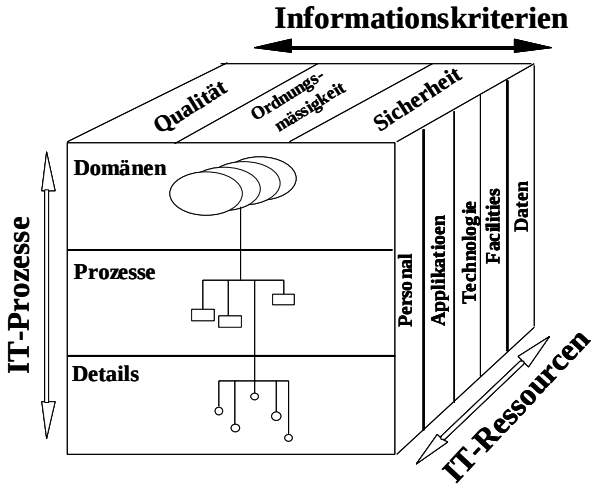


Abb 12: COBIT Würfel [vgl. ISA00-3, S 16]

Wasserfallmodell

Das Wasserfallmodell, enthält und beschreibt das High-Level Kontrollziel, ist für jeden Prozess gleich aufgebaut und fokussiert die Kontrollen auf die Erfüllung der Geschäftsanforderungen. Das Wasserfallmodell ist in Abbildung 13 dargestellt.

Durch das Wasserfallmodell ist die klare Verbindung zwischen der Anforderung des Geschäftsprozesses oder der Anforderung des Kerngeschäfts und dem IT Prozess erkennbar.

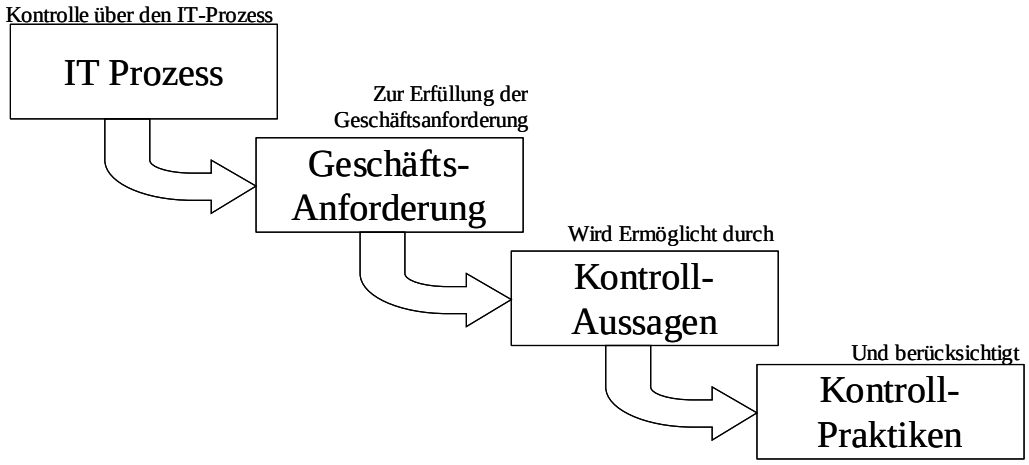


Abb 13: High-Level Kontrollziele nach dem COBIT Wasserfallmodell [vgl. ISA00-1, S 21]

Detaillierte Kontrollziele

Nach COBIT ist **"Control"** definiert als: *„the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected."* [ISA00-4, S 13] und **"Control Objective"** als: *"a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity."* [ISA00-4, S 13]
Demzufolge ist ein Kontrollziel die Vorgabe für das gewünschte Verhalten bei Aktivität unter der Berücksichtigung der eingesetzten Kontrollen, die ihrerseits – in der Form von Anweisungen, Ablaufbeschreibungen und ähnlichem – unerwünschtes Verhalten verhindern, aufdecken und korrigieren sollen.

Je nach IT Prozess sind diesem zwischen 3 und 30 detaillierte Kontrollziele zugeordnet, in Summe sind 318 Kontrollziele vorhanden.

Reifegradmodel

In Anlehnung an das „Capability Maturity Model^{SM} for Software" [vgl. PAU03] wurde ein Reifegradmodell für die IT Prozesse entwickelt und die typischen Ausprägungen des Prozesses, je nach Reifegrad definiert.

Die Reifegrade sind:

0 **Nicht Vorhanden (Non-Existent):** Ein erkennbarer Prozess ist nicht vorhanden und die Organsiation hat den Bedarf einer Aktivität nicht erkannt.
1 A**d hoc (Initial):** Es sind Anzeichen vorhanden, dass die Organisation die Aufgabe erkannt hat und diese in Angriff genommen werden sollten. Es sind jedoch keine standardisierten Abläufe vorhanden, sondern die

Aufgaben werden individuell unterschiedlich und ad hoc gelöst. Die gesamte Vorgehensweise ist nicht organisiert.

2 **Wiederholbar (Repeatable):** Prozesse wurden soweit entwickelt, dass Abläufe durch unterschiedliche Personen auf ähnliche Weise durchgeführt werden. Es wird keine formale Schulung oder Kommunikation der Abläufe durchgeführt; die Verantwortlichkeit für den Problemlösungsweg ist individuell. Es existiert eine hohe Abhängigkeit vom Wissen Einzelner und Fehler sind wahrscheinlich.

3 **Definiert (Defined):** Abläufe wurden standardisiert, dokumentiert und in Schulungen kommuniziert. Es besteht jedoch keine Verpflichtung, nach dem definierten Ablauf vorzugehen und es ist nicht wahrscheinlich, dass Abweichungen erkannt werden. Die Abläufe sind nicht hoch entwickelt oder detailliert beschrieben, stellen jedoch die angewandte Praxis dar.

4 **Überwacht (Managed):** Es besteht die Möglichkeit, den Prozess zu überwachen und die Einhaltung der definierten Abläufe sicherzustellen sowie bei suboptimalen Abläufen oder nicht eingehaltenen Abläufen entsprechende korrektive Maßnahmen zu setzen. Die Prozesse werden laufend verbessert und sind hoch entwickelt. Automatisierte und/oder durch Werkzeuge unterstützte Abläufe sind rar und nicht integriert.

5 **Optimiert (Optimised):** Prozesse sind nach den Best Practices definiert, sie basieren auf dem Ergebnis der kontinuierlichen Verbesserung und der Zusammenarbeit mit externen Organisationen. Die IT stellt eine in den Workflow integrierte Einheit dar, sie stellt Werkzeuge zur Verfügung, die die Qualität und Effektivität des Unternehmens erhöht und dem Unternehmen eine schnelle Anpassung erlauben. [vgl. ISA00-2, S 11]

Mit diesem Reifegradmodell stimme ich überein, mit Ausnahme des letzten Satzes der Stufe 5, denn auch in anderen Stufen kann die IT durchaus in der Lage sein, integrierte Werkzeuge zu erstellen und zu betreiben, lediglich die Wahrscheinlichkeit, dass mit höherer Reife der IT Prozesse die Qualität der Werkzeuge und folglich auch die Effizienz der gesamten Organisation steigt, ist höher. Meines Erachtens sollte der Satz lauten: „Der Prozess ist durchgehend in einem Workflow abgebildet und Schnittstellen zu anderen Prozessen sind definiert; es werden integriert Werkzeuge verwendet, die geänderte Anforderungen erkennen helfen und darauf eine rasche Reaktion ermöglichen.“

Durch die Verwendung des Reifegradmodells ist es – auch für außenstehende Personen – relativ einfach, die Reife der einzelnen Prozesse festzustellen. Durch Vergleich des Reifegrades des Prozesses mit jenem anderer Organisationen oder durch den Vergleich mit Standards und durch das Setzen von Zielen kann der

Zielreifegrad für jeden Prozess definiert werden und die Maßnahmen für die Zielerreichung können eruiert werden.

Kritische Erfolgsfaktoren (CSF)
Die kritischen Erfolgsfaktoren sind nach der Zielsetzung durch den Reifegrad die zweite Möglichkeit für die Geschäftsführung, jene Strukturen zu schaffen, die IT Prozesse benötigen, um den gesetzten Zielreifegrad und somit den Output in den angestrebten Kriterien erbringen zu können. Die kritischen Erfolgsfaktoren sind auf strategischer, taktischer und administrativer Ebene definiert, wenngleich diese Unterscheidung lediglich in der Einleitung der Management Guidelines explizit erfolgt [vgl. ISA00-2, S 14], in den Erfolgsfaktoren, die zu den Prozessen angeführt sind, erfolgt diese Unterscheidung nicht.

Allgemein erfolgt in COBIT die Steuerung des Prozesses durch das Setzen von Standards für einen Prozess und der laufenden oder periodischen Messung auf Abweichung vom Standard und dem Einleiten von korrektiven Maßnahmen. Diese Vorgehensweise entspricht im wesentlichen dem kybernetischen Prinzip, das nach Heinrich *„Die systematische Anwendung des Prinzips der Regelung und Steuerung als spezifische Form des Verhaltens eines Systems zur Erreichung des Systemgleichgewichts.“* [HEI98, S 320] ist. Ein Beispiel aus dem Alltag verdeutlicht diese Vorgehensweise: Durch die Einstellung eines Temperaturreglers wird eine Standardtemperatur (Standard) für ein Heizungssystem (Prozess) gesetzt. Ein Temperaturfühler misst die Temperatur (Messwert) und Abweichungen werden durch Vergleich mit dem Standard (Prüfung) festgestellt und bei Bedarf die Heizung eingeschaltet (Korrektur).

Zusammenfassend wird dies an Hand der folgenden Grafik festgehalten:

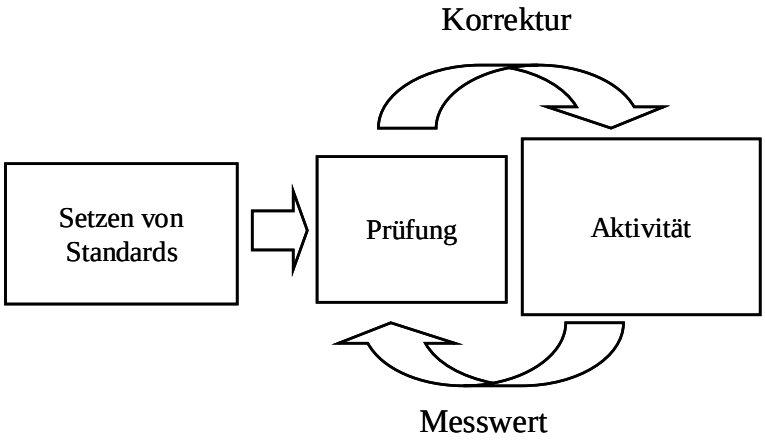


Abb 14: Steuerung eines Prozesses

In Zusammenhang mit IT Governance möchte ich nochmals die IT Governance Illustration darstellen, die auf die oben beschriebene Vorgehensweise zurückgeht:

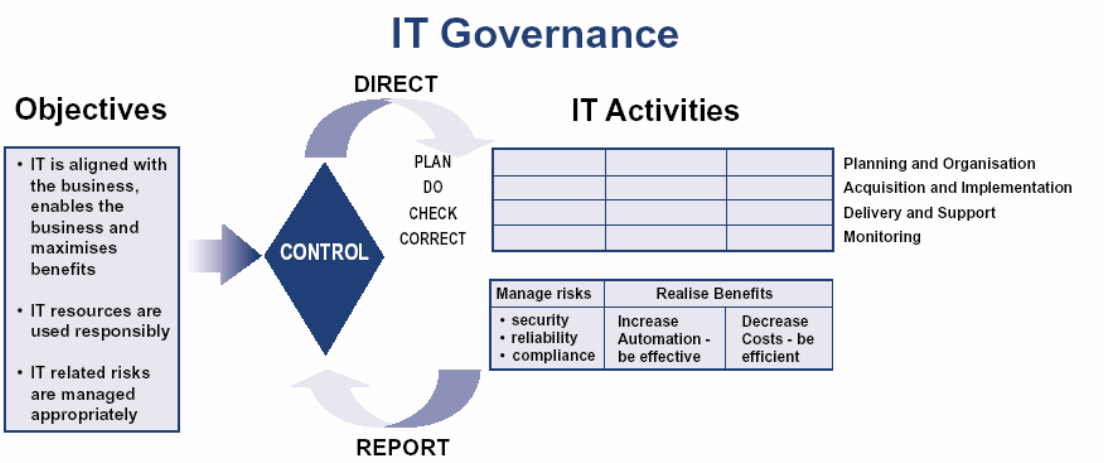


Abb 15: Steuerung des IT Prozesses durch Vorgabe von Zielen und kritischen Erfolgsfaktoren [vgl. ISA00-2, S 15]

Die CSF sind in drei Gruppen eingeteilt:

- Für alle Prozesse zutreffend
  - Prozesse sind definiert und dokumentiert
  - Die Erwartungen an den Output des Prozesses sind bekannt (Anforderungen der Kunden)
  - Die für die Prozesse zur Verfügung stehenden Ressourcen werden angemessen verwaltet
  - Die Leistung wird nach finanziellen Gesichtspunkten, Zufriedenheitsmaßzahlen, nach Effektivität des Prozesses gemessen und es wird die Angemessenheit des Prozesses geprüft und die IT-Leitung wird entsprechend der Zielerreichung belohnt.
  - Die erforderliche Qualität der Mitarbeiter (Schulung, Weitergabe von Wissen, Moral etc.) und die Verfügbarkeit der Fähigkeiten ist durch geeignete Maßnahmen (Rekrutierung, Bindung, Umschulung) gesichert.
  - Ein kontinuierlicher Verbesserungsprozess ist im Einsatz.
- Für die meisten Prozesse zutreffend
  - Alle am Prozess beteiligten und die vom Prozess (auch indirekt) betroffenen (z.B. Geschäftsführer, Benutzer, etc.) sind sich der Risiken, der Bedeutung und dem Möglichkeiten der IT bewusst und von diesen Personengruppen ist mit Unterstützung zu rechnen.
  - Die Ziele und Vorgaben sind für den jeweiligen Prozess bekannt, ebenso wie die Verantwortung bezüglich der Leistung des

Prozesses zugewiesen ist, wie Prozesse die Zielerreichung ermöglichen und wie dies überwacht wird.
    - Personen sind zielorientiert und verfügen über richtige und ausreichende Information über Prozesse des Prozesskunden, interne Prozesse und über die Konsequenzen ihrer Entscheidungen.
    - Die Unternehmenskultur lässt abteilungsübergreifende Zusammenarbeit, Teamwork zu und eine Klutur der kontinuierliche Verbesserung ist etabliert.
    - Die wichtigen Abläufe sind harmonisiert und erfolgen einheitlich (z.B. Änderungswesen, Problemmanagement und Konfigurationsmanagement)
    - Die Verwendung von Kontrollen dient dazu, die effiziente und effektive Nutzung der Ressourcen zu sichern und die Effektivität der Prozesse zu verbessern.
- Auf IT Governance zutreffend
    - Die Verwendung von Kontrollen dient dazu, die Transparenz zu erhöhen, Komplexität zu verringern, zu lehren, Flexibilität und Skalierbarkeit zu ermöglichen und eine Störung des internen Kontrollsystems ebenso, wie die Übersicht und Transparenz zu verhindern.
    - Die Verwendung von Methoden, die einen Überblick verschaffen: eine Kultur von Kontrolle, ein Verhaltenskodex, üblicherweise und laufend angewandte Risikobewertung, Selbsteinschätzung, formale Prüfung der Einhaltung externer Standards, Überwachung von Risiken und von Abweichungen.
    - IT Governance ist anerkannt, definiert und in die Corporate Governance integriert und von der Geschäftsleitung sind klare Vorgaben für die Strategie, Risikomanagement, Kontrollsysteme und eine Sicherheitspolitik vorhanden.
    - IT Governance ist auf wichtige IT-Projekte, Änderungs- und Qualitätsverbesserungsmöglichkeiten, Bewusstseinsbildung für wichtige IT Prozesse, Verantwortlichkeiten und die Ressourcenverwendung und -potentialausschöpfung fokussiert.
    - Eine Kontrollinstanz (Audit Komitee) ist etabliert, die Auditoren überwacht, die Kontrolle über Erstellung und Ausführung des Auditplans übernimmt und die Prüfung Ergebnisse einer Überprüfung und die Abarbeitung offener Punkte aus einer internen oder externen Überprüfung sicherstellt.

Zielerreichungsindikatoren (KGI)

Wie oben dargestellt, erfüllt jeder IT Prozess im Rahmen des High-Level Kontrollziels eine Anforderung des Geschäfts. Diese Anforderungen werden mit den *„Key Goal Indicators“* gemessen. Durch das Wasserfallmodell ist dies wie folgt darstellbar:

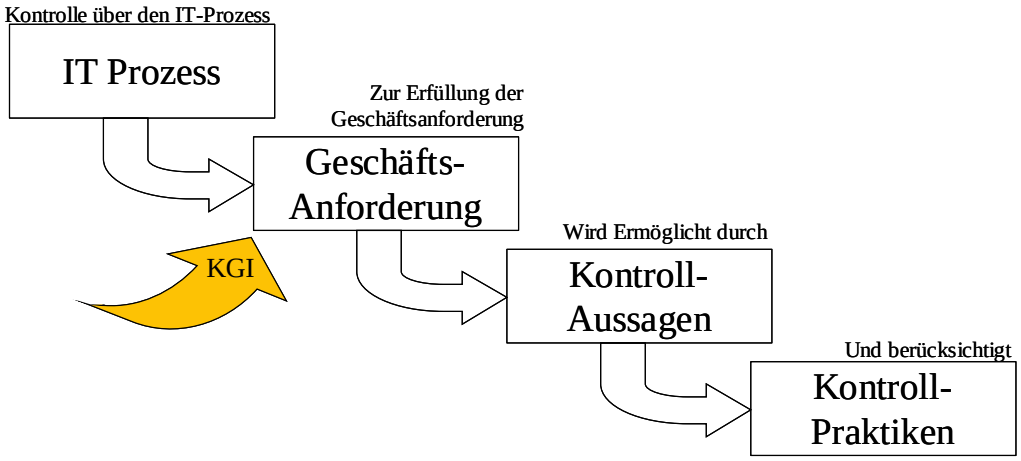


Abb 16: Key Goal Indicators zeigen die Erfüllung der Anforderungen des Geschäfts an

In der Festlegung des Prozessablaufs soll die Messung der Zielerreichung fixer Bestandteil im Ablauf des Prozesses sein, so wird zum Beispiel im Prozess PO 10 (Manage Projects) als KGI „Anzahl der Projekte, die innerhalb der Zeit- und Budgetvorgaben fertiggestellt wurden“ angeführt. Dies erfordert im Prozess sowohl die Aktivität der Festlegung des Zeit- und Finanzbudgets, sowie die Aktivität der Überprüfung und Dokumentation der tatsächlich aufgewandten Mittel.

Auf eine weitere Ausführung über die Messung und eine Darstellungsmöglickeit in einer Balanced Business Scorecard oder ähnlichem möchte ich verzichten, da dies nicht den Kern der Arbeit darstellt und den Rahmen derselben sprengen würde. Es sei lediglich darauf hingewiesen, dass die Transparenz eines Prozesses für nicht am Prozess beteiligte durch die Verfügbarkeit von Messgrößen und Messwerten, die in ein Messsystem eingebunden sind, im Grunde erst ermöglicht wird.

Leistungsindikatoren (KPI)

Im Gegensatz zu den KGI sind die Key Performance Indikatoren auf die Ressourcen und die IT Prozesse fokussiert und drücken darob die Qualität des Ressourcenmanagements und der Prozessperformance aus, dies immer mit dem Ziel, die Prozesse und deren Performance zu verbessern.

Beispiele für derartige Indikatoren sind:

- Verfügbarkeit der Anwendungen
- Antwortzeiten
- Anzahl des geschulten Personals
- Anzahl unbesetzter Stellen
- ...

2.2.14 Zusammenfassung

Die Breite (Umfang) und die Tiefe (Detaillierung) der analysierten Standards stellt sich in einer Übersicht wie folgt dar:

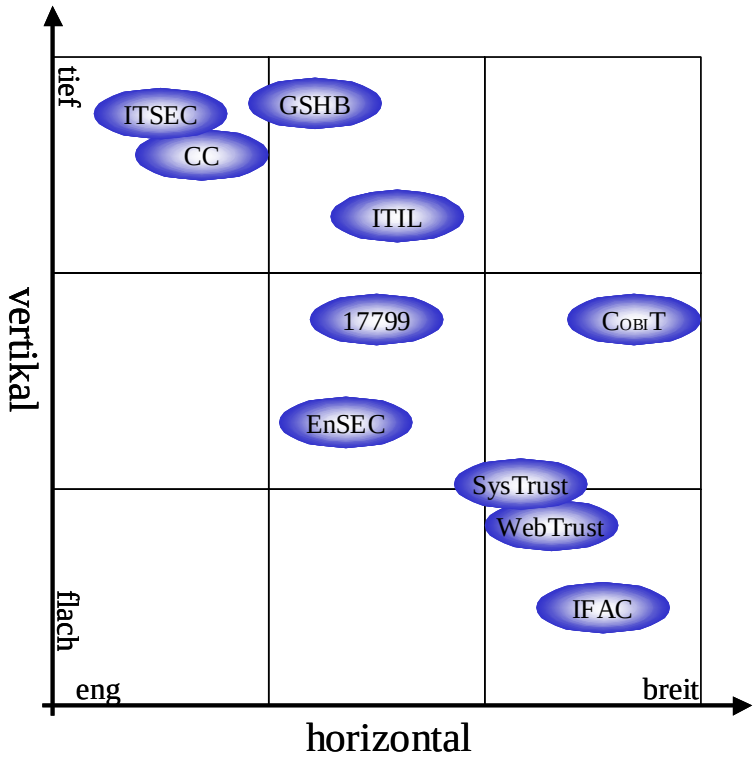


Abb 17: Umfang und Detaillierung der untersuchten Standards

Wie erwartet, ist CobiT der breiteste Standard. Die sehr technisch orientierten Standards ITSEC und die Common Criteria, das IT-Grundschutzhandbuch und ITIL sind inhaltlich nicht derart umfassend, oder wie oben bezeichnen breit. Die Zertifizierungsstandards WebTrust und SysTrust sind breit, jedoch nicht detailliert, die Standards der Informationssicherheit liegen in beiden Kriterien im Mittelfeld.

3 Praxisteil

Im praktischen Teil möchte ich die Inhalte der oben beschriebenen Werke den Prozessen und Kontrollzielen von COBIT zuordnen. Dies auch unter jener Begründung, dass im Rahmen einer Einführung bzw. der Implementierung von COBIT in einer Organisation die Berücksichtigung unterschiedlicher Standards gefordert ist. Auch ohne eine Konkrete Anforderung durch eine Organisation, erlaubt die Berücksichtigung unterschiedlicher Standards die möglichst vollständige Abdeckung der Aufgaben der IT im Rahmen eines Implementierungsprojektes.

Wie oben erwähnt, werden auch die Policies des HIPAA zugeordnet. Auf die Zuordnung des sehr speziellen Standards ITSEC möchte ich verzichten, da dieser konzentriert auf die Sicherheit eines Produktes detaillierte Kriterien im Rahmen der Überprüfung der Herstellung des Produktes darstellt und möchte es mit der Aussage belassen, dass der Standard in seiner Gesamtheit der AI-Domäne zuzuordnen ist.

Von den einzelnen Standards werden die folgenden Teile zugeordnet:

ISO/IEC 17799:2000	Maßnahmenkatalog, somit ist auch der British Standard 7799 abgedeckt
IT-GSHB	Maßnahmenkatalog
Common Criteria	Kriterienkatalog der „Functional Criteria“
ITIL	Die Teile “Service and Support” und “Service Delivery”, die anderen Werke standen nicht zur Verfügung.
IFAC IT Guidelines	Approach der Richtlinie 2 (Planung), 3 (Beschaffung von Technologie) und 4 (Beschaffung von Anwendungen). Die Richtlinie 1 enthält die Prinzipien, keine Kontrollen, Maßnahmen oder Kriterien, die Richtlinien 5 („*IT Service Delivery and Support*“) und 6 („*IT Monitoring*“) sind mit den entsprechenden COBIT-Domänen deckungsgleich und textlich fast gleichlautend, diese wurden folglich nicht zugeordnet.
EnSEC	„Allgemeiner Anforderungskatalog“
WebTrust und SysTrust	Kriterienkatalog des Nachfolgestandards „Trust Services“
HIPAA	HIPAA Security Policies Manual

Tabelle 2: Standards, die zugeordnet werden

3.1 Vorgehen der Zuordnung

Nachdem die entsprechenden Kapitel nach Verfügbarkeit von notwendigen Maßnahmen, der Anführung von Kriterien oder Anleitungen identifiziert wurden, werden diese in einem ersten Schritt strukturell harmonisiert.

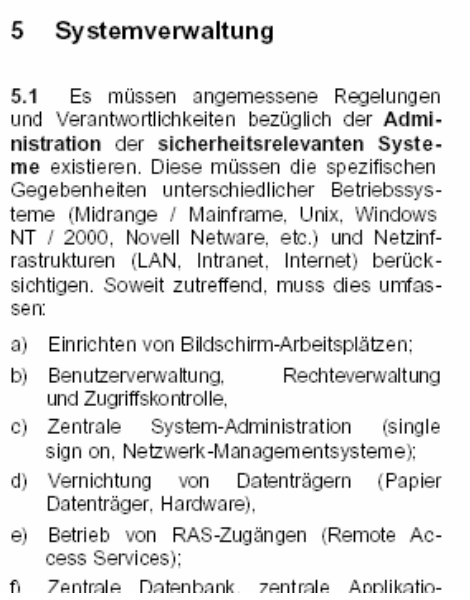
Die Harmonisierung verläuft folgendermaßen:

- **Aufteilung** der in den Werken angeführten Anforderungen, Maßnahmen etc. in Einheiten, die einem Kontrollziel zuordenbar sind
- **Gliederung** der Einheiten, damit eine Zuordnung nach der Aufteilung möglich ist und der Gesamtzusammenhang nicht verloren geht. Der Zusammenhang ist für das rasche Verständnis über den Inhalt der Einheit unter Umständen unabdingbar. Aus diesem Grund bleiben die Überschriften etc. erhalten, ihnen kommt nicht nur in der Nummerierung zentrale Bedeutung zu, sondern speziell für eine spätere, retrograde Zuordnung.
- **Zuordnung** der Einheiten zu einem COBIT Prozess und einem in diesem Prozess angeführten Kontrollziel
    - Falls die Einheit mehreren Kontrollzielen zugeordnet werden kann, erfolgt eine Mehrfachzuordnung
    - Falls die Einheit einem COBIT-Prozess gesamtheitlich zugeordnet werden kann, wird sie dem von mir eingefügten Kontrollziel Nummer Null zugeordnet
    - Falls die Einheit keinem Kontrollziel zugeordnet werden kann, wird dieses dem von mir eingeführten Prozess Null zugewiesen um den Bedarf eines weiteren Prozesses zu erkennen und diesen entsprechend den Anforderungen aus anderen Standards zu beschreiben.

Diese Vorgehensweise möchte ich an Hand eines Beispiels aus dem Standard EnSEC erläutern:

3.1.1 Erster Schritt: Aufteilung der Anforderungen

Originaltext (Ausschnitt aus dem Standard):



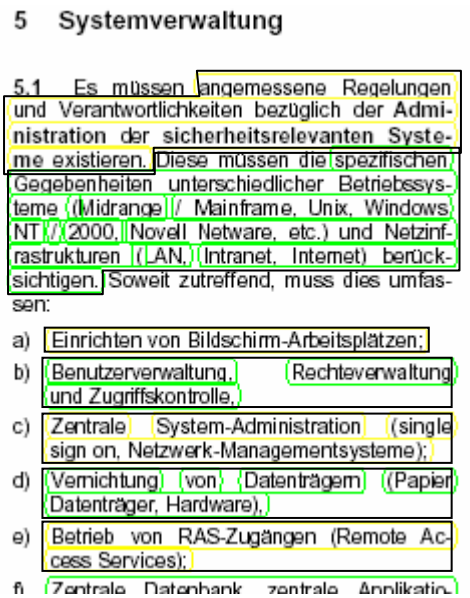
5 Systemverwaltung

5.1 Es müssen angemessene Regelungen und Verantwortlichkeiten bezüglich der **Administration** der **sicherheitsrelevanten Systeme** existieren. Diese müssen die spezifischen Gegebenheiten unterschiedlicher Betriebssysteme (Midrange / Mainframe, Unix, Windows NT / 2000, Novell Netware, etc.) und Netzinfrastrukturen (LAN, Intranet, Internet) berücksichtigen. Soweit zutreffend, muss dies umfassen:

a) Einrichten von Bildschirm-Arbeitsplätzen;
b) Benutzerverwaltung, Rechteverwaltung und Zugriffskontrolle,
c) Zentrale System-Administration (single sign on, Netzwerk-Managementsysteme);
d) Vernichtung von Datenträgern (Papier Datenträger, Hardware),
e) Betrieb von RAS-Zugängen (Remote Access Services);
f) Zentrale Datenbank zentrale Applikatio-

Abb 18: Originaltext aus dem EnSEC Anforderungskatalog

Aus diesem werden die folgenden Einheiten definiert und farblich und durch Umrahmung gekennzeichnet, wobei die unterschiedlichen Farben nicht wertend sind, sondern lediglich die Unterscheidung der Einheiten ermöglichen sollen:



5 Systemverwaltung

5.1 Es müssen angemessene Regelungen und Verantwortlichkeiten bezüglich der Administration der sicherheitsrelevanten Systeme existieren. Diese müssen die spezifischen Gegebenheiten unterschiedlicher Betriebssysteme (Midrange / Mainframe, Unix, Windows NT / 2000, Novell Netware, etc.) und Netzinfrastrukturen (LAN, Intranet, Internet) berücksichtigen. Soweit zutreffend, muss dies umfassen:

a) Einrichten von Bildschirm-Arbeitsplätzen;
b) Benutzerverwaltung, Rechteverwaltung und Zugriffskontrolle,
c) Zentrale System-Administration (single sign on, Netzwerk-Managementsysteme);
d) Vernichtung von Datenträgern (Papier Datenträger, Hardware),
e) Betrieb von RAS-Zugängen (Remote Access Services);
f) Zentrale Datenbank zentrale Applikatio-

Abb 19: Identifikation der Einheiten

3.1.2 Zweiter Schritt: Gliederung

Die Einheiten werden so gegliedert, dass nach einer erfolgten Zuordnung zu einem Kontrollziel die Rückverfolgbarkeit ermöglicht wird. Es ist beispielsweise nicht auf einfache und schnelle Weise die Einheit „Vernichtung von Datenträgern (Papier, Datenträger, Hardware)“ dem EnSEC Kapitel der Systemverwaltung zuzuordnen, nach der erfolgten Gliederung ist dies jedoch sehr wohl möglich.

Das Ergebnis der Gliederung ist wie folgt:

- EnSEC 5: Systemverwaltung
- EnSEC 5.1: angemessene Regelungen und Verantwortlichkeiten bezüglich der Administration der sicherheitsrelevanten Systeme
- EnSEC 5.1.1: nach unterschiedlichen Betriebssystemen gegliedert (Midrange / Mainframe, Unix, Windows NT / 2000, Novell Netware, etc.)
- EnSEC 5.1.2: Netzinfrastrukturen (LAN, Intranet, Internet) sind berücksichtigt
- EnSEC 5.1.3: Einrichten von Bildschirm-Arbeitsplätzen
- EnSEC 5.1.4: Benutzerverwaltung, Rechteverwaltung und Zugriffskontrolle
- EnSEC 5.1.5: Zentrale System-Administration (single sign on, Netzwerk-Managementsysteme)
- EnSEC 5.1.6: Vernichtung von Datenträgern (Papier Datenträger, Hardware)
- EnSEC 5.1.7: Betrieb von RAS-Zugängen (Remote Access Services)

3.1.3 Dritter Schritt: Zuordnung

Nach der oben beschriebenen Vorgehensweise wird das Kontrollziel, bzw. bei Bedarf die Kontrollziele zugeordnet, wobei bei einer mehrfachen Zuordnung die zuzuordnende Einheit nach Bedarf vervielfältigt wird. Die Überschrift (EnSEC 5: Systemverwaltung) wird nicht zugeordnet, wie erwähnt dient sie der Gliederung.

EnSEC Einheit	COBIT Prozess	COBIT Kontrollziel
EnSEC 5.1 angemessene Regelungen und Verantwortlichkeiten bezüglich der Administration der sicherheitsrelevanten Systeme	PO 4 – Define the IT Organisation and Relationships	PO 4.4 Roles and Responsibilities
EnSEC 5.1 angemessene Regelungen und Verantwortlichkeiten bezüglich der Administration der sicherheitsrelevanten Systeme	DS 13 – Manage Operations	DS 13.1 Processing Operations Procedures and Instructions Manual
EnSEC 5.1.1 nach unterschiedlichen Betriebssystemen gegliedert (Midrange / Mainframe, Unix, Windows NT / 2000, Novell Netware, etc.)	DS 13 – Manage Operations	DS 13.1 Processing Operations Procedures and Instructions Manual
EnSEC 5.1.2 Netzinfrastrukturen (LAN, Intranet, Internet) sind berücksichtigt	DS 13 – Manage Operations	DS 13.1 Processing Operations Procedures and Instructions Manual
EnSEC 5.1.3 Einrichten von Bildschirm-Arbeitsplätzen	AI 4 – Acquire and Maintain Technology Infrastructure	AI 3.4 System Software Installation
EnSEC 5.1.4 Benutzerverwaltung, Rechteverwaltung und Zugriffskontrolle	DS 5 – Ensure Systems Security	DS 5.4 User Account Management
EnSEC 5.1.5 Zentrale System-Administration (single sign on, Netzwerk- Managementsysteme)	DS 5 – Ensure Systems Security	DS 5.9 Central Identification and Access Rights Management
EnSEC 5.1.6 Vernichtung von Datenträgern (Papier Datenträger, Hardware)	DS 11 – Manage Data	DS 11.18 Protection of Disposed Sensitive Information
EnSEC 5.1.7 Betrieb von RAS-Zugängen (Remote Access Services)	DS 13 – Manage Operations	DS 13.8 Remote Operations
EnSEC 5.1.7 Betrieb von RAS-Zugängen (Remote Access Services)	DS 5 – Ensure Systems Security	DS 5.20 Firewall Architectures and Connections with Public Networks

Tabelle 3: Zuordnung zu COBIT-Kontrollzielen

Durch eine Sortierung nach COBIT Prozess und Kontrollziel ist das Ergebnis aus dem obigen Beispiel:

PO 4.4 Roles and Responsibilities
EnSEC 5.1 angemessene Regelungen und Verantwortlichkeiten bezüglich der Administration der sicherheitsrelevanten Systeme
AI 3.4 System Software Installation
EnSEC 5.1.3 Einrichten von Bildschirm-Arbeitsplätzen
DS 5.4 User Account Management
EnSEC 5.1.4 Benutzerverwaltung, Rechteverwaltung und Zugriffskontrolle
DS 5.9 Central Identification and Access Rights Management
EnSEC 5.1.5 Zentrale System-Administration (single sign on, Netzwerk- Managementsysteme)
DS 5.20 Firewall Architectures and Connections with Public Networks
EnSEC 5.1.7 Betrieb von RAS-Zugängen (Remote Access Services)
DS 11.18 Protection of Disposed Sensitive Information
EnSEC 5.1.6 Vernichtung von Datenträgern (Papier Datenträger, Hardware)
DS 13.8 Remote Operations
EnSEC 5.1.7 Betrieb von RAS-Zugängen (Remote Access Services)
DS 13.1 Processing Operations Procedures and Instructions Manual
EnSEC 5.1 angemessene Regelungen und Verantwortlichkeiten bezüglich der Administration der sicherheitsrelevanten Systeme
EnSEC 5.1.1 nach unterschiedlichen Betriebssystemen gegliedert (Midrange / Mainframe, Unix, Windows NT / 2000, Novell Netware, etc.)
EnSEC 5.1.2 Netzinfrastrukturen (LAN, Intranet, Internet) sind berücksichtigt

Tabelle 4: Ergebnis der Zuordnung

Mit der obigen Tabelle ist auch ersichtlich, dass die retrograde Zuordnung möglich ist, so ist dem Kontrollziel DS 13.8 die Einheit 5.1.7 von EnSEC zugeordnet. Über die ursprüngliche Gliederung ist erkennbar, dass es sich um Regelungen in der Systemverwaltung handelt und nicht etwa um Konfigurationsrichtlinien oder ähnliches.

3.2 Durchführung der Zuordnung

Die oben angeführten Standards werden nach der angeführten Vorgehensweise aufgeteilt und den Prozessen und Kontrollzielen zugeordnet.

Da das Ergebnis der Zuordnungen lediglich ein Zwischenergebnisse darstellt, wird dieses auf Grund des Umfangs hier nicht angeführt

In der Zuordnung wurde zur Unterscheidung der Ursprungswerke (wie bereits oben im Beispiel gezeigt) eine Kurzbezeichnung der Standards mit eingefügt, wobei die Abkürzungen wie folgt gewählt wurden:

Werk(e)	**Abkürzung**
ISO/IEC 17799:2000	ISO17799
IT-Grundschutzhandbuch	BSI
Common Criteria / ISO/IEC 15408	CC
ITIL Service Delivery ITIL Service Support	ITIL-SD ITIL-SS
IFAC IT Guideline 2 IFAC IT Guideline 3 IFAC IT Guideline 4	IFAC-2 IFAC-3 IFAC-4
EnSEC	EnSEC
WebTrust und SysTrust	Trust
HIPAA	HIPAA

Tabelle 5: In der Zuordnung verwendete Abkürzungen

In der Folge sind die Ergebnisse der Zuordnung je Standard und in Summe zusammengefasst:

3.2.1 ISO/IEC 17799:2000

Anzahl der zugeordneten Einheiten:	130
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	34
Anzahl mehrfach zugeordneter Einheiten	0
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	0
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	21
Anzahl der Kontrollziele, zu denen zugeordnet wurde	66

Tabelle 6: Übersicht über das Ergebnis der Zuordnung des ISO/IEC 17799:2000

Die Verteilung ist in der folgenden Grafik abgebildet:

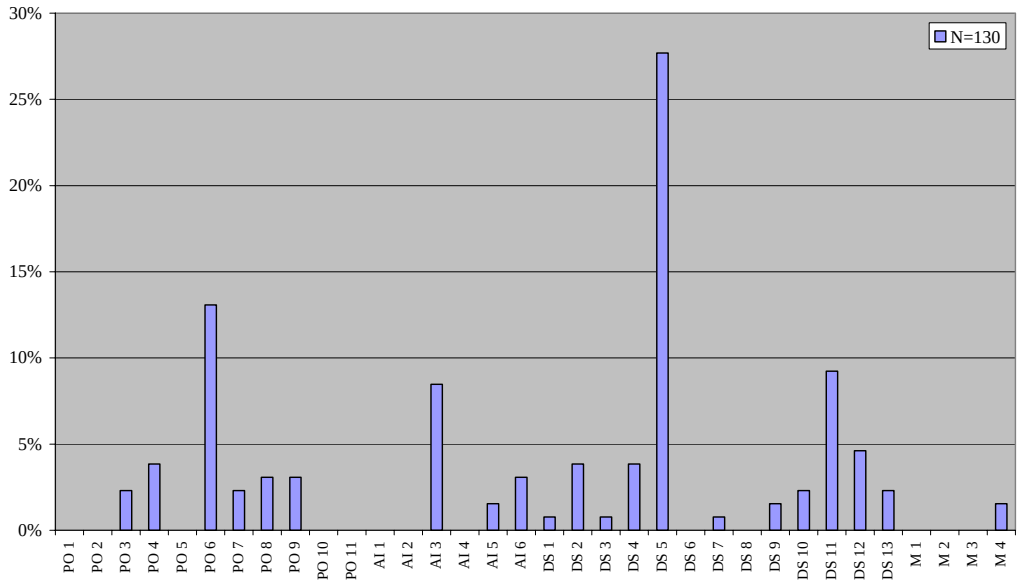


Abb 20: Verteilung von ISO/IEC 17799:2000 im Verhältnis zu COBIT

3.2.2 IT-Grundschutzhandbuch

Anzahl der zugeordneten Einheiten:	608
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	0
Anzahl mehrfach zugeordneter Einheiten	2
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	0
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	25
Anzahl der Kontrollziele, zu denen zugeordnet wurde	107

Tabelle 7: Übersicht über das Ergebnis der Zuordnung des IT-Grundschutzhandbuches

Die Verteilung ist in der folgenden Grafik abgebildet:

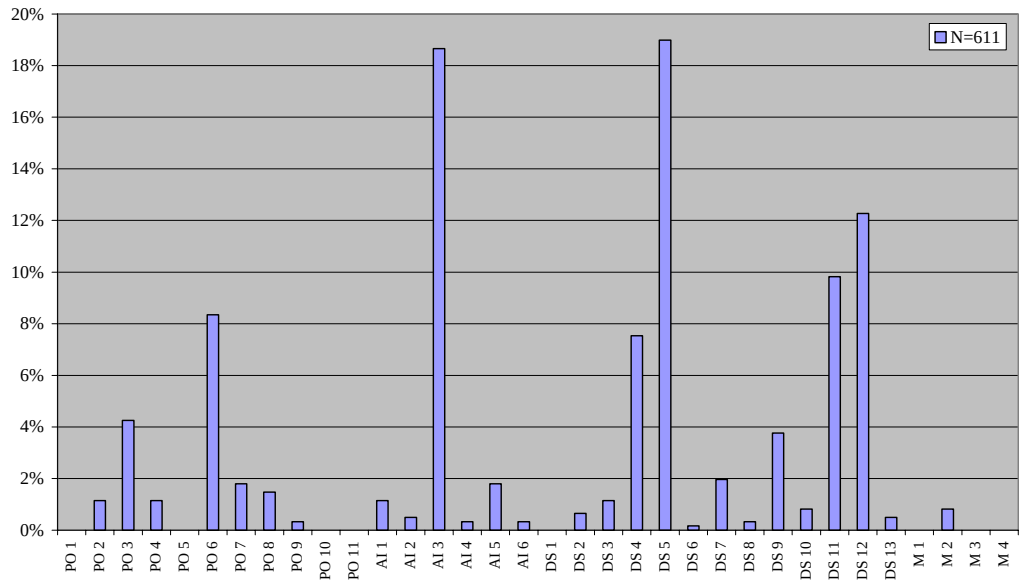


Abb 21: Verteilung des BSI IT-Grundschutzhandbuches im Verhältnis zu COBIT

3.2.3 Common Criteria / ISO/IEC 15408

Anzahl der zugeordneten Einheiten:	68
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	19
Anzahl mehrfach zugeordneter Einheiten	2
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	0
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	7
Anzahl der Kontrollziele, zu denen zugeordnet wurde	31

Tabelle 8: Übersicht über das Ergebnis der Zuordnung der Common Criteria

Die Verteilung ist in der folgenden Grafik abgebildet:

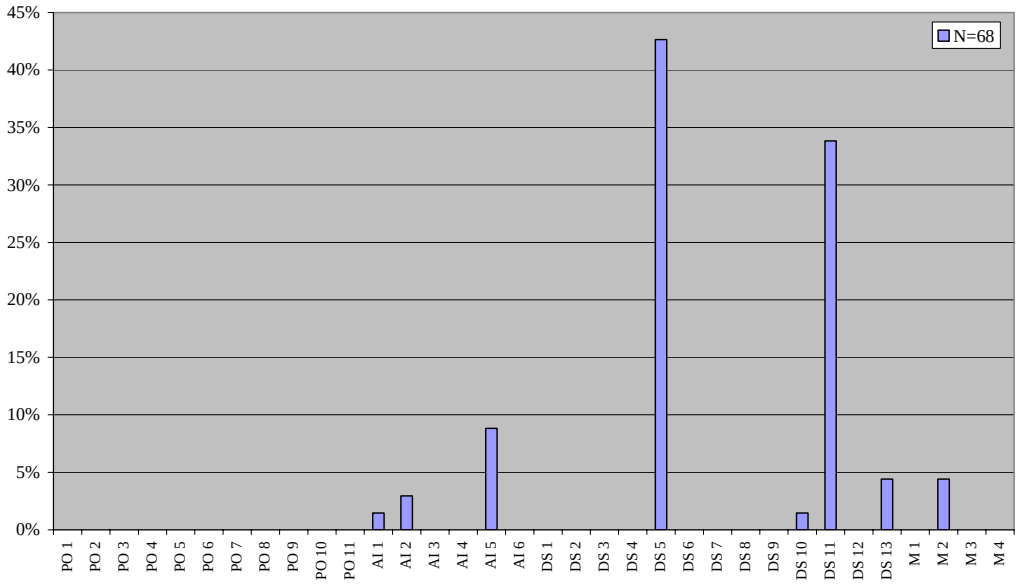


Abb 22: Verteilung der Common Criteria im Verhältnis zu COBIT

3.2.4 ITIL Service Delivery

Es wurden nicht nur Überschriften der Kapitel mit Maßnahmencharakter nicht zugeordnet, sondern auch Überschriften von Einleitungen, Aufzählungen etc.). Daraus ergibt sich die relativ hohe Zahl an nicht zugeordneten Einheiten.

Anzahl der zugeordneten Einheiten:	61
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	28
Anzahl mehrfach zugeordneter Einheiten	4
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	22
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	17
Anzahl der Kontrollziele, zu denen zugeordnet wurde	38

Tabelle 9: Übersicht über das Ergebnis der Zuordnung des ITIL Werkes „Service Delivery“

Die Verteilung ist in der folgenden Grafik abgebildet:

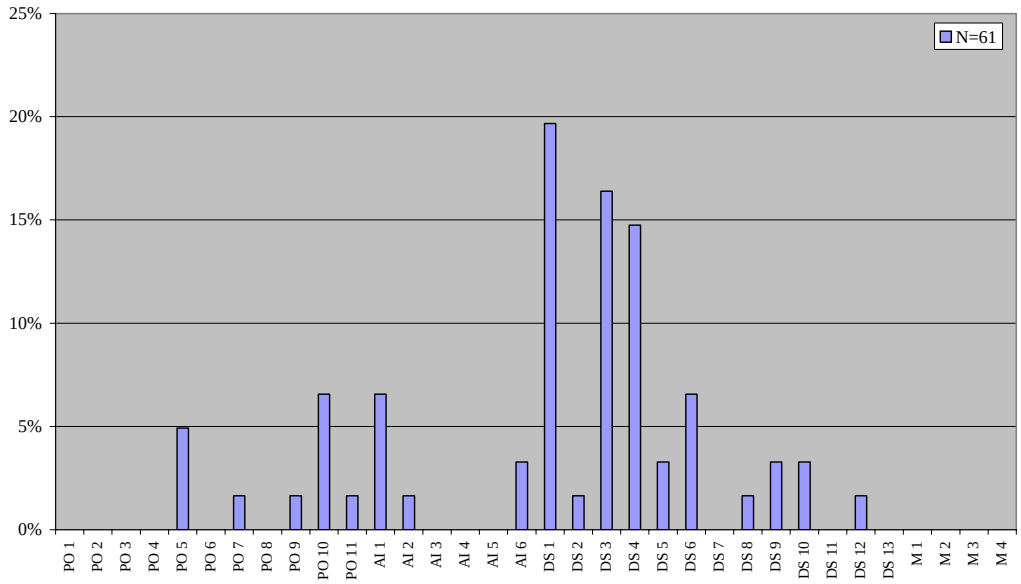


Abb 23: Verteilung von ITIL Service Delivery im Verhältnis zu COBIT

3.2.5 ITIL Service Support

Es wurden nicht nur Überschriften der Kapitel mit Maßnahmencharakter nicht zugeordnet, sondern auch Überschriften von Einleitungen, Aufzählungen etc. Die Kapitel 2 und 3 wurden bereits im Rahmen der Zuordnung von ITIL Service Delivery behandelt.

Anzahl der zugeordneten Einheiten:	52
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	31
Anzahl mehrfach zugeordneter Einheiten	0
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	14
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	8
Anzahl der Kontrollziele, zu denen zugeordnet wurde	28

Tabelle 10: Übersicht über das Ergebnis der Zuordnung des ITIL Werkes „Service Support“

Die Verteilung ist in der folgenden Grafik abgebildet:

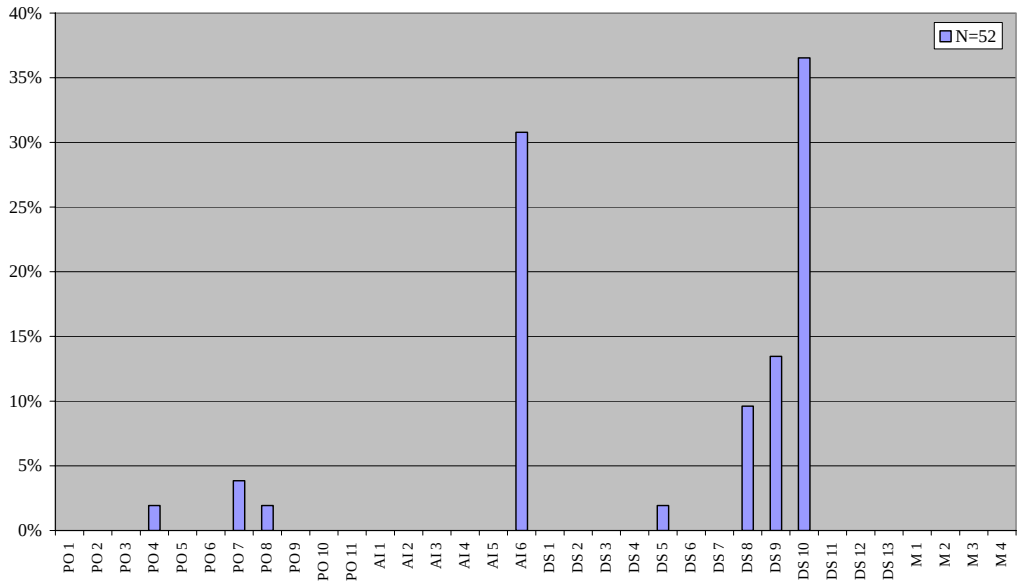


Abb 24: Verteilung von ITIL Service Support im Verhältnis zu COBIT

3.2.6 IFAC IT Guideline 2

Anzahl der zugeordneten Einheiten:	69
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	9
Anzahl mehrfach zugeordneter Einheiten	0
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	0
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	2
Anzahl der Kontrollziele, zu denen zugeordnet wurde	7

Tabelle 11: Übersicht über das Ergebnis der Zuordnung der IFAC IT Guideline 2

Die Verteilung ist in der folgenden Grafik abgebildet:

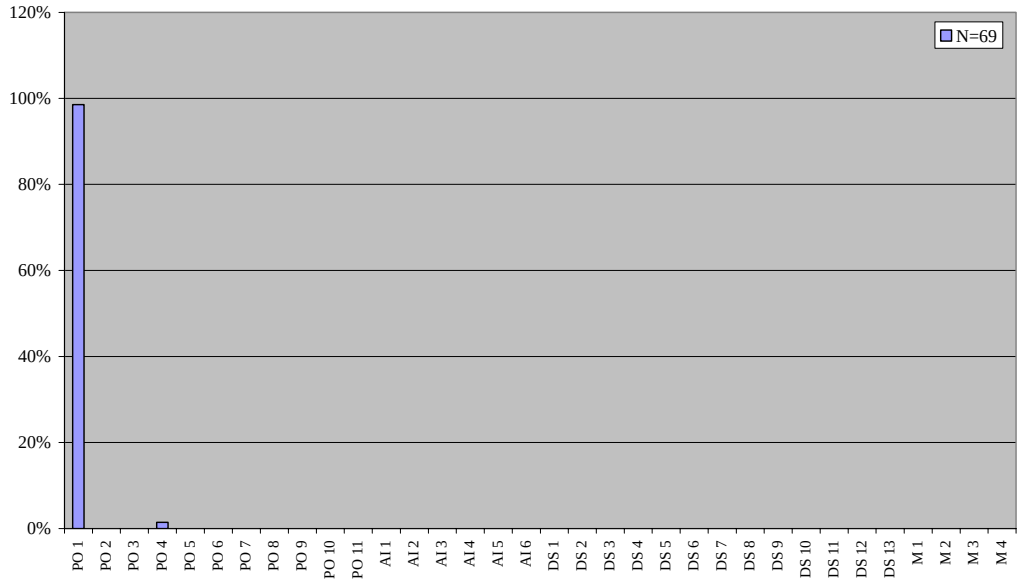


Abb 25: Verteilung der IFAC Richtlinie 2 (Planung) im Verhältnis zu COBIT

3.2.7 IFAC IT Guideline 3

Anzahl der zugeordneten Einheiten:	68
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	3
Anzahl mehrfach zugeordneter Einheiten	1
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	0
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	3
Anzahl der Kontrollziele, zu denen zugeordnet wurde	16

Tabelle 12: Übersicht über das Ergebnis der Zuordnung der IFAC IT Guideline 3

Die Verteilung ist in der folgenden Grafik abgebildet:

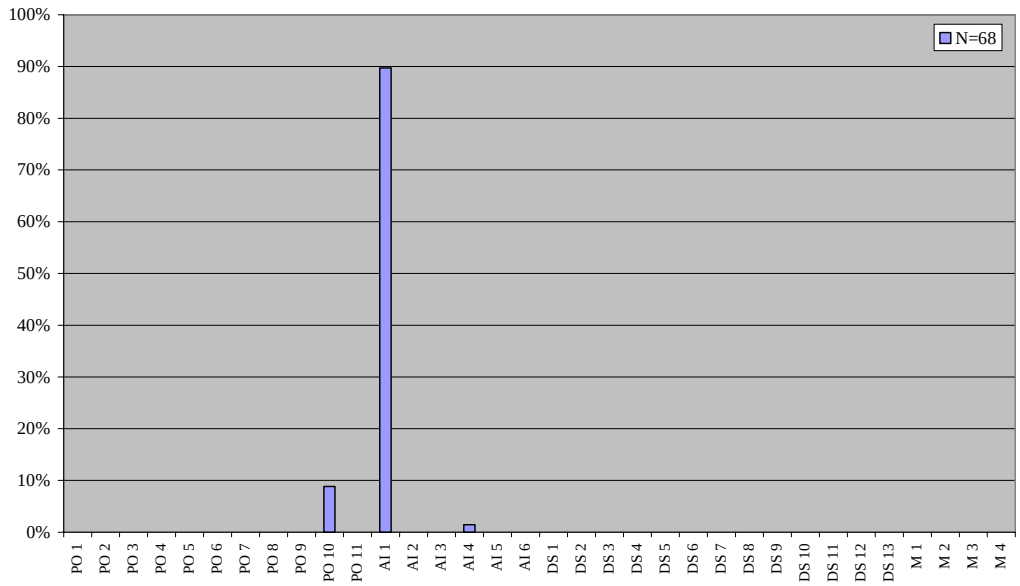


Abb 26: Verteilung der IFAC Richtlinie 3 (Beschaffung von Technologie) im Verhältnis zu COBIT

3.2.8 IFAC IT Guideline 4

Anzahl der zugeordneten Einheiten:	43
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	14
Anzahl mehrfach zugeordneter Einheiten	3
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	3
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	12
Anzahl der Kontrollziele, zu denen zugeordnet wurde	25

Tabelle 13: Übersicht über das Ergebnis der Zuordnung der IFAC IT Guideline 4

Die Verteilung ist in der folgenden Grafik abgebildet:

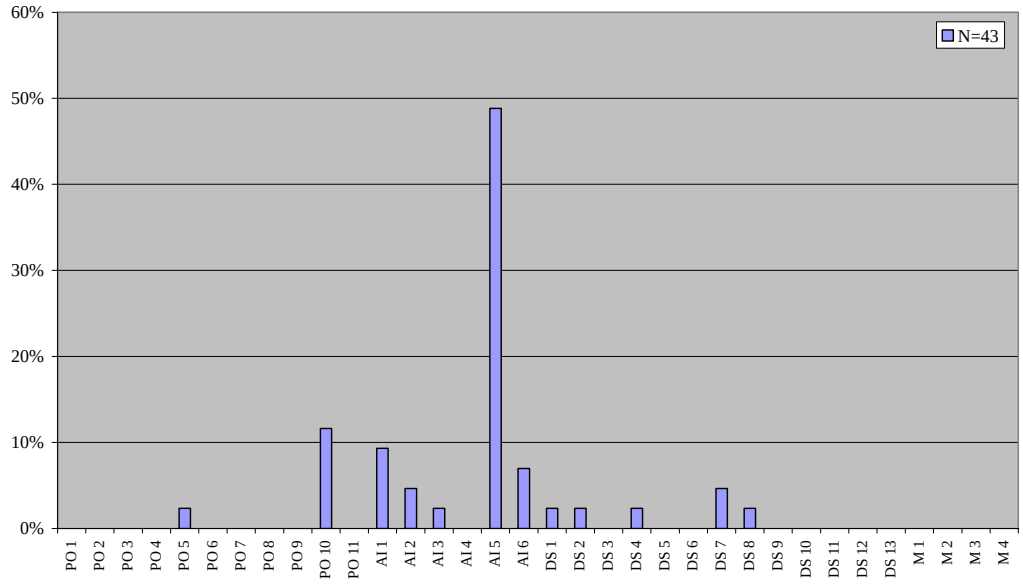


Abb 27: Verteilung der IFAC Richtlinie 4 (Beschaffung von Anwendungen) im Verhältnis zu COBIT

3.2.9 EnSEC

Anzahl der zugeordneten Einheiten:	88
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	14
Anzahl mehrfach zugeordneter Einheiten	1
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	1
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	15
Anzahl der Kontrollziele, zu denen zugeordnet wurde	41

Tabelle 14: Übersicht über das Ergebnis der Zuordnung des Enterprise Secuirty Standards

Die Verteilung ist in der folgenden Grafik abgebildet:

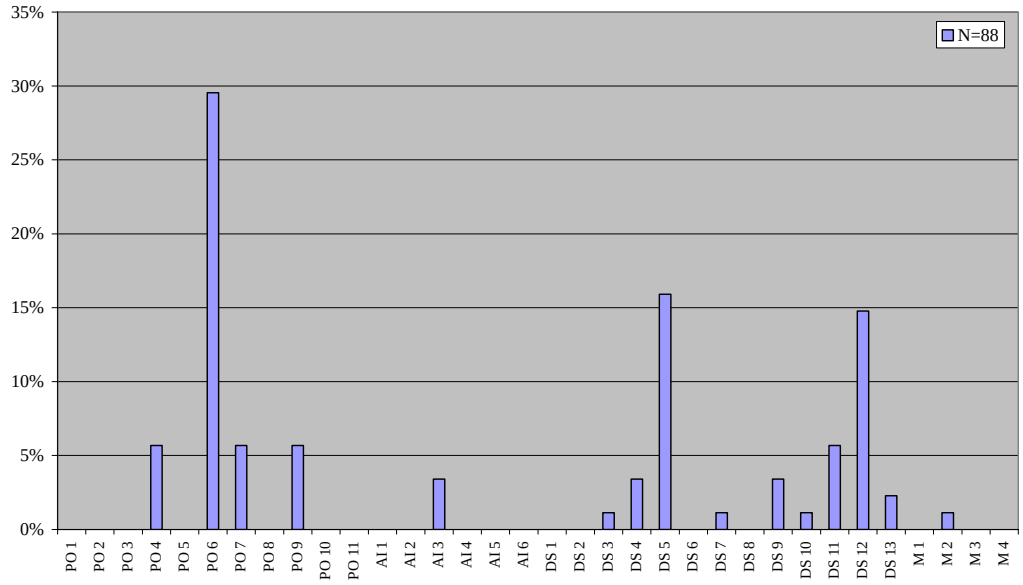


Abb 28: Verteilung von EnSEC im Verhältnis zu COBIT

3.2.10 Trust Services

Drei Einheiten wurden nicht zugeordnet, sie definieren die Qualität Leistungserbringung des Kerngeschäftes und fallen darob nicht in den Verantwortungsbereich der IT:

- "Trust 3.3.2: 3.2 The procedures related to completeness, accuracy, timeliness and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. If the system is an electronic commerce system, the entity's procedures include, but are not necessarily limited to, the following matters:"
- "Trust 3.3.2.1: o The correct goods are shipped in the correct quantities in the time frame agreed, or services and information are provided to the customer as requested"
- "Trust 3.3.2.2: o Transaction exceptions are promptly communicated to the customer"

Weitere 76 Einheiten wurden nicht zugeordnet, da sie Wiederholungen in unterschiedlichen Kapiteln darstellen, die jeweils nur einmal zugeordnet wurden.

Anzahl der zugeordneten Einheiten:	195
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	114
Anzahl mehrfach zugeordneter Einheiten	3
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	7
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	18
Anzahl der Kontrollziele, zu denen zugeordnet wurde	46

Tabelle 15: Übersicht über das Ergebnis der Zuordnung Kriterien aus dem Entwurfs der „Trust Services"

Die Verteilung ist in der folgenden Grafik abgebildet:

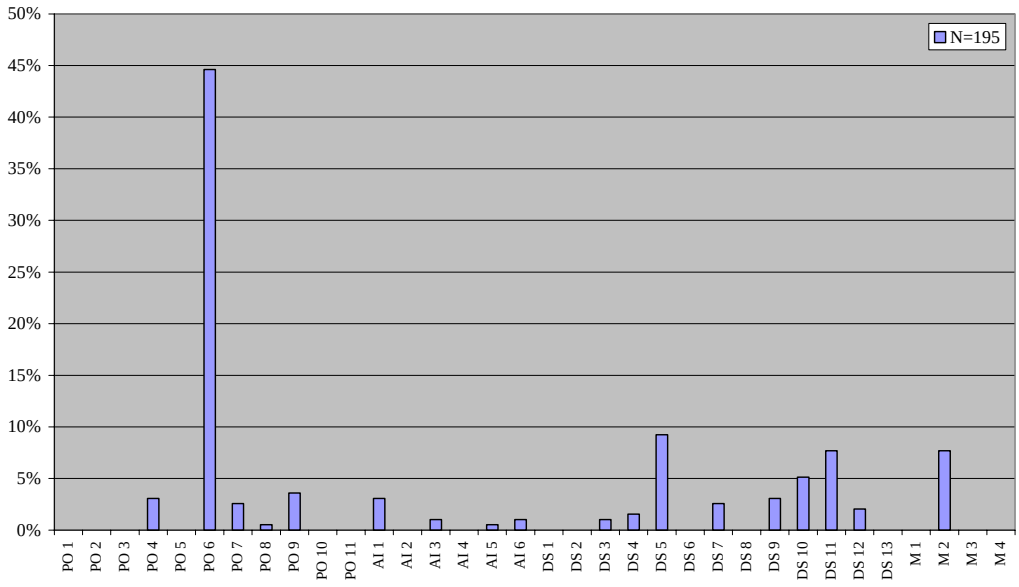


Abb 29: Verteilung von Trust Services im Verhältnis zu COBIT

3.2.11 HIPAA

Anzahl der zugeordneten Einheiten:	573
Anzahl nicht zugeordneter Einheiten (Überschriften, Zusammenfassungen etc.):	109
Anzahl mehrfach zugeordneter Einheiten	1
Anzahl der Einheiten, die einem Prozess gesamtheitlich zugeordnet wurden (Kontrollziel 0):	1
Anzahl der nicht zuordenbaren Einheiten (Prozess 0):	0
Anzahl der Prozesse, zu denen zugeordnet wurde	26
Anzahl der Kontrollziele, zu denen zugeordnet wurde	86

Tabelle 16: Übersicht über das Ergebnis der Zuordnung von HIPAA

Die Verteilung ist in der folgenden Grafik abgebildet:

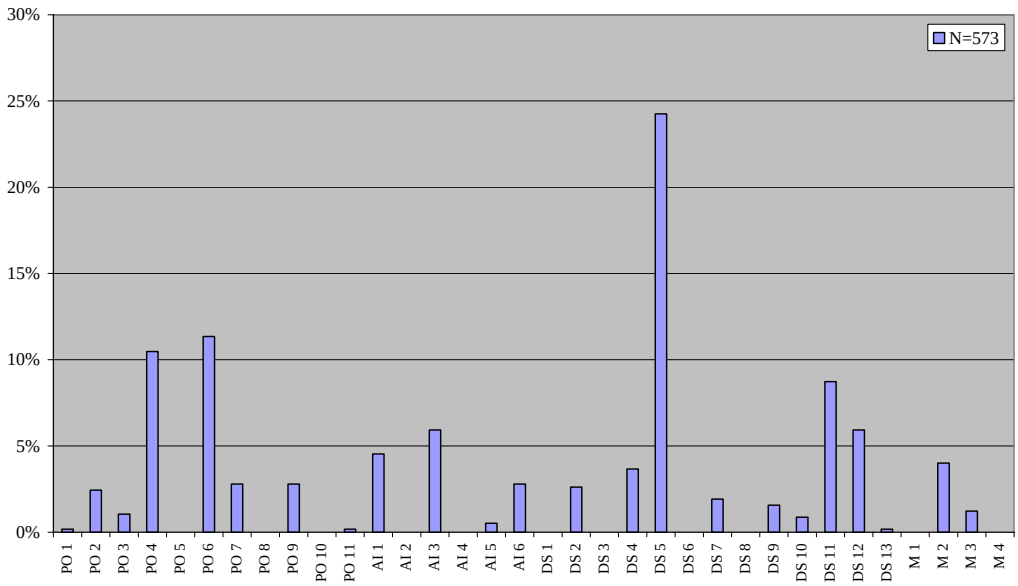


Abb 30: Verteilung des HIPAA im Verhältnis zu COBIT

3.3 Ergebnis der Zuordnung

Das Ergebnis der Zuordnung ist, geordnet nach den Domänen, Prozessen und Kontrollzielen im Anhang A in Form einer Liste dargestellt. Den 318 Kontrollzielen in den 34 Prozessen des COBIT Modells wurden in Summe 1958 Informationseinheiten zugeordnet, die Verteilung ist wie folgt:

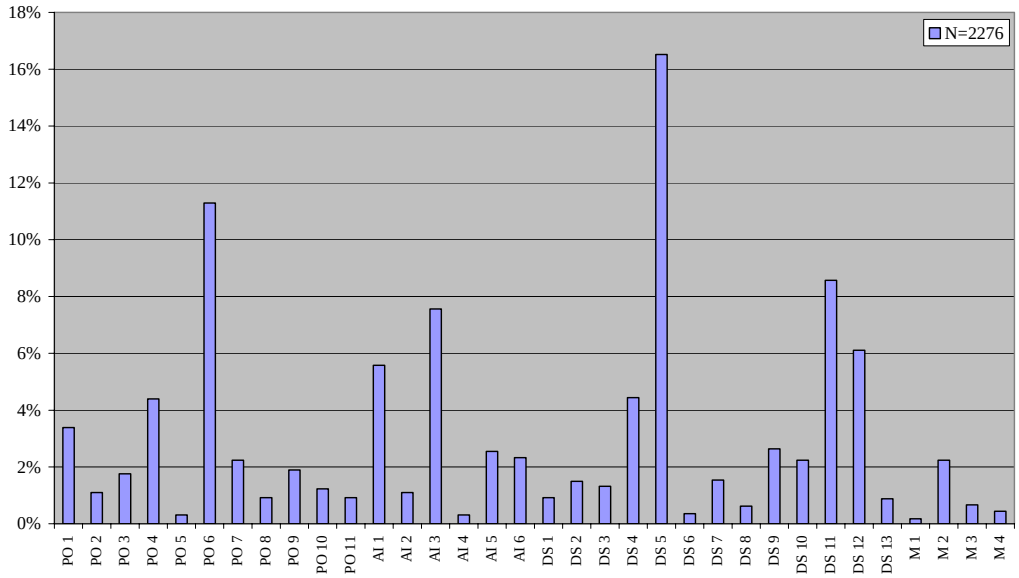


Abb 31: Verteilung aller zugeordneten Informationseinheiten

Mit Hilfe der geordnet vorliegenden Informationen ist es nun möglich, ein interenes Kontrollsystem im IT-Bereich zu etablieren.

Ausgehend von der Zielsetzung der einzelnen Prozesse - sowohl durch die Bestimmung des Reifegrades, als auch durch die Definition von KGIs – können dieselben unter Berücksichtigung von unterschiedlichen Standards und Best Practices definiert werden. Nach der Modellierung wird die Einhaltung der Kriterien laufend geprüft und der Prozess über definierte KPI laufend gemessen. Bei etwaigen Abweichungen sind diese zu analysieren und in der Folge entsprechende Korrekturmaßnahmen zu treffen.

Durch die Modellierung der einzelnen Prozesse mit Hilfe dieses nunmehr horizontal wie vertikal ausreichend ausgeprägten Modells kann – die Einhaltung der Kriterien nach Maßgabe der Geschäftsführung und deren Anforderungen vorausgesetzt – von einer IT-Governance insofern gesprochen werden, als dass die Einhaltung der international anerkannten Standards als maßgebliches Kriterium im Rahmen der Beurteilung des internen Kontrollsystems gilt.

4 Literatur

[ACC99] *The Institute of Chartered Acountants in England & Wales (Hrsg.):* Internal Control – guidance for Directors on the Combined Code. Accountancy Books, London 1999

[AIC00-1] *AICPA / CICA (Hrsg.):* WebTrust$^{SM/TM}$ – Program for Online Privacy, Version 3.0. 2000. Online im Internet: URL: http://ftp.webtrust.org/webtrust_public/privacy_fin.doc [Stand 11. Juli 2002]

[AIC00-2] *AICPA / CICA (Hrsg.):* SysTrust$^{SM/TM}$ –Principle and Criteria, Version 2.0. 2000 Online im Internet: URL: http://www.aicpa.org-/assurance/systrust/princip.htm [Stand 11. Juli 2002]

[AIC01-1] *AICPA / CICA (Hrsg.):* WebTrust$^{SM/TM}$ – Confidentiality Principle and Criteria, Version 3.0. 2001. Online im Internet: URL: http://ftp-.webtrust.org/webtrust_public/confprinc_fin.doc [Stand 11. Juli 2002]

[AIC01-2] *AICPA / CICA (Hrsg.):* WebTrust$^{SM/TM}$ – Security Principle and Criteria, Version 3.0. 2001. Online im Internet: URL: http://ftp.webtrust.org/webtrust_public/security_fin.doc [Stand 11. Juli 2002]

[AIC01-3] *AICPA / CICA (Hrsg.):* WebTrust$^{SM/TM}$ – Business Practices / Transaction Integrity Principle and Criteria, Version 3.0. 2001. Online im Internet: URL: http://ftp.webtrust.org/webtrust_public-/buspractrans_fin.doc [Stand 11. Juli 2002]

[AIC01-4] *AICPA / CICA (Hrsg.):* WebTrust$^{SM/TM}$ – Availability Principle and Criteria, Version 3.0. 2001. Online im Internet: URL: http://ftp.webtrust.org/webtrust_public/avail_fin.doc [Stand 11. Juli 2002]

[AIC02-1] *AICPA / CICA (Hrsg.):* What are SysTrust Services and Why Should I Get Involved? Online im Internet: URL: http://www.aicpa.org/assurance/systrust/what.htm [Stand 11. Juli 2002]

[AIC02-2] *AICPA / CICA (Hrsg.):* PowerPoint File for Presentation to CPAs. Online im Internet: http://ftp.aicpa.org/public/download-/assurance/SysTrust6B.ppt [Stand 11.Juli 2002]

[AIC02-3] *AICPA / CICA (Hrsg.):* Trust Services Principles and Criteria (Incorporating SysTrust^{TM} and WebTrust^{TM}), Version 1. Online im Internet: URL: http://ftp.webtrust.org/webtrust_public/ ed_princ_criteria.pdf [Stand 14. Juli 2002]

[BAS01-1] *Basler Ausschuss für Bankenaufsicht (Hrsg.):* Konsultationspapier "Die Neue Basler Eigenkapitalvereinbarung" in einer Übersetzung

der Deutschen Bundesbank, Bank für internationalen Zahlungsausgleich, 2001.

[BAS01-2] *Basel Committee on Banking Supervision (Hrsg.):* Sound Practices for the Management and Supervision of Operational Risk. Bank for International Settlements, 2001

[BMF78] *Bundesministerium für Finanzen (Hrsg.):* Schreiben des deutschen Bundesministers für Finanzen vom 5. Juli 1978, IV A 7 – S 0136 – 7/1978 (BStBl. I, S. 250). AWV-Arbeitsergebnis, Grundsätze ordnungsmäßiger Speicherbuchführung (GoS). 1977

[BSI00] *Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):* IT-Grundschutzhandbuch – Standard-Sicherheitsmaßnahmen. Bundesanzeiger-Verlaggesellschaft, Köln 2000

[BSI02-1] *Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):* BSI Tool IT-Grundschutz – Leistungsmerkmale. Online im Internet: URL: http://www.bsi.de/gstool/leistung.htm [Stand 5. Juli 2002]

[BSI02-2] *Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):* BSI Tool IT-Grundschutz – Leistungsmerkmale. Online im Internet: URL: http://www.bsi.de/gshb/deutsch/aktuell/gs_faq.htm#s5 [Stand 5. Juli 2002]

[BSI99-1] *British Standards Institution (Hrsg.):* Information security management – Part1: Code of practice for information security management. London 1999

[BSI99-2] *British Standards Institution (Hrsg.):* Information security management – Part2: Specification for information security management systems. London 1999

[CCI99-1] *Common Criteria Interpretations Management Board (Hrsg.):* Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and gerneral model. 1999 Online im Internet: URL: http://csrc.nist.gov/cc/ccv20/p1-v21.pdf [Stand 5. Juli 2002]

[CCI99-2] *Common Criteria Interpretations Management Board (Hrsg.):* Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements. 1999 Online im Internet: URL: http://csrc.nist.gov/cc/ccv20/p2-v21.pdf [Stand 5. Juli 2002]

[CCI99-3] *Common Criteria Interpretations Management Board (Hrsg.):* Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements. 1999 Online im Internet: URL: http://csrc.nist.gov/cc/ccv20/p3-v21.pdf [Stand 5. Juli 2002]

[CEC91] *Commission of the European Communities, Directorate XIII/F (Hrsg.):* ITSEC. Brüssell 1991 Online im Internet: http://www.itsec.uk.gov/download/itsec_brochure_finale.zip [Stand 4. Juli 2002]

[DÖR99] *Dörner, D.:* Was bringt das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich?. In: Ernst & Young – Kontrolle und Transparenz im Unternehmensbereich. Stuttgart 1999

[EUR01] *Europa Treuhand Ernst & Young (Hrsg.):* Welcome to WebTrust. Wien 2001 Online im Internet: URL: http://www.webtrust.at-/prinzipien.html [Stand 11. Juli 2002]

[FAC92] *The Committee on the Financial Aspects of Corporate Governance and Gee and Co. Ltd (Hrsg.):* The Financial Aspect of Corporate Governance, aka Cadbury-Report. London 1992 Online im Internet: URL: http://www.worldbank.org/html/fpd/privatesector/cg/docs-/cadbury.pdf [Stand 26. Juni 2002]

[FIN02] *Despeignes, P.:* Enron's directors 'contributed to collapse', In: Financial Times, 7. Juli 2002, Washington 2002 Online im Internet: URL: http://news.ft.com/servlet/ContentServer?pagename=-FT.com/StoryFT/FullStory&c=StoryFT&cid=1025793376057-&p=1024578257992 [Stand 8. Juli 2002]

[FIS76] *Fischer, T.:* Die Gestaltung der internen Kontrolle bei elektronischer Datenverarbeitung, Schweizerische Treuhand- und Revisionskammer, Zürich 1976

[HEI02] *Heinrich, L. J.:* Informationsmanagement 6. Auflage, Oldenbourg, München 1999

[HEI98] *Heinrich, L. J.; Roithmayr, F.:* Wirtschaftsinformatik-Lexikon 6. Auflage, Oldenbourg, München/ Wien 1998

[HOF93] *Hofmann, R.:* Unternehmensüberwachung – Ein Aufgaben und Arbeitskatalog für die Revisionspraxis 2. Auflage, Schmidt, Berlin 1993

[HOL02] *Holly, G. et al:* Comparative Study Of Corporate Governance Codes Relevant to the European Union and Its Member States. ECGN, 2002 Online im Internet: URL: http://europa.eu.int/comm-/internal_market/en/company/company/news-/corp-gov-codes-rpt-part1_en.pdf [Stand 2. Juli 2002]

[IDW87] *Institut der Wirtschaftsprüfer (Hrsg.):* Fachgutachten 1/1987 – Grundsätze ordnungsmäßiger Buchführung bei computergestützen Verfahren und deren Prüfung. In: Die Wirtschaftsprüfung ½ 1988, S 1 - 35

[IDW99] *Institut der Wirtschaftsprüer (Hrsg.):* Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Absatz 4 HB (IDW PS 340), in: Die Wirtschaftsprüfung, Heft 16/1999, 657-662

[IFA98] *International Federation of Accountants (Hrsg.):* Information Technology Guideline 1 – Managing Security of Information. New York 2002

[IFA00-1] *International Federation of Accountants (Hrsg.):* Information Technology Guideline 3 – Acquisition of Information Technology. New York 2000

[IFA00-2] *International Federation of Accountants (Hrsg.):* Information Technology Guideline 4 – Implementation of Information Technology Solutions. New York 2000

[IFA00-3] *International Federation of Accountants (Hrsg.):* Information Technology Guideline 5 – IT Service Delivery and Support. New York 2000

[IFA99] *International Federation of Accountants (Hrsg.):* Information Technology Guideline 2 – Planning for Busines Impact. New York 1999

[IFA02] *International Federation of Accountants (Hrsg.):* Information Technology Guideline 6 – IT Monitoring. New York 2002

[INI01] *Initiative D21 (Hrsg.):* IT-Sicherheitskriterien im Vergleich, Ein Leitaden der Projektgruppe IT-Sicherheitskriterien und IT-Grundschutz-Zertifikat/Qualifizierung. 2001 Online im Internet: URL: http://www.initiatived21.de/arbeitsgruppen-/5sicherheit/leitfaden.pdf [Stand 2. Juli 2002]

[ISA00-1] *Inforation Systems Audit and Control Foundation (Hrsg.):* COBIT 3rd Edition: Framewok. Rolling Meadows 2000

[ISA00-2] *Inforation Systems Audit and Control Foundation (Hrsg.):* COBIT 3rd Edition: Management Guidelines. Rolling Meadows 2000

[ISA00-3] *Inforation Systems Audit and Control Foundation (Hrsg.):* COBIT 3rd Edition: Control Objectives. Rolling Meadows 2000

[ISA00-4] *Inforation Systems Audit and Control Foundation (Hrsg.):* COBIT 3rd Edition: Implementation Tool Set. Rolling Meadows 2000

[ISA00-5] *Inforation Systems Audit and Control Foundation (Hrsg.):* COBIT 3rd Edition: Framework. Rolling Meadows 2000

[ISA00-6] *Inforation Systems Audit and Control Foundation (Hrsg.):* COBIT 3rd Edition: Audit Guidelines. Rolling Meadows 2000

[ISA01] *Inforation Systems Audit and Control Foundation (Hrsg.):* Board Briefing on IT Governance. Rolling Meadows 2001

[ISA02-1] *Inforation Systems Audit and Control Foundation (Hrsg.):* Website. Online im Internet: URL: http://www.isaca.org/isacafx.htm (Stand 15. Juli 2002]

[ISO00] *ISO/IEC (Hrsg.):* Information technology – Code of practice for information security management. Genf 2000

[ITI02] *Office of Government Commerce (Hrsg.):* ITIL – Concepts of ITIL, Online im Internet: URL: http://www.itil.co.uk/about_itil-/concept.htm [Stand 9. Juli 2002]

[KDW77] *Kammer der Wirtschaftstreuhänder (Hrsg.):* Fachgutachten Nr. 58 des Instituts für Betriebswirtschaft, Steuerrecht und Organisation der Kammer der Wirtschaftstreuhänder: „Die Ordnungsmäßigkeit der Buchhaltung beim Einsatz von Datenverarbeitungsanlagen“. In: Amtsblatt der Kammer der Wirtschaftstreuhänder Nr. 5/1977, S 209 ff.

[KDW99] *Fachsenat für Datenverarbeitung des Institutes für Betriebswirtschaft, Steuerrecht und Organisation der Kammer der Wirtschaftstreuhänder (Hrsg.):* Kommentierte Fassung des Fachgutachtens "Die Ordnungsmäßigkeit von EDV-Buchführungen". 1999

[LEO02] Leo – English/German Dictionary, Online im Internet: URL: http://dict.leo.org [Stand 26. Juni 2002]

[ÖAC02] *Österreichischer Arbeitskreis für Corporate Governance (Hrsg.):* Austrian Code of Corporate Governance – Erstentwurf, V1.03 Stand 25. April 2002.Wien 2002

[OEC99] *Organisation for Economic Co-operation and Development (Hrsg.):* SG/CG(99)5, OECD Principles of Corporate Governance. Paris 1999

[OEN02] *Österreichisches Normungsinstitut (Hrsg.):* Informationsverarbeitung – Leitfaden für das Management von Informationssicherheit (ISO/IEC 17799:2000). Wien 2002 Online im Internet: URL: http://www.oenorm.at/ONNET?Mival=/ONNET-/NET_detail_start.html [Stand 27. März 2002]

[PAU93] *Paulk, M.C., et al:* Capability Maturity Model^{SM} for Software, CMU/SEI-93-TR-24. Carnegie Mellon University, Software Engineering Institute, Pittsburgh 1993

[POR98] *Porter, M. E.:* Competitive Advantage: Creating and Sustaining Superior Performance. Free Press, New York 1998

[RIS02] BKA/RIS - Bundesrecht, Online im Internet: URL: http://ris.bka.gv.at/bundesrecht/ [Stand 20. Juli 2002]

[ROB01] *Robinson, E.:* Starting Over. In: Bloomberg Markets Magazine October 2001. Online im Internet: URL: http://www.bloomberg.com/marketsmagazine/cv_0110.html [Stand 21. Juli 2002]

[ROM00] *Romeike, F.:* KonTraG – Gesetzlich verordnetes Risk Management?, Online im Internet: URL: http://www.risknet.de-/Data/risknews07_2000.pdf [Stand 26. Juni 2002]

[SCH96] *Schneider, V. / Kenis, P.:* Verteilte Kontrolle: Institutionelle Steuerung in modernen Gesellschaften. In: Schneider, V. / Kenis, P.

(Hrsg.): Organisation und Netzwerk, Institutionelle Steuerung in Wirtschaft und Politik. Campus Verlag, Frankfurt/New York 1996

[SCH98] *Schuppenhauer, R.:* Grundsätze für ein ordnungsgemäße DV (GoDV), Handbuch der DV-Revision, 5. Aufl., Düsseldorf 1998

[STA02-1] Enron-Aufsichtsrat wusste von Bilanzfälschungen. In: Der Standard, 8. Juli 2002, Wien 2002 Online im Internet: http://derstandard.at/standard.asp?id=1003875 [Stand 8. Juli 2002]

[STA02-2] Basel II: Umsetzung bis Ende 2006. In: Der Standard, 12. Juli 2002, Wien 2002 Online im Internet: http://www.derstandard.at-/standard.asp?id=1007797 [Stand 12. Juli 2002]

[TED01] *Tedeschi, B.:* Picking Up the Pieces. In: Smart Business, 1. Dezember 2001. Online im Internet: http://www.smartbusinessmag-.com/print_article/0,3668,a=19522,00.asp [Stand 21. Juli 2002]

[TÜV00] *TÜV Secure iT GmbH (Hrsg.):* Informationsicherheitsmanagement für System- und Entwicklungs-Partner der Automobilindustrie – Ergänzende Anforderungen zum EnSEC Anforderungskatalog, Version 1.0. Köln 2000

[TÜV01-1] *TÜV Secure iT GmbH (Hrsg.):* Enterprise Security Management (EnSEC). Köln 2001

[TÜV01-2] *TÜV Secure iT GmbH (Hrsg.):* Enterprise Security Management (EnSEC) Anforderungskatalog, Version 1.12. Köln 2001

[WOR00] *Grundsatzkommission Corporate Governance (Hrsg.):* Corporate Governance-Grundsätze ('Code of Best Practice') für börsennotierte Gesellschaften. Frankfurt 2000, Online im Internet: URL: http://www.worldbank.org/html/fpd/privatesector/cg/docs-/germany%20code%20g.pdf [Stand 3. Juli 2002]

[WIR00] *Wirtschaftsprüferkammer (Hrsg.):* International Standards on Auditing (ISAs) – Internationale Prüfungsgrundsätze. Schäffer-Poeschel, Stuttgart, 2000

Anhang A: Ergebnis der Zuordnung

Kontroll-Ziel	Informationseinheit
PO 1	**Define a Strategic IT Plan**
PO 1.1	*COBIT PO 1.1 IT as Part of the Organisation's Long- and Short-Range Plan*

Falls sie die weitere Tabelle lesen möchten, wenden Sie sich an mich unter jimmy@heschl.at.

Anhang B: Konzept zur Diplomarbeit

IT-Governance

21. Mai 2002

Karlheinz Heschl, 9255956

karlheinz.heschl@at.eyi.com
jimmy@heschl.at

Problem

Durch die steigende Durchdringung (z.B. Automatisierung und Integration von Kerngeschäftsprozessen), das Zusammenwachsen von Unternehmen (z.B. durch verstärkten und automatisierten Austausch von Informationen) sowie auch durch die Anforderungen von Stakeholdern wird eine erhöhte Transparenz und eine aktive Steuerung des Unterstützungsprozesses IT gefordert.

Die Gesetzgeber - sowohl auf europäischer Ebene, als auch auf Ebene der Einzelstaaten – verlangen von Unternehmen die Schaffung und Aufrechterhaltung eines Internen Kontrollsystems, wie dies im §82(1) AktG bzw. im §22 GmbHG bezeichnet wird. In der BRD existiert das KonTraG, das noch weitere diesbezügliche Forderungen - vor allem im Bereich der

Offenlegung - stellt. Weiters sind derzeit verschiedenartige nationale und internationale Standards, Normen und Empfehlungen (z.B. BS7799, BSI-Grundschutzhandbuch, Turnbull-Report, Basel-II, ÖNORM-17799, ISO/IEC-17799, Fachgutachten FAMA, Fachgutachten KFS/DV1 der Kammer der Wirtschaftstreuhänder, EnSec, IT-Monitoring der IFAC etc.) in Kraft beziehungsweise in Begutachtung, die sich unter anderem mit der Anforderung für eine Steuerung und Kontrolle des Unterstützungsprozesses IT beschäftigen.

Am 25. April 2002 wurde auch in Österreich der erste Entwurf des österreichischen Corporate Governance Codex vorgestellt. Er wurde von Vertretern vom ÖVFA[1] , IWP[2] und wissenschaftlichen Beiräten verschiedener Universitätsinstitute sowie dem Regierungsbeauftragten für den Kapitalmarkt erstellt. Die Möglichkeit zur Stellungnahme zu diesem Entwurf verläuft mit 30. Juni 2002 ab. Eine endgültige Version dieses Code of Corporate Governance für Österreich wird im Herbst 2002 vom österr. Arbeitskreis für Corporate Governance der Öffentlichkeit vorgestellt werden.

EU-weit (siehe oben) und weltweit sind Bestrebungen zur Umsetzung von Corporate Governance zu erkennen, die sich mit Information Technology und insbesondere auch IT-Sicherheit beschäftigen, und umfassende, neue Anforderungen für die IT mit sich bringen.

Nicht nur das Unternehmen als Ganzes will gesteuert werden (Corporate Governance), auch die IT als ein wichtiges Element im Unternehmen im Hinblick auf die Zielerreichung bedarf einer regelmäßigen Neuausrichtung. Und somit wurde die IT-Governance als eigene Disziplin geboren. IT-Governance beschäftigt sich mit der Steuerung, Kontrolle, Überwachung und Messung der IT (Prozesse) in einer Unternehmung durch jene Personen, die auch mit der Unternehmenssteuerung (Corporate Governance) betraut sind.

Obwohl in Österreich noch relativ unbekannt, gibt es international schon zahlreiche Bestrebungen und Gruppierungen, die sich mit IT-Governance beschäftigen sowie auch diesbezügliche Stellungnahmen und Arbeitspapiere. Die Organisation, die sich bisher am eingehendsten mit IT-Governance beschäftigt, ist das IT Governance Institute, eine Tochterorganisation der ISACA (Information Systems Audit Control Association).

Nach dem “IT Governance Institute” ist IT-Governance wie folgt definiert:

[1] www.oevfa.at (Österr. Vereinigung für Finanzanalyse und Asset Management)
[2] www.iwp.or.at (Institut Österr. Wirtschaftsprüfer)

„IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives."
Die wichtigen Punkte aus dieser Definition sind:

- Nicht nur das mittlere Management (CIOs), sondern auch die Geschäftsleitung ist verantwortlich („responsibility of the board of directors and executive management")
- IT-Governance ist nicht als isoliertes Projekt, sondern als Bestandteil des Geschäftsführungsprozesses zu betrachten. („integral part of enterprise governance")
- "sustains or extends … strategies and objectives": Die Ziele der Organisation sind durch IT zu unterstützen oder auszubauen.

Derzeit ist kein umfassendes Modell verfügbar, mit Hilfe dessen die IT Prozesse gestaltet und gemessen werden können, lediglich das COBIT IT Prozessmodell kann als Ansatz gesehen werden.

Ich bin seit September 2000 im Bereich TSRS (Technology and Security Risk Services) bei dem österreichischen Wirtschaftsprüfer Europa Treuhand Ernst & Young tätig und beschäftige mich dort mit der Einführung eines umfassenden IT Prozessmodells, der Vereinheitlichung und mit der Dokumentation von IT Prozessen in österreichischen Unternehmen. Ich bin sehr häufig mit dem Problem konfrontiert, dass derzeit kein Modell zur Verfügung steht, das einerseits den diversen Regelwerken entspricht, andererseits messbare Größen zur Zielsetzung und zur Kontrolle der Prozesse beinhaltet.

Problemlösungsweg

Nach der Darstellung der rechtlichen Rahmenbedingungen in Österreich, EU-Ländern, der EU und internationalen gesetzlichen Regelungen zur Schaffung und Aufrechterhaltung des Internen Kontrollsystems und dessen Auswirkungen auf die IT möchte ich die entsprechenden Standards, Normen und Richtlinien auflisten und erörtern. Weiters möchte ich die in Literatur und Praxis verfügbaren Mess- und Steuerungsmöglichkeiten für IT Prozesse darstellen, sowie auch die jeweiligen Verantwortlichen für die Durchführung von Überwachungsmaßnahmen herausarbeiten.

In einem Praxisteil möchte ich versuchen, mit Hilfe des Standard IT Prozessmodells COBIT die diversen Regularien zu strukturieren, um ein Modell zu entwickeln, das die Einführung eines Kontrollsystems sowie dessen Überprüfung auf Einhaltung ermöglicht. Ein derartiges Modell beinhaltet jedoch nicht nur die beschriebenen Regularien, sondern muss meines Erachtens auch messbare Größen für die unterschiedlichen Prozesse beinhalten, um den Anforderungen der IT-Governance zu genügen. Dies kann ähnlich dem Wirkungskreislauf der Controlling-Teilfunktionen gesehen werden, der sich vom Setzen von messbaren Zielen, bis hin zur Analyse und Beseitigung der Abweichungsursachen zieht.

Ergebnis

Das Ergebnis der Arbeit soll ein Modell zur Überprüfung der Einhaltung von Standards, Normen und Richtlinien beim Unterstützungsprozess IT sein, das die lokalen gesetzlichen Anforderungen, die international anerkannten Best Practices sowie messbare Größen inkludiert und somit den Stakeholdern die Möglichkeit gibt, den IT Prozess auf Grund seiner Transparenz und Messbarkeit rasch zu bewerten.

Grobgliederung

Inhaltsverzeichnis
Akronyme
Kurzfassung
Grundlagen
- Gesetzlicher Rahmen
  - AktG/GmbHG/HGB
  - BWG
  - KonTraG
  - Turnbull Report
  - ...
- Standards, Normen und Modelle
  - ISO/IEC 17799, ÖNORM 17799
  - BS 7799
  - BSI-GSHB
  - IT-Governance Guideline

- COBIT
- ITIL
- HIPAA
- CoSo
- IFAC International IT Guidelines
- Fachgutachten FAMA
- Fachgutachten KFS/DV1 der Kammer der Wirtschaftstreuhänder
- EnSec
- WebTrust
- SysTrust
- ...
- IFAC-2: 4.1.1.1.1: Messgrößen
- Einhaltung von Anforderungen
- Reifegradmodell
- Key Performance Indikatoren
- Key Goal Indikatoren

Verantwortung
- Für die Definition von Messgrößen und Meßmethoden
- Für die Durchführung der Bewertung
- Für die Berichterstellung
- Für die Interpretation von Ergebnissen
- Für die Kommunikation von Maßnahmen

Praxisteil
- Vorgehen des Mapping
- Durchführung des Mapping
- Ergebnis des Mapping
- Modell zur Implementierung des Kontrollsystems

Glossar
Literaturverzeichnis

Literatur

Heinrich, L. J.; Roithmayr, F.: Wirtschaftsinformatik-Lexikon 6. A., Oldenbourg, München/ Wien 1998

Heinrich, L. J.; Informationsmanagement 6. Auflage, Oldenbourg, München 1999

IT Governance Institute (Hrsg.); COBIT 3rd Edition – Control Objectives, Rolling Meadows 2000

IT Governance Institute (Hrsg.); COBIT 3rd Edition – Management Guidelines, Rolling Meadows 2000
Basel Committee on Banking Supervision (Hrsg.); Risk Management Subgroup of the Basle Committee on Banking Supervision; Basel 1998
IFAC; Managing IT Monitoring, New York, 2002
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.); IT-Grundschutzhandbuch; Bonn 2000
Schirmbrand, M.; Die Ordnungsmäßigkeit der Buchführung beim Einsatz von großen und mittelgroßen IT-Systemen, Wien, Linde 1997
IFAC (Hrsg.); Managing IT Monitoring Proposed International Guideline on Information Technology, New York, 2002

Umfangreiche Informationsquellen zu den diversen Regularien finden sich im Internet, vor allem auf den Sites unterschiedlicher Verbände und Gremien:
IT Governance Institute: www.itgovernance.org
ISACA: www.isaca.at
IFAC: www.ifac.org
BSI: www.bsi.de

EEEEEEEEEEEEEEEEEEEE
NNNNNNNNNNNNNNNNN
DDDDDDDDDDDDDDDDD
EEEEEEEEEEEEEEEEEEEE
Drucken:

Farbe:
14;78;86;88;90;93;98-110
Ich kann die Endnoten leider nicht löschen: