Einführung Control Objectives for Information and Related Technology (CobiT) 4.1 und verwendete Indikatoren

Erik Muttersbach

Software Engineering for Business Information Systems (sebis)
Proseminar: IT-Kennzahlen und Softwaremetriken, SS 2010

Institut für Informatik I19
Technische Universität München
Boltzmannstr. 3
D-85748 Garching
muttersb@in.tum.de

Abstract: CobiT ist ein weit verbreitetes und anerkanntes Framework zur IT Governance. In dieser Arbeit sollen die in CobiT vorgeschlagenen und unterstützten Möglichkeiten zur Messung der IT erläutert werden. Der ersten beiden Abschnitte zeigen den grundsätzlichen Aufbau des Frameworks, der dritte Teil befasst sich mit dem Messen in CobiT und im vierten und fünften Teil wird ein Überblick über den Einsatz von CobiT in der Praxis und die dessen zukünftige Entwicklung gegeben.

1 Motivation

In vielen Unternehmen sind Informationen und IT einer der wichtigsten, aber auch einer der vom Management am wenigsten verstandenen Teile. Die Information Systems Audit and Control Association (ISACA), die CobiT entwickelt hat, schreibt in der Publikation dazu: „Erfolgreiche Unternehmen erkennen den Nutzen der Informationstechnologie und verwenden sie, um den Stakeholder-Value zu erhöhen […]“ [IT05]. Daher sollten Organisationen die Qualität der IT und Sicherheit der Informationen sicherstellen, über Steuerungsmöglichkeiten über die IT verfügen, ihre IT Ressourcen optimieren und den Status der unternehmensweiten IT verstehen.

Bei der Erreichung dieser Ziele hilft das CobiT Framework. Es wird von Führungskräften im Unternehmen angewandt, um die IT aus Unternehmenssicht zu steuern. CobiT bietet dem Management eine verständliche Sichtweise auf die IT, hilft Ziele für die IT zu definieren und diese an die Unternehmensziele anzupassen und definiert Metriken und Kennzahlen, die die zuverlässige Messung der IT erlauben.

2 Komponenten des Frameworks

2.1 Control Objectives

Controls werden in der CobiT 4.1 Publikation definiert als „Richtlinien, Verfahren, Praktiken und Organisationsstrukturen […]“ [IT05] die der Erreichung der Unternehmensziele dienen. *Controls* könnten zum Beispiel E-Mail Sicherheitsstandards, Firewall- und Antivirensoftware, Passwortregeln die eine bestimmte Komplexität vorschreiben oder ein Komitee zur Überwachung der Einhaltung der Sicherheitsrichtlinien des Unternehmens sein.

Control Objectives, namensgebend für das CobiT Framework, sind darauf aufbauend „Aussage(en) über das gewünschte Ergebnis oder den zu erreichenden Zweck, der mit der Umsetzung von, in bestimmten Aktivitäten integrierten Controls […] erreicht werden soll.“ [IT05]. Ein mögliches *Control Objective* ist „Stelle den kontinuierlichen Betrieb der angebotenen Services sicher“. Dies kann z.B. durch das regelmäßige Erstellen eines Backups und der Erstellung eines Systemausfallplans erreicht werden. Beide Maßnahmen stellen *Controls* in Bezug auf das genannte *Control Objective* dar.

2.2 Goals

Um die IT erfolgreich zur Unterstützung der Unternehmensstrategie einzusetzen, müssen klare Ziele für alle Verantwortlichen in einer einheitlichen Geschäftssprache entwickelt werden. Diese Ziele sind in CobiT durch *Goals* repräsentiert, die auf 4 verschieden Ebenen definiert werden.

Ausgehend von der Unternehmensstrategie werden Unternehmensziele für die IT bestimmt, in CobiT als *Business Goals* bezeichnet. Zur Realisierung eines *Business Goals* werden wiederum *IT Goals* abgeleitet, die zur Erreichung der *Business Goals* auf IT Ebene notwendig sind. Zur Erreichung der *IT Goals* werden *Prozesse* implementiert, von denen jeder einen oder mehrere *Process Goals* hat, die eine Aussage darüber treffen welche konkreten Ziele durch den Prozess erreicht werden. Zur Durchführung der *Prozesse* und der damit verbundenen Erreichung der *Process Goals* wiederum werden von CobiT Activities angegeben die die konkrete Umsetzung der *Process Goals*

erlauben. Jede der *Activities* hat *Activity Goals* die, analog zu *Process Goals*, die konkreten Ziele die mit der *Activity* verfolgt werden spezifizieren. Die Ableitung der Goals erfolgt also strikt Top-Down. Anforderungen die die IT an das Unternehmen und die Unternehmensziele, z.B. durch technischen Fortschritt getrieben, hat werden nicht beachtet.

Im Beispiel (Abbildung 1) ist eines der Ziele der Unternehmensstrategie „Erhalte den Ruf und die Vormachtstellung des Unternehmens“. Zur Erreichung dieses Ziels wird unter anderem die Erreichung des *IT Goals* „Sicherstellen, dass IT Services Angriffe überstehen und wieder hergestellt werden können“ nötig sein. Dieses *IT Goal* durch verschiedene Prozesse umgesetzt, von denen einer das *Process Goal* „Erkenne und kläre Unberechtigten Zugang zu Informationen, Anwendungen und Infrastruktur auf“ besitzt. Konkrete Maßnahmen wie das *Process Goal* zu erreichen ist, liefern die *Activities* und deren *Activity Goals*.

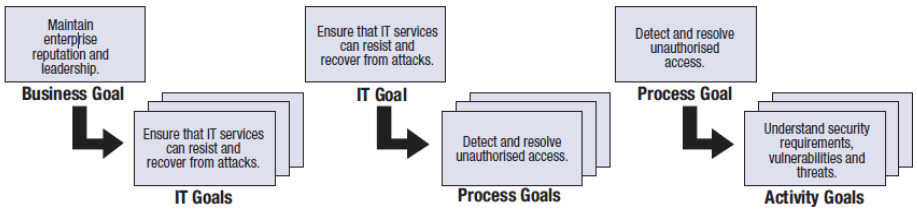

Abbildung 1 - Business, IT, Process und Activity Goals [IT07]

Die Top-Down Ableitung vermittelt den Eindruck als ob die Goals in einer baumartigen Struktur organisiert sind. Dies ist jedoch nur bei Betrachtung eines einzigen Business Goals der Fall. Es ist durchaus üblich das *IT* oder *Process Goals* verschiedenen *Business*, bzw. *IT Goals* zugeordnet werden, sodass ein gerichteter Graph entsteht.

Sind die *Business Goals* des Unternehmens bestimmt, müssen die Mappings zu den weiteren Goals nicht manuell vorgenommen werden. CobiT 4.1 liefert dazu zwei Tabellen:

1. *Linking Business Goals to IT Goals.* Diese Tabelle verbindet generische Unternehmensziele mit den IT Zielen, die normalerweise die angegebenen Business Goals unterstützen.
2. *Linking IT Goals to IT Processes.* Die Tabelle zeigt wie IT Goals mit den IT Prozessen verknüpft werden.

Da die konkreten Unternehmensziele in jedem Unternehmen verschieden sind, gibt CobiT 17 generische Unternehmensziele vor, die an die konkreten Unternehmensziele angepasst werden müssen.

2.3 Prozesse

Das Management eines Unternehmens nutzt Prozesse um die Aktivitäten der IT zu strukturieren und zu organisieren. CobiT bietet hierzu ein generisches Prozessmodell an, das zugleich eines der Kernkomponenten des Frameworks darstellt. Prozesse bilden eine zentrale Einheit, denn sie werden genutzt um die von den Business Goals abgeleiteten IT Goals zu erreichen und enthalten *Activities*, die definieren welche konkreten Handlungen durchgeführt werden müssen um die zugehörigen *Activity Goals* zu erreichen und damit die unterstützenden Prozesse.

Die CobiT Publikation (IT Governance Institute, 2007) definiert 34 Prozesse die in 4 Domänen aufgeteilt sind, welche im Folgenden erläutert werden:

1. **PO – Plan an Organize.** Diese Domäne enthält Prozesse die der Entwicklung und Kommunikation einer IT Strategie und der Anbindung dieser an die Unternehmensstrategie dienen.
2. **AI – Acquisition and Implementation** beinhaltet diejenigen Prozesse, die IT Lösungen identifizieren und diese entwickeln oder beschaffen. Außerdem enthält diese Domäne Prozesse die bestehende Systeme Warten und Änderungen durchführen um sicherzustellen, dass die Lösungen weiterhin den Unternehmenszielen entsprechen.
3. **DS – Delivery and Support.** In dieser Domäne sind Prozesse gesammelt die der eigentlichen Erbringung der Leistung, dem Daten-, Sicherheits- und Kontinuitätsmanagement und dem Support für IT Kunden dienen.
4. **ME – Monitoring and Evaluation** enthält alle Prozesse die das Messen der Prozesse und die Einhaltung von Regulativen (z.B. Gesetze, Unternehmensrichtlinen) denen die Prozesse unterliegen.

3 Messen in CobiT

Eines der Ziele die CobiT verfolgt, ist dass das Management eines Unternehmens seine IT besser versteht und eine Sichtweise auf die IT erhält, die es erlaubt Aussagen über Entwicklung und Stand des Unternehmens zu treffen. Hierzu werden in CobiT zwei Möglichkeiten die IT zu messen vorgeschlagen: Sogenannte Maturity Models werden angewandt um den Grad der Implementierung eines Prozesses zu messen. Weiterhin wird ein Kennzahlensystem definiert welches die Effektivität und Performance von CobiT Goals misst. Auf beide Möglichkeiten wird im Folgenden eingegangen.

3.1 Maturity Models

Das CobiT Reifegradmodell hat zum Ziel, den Grad der Implementierung eines Prozesses, also dessen Leistungsfähigkeit, zu messen und diesen mit einem angestrebten Reifegrad und dem Durchschnitt der Industrie zu vergleichen.

Damit hilft es Fachleuten der IT, dem Management den aktuellen Stand der Unternehmensprozesse darzustellen und eine verständliche Sichtweise anzubieten. Dem Management hilft es festzustellen, wie weit das Unternehmen von angestrebten Reifegraden entfernt ist und welche Schritte nötig sein werden um diese zu erreichen. Außerdem bietet es einen Benchmark an der eine Einordnung des Unternehmens in der Branche vorgenommen wird.

Ein Prozess wird mit einer Skala von 0 bis 5 bewertet. Ein Reifegrad von 0 bedeutet der Prozess ist nicht implementiert, Reifegrad 5 sagt aus das der Prozess voll umgesetzt und optimiert ist. CobiT stellt eine generische Definition der Reifegrade bereit, welche folgend im Einzelnen dargestellt werden:

0. **Nicht Implementiert.** Ein Reifegrad 0 bedeutet, dass der Prozess nicht implementiert ist.
1. **Initial.** Wird ein Prozess mit Grad 1 beurteilt beutet dies, das Problemlösungsansätze bei jeder Umsetzung des Prozesses neu erarbeitet werden, voneinander abweichen und kein geregelter Ablauf des Prozesses definiert ist.
2. **Wiederholbar.** Bei Beurteilung mit Reifegrad 2 sind sich wiederholende Abläufe bei der Umsetzung erkennbar, jedoch ist die erfolgreiche Durchführung stark von individuellen Qualitäten der Durchführenden abhängig.
3. **Definiert.** Ein Prozess der mit Grad 3 bewertet wird, ist standardisiert und dokumentiert und kann jederzeit wiederholt werden. Abweichungen und Fehler bei der Umsetzung werden jedoch nicht erkannt.
4. **Gemanagt.** Die Beurteilung mit Grad 4 kann stattfinden, wenn der Prozess einem Monitoring unterliegt, d.h. Messungen durchgeführt werden und somit auf Abweichungen und Fehler bei der Realisierung reagiert werden kann. Weiterhin wird ein Prozess mit Grad 4 fortwährend verbessert und an Entwicklungen angepasst.
5. **Optimiert.** Durch laufende Verbesserungen und Vergleiche mit anderen Unternehmen sind die Prozesse auf Best-Practice Niveau. Auf unternehmensexterne und interne (z.B. geänderte Unternehmensanforderungen für die IT) Änderungen kann reagiert werden. Automatisierung findet umfassend statt und stellt Werkzeuge zur Qualitätssicherung bereit.

Eine detailliertere Beschreibung der Reifegradstufen und deren Klassifikation nach den 6 Kriterien „Bewusstsein und Kommunikation“, „Policies, Standards und Verfahren“, „Werkzeuge und Automatisierung“, „Skills und Expertise“, „Zuständigkeit und Verantwortung“ sowie „Zielsetzung und Messung“ befindet sich in der CobiT 4.1 Publikation [IT07].

Um einen Prozess zu bewerten müssen nun nicht die konkreten Klassifikationen für einen Reifegrad in Bezug auf den Prozess von dem oben genannten generischen Modell ermittelt werden, sondern diese können direkt aus der CobiT Prozessbeschreibung entnommen werden. Die CobiT 4.1 Publikation liefert zu jedem Prozess ein umfangreiches Maturity Model, welches Helfen soll den vorhandenen Prozess einzuschätzen. So wird für den Prozess *DS5 Ensure Systems Security* [IT07] folgende Beschreibung zur Klassifikation in Reifegradstufe 1 angegeben:

„Das Unternehmen erkennt die Notwendigkeit der IT-Sicherheit. Das Bewusstsein für die Notwendigkeit der Sicherheit hängt hauptsächlich von der Einzelperson ab. Die IT-Sicherheit ist reaktiv ausgerichtet. IT-Sicherheit wird nicht gemessen. Erkannte IT-Sicherheitsverstöße provozieren die Suche nach Schuldigen, da die Verantwortlichkeiten unklar sind. Die Reaktion auf Verstöße gegen die IT-Sicherheit ist unvorhersehbar.“ [IT07].

Aufgrund der verschiedenen Aspekte die zur Bewertung der Reife herangezogen werden, sind Prozesse natürlich nicht diskreten Werten zwischen 0 und 5 zuzuordnen sondern können bezüglich verschiedener Kriterien auf unterschiedlichen Stufen eingeordnet werden. Eine mögliche Beispielausprägung der Reife des Prozesses *DS5 Ensure Systems Security* zeigt Abbildung 2.

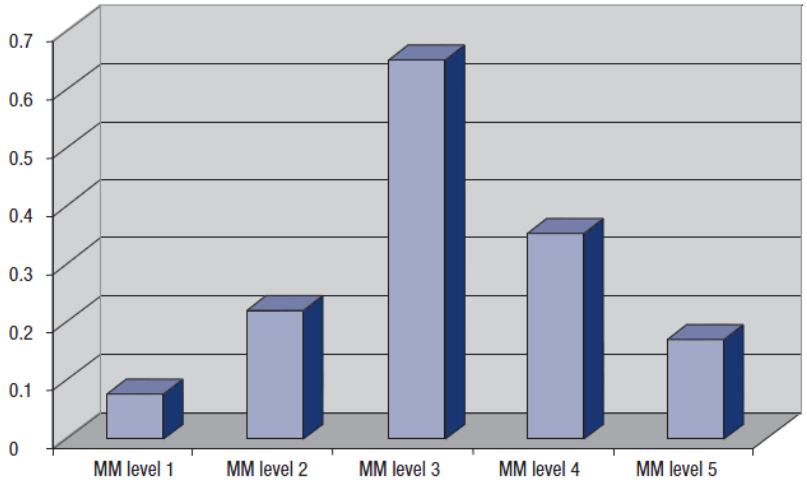

Abbildung 2 - Mögliche Ausprägung der Reife des Prozesses *DS5 Ensure Systems Security*

Bezugnehmend auf obiges Beispiel könnte der Prozess zwar größtenteils Reifegrad 3 oder mehr erreicht haben, wird in einigen Aspekten, z.B. *Werkzeuge und Automatisierung* aber trotzdem noch mit Grad 1 und 2 bewertet da z.B. die IT Sicherheit nicht gemessen wird und das Bewusstsein für die Notwendigkeit eines Sicherheitskonzept noch limitiert ist.

Um ein Benchmarking durchzuführen wird vereinfachend der Durschnitt der Maturity Levels genutzt um den Prozess auf einer Skala abzutragen (siehe Abbildung 3 - Benchmarking mit dem Maturity Modell). Auf dieser Skala kann der Prozess mit der „Ziel-Reife“ und dem Industriedurchschnitt verglichen werden. Die angestrebte Reife des Prozesses muss vor Anwendung des Maturity Models aus den Unternehmenszielen abgeleitet werden. Hierbei ist zu beachten, dass aus zweierlei Gründen nicht pauschal Maturity Level 5 angestrebt wird. Einerseits ist es aus praktischen Sicht nicht immer erforderlich Grad 5 zu erreichen. Als Beispiel sei der Prozess „*DS8 Manage Service Desk and Incidents*“, der die Einrichtung eines Service Desks und effiziente Abarbeitung von IT User Anfragen zum Inhalt hat, genannt. Die Relevanz dieses Prozesses in stark endkundenorientierten Unternehmen dürfte deutlich höher sein als beim Durschnitt der IT Unternehmen. Andererseits erfordert das Weiterentwickeln des Prozesses bezüglich seiner Reife natürlich die Aufwendung von zeitlichen, personellen und finanziellen Ressourcen. Hierbei muss zwischen Kosten und Relevanz abgewogen werden um einen optimalen „Return On Investment“ zu erhalten.

Das Management kann nun anhand der Reife des Prozesses folgende Fragestellungen entscheiden:

– Wo steht das Unternehmen zurzeit bezüglich der Prozesszielerfüllung?
– Was ist das angestrebte Ziel, bzw. der angestrebte Reifegrad und wie weit ist das Unternehmen davon entfernt?
– Ist das Unternehmen besser oder schlechter positioniert als Unternehmen der gleichen Branche?

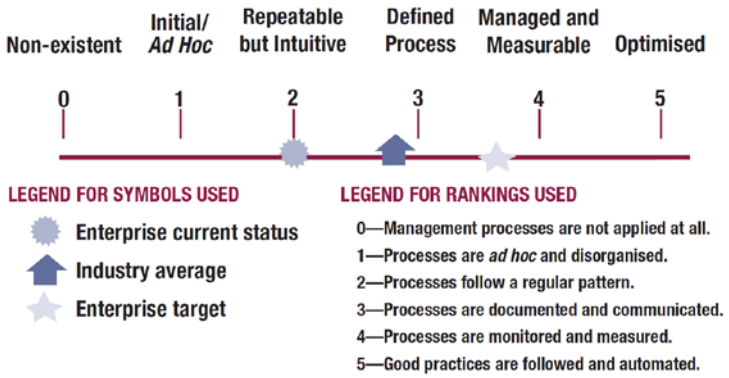

Abbildung 3 - Benchmarking mit dem Maturity Modell [IT07]

Abbildung 3 zeigt eine mögliche Einordnung der Prozessreife auf einer Skala von 0 bis 5 zusammen mit dem durchschnittlichen Reifegrad des Prozesses in Unternehmen der gleichen Branche und dem „Zielreifegrad“ des Unternehmens.

3.2 Outcome Measures und Performance Indicators

Wie in der Motivation zur Nutzung des CobiT Frameworks beschrieben, ist eines der Ziele CobiTs dem Management des Unternehmens zu helfen die IT zu verstehen, zu steuern und zu überwachen. Um dieses Ziel zu erreichen werden neben *Maturity Models* auch sogenannte *Outcome Measures* und *Performance Indicators* eingesetzt. *Outcome Measures* messen die Effektivität eines Goals, geben also Aufschluss über den Grad der Erreichung des Goals. Diese Aussage wird von *Outcome Measures* rückwirkend getroffen. *Performance Indicators* messen die Effizienz eines Goals, also wie wahrscheinlich die Erreichung des Goals, in Bezug auf den Teilaspekt den der *Performance Indicator* misst, ist.

CobiT verknüpft die *Outcome Measures* und *Performance Indicators* zweier Ebenen nun so, dass die *Outcome Measures* der n. Ebene die *Performance Indicators* der (n+1). Ebene bilden. Dies wird möglich, da die Goals Top-Down abgeleitet wurden und die Goals der N. Ebene der Erreichung der (N+1). Ebene dienen. Anhand von Abbildung 4 ist diese Verknüpfung exemplarisch gezeigt.

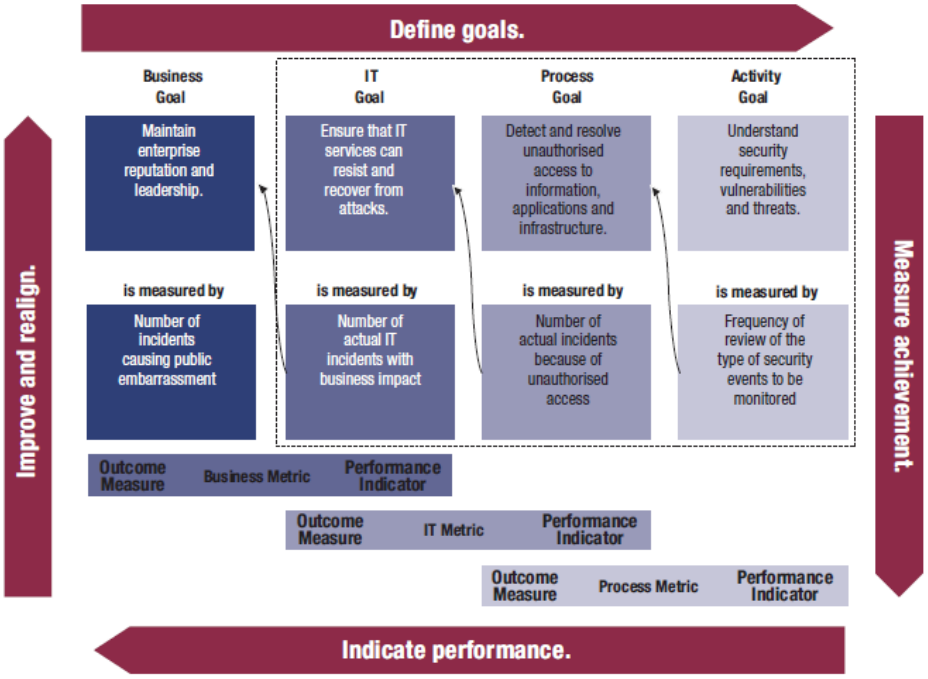

Abbildung 4 - Outcome Measures für verschiedenene Goals [IT07]

Neben den *Maturity Models* sind die *Outcome Measures* und *Performance Indicators* direkt von Cobit unterstützte Möglichkeiten Effizienz und Effektivität zu messen. Das bedeutet, dass in jeder Prozessbeschreibung Kennzahlen angegeben werden die *Outcome Measures* und *Performance Indicators* für diesen Prozess darstellen.

4 Entwicklung und Ausblick

CobiT wurde ursprünglich vom Information Systems Audit and Control Association (ISACA), dem internationalen Verband der IT Prüfer entwickelt. 1996 erschien CobiT in der Version 1.0, die Version 2.0 folgte 1998. Seit CobiT 3.0, welches im Jahr 2000 veröffentlicht wurde, obliegt CobiT dem IT Governance Institute (ITGI) und wird von diesem weiterentwickelt und verwaltet. 2005 publizierte das ITGI Cobit 4.0.

Zurzeit liegt das Framework in der 2007 erschienenen Version 4.1 vor. Eine Veröffentlichung der Version 5 wird voraussichtlich 2011 stattfinden. In dieser Version wird inbesondere die Integration mit den von der ISACA entwickelten Frameworks Val IT und Risk IT vorangetrieben.

5 CobiT in der Praxis

Seit der Veröffentlichung der ersten Version von CobiT, 1996, hat sich das Framework zum De-Facto Standard für IT Governance entwickelt. Laut einer Studie der ISACA setzen 95% der amerikanischen Großunternehmen CobiT ganz oder teilweise ein [Wi10].

Es existieren zahlreiche Publikationen des IT Governance Institute (ITGI), die eine Ausrichtung und Integration mit anderen Frameworks beschreiben, beispielsweise das wirtschafts- und managementorientierte COSO (Committee of Sponsoring Organizations of the Treadway Commission) Framework oder die IT-spezifische IT Infrastructure Library (ITIL).

Es gibt zwei zentrale Gründe warum CobiT in Unternehmen eingeführt wird. Ein häufiges Einsatzgebiet sind IT Audits und IT Revisionen. Hier findet eine Orientierung an relevanten CobiT Prozessen und eine Evaluierung der ausgewählten Prozesse mit dem *Maturity Model* statt. Weiterhin kann CobiT auch „konstruktiv“ in einem Unternehmen eingeführt werden um die IT zu kontrollieren und strukturieren. Hierbei werden die CobiT Prozesse als Modell für die Implementierung im Unternehmen genutzt.

6 Literaturverzeichnis

[IT05] IT Governance Institute. (2005). *CobiT 4.0 Deutsche Version.* Rolling Meadows: IT Governance Institute.

[IT07] IT Governance Institute. (2007). *CobiT 4.1*. Rolling Meadows: IT Governance Institute.

[Wi10]Wikipedia. (03. 08 2010). *Wikipedia*. Abgerufen am 03. 08 2010 von Wikipedia: http://de.wikipedia.org/wiki/CobiT

Anmerkung: Für diese Arbeit wurde als Hauptquelle das CobiT 4.1 Dokument (englisch) verwendet. Cobit 4.0 in der deutschen Version wurde herangezogen um korrekte deutsche Übersetzungen zu verwenden, sofern eine Entsprechung des Inhalts der Version 4.1 in der Version 4.0 zu finden war.