eBook

Stefan Tönnissen

Revision der IT-Governance mit CoBiT

Leitfaden für die Prüfungspraxis

ESV

ERICH SCHMIDT VERLAG

Revision der IT-Governance mit CoBiT

Leitfaden für die Prüfungspraxis

Von
Stefan Tönnissen

ERICH SCHMIDT VERLAG

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978 3 503 13013 9

Gedrucktes Werk: ISBN 978 3 503 13012 2
eBook: ISBN 978 3 503 13013 9

Geleitwort von Prof. Dr. Hufnagel

Mit dem im Mai 2009 in Kraft getretenen BilMoG ist sowohl der Vorstand als auch der Aufsichtsrat verpflichtet, die Angemessenheit eines wirksamen internen Kontrollsystems sicherzustellen. In der Gesetzesbegründung wird explizit darauf hingewiesen, dass sich die Überwachungsfunktion nicht nur auf die Rechnungslegung bezieht, sondern auch auf die Internen Kontrollen der Informationstechnologie.

Die Unternehmen sind gegenüber dem Gesetzgeber und Wirtschaftsprüfern gefordert, diese notwendige Wirksamkeit des internen Kontrollsystems für die Informationstechnologie nachzuweisen. Doch wie kann die Wirksamkeit eines internen Kontrollsystems für die Informationstechnologie gegenüber Wirtschaftsprüfern nachgewiesen werden?

Stefan Tönnissen greift in seinem Fachbuch diese Problematik auf und zeigt einen auf dem international anerkannten Standard CoBiT basierten Prüfungskatalog aus verschiedenen Perspektiven auf. Der Standard CoBiT lehnt sich stark an COSO an und erfüllt damit die Anforderungen an ein wirksames Kontrollsystem für Informationstechnologie.

Dieser Prüfungskatalog ist in der betrieblichen Praxis als Revisor eines mittelständischen Konzerns entstanden und somit aus der Praxis für die Praxis.

Dieses Fachbuch stellt eine wertvolle Hilfe für den Revisor oder Prüfer zur Prüfung der Informationstechnologie und IT-Governance in den Unternehmen dar.

Münster, im Januar 2011

Prof. Dr. Wolfgang Hufnagel
Leiter Verbundstudiengänge Fachhochschule Münster

Vorwort

Unsere Wünsche wachsen mit den Schwierigkeiten, denen sie begegnen.

- Michel Eyquem de Montaigne -

Der Wunsch nach einem Prüfungskatalog für IT-Governance entstand bei der Aufgabe, als neuer Mitarbeiter in der Konzernrevision eines mittelständischen Konzerns die Informationstechnologie prüfen zu müssen. Es gab eine große Zahl von vorhandenen Prüfungskatalogen, Richtlinien, Prüfungsstandards und Verfahrensanweisungen. Jede davon erlaubte einen sehr speziellen Blick auf einen spezifischen Sachverhalt der Informationstechnologie.

Mir fehlten jedoch der Überblick und eine Möglichkeit, die Informationstechnologie in ihrem Lebenszyklus und ganzheitlich zu erfassen. Meine Recherchen beim Deutschen Institut für Interne Revision und bei Wirtschaftsprüfungsgesellschaften führten mich sehr schnell zu einem international anerkannten Referenzmodell zur Entwicklung und Prüfung der IT-Governance, CoBiT.

Common Objectives for Information and related Technology (CoBiT) ist 1994 entstanden durch eine Initiative von IT-Revisoren und wurde im Laufe der Jahre weiterentwickelt zu einem Rahmenmodell für IT-Governance mit 34 IT-Prozessen.

Somit findet der Prüfungsneuling als auch der erfahrende Prüfer in diesem Buch eine Anleitung vor, mit der die IT-Governance ganzheitlich und nach einem international anerkannten Standard geprüft und bewertet werden kann. Dabei wird auf die verschiedenen Perspektiven der IT-Prüfung eingegangen und ein sofort einsetzbarer Prüfungskatalog für jede Perspektive aufgezeigt.

Ein Fachbuch „Aus der Praxis – für die Praxis“ schreibt sich vielleicht von alleine, die inhaltliche Gestaltung bedarf jedoch einer umfangreichen fachlichen Diskussion mit am Thema betroffenen oder mit dem Thema vertrauten Fachleuten.

Danken möchte ich an dieser Stelle meinen Arbeitskollegen Dieter Oskamp und Ernst Sybon der Konzernrevision der Schmitz Cargobull AG. Beide Kollegen haben einen großen Anteil am Gelingen dieses Buches. Der Anspruch dieses Buches, einen

Prüfungskatalog für IT-Governance aus der Praxis für die Praxis zu erstellen, konnte nur durch den konstruktiven Dialog mit den beiden Kollegen gelingen.

Frau Brand-Noé danke ich für die Erlaubnis, die in Ihrem hervorragenden Buch „Revision des Personalbereich“ dargestellte Idee der Prüfungslandkarten in mein Buch übernehmen zu dürfen.

Des Weiteren möchte ich Herrn Prof. Dr. Hufnagel und Dipl.-Betriebswirtin Ruth Kühn M.A. von der Fachhochschule Münster für Ihre vielen Anregungen und Ideen für diese Arbeit während meiner berufsbegleitenden Studienzeit am Institut für Technische Betriebswirtschaft danken.

Zu guter Letzt möchte ich Frau Splittgerber und Frau Ludwig vom Erich Schmidt Verlag für die tolle Zusammenarbeit im Rahmen der Erstellung dieses Buches danken.

Ich wünsche Ihnen viel Erfolg bei der IT-Prüfung mit CoBiT und den in diesem Buch dargestellten Prüfungskatalogen. Mögen diese Prüfungskataloge Ihnen den Einstieg in die IT-Prüfung erleichtern und viele neue Ideen generieren.

Wettringen, im Januar 2011 Stefan Tönnissen

Inhaltsverzeichnis

Geleitwort von Prof. Dr. Hufnagel 5

Vorwort 7

Inhaltsverzeichnis 9

Abkürzungsverzeichnis 11

Abbildungsverzeichnis 13

I. Einführung 15

1 Ziel des Buches 16

2 Aufbau des Buches 16

3 Benutzung des Buches 18

II. Darstellung der Standards, Normen und Begriffe 19

1 Corporate Governance 19

2 IT-Governance 20

3 CoBiT als Rahmenwerk 22

III. Reifegrade der IT-Prozesse 27

1 Planung und Organisation 29

2 Akquisition und Implementierung 35

3 Delivery und Support 40

4 Monitoring und Evaluierung 50

IV. Prozesslandkarte CoBiT 53

1 Planung und Organisation 54

2 Akquisition und Implementierung 61

3 Delivery und Support 65

4 Monitoring und Evaluierung 72

V. Prüfungslandkarte CoBiT 75

1 Planung und Organisation 76

2 Akquisition und Implementierung 87
3 Delivery und Support 92
4 Monitoring und Evaluierung 102
VI. Prüfungslandkarte Informationsanforderungen der Prozesse 105
1 Effektivität 108
2 Effizienz 129
3 Vertraulichkeit 148
4 Integrität 149
5 Verfügbarkeit 152
6 Compliance 156
7 Reliability 156
VII. Prüfungslandkarte IT-Governance Fokusbereich 159
1 Strategische Ausrichtung 161
2 Wertbeitrag 171
3 Ressourcenmanagement 182
4 Risikomanagement 192
5 Performance Management 202
VIII. Prüfungslandkarte IT-Ressourcen 205
1 Anwendungen 207
2 Information 227
3 Infrastruktur 245
4 Personal 263
IX. Anforderungen aus BilMoG 285
X. Ausblick auf CoBiT 5 289
Anhang 1 IT-Governance Fokusbereich 291
Anhang 2 Informationsanforderungen der Prozesse 293
Anhang 3 Vollständiger Prüfungskatalog 295
Literaturverzeichnis 317
Stichwortverzeichnis 321

Abkürzungsverzeichnis

CoBiT	Common Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ISACA	Information Systems Audit and Control Association
ITAF	IT Assurance Framework
BMIS	Business Model for Information Security
AI	Akquisition & Implementierung
BilMoG	Bilanzrechtsmodernisierungsgesetz
CIA	Certified Internal Auditor
CoBiT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DCGK	Deutscher Corporate Governance Kodex
DIIR	Deutsches Institut für Interne Revision
DS	Delivery & Support
EPK	Ereignisgesteuerte Prozesskette
EPS	Entwurf Prüfungsstandard
HMD	Handbuch der maschinellen Datenverarbeitung
IDW	Institut der Wirtschaftsprüfer
IIA	The Institute of Internal Auditors
IIR	Institut für Interne Revision
IS	Informationssysteme
ISACA	Information Systems Audit and Control Association
IT	Informationstechnologie
ITGI	IT Governance Institute
ME	Monitoring & Evaluierung
Org	Organisation
PO	Planung & Organisation
PWC	PriceWaterhouseCoopers
QMS	Qualitätsmanagement-System
SCB	Schmitz Cargobull AG
SEK	Strategischer Einkauf
SLA	Service Level Agreement
SW	Software
TECHNOL.	technologisch
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WP	Wirtschaftsprüfer

Abbildungsverzeichnis

Abbildung 1: Buchnavigation 18
Abbildung 2: Kernbereiche der IT-Governance nach ITGI 21
Abbildung 3: Die Entwicklung von CoBiT 23
Abbildung 4: Entwicklung und Ausrichtung von CoBiT 23
Abbildung 5: CoBiT-Framework 24
Abbildung 6: Übersicht der CoBiT-Informationsanforderungen 25
Abbildung 7: Übersicht der Prozesse der CoBiT-Domänen 26
Abbildung 8: Erfüllung der Anforderungen nach BilMoG 286
Abbildung 9: Ausblick auf CoBiT 5 289

I. Einführung

Der hohe Automatisierungsgrad der Geschäftsprozesse hat die Informationstechnologie zu einer Angriffsfläche für Verletzungen der Compliance und Governance werden lassen, da die Ausrichtung der IT an betriebswirtschaftlichen Zielen (auch Business IT Alignment oder Strategic Alignment genannt) in der Praxis häufig mit einer Vernachlässigung von Kontrollzielen einhergeht.[1] „IT-Compliance und IT-Governance bedeuten für viele Führungskräfte eine ernsthafte persönliche Bedrohung, da sie wegen der nicht delegierbaren Prozessverantwortung für Verletzungen persönlich haftbar sind.“[2] Nach § 93 Abs. 1 AktG haben die Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. „Angesichts der Bedeutung von IT für das Funktionieren und den Fortbestand des Unternehmens gehört es damit zu den Pflichten eines gewissenhaften Geschäftsführers, das Unternehmen vor erkennbaren Gefahren zu schützen.“[3]

Wenn die Prinzipien und Anliegen der Corporate Governance auf den IT-Bereich angewendet werden, so spricht man von IT-Governance.[4] Die ISACA fasst unter IT-Governance Grundsätze, Verfahren und Maßnahmen zusammen, die sicherstellen sollen, dass mithilfe der IT die Geschäftsziele abgedeckt, Ressourcen verantwortungsvoll eingesetzt und Risiken angemessen überwacht werden.[5]

Richtlinien und Handlungsanweisungen im Unternehmen liefern als Soll-Vorgaben das operative Handwerkszeug für die operative Revisionsarbeit.[6] Für die Überwachung und Kontrolle der IT-Governance fehlen in den Unternehmen entweder entsprechende Richtlinien und Handlungsanweisungen oder es fehlt eine Einordnung vereinzelter Anweisungen in ein ganzheitliches Rahmenwerk. Die Revision ist somit oft nicht in der Lage, eine angemessene und ganzheitliche Prüfung der IT-Governance durchzuführen.

---

1 Vgl. Müller, G.; Terzidis, O.: IT-Compliance und IT-Governance, 5/2008, Seite 341.

2 Vgl. Müller, G.; Terzidis, O.: IT-Compliance und IT-Governance, 5/2008, Seite 342.

3 Rath, M.: Rechtliche Aspekte von IT-Compliance, 2008; Seite 120.

4 Vgl. Rüter, A. et.al.: IT-Governance in der Praxis, Heidelberg 2006, Seite 28.

5 Vgl. Rüter, A. et.al.: IT-Governance in der Praxis, Heidelberg 2006, Seite 28.

6 Vgl. Berwanger, J. et al.: Interne Revision, 1. Auflage 2008, Seite 89.

1 Ziel des Buches

Das Buch möchte zum einen dem Revisor im Unternehmen einen Leitfaden an die Hand geben, wie in Anlehnung an den Standard CoBiT eine angemessene und ganzheitliche Prüfung der IT-Governance durchzuführen ist. Zum anderen soll der Revisor auch einen detaillierten Einblick in den Standard CoBiT erhalten.

In Kapitel V zeigt die Prüfungslandkarte CoBiT die vier Domänen von CoBiT sowie die jeweils zugehörigen IT-Prozesse.

Der komplexe Standard CoBiT wird des Weiteren in einzelne Sichten zerlegt und anhand von drei unterschiedlichen Prüfungslandkarten nachvollziehbar dargestellt. Der Leser erhält zu jeder Prüfungslandkarte eine detaillierte Übersicht der Prüffelder sowie für die Erstellung eines Prüfungskataloges beispielhafte Prüfungsfragen.

Neben dem Abgleich eines im eigenen Unternehmen definierten Soll-Zustandes mit dem ermittelten Ist-Zustand anhand der Prüfungskataloge findet der Leser eine Anleitung, wie die Prozesse in CoBiT anhand eines generischen Reifegradmodells bewertet werden können. Zu jedem Prozess findet sich eine ausführliche Anleitung mit Hinweisen zur Bewertung.

Dem Wirtschaftsprüfer bietet das Buch eine Orientierung, welche Themen und Perspektiven in der Prüfung von IT-Systemen nach CoBiT relevant sein können.

2 Aufbau des Buches

Zu Beginn des Buches werden die wichtigsten Begriffe Corporate Governance und IT-Governance kurz erläutert sowie das Grundmodell des Standard CoBiT detailliert beschrieben.

Die Reifegrade der IT-Prozesse sind Inhalt des dritten Kapitels. Die aus dem Balanced Scorecard Konzept von Kaplan/Norten bekannte Aussage „If you can’t measure it, you can’t manage it“ findet ebenfalls ihren Niederschlag im Reifegradmodell von CoBiT. Das generische Reifegradmodell mit sechs Reifestufen wird für jeden Prozess in den CoBiT Domänen beschrieben.

Im vierten Kapitel wird CoBiT als Prozesslandkarte mit den Domänen und zugehörigen Prozessen übersichtlich dargestellt. Die einzelnen Domänen sowie deren Prozesse und Kontrollobjekte aus dem CoBiT Standard werden anschließend detailliert

beschrieben. Zu jedem Kontrollobjekt wird ein begründeter Hinweis auf die Notwendigkeit dargestellt.

Der Revisor, der seinen Prüfungskatalog streng nach den Objekten von CoBiT aufbaut, erhält in Kapitel Fünf eine Prüfungslandkarte aufgebaut nach den Domänen und Prozessen des CoBiT Standard.

Das sechste Kapitel zeigt zunächst anschaulich eine Prüfungslandkarte für die Informationsanforderungen der Prozesse. Diese acht Informationsanforderungen werden detailliert beschrieben und deren Bedeutung für die IT-Governance herausgestellt. Anschließend werden jeder Informationsanforderung CoBiT Prozesse mit beispielhaften Prüfungsfragen zugeordnet.

Das siebente Kapitel behandelt die Kernbereiche der IT-Governance vom IT Governance Institute als weitere CoBiT Perspektive und zeigt dies ebenfalls anhand einer Prüfungslandkarte schnell und übersichtlich. Für jede der fünf Kernbereiche werden die zugehörigen CoBiT Prozesse aufgezeigt und beispielhafte Prüfungsfragen zugeordnet.

Eine dritte Perspektive zeigt in Kapitel Acht die in CoBiT dargestellten IT-Ressourcen Anwendungen, Information, Infrastruktur und Personal. Zunächst wird wiederum eine übersichtliche Prüfungslandkarte mit den zugehörigen IT-Prozessen dargestellt, gefolgt von den beispielhaften Prüfungsfragen zu jedem Prozess.

Die Anforderungen aus dem Bilanzrechtsmodernisierungsgesetz sind Gegenstand des Kapitels Neun. Es wird gezeigt, wie eine Prüfung der Informationstechnologie in Anlehnung an den Standard CoBiT die Anforderungen an die Wirksamkeit eines internen Kontrollsystems nach BilMoG erfüllen kann.

Einen Ausblick auf das für 2012 angekündigte CoBiT 5 erhalten Sie in Kapitel Zehn.

3 Benutzung des Buches

Der Einstieg in dieses Fachbuch gelingt durch die Orientierung am Prüfungsobjekt. Nach Auswahl des Prüfungsobjektes und des entsprechenden Kapitels im Buch schließt sich Kapitel IV mit der Bewertung der geprüften IT-Prozesse nach dem Reifegradmodell an. Üblicherweise wird ein ermittelter Reifegrad im Rahmen eines Benchmarkings mit internen oder externen Betrieben oder Unternehmen verglichen. Aus den gewonnenen Erkenntnissen werden entsprechende Handlungsempfehlungen für die notwendigen Anpassungen im Unternehmen abgeleitet.

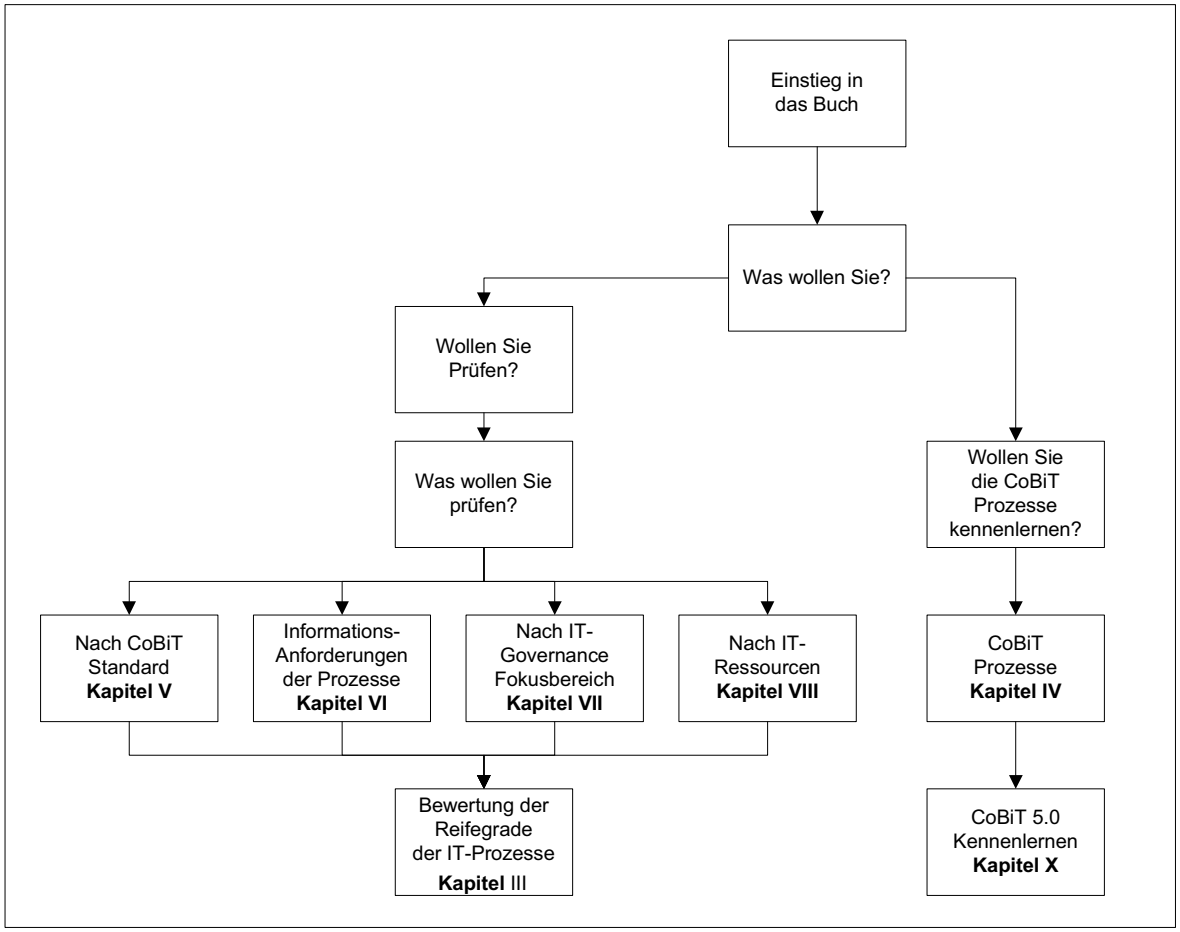

Abbildung 1: Buchnavigation

II. Darstellung der Standards, Normen und Begriffe

Standards, Rahmenwerke, Normen und Best Practices dienen entweder als Orientierungshilfe oder sind als konkrete Vorgaben für die Implementierung und den Einsatz einer IT-Governance zu verstehen.[7] Nachfolgend werden die für das Verständnis dieses Buches notwendigen Begriffe Corporate Governance, IT-Governance und CoBiT beschrieben.

1 Corporate Governance

Der Begriff Corporate Governance wird in der Fachliteratur sehr unterschiedlich benutzt und je nach Zielgruppe ausgelegt. Nachfolgend werden bedeutende Beschreibungen dargestellt.

Für Paetzmann stellt sich Corporate Governance als zielgerichtete Führung und Überwachung von Unternehmen dar und beinhaltet Mechanismen zur Regelung von Kompetenzen, Schaffung von Anreizen und Installierung von Überwachungsprozessen.[8] Paetzmann stellt vor dem Hintergrund der Trennung von Eigentum und Verfügungsmacht an Unternehmen die Überwachung und die Installation eines Überwachungssystems in den Vordergrund des Corporate-Governance-Begriffes.[9]

Wird Corporate Governance im Zusammenhang mit der Prinzipal-Agent-Theorie betrachtet, so steht das Problem der Organisation von Leitung und Kontrolle in einem Unternehmen mit mehreren Interessengruppen, bei dem es vor allem in der Interaktion von Anteilseignern und Managern zu Effizienzverlusten kommen kann.[10]

---

7 Vgl. Fröhlich, M.; Glasner, K.: IT-Governance, Wiesbaden 2007, Seite 62.

8 Vgl. Paetzmann, K.; Bedeutung der Internen Revision im Rahmen der Reformbestrebungen zur Verbesserung der Corporate Governance, Berlin 2008, Seite 19.

9 Vgl. Paetzmann, K.; a.a.O., Seite 19.

10 Vgl. Witt, P.; Corporate Governance in Familienunternehmen, 2/2008 Seite 2.

Johannsen und Goeken sehen Corporate Governance als verantwortliche, transparente und nachvollziehbare Leitung und Überwachung von Organisationen und ihre Ausrichtung an Regulierungen, Standards und ethischen Grundsätzen. [11]

In Deutschland wurde 2002 von der Bundesministerin für Justiz der Deutsche Corporate Governance Kodex verabschiedet.[12] Der Deutsche Corporate Governance Kodex stellt wesentliche gesetzliche Vorschriften zur Leitung und Überwachung deutscher börsennotierter Gesellschaften (Unternehmensführung) dar und enthält international und national anerkannte Standards guter und verantwortungsvoller Unternehmensführung. Der Kodex soll das deutsche Corporate-Governance-System transparent und nachvollziehbar machen. „Er will das Vertrauen der internationalen und nationalen Anleger, der Kunden, der Mitarbeiter und der Öffentlichkeit in die Leitung und Überwachung deutscher börsennotierter Gesellschaften fördern.“[13]

2 IT-Governance

Der Begriff IT-Governance wird ebenfalls in der aktuellen Literatur sehr unterschiedlich ausgelegt.

Heschl und Middelhoff verstehen unter IT-Governance die Beschäftigung mit der Steuerung, Messung, Kontrolle und Überwachung der IT in einer Unternehmung.[14] Dieser eher prüfungsorientierte Ansatz wird ebenfalls von der Wirtschaftsprüfungsgesellschaft PriceWaterhouseCoopers (PWC) verwendet. PWC definiert IT-Governance als Organisation, Steuerung und Kontrolle der IT eines Unternehmens zur konsequenten Ausrichtung der IT-Prozesse der Unternehmensstrategie.[15]

In der Fachliteratur werden ebenfalls Konzepte der IT-Governance vorgestellt, in denen eher die Sicht der Unternehmensleitung hervorgehoben wird: „IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise’s IT sustains and extends the organisation’s strategies and objectives“[16] sowie „IT-Governance ist die Verantwortung von Führungskräften und Aufsichtsräten und besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die

---

11 Vgl. Johannsen W., Goecken M.: Referenzmodelle für IT-Governance, Seite 2.

12 Vgl. Heschl; Middelhoff: IT Governance, Books on Demand, Norderstedt 2005, Seite 30.

13 Regierungskommission, DCGK in der Fassung vom 6. Juni 2008, Seite 1.

14 Vgl. Heschl, J.; Middelhoff, D.: a.a.O., Seite 16.

15 Vgl. Fröhlich, M.; Glasner, K.: a.a.O., Seite 45.

16 Brand, K.; Bonnen, H.: IT Governance based on CoBiT 4.1, Amersfoort NL 2005, Seite 1.

Unternehmens-IT dazu beiträgt, die Organisationsstrategie und -ziele zu erreichen und zu erweitern“[17].
Das IT Governance Institute (ITGI) sieht das Hauptziel von IT-Governance in einem Verständnis der Anforderungen an die IT sowie darin, die strategische Bedeutung von IT zu verstehen, um den optimalen Betrieb der Unternehmensziele sicherzustellen und Strategien für die zukünftige Erweiterung des Geschäftsbetriebes zu schaffen. „IT Governance zielt darauf ab, dass Erwartungen an die IT erfüllt und mögliche Risiken entschärft werden.“[18]

Die Kernbereiche der IT-Governance sind nach dem IT-Governance Institut:
– Strategic Alignment,
– Value Delivery,
– Risk Management,
– Resource Management und
– Performance Management.

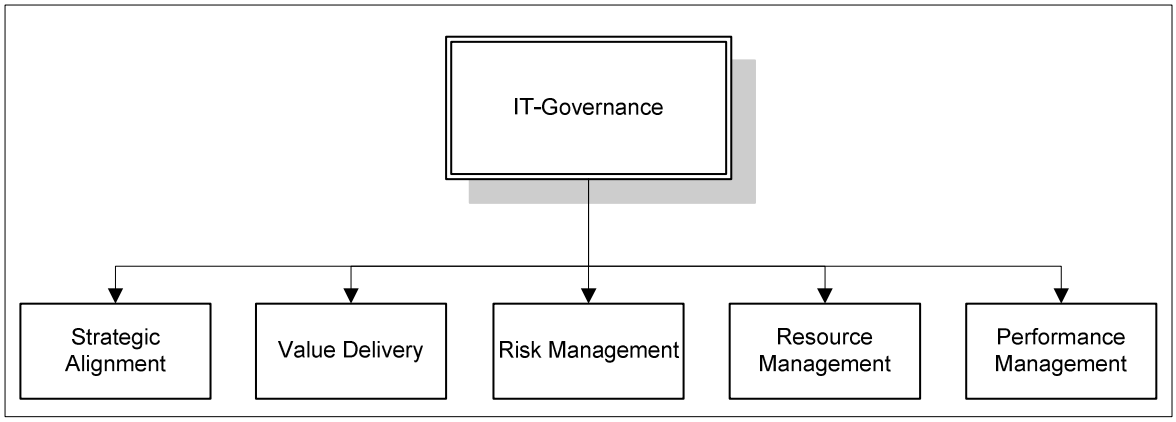

Abbildung 2: Kernbereiche der IT-Governance nach ITGI

Strategic Alignment
Die Strategische Ausrichtung der IT muss sich an der strategischen Ausrichtung des Unternehmens orientieren. Die Aktivitäten und Entscheidungen im Hinblick auf die Informationstechnologie sind in Abstimmung mit den Unternehmenszielen zu treffen, um somit die Effektivität und die Leistung des Unternehmens zu erhöhen.

---

17 Freidank C.-C.; Peemöller, V.: a.a.O., Seite 247.

18 Vgl. IT Governance Institute: IT Governance für Geschäftsführer und Vorstände, Rolling Meadows 2003, Seite 8.

Value Delivery
Die Informationstechnologie im Unternehmen muss einen Wertbeitrag zum Unternehmenserfolg bringen. Die Automatisierung von Geschäftsprozessen muss zu operativen Effekten durch Zeit- und Kostenvorteilen führen.

Risk Management
Der hohe Automatisierungsgrad der Geschäftsprozesse und die hohe Vernetzung sowohl mit Tochtergesellschaften als auch mit Lieferanten und Kunden erfordert ein konsequentes Risikomanagement der Informationstechnologie. Regulatorische Anforderungen erfordern ein Risikoverständnis im IT-Management und in der Unternehmensleitung.

Resource Management
Der effiziente und effektive Einsatz der IT-Ressourcen muss durch ein Ressourcen Management sichergestellt werden. Die Investitionen in IT-Ressourcen erfordern eine optimale Steuerung und Ausrichtung an den Geschäfts- und Unternehmenszielen.

Performance Management
Die Leistungen der Informationstechnologie müssen kontrolliert und gesteuert werden um eine Verbesserung der Performance erreichen zu können.

3 CoBiT als Rahmenwerk

„IT-Governance setzt voraus, dass IT-Prozesse angemessen gesteuert und überwacht werden.“[19] Die Einhaltung der Angemessenheit kann mit der Berücksichtigung des internationalen Prüfungsstandards CoBiT als Rahmenwerk gewährleistet werden. Common Objectives for Information and related Technology (CoBiT) ist ein akzeptiertes Referenzmodell bezogen auf die Kernaufgabengebiete der IT-Governance.[20]

Dieses Rahmenwerk verbessert nicht nur den Abgleich zwischen Geschäfts- und IT-Strategie, sondern kann ebenfalls eingesetzt werden, um IT-Prozesse zu kontrollieren und zu beschreiben.[21] „CoBiT ist ein IT-Governance-Referenzmodell, das

---

19 Gaulke, M.: CoBiT als IT-Governance Leitfaden, in: HMD, August 2006, Seite 21.

20 Vgl. Kozlova, E.: IT-Governance, in: Wirtschaftsinformatik, Ausgabe 5/2008, Seite 418.

21 Vgl. Kozlova, E.: IT-Governance, a.a.O., Seite 419.

branchen- und betriebsgrößenunabhängig angewendet werden kann und allgemeine sowie international akzeptierte Grundsätze und Ziele für die IT definiert.“[22]

Die zeitliche Entwicklung von CoBiT beginnt mit der Veröffentlichung der Version 1 in 1996 und führte über zahlreiche Verbesserungen und Weiterentwicklungen zur aktuellen Version 4.1.

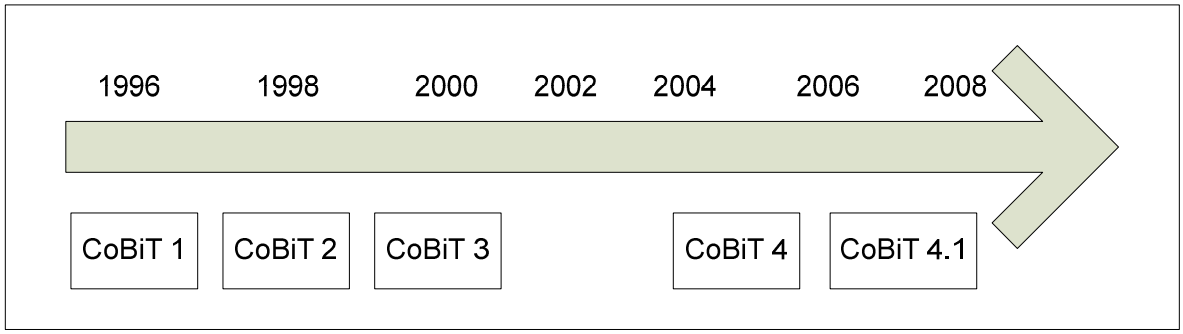

Abbildung 3: Die Entwicklung von CoBiT

Zu Beginn der Entwicklung war CoBiT ein Kontroll-Framework für Prüfer von Informationstechnologien und IT-Prozessen. Durch konsequente Weiterentwicklung ist CoBiT in der Version 4.1 nun ein Framework für IT-Governance (siehe nachfolgendes Schaubild).

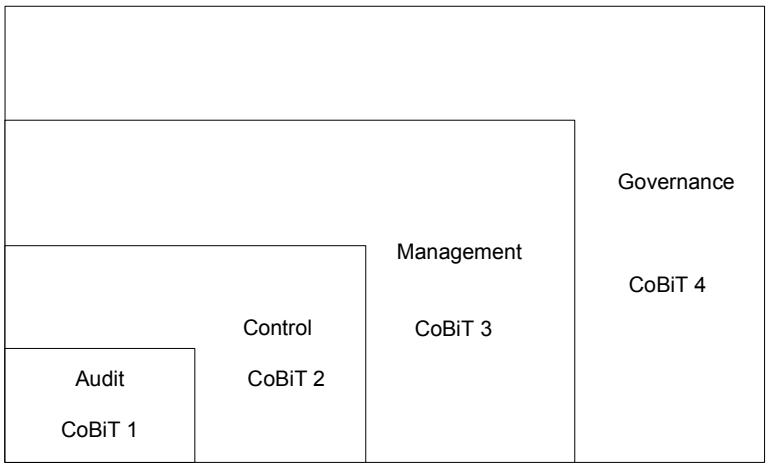

Abbildung 4: Entwicklung und Ausrichtung von CoBiT[23]

Das CoBiT-Framework orientiert sich am Lebenszyklus der Informationstechnologie.

---

22 Johannsen, W.; Goeken, M.: Referenzmodelle für IT-Governance, Heidelberg 2007, Seite 40.

23 Vgl. itSMF Internationale; IT Governance based on CoBiT 4.1, Seite 21.

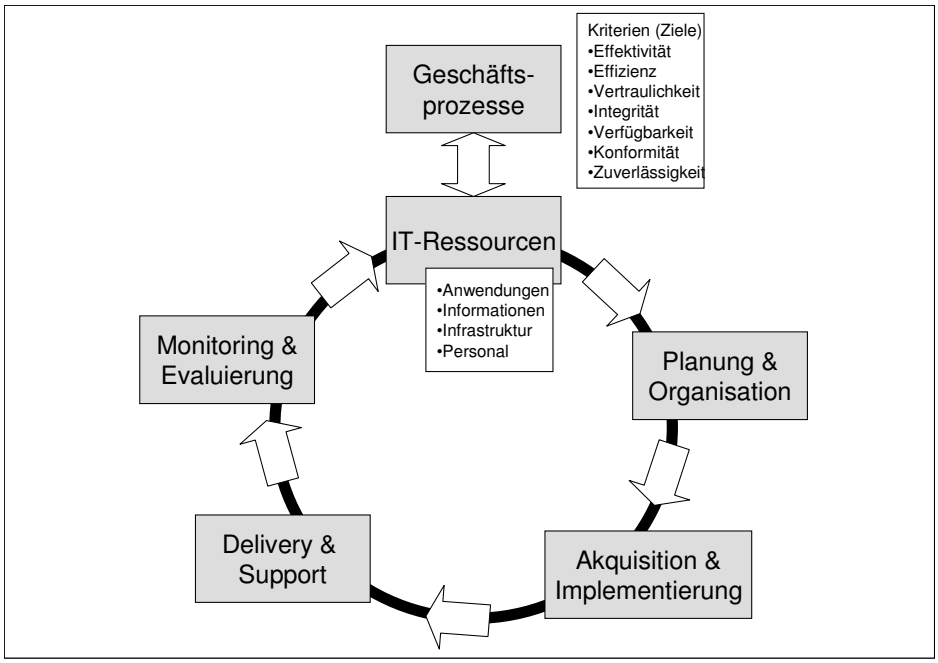

Abbildung 5: CoBiT-Framework[24]

„Der Einstiegspunkt in den IT-Governance-Zyklus ist die Abstimmung der geschäftlichen Zielsetzung mit den IT-Zielen.“[25] Diese aus den Geschäftsprozessen abgeleiteten Anforderungen lassen sich als Informationsanforderungen in drei Informationskategorien einteilen. Jedem CoBiT-Prozess sind die aus den Geschäftsprozessen relevanten Informationsanforderungen zugeordnet und dadurch ist gekennzeichnet, ob dieser IT-Prozess die Erfüllung einer Informationsanforderung primär oder sekundär unterstützt.[26] „Das CoBiT zu Grunde liegende Prinzip ist es, dass die Kontrolle der IT am besten funktioniert, wenn die für das Geschäft notwendige Information in Betracht gezogen wird.“[27] Ein primäres Informationskriterium (P) wird direkt durch das Kontrollziel beeinflusst, während bei einem sekundären Informationskriterium (S) das Kontrollziel dieses nur indirekt beeinflusst.[28]

---

24 Vgl. Rüter A. et al.: IT-Governance in der Praxis, Berlin Heidelberg 2006, Seite 31.

25 Gaulke, M.: a.a.O., Seite 23.

26 Gaulke, M.: a.a.O., Seite 23.

27 Goltsche, W., CoBiT kompakt und verständlich, Wiesbaden 2007, Seite 35.

28 Goltsche, W., a,a,C, Seite 38.

Informationskategorie	Informationsanforderung	Kurzerläuterung
Qualität	Effektivität	Informationen sind relevant für den Geschäftsprozess und werden zeitnah, korrekt, konsistent und in einer verwendbaren Form geliefert.
	Effizienz	Informationen werden unter optimaler Ressourcenverwendung bereitgestellt.
Sicherheit	Vertraulichkeit	Informationen sind vor unberechtigter Veröffentlichung geschützt.
	Verfügbarkeit	Informationen sind dann verfügbar, wenn sie vom Geschäftsprozess benötigt werden.
	Integrität	Informationen sind richtig, gültig und vollständig.
Ordnungsmäßigkeit	Compliance	Einhaltung derjenigen Gesetze, Vorschriften und vertraglichen Regelungen, denen der Geschäftsprozess unterliegt.
	Verlässlichkeit	Informationen werden geeignet bereitgestellt, damit das Management die Organisation steuern kann und der Verantwortung für die gesetzlich oder vertraglich geforderte Berichterstattung nachkommen kann.

Abbildung 6: Übersicht der CoBiT-Informationsanforderungen[29]

Das CoBiT-Framework wird unterteilt in die vier Domänen Planung & Organisation, Akquisition & Implementierung, Delivery & Support sowie Monitoring & Evaluierung. Innerhalb dieser vier Domänen sind 34 IT-Prozesse definiert, die das Unternehmen hinsichtlich der Installierung eines vollumfänglichen Kontrollumfeldes zur Sicherstellung von internen und externen Sicherheitsanforderungen unterstützt.[30]

Diese vier Domänen benötigen IT-Ressourcen in der Form von Anwendungen, Informationen, Infrastruktur und Personal, um die Ziele der Geschäftsprozesse erfüllen zu können.

CoBiT ist ein systematischer Ansatz zur Unterstützung der IT-Governance, um als Kontrollmodell für das Management die Anforderungen aus dem Risikomanagement und an das Interne Kontrollsystem erfüllen zu können.[31]

Der Aufbau dieses Buches mit der Entwicklung eines Modells zur Prüfung der IT-Governance orientiert sich an dem IT-Lifecycle orientierten Ansatz von CoBiT und berücksichtigt die vier Domänen Planung & Organisation, Akquisition & Implementierung, Delivery & Support sowie Monitoring & Evaluierung.[32]

---

29 Gaulke, M.: a.a.O., Seite 23.

30 Vgl. Rüter A. et al.: a.a.O., Seite 32.

31 Vgl. Taubenberger, S.: IT-Prüfungsplanung, Ausgabe 5.2008, Seite 206.

32 Vgl. Goltsche, W.: a.a.O., Seite 25.

Planung & Organisation	Delivery & Support
PO1 Definieren eines strategischen IT-Plans	DS1 Service Level Management
PO2 Definieren der Informationsarchitektur	DS2 Lieferanten-Management
PO3 Definieren der technischen Ausrichtung	DS3 Performance und Kapazitätsmanagement
PO4 Definition der IT-Org. & ihrer Beziehungen	DS4 Continuity Management
PO5 IT-Investitionsmanagement	DS5 System Security Management
PO6 Kommunizieren der Management-Ziele und -Strategien	DS6 Kostenmanagement
PO7 IT-Personalführungsmanagement	DS7 Anwenderschulung und Training
PO8 Managen der Qualität	DS8 Anwenderunterstützung
PO9 Risikomanagement	DS9 Konfigurationsmanagement
PO10 Projektmanagement	DS10 Problem-Management
Akquisition & Implementierung	DS11 Data Management
AI1 Identifizierung automatisierter Lösungen	DS12 Facility Management
AI2 Erwerb und Pflege von Applikations-Software	DS13 Operationsmanagement
AI3 Erwerb und Pflege der technischen IS	Monitoring & Evaluierung
AI4 Befähigung des Betriebes	ME1 Überwachung und Evaluieren IT Perform.
AI5 Zurverfügungstellung von IT-Ressourcen	ME2 Überwachen und Evaluieren intern.Kontr.
AI6 Change Management	ME3 Sicherstellung Compliance
AI7 Installieren und Abnehmen von Systemen und Änderungen	ME4 Sorgen für IT-Governance

Abbildung 7: Übersicht der Prozesse der CoBiT-Domänen[33]

[33] Goltsche, W.: a.a.O., Seite 28.

III. Reifegrade der IT-Prozesse

„If you can't measure it, you can't manage it". [34] Diese Kernaussage aus dem Balanced Scorecard Konzept von Kaplan/Norton ist ebenfalls auf die Prüfung und Steuerung einer IT-Governance anzuwenden.

Für die Prüfung der IT-Governance in einem Unternehmen heißt die Übertragung dieses Prinzips, dass eine Steuerung der Informationstechnologie und der IT-Prozesse nicht möglich ist, wenn nachvollziehbare und vergleichbare Bewertungskriterien fehlen. Die Unternehmensberatung Horvath & Partner stellt dieses Prinzip aus einem anderen Blickwinkel dar: „Was gemessen wird, dem wird Aufmerksamkeit geschenkt".[35]

Beide Aussagen betonen die Wichtigkeit von nachvollziehbaren Bewertungskriterien. Auf diese Anforderungen gibt CoBiT mit dem Reifegradmodell und sechs Reifestufen für jeden IT-Prozess eine Antwort.

Die Verwendung des Reifegradmodells erlaubt es dem Management[36]
- die aktuelle Performance der IT-Prozesse zu bestimmen,
- den gegenwärtigen Status im Rahmen eines Benchmarking mit anderen Betrieben oder Unternehmen zu vergleichen,
- das Unternehmensziel für die Verbesserung festzulegen.

---

34 Robert S. Kaplan; David P. Norton, The Balanced Scorecard – Translating Strategy into Action, Harvard Business School Press 1996, Boston, Massachusetts.

35 Horvath & Partner (Hrsg.), Balanced Scorecard umsetzen, 2. Auflage, Schaeffer Poeschel Verlag, Stuttgart 2001.

36 Vgl. IT Governance Institut, CoBiT 4.0, Seite 21.

Das generische Reifegradmodell von CoBiT sieht sechs Reifestufen vor:

Reife	Kurztext	Beschreibung
0	nicht existent	Ein Prozess ist nicht vorhanden und wird auch vom Unternehmen als nicht relevant eingestuft.
1	Initial	Es ist ebenfalls kein Prozess vorhanden, jedoch ist die Bedeutung eines solchen Prozesses vom Unternehmen erkannt worden.
2	wiederholbar aber intuitiv	Es gibt keinen formalen und abgestimmten Prozess, obwohl verschiedene Personen ähnliche Funktionen wiederholt ausüben.
3	definiert	Es gibt standardisierte Prozesse, die sowohl dokumentiert als auch geschult wurden. Den einzelnen Mitarbeitern im Unternehmen ist jedoch die Einhaltung des definierten Prozessablaufs überlassen.
4	gemanaged und messbar	Prozesse sind definiert, geschult und dokumentiert. Die Einhaltung der Abläufe wird überwacht. Es finden regelmäßige Prozessverbesserungen statt. Die Automatisierung durch IT ist flächendeckend nicht vorhanden.
5	optimiert	Laufende Verbesserungen und ein Benchmarking haben zu optimalen Prozessen mit hoher Automatisierung durch die IT geführt.

Die Reifestufe 4 wird als gemanaged bezeichnet und beinhaltet die Überwachung der Einhaltung der Abläufe. Diese Reifestufe 4 muss nach dem neuen Bilanzrechts-modernisierungsgesetz als Mindestanforderung für die Wirksamkeit eines internen Kontrollsystems gelten. Nähere Einzelheiten dazu finden Sie im Kapitel VIII dieses Buches.

Nachfolgend werden für jeden der 34 IT-Prozesse die Kriterien für die Beurteilung der Reife beschrieben.

1 Planung und Organisation

1.1 PO1 Definieren eines strategischen IT-Plans

Reife	Kurztext	Beschreibung
0	nicht existent	Es gibt keinen strategischen IT-Plan. Die Unternehmensleitung sieht keine Notwendigkeit zur Festlegung eines strategischen IT-Plans.
1	Initial	Die Unternehmensleitung hat das Bewusstsein zur Notwendigkeit eines strategischen IT-Plans. Eine IT-Planung erfolgt nur nach Bedarf und folgt keiner festgelegten Strategie.
2	wiederholbar aber intuitiv	Ein Abgleich des strategischen IT-Plans mit der Unternehmensleitung erfolgt nur fallweise. Risiko und Nutzen von strategischen IT-Entscheidungen werden intuitiv festgelegt.
3	definiert	Eine strategische IT-Planung ist vorhanden und dokumentiert. Ein Austausch mit der Unternehmensleitung erfolgt in regelmäßigen Besprechungen. Der Prozess der strategischen IT-Planung wird von Managern durchgeführt, die jedoch auf Einhaltung der Vorgaben nicht geprüft werden.
4	gemanaged und messbar	Die strategische IT-Planung ist fester Bestandteil des Unternehmens und wird von der Unternehmensleitung überwacht. Die IT-Strategie ist mit der Unternehmensstrategie abgestimmt.
5	optimiert	Die strategische IT-Planung spiegelt die Berücksichtigung von technologischen und wirtschaftlichen Veränderungen wieder und orientiert sich an aktuellen Benchmarking Ergebnissen. Eine fortlaufende Aktualisierung ist gewährleistet.

1.2 PO2 Definieren der Informationsarchitektur

Reife	Kurztext	Beschreibung
0	nicht existent	Die Bedeutung der Informationsarchitektur für das Unternehmen ist vom Unternehmen nicht erkannt worden. Das Wissen und die Fähigkeiten zur Beurteilung einer Informationsarchitektur sind nicht vorhanden.
1	Initial	Die Notwendigkeit der Bedeutung der Informationsarchitektur ist dem Unternehmen bewusst. Eine Berücksichtigung erfolgt jedoch nur fallweise und nicht konsistent.
2	wiederholbar aber intuitiv	Die Informationsarchitektur wird von mehreren Mitarbeitern im Unternehmen regelmäßig durch einen intuitiven Prozess berücksichtigt. Die Fachkenntnisse werden durch die Erfahrungen dieser Mitarbeiter entwickelt.
3	definiert	Die Informationsarchitektur hat eine hohe Bedeutung und findet seinen Niederschlag in einer verantwortungsvollen Umsetzung. Verantwortlichkeiten sind definiert und kommuniziert. Schulungen werden unregelmäßig durchgeführt.

4	gemanaged und messbar	Es gibt einen standardisierten Prozess zur Entwicklung und Umsetzung der Informationsarchitektur. Methoden und Techniken zur Unterstützung sind vorhanden und werden eingesetzt. Verschiedene IT-Werkzeuge zur Unterstützung sind vorhanden, jedoch nicht integriert.
5	optimiert	Die Informationsarchitektur ist umfassend umgesetzt worden. Die IT-Mitarbeiter haben hohe Fachkenntnisse und werden regelmäßig auf neue technologische Anforderungen vorbereitet. Ein kontinuierlicher Verbesserungsprozess gewährleistet eine permanente Optimierung.

1.3 PO3 Definieren der technischen Ausrichtung

Reife	Kurztext	Beschreibung
0	nicht existent	Das Unternehmen sieht keine Notwendigkeit, eine technische Ausrichtung der IT zu definieren. Ein Verständnis ist nicht vorhanden.
1	Initial	Die Notwendigkeit zur Definition der technischen Ausrüstung ist vom Unternehmen erkannt worden. Eine Umsetzung von Anforderungen erfolgt jedoch nur im Bedarfsfall. Anbieter von Hard- und Software nehmen Einfluss auf die technologische Ausrichtung.
2	wiederholbar aber intuitiv	Die notwendige Planung einer technischen Ausrichtung der IT ist erkannt und kommuniziert. Einzelne Personen haben eigene Verfahren entwickelt und Abläufe entwickelt und aufgrund ihrer Erfahrungen weiterentwickelt.
3	definiert	Die Unternehmensleitung hat ein klares Signal für die Wichtigkeit der Planung der technischen Ausrichtung gegeben. Diese ist ausgerichtet auf den strategischen IT-Plan und in einem Prozess niedergeschrieben. Ein aktueller IT-Infrastrukturplan ist vorhanden, der jedoch nicht vollständig Verwendung findet.
4	gemanaged und messbar	Die Sicherstellung der Aufrechterhaltung und Weiterentwicklung der technischen Ausrichtung erfolgt durch die Unternehmensleitung. Die IT-Mitarbeiter besitzen die notwendigen Fachkenntnisse zur Beurteilung der technischen Möglichkeiten und Entwicklungen.
5	optimiert	Neue Technologien werden erforscht und untersucht. Industrienormen werden berücksichtigt und für die Ausrichtung der IT im Unternehmen bewertet. Änderungen in der technologischen Ausrichtung werden von der Unternehmensleitung geprüft und genehmigt.

1.4 PO4 Definieren der IT-Organisation und deren Beziehungen

Reife	Kurztext	Beschreibung
0	nicht existent	Die IT-Organisation unterstützt nicht oder nicht wirksam die Erreichung der Unternehmensziele.
1	Initial	Das Verständnis für die Errichtung einer wirksamen IT-Organisation ist vorhanden, die Umsetzung jedoch nicht erfolgt. Ein formalisierter Prozess ist nicht vorhanden, die IT-Organisation reagiert erst spät auf Anforderungen.
2	wiederholbar aber intuitiv	Eine IT-Organisation ist vorhanden und im Unternehmen kommuniziert. Die Reaktionen auf Anforderungen der Fachbereiche werden jedoch unabgestimmt durchgeführt und von wenigen Schlüsselpersonen durchgeführt.
3	definiert	Die IT-Organisation ist mit Rollen und Verantwortlichkeiten definiert und hat sich an den Unternehmensanforderungen und der IT-Strategie orientiert. Das Beziehungsmanagement ist eingerichtet und formal definiert.
4	gemanaged und messbar	Die Anforderungen aus den Fachbereichen werden von der IT-Organisation vorausschauend aufgenommen. Die Rollen in der IT-Organisation sind klar definiert und die Beziehungen festgelegt. Fachkenntnisse und Fertigkeiten sind bei den IT-Mitarbeitern zur Ausführung der Tätigkeiten vorhanden.
5	optimiert	Es existiert eine flexible IT-Organisationsstruktur. Benchmarking wird regelmäßig genutzt, um sich an den Best Practices der Industrie zu orientieren. Es findet ein kontinuierliche Verbesserungsprozess statt.

1.5 PO5 IT-Investitionsmanagement

Reife	Kurztext	Beschreibung
0	nicht existent	Investitionen in die Informationstechnologie werden im Unternehmen als unbedeutend behandelt. Ein Bewusstsein für die Wichtigkeit der Überwachung und Verfolgung von IT-Investitionen ist nicht vorhanden.
1	Initial	Ein IT-Investitionsmanagement ist nicht vorhanden, wird jedoch von der Unternehmensleitung als notwendig erkannt. Dennoch unterliegen IT-Investitionen keinem standardisierten Ablauf und werden fallweise geregelt. Dokumentationen der Investitionen sind lückenhaft und unzureichend vorhanden.
2	wiederholbar aber intuitiv	Ein IT-Investitionsmanagement ist vorhanden und den Mitarbeitern der IT bekannt. Für die Auswahl und Budgetierung von IT-Investitionen gibt es einen Prozess, dessen Einhaltung jedoch nur durch vereinzelte Mitarbeiter geschieht.
3	definiert	Ein Prozess für das IT-Investitionsmanagement ist vorhanden, dokumentiert und geschult. Die Budgetierung orientiert sich an den strategischen Plänen des Unternehmens. Ein formalisiertes Verfahren zur Freigabe von IT-Investitionen ist eingerichtet.

4	gemanaged und messbar	Die Lebenszykluskosten einer IT-Investition werden untersucht und Budgetabweichungen analysiert und dokumentiert. Der Nutzen und Ertrag einer IT-Investition werden berechnet.
5	optimiert	Ein branchenspezifisches Benchmarking wird durchgeführt und Erkenntnisse daraus führen zu neuen Ansätzen zur Effizienzsteigerung im Unternehmen. Die Lebenszykluskosten einer IT-Investition werden für die Entscheidung berücksichtigt.

1.6 PO6 Kommunizieren der Management-Ziele und -Strategien

Reife	Kurztext	Beschreibung
0	nicht existent	Eine Kommunikation der IT-Management-Ziele und IT-Strategien erfolgt nicht und es besteht auch kein Verständnis für die Notwendigkeit.
1	Initial	Die Kommunikation von Richtlinien, Verfahren und Standards erfolgt erst bei einem tatsächlichen Bedarf, und dann im Nachhinein. Dies oft in nicht abgestimmter und inkonsistenter Art und Weise.
2	wiederholbar aber intuitiv	Eine Notwendigkeit zur Kommunikation wird gesehen, jedoch im Unternehmen nicht konsistent behandelt. Die vorhandenen Verfahren sind aus der täglichen Arbeit entstanden und weder abgestimmt noch formalisiert.
3	definiert	IT-Management-Ziele und IT-Strategien unterliegen einem standardisierten und kommunizierten Prozess. Die Unternehmensleitung hat die hohe Bedeutung erkannt und entsprechende Maßnahmen veranlasst.
4	gemanaged und messbar	Die Unternehmensleitung ist für die Kommunikation der IT-Ziele und IT-Strategien verantwortlich. Diese Verantwortung hat sie delegiert und für ausreichende Ressourcen gesorgt. Richtlinien und Anweisungen sind vollständig vorhanden.
5	optimiert	Eine Ausrichtung auf die Vision des Unternehmens ist gewährleistet und wird durch regelmäßige Reviews aktualisiert. Externe Experten werden zur neutralen und objektiven Beurteilung eingesetzt.