Ramin, Lars; Klotz, Michael

Working Paper

Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT

SIMAT Arbeitspapiere, No. 01-09-003

Provided in Cooperation with:
Hochschule Stralsund, Stralsund Information Management Team (SIMAT)

Suggested Citation: Ramin, Lars; Klotz, Michael (2009) : Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT, SIMAT Arbeitspapiere, No. 01-09-003, Fachhochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund, https://nbn-resolving.de/urn:nbn:de:0226-simat01090039

This Version is available at:
https://hdl.handle.net/10419/60094

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 01-09-003

Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT

Lars Ramin
Prof. Dr. Michael Klotz

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team

September 2009

ISSN 1868-064X

Ramin, Lars; Klotz, Michael: Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2009 (SIMAT AP, 1 (2009), 3), ISSN 1868-064X

Download über URN vom Server der Deutschen Nationalbibliothek:
http://nbn-resolving.de/urn:nbn:de:0226-simat01090039

Impressum
Fachhochschule Stralsund
SIMAT Stralsund Information Management Team
Zur Schwedenschanze 15
18435 Stralsund
www.fh-stralsund.de
www.simat.fh-stralsund.de

Herausgeber
Prof. Dr. Michael Klotz
Fachbereich Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@fh-stralsund.de

Autoren

Lars Ramin, Dipl. Betriebswirt, beendete im Jahr 2008 erfolgreich sein Studium der Betriebswirtschaftslehre (Schwerpunkt: Marketing/Controlling/Organisation) an der FH Stralsund. Seitdem arbeitete er in verschiedenen Projekten als Projektcontroller und Projektleiter. Im August 2009 gründete er zusammen mit zwei weiteren Kommilitonen die „emwena UG (haftungsbeschränkt)“, wobei er für Strategieberatung und Projektentwicklung verantwortlich zeichnet.

Prof. Dr. Michael Klotz lehrt und forscht am Fachbereich Wirtschaft der FH Stralsund auf den Gebieten der Unternehmensorganisation und des Informationsmanagements. Er ist u. a. Wissenschaftlicher Leiter des SIMAT, regionaler Ansprechpartner der gfo Gesellschaft für Organisation e.V., wissenschaftlicher Beirat der ISACA und Mitherausgeber der Zeitschrift „IT-Governance“.

Aufgaben und Verantwortlichkeiten von IT-Nutzern nach COBIT

Lars Ramin[1]
Prof. Dr. Michael Klotz[2]

Zusammenfassung: Als wesentliche Beteiligte am IT-Management (bzw. Informationsmanagement) werden für gewöhnlich die Unternehmensleitung, die Fachabteilung und die IT-Abteilung genannt. Demgemäß konzentriert sich die Diskussion um die Verantwortung für die effektive und effiziente Nutzung der informationellen Ressourcen eines Unternehmens auf die Aufgabenteilung und die daraus resultierende Verantwortung dieser drei Gruppen. IT-Nutzer in der Fachabteilung stellen in dieser Diskussion regelmäßig keine eigenständige Gruppe keine, sondern fungieren lediglich als Adressat der IT-Abteilung. Das Ziel des Arbeitspapiers besteht darin, anhand des Referenzwerkes „COBIT“ aufzuzeigen, welche Aufgaben und Verantwortlichkeiten IT-Nutzern in der Fachabteilung prinzipiell übertragen werden können.

Gliederung

Schlüsselwörter: COBIT – Control-Objectives – Informationsmanagement – Informations- und Kommunikationstechnologien – IT-Governance – IT-Nutzer – IT-Prozess

JEL-Klassifikation: L15, L21, M21

---

[1] Lars Ramin, Dipl. Betriebswirt, emwena UG (haftungsbeschränkt), larsramin@freenet.de
[2] Prof. Dr. Michael Klotz, FH Stralsund, Fachbereich Wirtschaft, Zur Schwedenschanze 15, 18435 Stralsund, michael.klotz@fh-stralsund.de

1. Einleitung und Überblick

Der IT-Nutzer soll die ihm zur Verfügung gestellten IT-Systeme effektiv und effizient für die Erfüllung seiner Arbeitsziele einsetzen. Eine Beteiligung beim Management von IT-Systemen, d. h. an planenden, konzeptionellen oder steuernden Aufgaben, beschränkt sich im Rahmen partizipativer Ansätze meist nur auf den Input für die Systementwicklung. Zudem wird der IT-Nutzer aus Sicht der IT-Sicherheit überwiegend als Risiko eingestuft. Es wird ihm insgesamt kaum eine aktive Rolle zuerkannt; als passives Element des IT-Managements wird er stattdessen geschult, überwacht, betreut etc. Im Kontext der Kundenorientierung sowie der Qualifizierung der Information als Produktionsfaktor[3] stellt sich die Frage, ob dem IT-Nutzer heutzutage nicht eine aktivere Rolle übertragen werden muss, um den maximalen „Business Value“ aus der IT zu realisieren.

Vorgehensweise

Zuerst sollen im Arbeitspapier einige notwendige Begriffe aus dem Referenzmodell COBIT[4], der IT und dem IT-Management näher erläutert werden. Im Anschluss daran wird auf den Aufbau des COBIT-Modells eingegangen, vor allem mit einer Beschreibung des Prozessmodells. Im Hauptteil werden die Aufgaben der Business-Seite im IT-Management rekonstruiert. Hierbei soll der Rolle des IT-Nutzers besondere Aufmerksamkeit geschenkt werden. In den weiteren Ausführungen wird verstärkt auf die möglichen Verantwortungen und Aufgaben des IT-Nutzers eingegangen. Dazu werden diese den einzelnen Domänen des COBIT-Konstrukts zugeordnet. Anschließend wird eine vergleichende Betrachtung in Bezug auf die verschiedenen Domänen vorgenommen. Zum Abschluss der Arbeit wird ein Fazit hinsichtlich der potenziellen Ausgestaltung der Rolle des IT-Nutzers im IT-Management gezogen.

IT-Nutzer

Als **IT-Nutzer** oder auch IT-Benutzer wird eine Person bezeichnet, die unmittelbaren Kontakt zu DV-Anlagen und Programmen hat, d. h. direkt Anwendungen und Hardware einsetzt oder diese bedient[5]. Benutzer sind z. B. Entwickler, die selbst Anwendungssysteme bzw. Programme entwickeln, aber auch Mitarbeiter in den Fachabteilungen, die aktiv mit Software arbeiten (z. B. mit ERP-Programmen, Textverarbeitungs- oder Tabellenkal-

[3] Hierzu vgl. *Pietsch u. a. 2004*, S. 39ff.
[4] Im Arbeitspapier wird mit COBIT Bezug auf die deutsche Version von COBIT 4.0 genommen, vgl. ITGI 2005.
[5] Vgl. *Krause 2003*, S. 282.

kulationssoftware)[6]. Die Gruppe der IT-Spezialisten, die i. d. R. der IT-Abteilung zugeordnet sind, sollen im Folgenden nicht adressiert werden. Im Mittelpunkt der Ausführungen stehen stattdessen die IT-Nutzer in den Fachabteilungen[7], die im Rahmen ihrer Arbeit letztlich den Nutzen aus dem IT-Einsatz realisieren.

COBIT

COBIT steht für „Control Objectives for Information and related Technology“ und ist ein Kontroll- und Steuerungsmodell für die Informationstechnologie eines Unternehmens. Der Fokus liegt dabei auf den Bereichen der IT-Governance.[8] Seit 1993 wurde COBIT vom internationalen Prüfungsverband ISACA (Information Systems Audit and Control Association) entwickelt und erstmals Ende 1995 veröffentlicht. Aktuell liegt COBIT in der Version 4.1 vor (die deutsche Ausgabe in der Version 4.0), herausgegeben von der ISACA und dem IT Governance Institute (ITGI).

IT-Governance

IT-Governance ist ein wesentlicher Bestandteil der Unternehmensführung und liegt somit in der Verantwortung des Vorstandes und des Managements. IT-Governance beinhaltet Führung, Prozesse und Organisationsstrukturen, mit denen sichergestellt werden soll, dass die IT die Unternehmensziele und -strategien unterstützt. Die Umsetzung von IT-Governance wird durch leistungsfähige und international anerkannte Standards wie COBIT oder ITIL unterstützt.[9] Nach dem Modell des ITGI unterteilt sich IT-Governance in folgende fünf Bereiche, vgl. Abbildung 1.[10]

IT-Governance Kernbereiche

- Die strategische Ausrichtung (IT Strategic Alignment), d. h. Sicherstellung der gleichen Ausrichtung von Unternehmenszielen und IT-Zielen.
- Das Schaffen von Werten und Nutzen (IT Value Delivery), was soviel bedeutet wie die Realisierung des Wertbeitrags und Nutzens inklusive einer Kostenoptimierung der IT.
- Das Ressourcenmanagement (IT Resource Management), das sich mit der Optimierung der Investitionen in und der Nutzung von IT-Ressourcen beschäftigt.

---

[6] Vgl. *Stahlknecht/Hasenkamp 2002*, S. 12.
[7] Dieser Personenkreis wird von Laudon u. a. explizit als Endbenutzer bezeichnet, vgl. *Laudon u. a. 2006*, S. 134.
[8] Vgl. *Meier 2004*, S. 128.
[9] Vgl. *ITGI 2003*, S. 11.
[10] Vgl. *Meyer 2003*, S. 445ff.

Abbildung 1
Kernbereiche der IT-Governance[11]

- Das Risikomanagement (IT Risk Management), das Risikobewusstsein (Risk-Awareness) und akzeptierte Risikobereitschaft bei der Unternehmensleitung schaffen sowie die Einhaltung von Unternehmenserfordernissen (Compliance), die Transparenz der wichtigsten Risiken und die Integration der Verantwortlichkeit für Risikomanagement in die Unternehmensstruktur sicherstellen soll.
- Durch das Messen von Performance (IT Performance Measurement) soll die Umsetzung der Strategie verfolgt und überwacht werden. Gleiches gilt für Projekte und die Verwendung von Ressourcen. Die Messungen von Prozessperformance und Leistungserbringung werden z. B. mit Hilfe von Balanced Scorecards vorgenommen.

Control Objectives

Die **Control Objectives** sind der Hauptbestandteil des COBIT-Konstrukts und werden häufig mit „Kontrollziel“ übersetzt, bedeuten aber eigentlich Steuerungsvorgaben. Es handelt sich hierbei um generische Best-Practice-Steuerungsmechanismen für sämtliche Aufgaben und Aktivitäten der IT. Sie bilden das zentrale Instrument zur Gewinnung von Informationen zur Steuerung der IT. Anhand der Control Objectives lässt sich überprüfen, inwieweit die Geschäftsanforderungen eines Unternehmens durch seine Informationstechnologie abgedeckt werden oder ob sich insofern ein Nachsteuerungsbedarf ergibt.[12]

[11] Entnommen aus *ITGI 2005*, S. 7.
[12] Vgl. *Johannsen 2006*, S. 17.

2. Das COBIT Referenzmodell

COBIT Referenzmodell

COBIT ist ein IT-Governance-Referenzmodell (IT-Governance-Framework), das sowohl branchen- als auch betriebsgrößenunabhängig angewendet werden kann und allgemeine sowie international akzeptierte Grundsätze und Ziele für die IT definiert. Es bietet dem Management eine methodische Unterstützung zur effizienten und effektiven Nutzung und Steuerung der IT und soll sicherstellen, dass die IT die geschäftlichen Anforderungen unterstützt. Hierzu muss das Unternehmen die IT-Ressourcen durch eine strukturierte Menge an Prozessen managen und steuern.[13] COBIT konzentriert sich auf wesentliche Erfordernisse für ein angemessenes Management und die Steuerung der IT. Damit ist es auf der strategischen Ebene angesiedelt[14], was sich durch die Fokussierung auf folgende Bereiche zeigt:

1. Ausrichtung der IT auf das Kerngeschäft,
2. Geschäftsunterstützung und Gewinnmaximierung,
3. verantwortungsvoller Umgang mit IT-Ressourcen,
4. angemessenes Management von IT-Risiken.

Aufbau von COBIT

Im Kern beschreibt COBIT ein generisches Prozessmodell, das die Prozesse, die man üblicherweise in einer IT-Abteilung oder Organisation findet (bzw. finden sollte), darstellt.[15] COBIT beinhaltet unterschiedliche Dokumente, mit „COBIT 4.0“ als Kerndokument. Dieses beinhaltet das Prozess-Framework, die Control Objektives, die Management Guidelines und ein Maturity Model. Als Prozess-Framework zur Steuerung der IT und ist COBIT nach IT-Prozessen strukturiert, wobei eine Verbindung zwischen den Anforderungen der IT-Governance, den IT-Prozessen und den IT-Controls vorgenommen wird.

COBIT beschreibt in vier IT-Domänen 34 IT-Prozesse und verbindet diese mit verschiedenen Unternehmensanforderungen und IT-Ressourcen, vgl. Abbildung 2. Auf der Oberseite des „COBIT-Würfels“ sind die identifizierten Unternehmensanforderungen (Effektivität, Effizienz, Vertraulichkeit, Integrität, Verfügbarkeit, Compliance und Verlässlichkeit) dargestellt. Diese Anforderungen müssen durch die Steuerung der IT-Ressourcen (Anwendungen, Informationen, Infrastruktur und Personal), welche auf der rechten

[13] Vgl. *ITGI 2005*, S. 14.
[14] Vgl. *ITGI 2005*, S. 7.
[15] Vgl. *Johannsen 2007*, S. 40ff.

Seite dargestellt sind, realisiert werden. Die Steuerung der IT-Ressourcen soll durch die Anwendung der strukturierten IT-Prozesse erreicht werden, welche bildlich auf der Vorderseite des Würfels dargestellt sind.

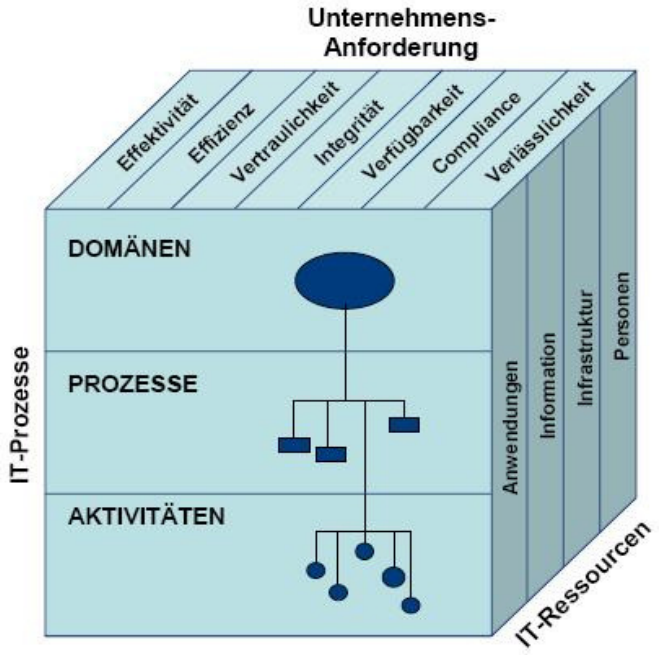

Abbildung 2
COBIT-Würfel[16]

Zusammenfassend lässt sich der Ansatz von COBIT so beschreiben, dass IT-Ressourcen durch IT-Prozesse gemanagt werden, um die IT-Ziele zu erreichen, die mit den Unternehmensanforderungen abgestimmt sind.[17]

3. Aufgaben des IT-Nutzers

Aufgaben der Business-Seite im IT-Management

Im Prozessmodell von COBIT werden unterschiedliche Funktionen betrachtet. Hierzu werden in einem RACI-Chart folgende, überwiegend IT-bezogene Funktionen gegenübergestellt:

- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- Business Executive
- Chief Information Officer (CIO)
- Geschäftsprozesseigner

[16] Entnommen aus *ITGI 2005*, S. 26.
[17] Vgl. *ITGI 2005*, S. 26.

- Leitung Betrieb
- Chief Architect
- Leitung Entwicklung
- Leitung Administration
- Projektbüro
- sowie Verantwortliche für Compliance, Audit, Risk und Security.

In der Domäne „Überwache und Evaluiere“ wird durch die hohe Relevanz für das Unternehmensmanagement zusätzlich die Funktion der Geschäftsführung (Board) betrachtet. Das heißt, von der Business-Seite her werden lediglich die Rollen des Business Executive und des Geschäftsprozesseigners verwendet. Daneben existieren aber noch andere Beteiligte, wie der IT-Benutzer und sonstige Mitarbeiter, denen von der Fachabteilungsleitung IT-Aufgaben übertragen werden können. Diese Aufgaben sollen anhand der COBIT-Systematik identifiziert und expliziert werden.

Die Business-Seite ist die wertschöpfende Funktion und bildet die Basis für den Geschäftserfolg eines Unternehmens. Durch sie werden die Unternehmensprodukte konstruiert, geplant, produziert, gelagert, vertrieben. Dabei verwendet die jeweilige Unternehmensfunktion die verschiedensten IT-Produkte zur Unterstützung ihrer Aufgabe. Zur Steuerung der Aufgaben, Verantwortlichkeiten und Infrastruktur der Unternehmens-IT können die betroffenen Fachabteilungen fachspezifisches Wissen und Erfahrungen einbringen. Zusätzlich kann die Fachabteilung die IT-Abteilung durch die Übernahme der Eigentümerschaft für Daten und Anwendungen entlasten und bei Entscheidungsfindungen unterstützend wirken.

Verantwortung und Aufgaben des IT-Nutzers

Mit Fokus auf die vier COBIT-Domänen und unter Betrachtung der Control Objectives sollen im Folgenden die möglichen Aufgaben und Verantwortlichkeiten des IT-Nutzers beschrieben und analysiert werden. Anhand der detaillierten Kontrollziele bzw. Steuerungsvorgaben, die die IT-Prozesse ausführlich beschreiben, wurde Schritt für Schritt eine Identifizierung möglicher Aufgaben und Verantwortlichkeiten für den IT-Nutzer durchgeführt.

3.1 Aufgaben in der Domäne PO

Aufgaben in der Domäne PO

Die Domäne „Plan and Organise“ (PO) umfasst IT-Strategie und -Taktiken und betrifft die Bestimmung der Art, wie die IT am besten zur Erreichung der Geschäftsziele beitragen kann.

Bei der Planung und Organisation im IT-Management kann der IT-Nutzer im Bereich der strategischen Planung und der IT-Infrastrukturplanung unterstützend wirken. Ebenso kann er an der Definition von IT-Prozessen, Organisationsstruktur und Unternehmensbeziehungen teilnehmen. Weitere mögliche Aufgabenbereiche innerhalb der IT sind im Investitionsmanagement, Kommunikationsmanagement, Ressourcenmanagement, Qualitätsmanagement sowie Risiko- und Projektmanagement auszumachen.

Tabelle 1 stellt die verschiedenen potenziellen Aufgaben und Verantwortlichkeiten in der Domäne im Überblick dar.

Tab. 1 Aufgaben und Verantwortlichkeiten in der Domäne PO

Lfd. Nr.	Aufgabe / Verantwortlichkeit	Prozess	Con. Obj.
1	Mitwirkung an der Erstellung von Business Cases	Definiere einen strategischen IT-Plan (PO1)	PO1.1
2	Mitwirkung an der Beurteilung von Business Cases		PO1.1
3	Geschäftliches Verständnis für innovativen IT-Einsatz schaffen und an Prüfung der IT-Einsatzpotentiale mitwirken		PO1.2
4	Mitwirkung an der Bewertung der Leistungsfähigkeit der eingesetzten Anwendungen		PO1.3
5	Ermittlung der Anforderungen an Ressourcen und Konkretisierung des Nutzens im Rahmen der taktischen IT-Planung		PO1.5
6	Mitwirkung an der Abstimmung von Anforderungen und eingesetzten Ressourcen und Umsetzungsbegleitende Nutzenüberwachung		PO1.5
7	Mitwirkung an der Identifikation, Definition, Priorisierung und Initiierung von IT-Investitionsvorhaben		PO1.6
8	Mitwirkung an der Evaluierung von IT-Investitionsvorhaben		PO1.6
9	Mitwirkung an Erstellung und Pflege anwendungsbezogener Informationsarchitekturen	Definiere die Informationsarchitektur (PO2)	PO2.1
10	Mitwirkung an der Erstellung eines Data Dictionary		PO2.2

11	Mitwirkung an der Erstellung und Pflege eines Datenklassifikationsschemas		PO2.3
12	Mitwirkung an der Überwachung von Trends in der Branche sowie der geschäftlichen und rechtlichen Umwelt	Bestimme die technologische Richtung (PO3)	PO3.3
13	Beratung und Unterstützung des IT-Architekturgremiums aus Fachabteilungssicht		PO3.5
14	Mitwirkung bei der Erstellung eines Frameworks für IT-Prozesse	Definiere die IT-Prozesse, Organisation und Beziehungen (PO4)	PO4.1
15	Übernahme der Verantwortung für Qualitätssicherung		PO4.7
16	Übernahme der Eigentümerschaft für IT-Risiken		PO4.8
17	Übernahme der Verantwortung für Informationssicherheit und physische Sicherheit		PO4.8
18	Übernahme der Eigentümerschaft für Daten und Anwendungen		PO4.9
19	Mitwirkung an der Erstellung von Koordinations-, Kommunikations- und Verbindungsstrukturen sowie Nutzung derselben		PO4.15
20	Mitwirkung an der Identifikation von Kostenabweichungen und ggf. an der Anpassung von Business Cases	Manage IT-Investitionen (PO5)	PO5.4
21	Mitwirkung an der Suche nach Potenzialen für eine Erhöhung des Wertbeitrages		PO5.5
22	Aktive und passive Unterstützung der Kommunikation von IT-Richtlinien	Kommuniziere Ziele und Richtung des Managements (PO6)	PO6.4
23	Aktive und passive Unterstützung der Kommunikation der Ausrichtung der IT, insb. von IT-Zielen und -Strategien		PO6.5
24	Aktive und passive Unterstützung der Kommunikation von IT-Sicherheitsthemen zur Förderung des IT-Sicherheitsbewusstseins		PO6.5
25	Regelmäßige Teilnahme an Schulungen und Weiterbildungsmaßnahmen im IT-Bereich	Manage die IT-Human-	PO7.4

26	Unterstützung durch sorgfältige Dokumentation der Aufgaben und Verantwortlichkeiten	Ressourcen (PO7)	PO7.5
27	Unterstützung bei der Beurteilung von Lieferanten und anderen Vertragspartnern		PO7.6
28	Eigenbeurteilung in Bezug auf gesteckte Ziele und durchgeführte Aufgaben		PO7.7
29	Mitwirkung an der Erstellung von IT-Qualitätsplänen	Manage Qualität (PO8)	PO8.1
30	Mitwirkung bei der Ermittlung von Anforderungen an IT-Standards		PO8.4
31	Mitwirkung an der Festlegung von Rollen und Verantwortlichkeiten zur Konfliktbewältigung		PO8.4
32	Aktive und passive Unterstützung der Kommunikation von IT-Qualitätsplänen		PO8.5
33	Ermittlung der Anforderungen an die erforderliche IT-Qualität		PO8.6
34	Mitwirkung an der Messung, am Management und am Review der Qualität sowie an Maßnahmen zur Sicherstellung der erforderlichen Qualität		PO8.6
35	Mitwirkung bei der Festlegung des Risikokontextes	Beurteile und Manage IT-Risiken (PO9)	PO9.2
36	Mitwirkung bei der Identifikation von Bedrohungen und Schwachstellen der IT		PO9.3
37	Mitwirkung an der Risikobewertung hinsichtlich Wahrscheinlichkeit und Auswirkungen		PO9.4
38	Übernahme der Eigentümerschaft für Risiken		PO9.5
39	Initiierung und Steuerung von Maßnahmen der IT-Sicherheit im Rahmen der Eigentümerschaft für Risiken		PO9.5
40	Mitwirkung an der Überwachung von Maßnahmen zur Risikobehandlung inkl. entsprechendem Reporting		PO9.6
41	Unterstützung der Erstellung eines Plans zur Risikobehandlung		PO9.6

42	Mitwirkung an der Erstellung und Weiterentwicklung eines hausinternen Projektmanagement-Standards	Manage Projekte (PO10)	PO10.2
43	Mitwirkung an der Einrichtung von Strukturen der Projektsteuerung		PO10.3
44	Mitwirkung an der Bestimmung der Art und des Umfanges von Projekten		PO10.5
45	Mitwirkung an der Abstimmung von Fachabteilungs- und IT-Ressourcen		PO10.7
46	Festlegung von Aufgaben, Verantwortlichkeiten und Befugnissen zugeordneter Projektmitarbeiter		PO10.8
47	Mitwirkung an der Planung, Identifikation und Analyse der Projektrisiken		PO10.9
48	Mitwirkung an der Erstellung eines Qualitätsmanagementplans im Rahmen des Projektplans		PO10.10
49	Mitwirkung an der Planung von Controls und Sicherheitseigenschaften in Bezug auf die festgelegten Anforderungen		PO10.12
50	Mitwirkung an der Projektsteuerung in Bezug auf Messung, Berichterstattung und Monitoring der Projektperformance		PO10.13
51	Mitwirkung an der Planung von Leistungsindikatoren zur Beurteilung des Projekterfolgs		PO10.13
52	Mitwirkung am Projektabschluss und an der Erstellung der Lessons-Learned		PO10.14

Aufgaben in PO1 (Definiere einen strategischen IT-Plan)

Die zentrale Zielsetzung des IT-Einsatzes muss es sein, den Beitrag der Nutzung von Informationen sowie Informations- und Kommunikationstechnologien zum Unternehmenswert zu maximieren (sog. „value delivery“). Um dies zu erreichen ist es erforderlich, dass Spezialisten aus den Fachabteilungen und der IT-Abteilung zusammenarbeiten, um diejenigen IT-Investitionen zu identifizieren, die den größten Nutzen für das Unternehmen erbringen. Hierzu sind fundierte Business Cases zu erstellen, an denen der IT-Nutzer seitens der Fachabteilungen hinsichtlich der Einschätzung von

erwartetem Nutzen und potenziellen Risiken mitzuwirken hat. Diese Business Cases sind nicht nur Grundlage der späteren Erfolgskontrolle, sondern auch der Erstellung von Service-Level-Agreements (SLA), die die Verantwortlichkeiten für das Erreichen des geplanten Wertbeitrags sowohl auf IT-Seite als auch auf Seite der Fachabteilung festlegen. Eine Hauptaufgabe im Rahmen des IT-Controlling besteht darin zu überprüfen, ob und inwieweit der mit IT-Investitionen geplante Wertbeitrag wirklich realisiert wurde (sog. „Nutzeninkasso"). Hierzu ist auf die in der IT-Planung angefertigten Business Cases zurückzugreifen. Der IT-Nutzer sollte dabei ex-post an der Beurteilung der Business Cases, die den Anforderungen der Transparenz, Wiederholbarkeit und Vergleichbarkeit genügen, mitwirken (PO1.1). In strategischer Hinsicht ist es wichtig, dass die Entwicklungen der IT kontinuierlich daraufhin geprüft werden, ob und inwieweit innovative Einsatzmöglichkeiten das Kerngeschäft des Unternehmens unterstützen können bzw. neue Geschäftschancen bieten. Hierbei ist es Aufgabe des Nutzers, zu einem klaren Verständnis der geschäftlichen Ziele, Prozesse und Bedarfe beizutragen, an denen sich der IT-Einsatz zu orientieren hat. Diese Ausrichtung der IT am Kerngeschäft wird auch als „IT/Business-Alignment" bezeichnet (PO1.2). Als Grundlage jeder Planung ist die aktuelle Leistungsfähigkeit der eingesetzten Anwendungen zu beurteilen. Für die Bewertung ihres Beitrags zum Erreichen der Geschäftsziele, der Funktionalität, der Stabilität aus Nutzersicht, der anwendungsbezogenen Komplexität (i. S. von Abhängigkeiten zwischen den Anwendungen), der Stärken und Schwächen sowie ggf. der Kosten ist das Mitwirken qualifizierter IT-Nutzer unerlässlich (PO1.3). Mit Hilfe der taktischen IT-Planung soll der strategische IT-Plan umgesetzt werden. Die Mitwirkung des IT-Nutzers richtet sich auf die Ermittlung der Anforderungen an benötigte Ressourcen und die erforderliche Qualität sowie die Konkretisierung des Nutzens als Voraussetzung einer Überwachung. In der Umsetzung der taktischen IT-Planung fallen diverse Kontrollaufgaben an, bei denen der IT-Nutzer sein Anwendungswissen beim IT-Portfoliomanagement einbringen kann. Dies bezieht sich vor allem auf die regelmäßige Abstimmung von definierten Anforderungen und eingesetzten Ressourcen und die umsetzungsbegleitende Überwachung der Realisierung des geplanten Nutzens (PO1.5). Der IT-Nutzer hat im Rahmen des IT-Portfoliomanagements an der fortlaufenden Identifikation, Definition und Evaluierung von IT-Investitionsvorhaben mitzuwirken. Im Ergebnis sind diese zusätzlich zu priorisieren und zu initiieren (PO1.6).

Aufgaben in PO2 (Definiere die Informationsarchitektur)

Als Grundlage für die Planung von Anwendungssystemen und die Verwendung informationeller Ressourcen dienen heute Informationsarchitekturen, die die optimale Benutzung von Informationen erleichtern sollen. Der Nutzer aus der Fachabteilung kann die Erstellung und Pflege von anwendungsbezogenen Informationsarchitekturen unterstützen (PO2.1). Gleiches gilt für die Mitarbeit an einem Data Dictionary, das ein gemeinsames Datenverständnis zwischen Fachabteilung und IT-Abteilung fördern soll (PO2.2). Ein Datenklassifikationsschema, in dem die Kritikalität und Sensitivität von Daten dokumentiert wird, ist die zentrale Grundlage für die operative Gewährleistung der IT-Sicherheit. Aus Sicht der Fachabteilung werden die Dateneigentümerschaft, Sicherheitsstufen (z. B. öffentlich, interner Gebrauch, vertraulich, streng geheim), Vorgaben zu Speicherung und Archivierung festgelegt. Hierfür ist eine anwendungsbezogene Sichtweise erforderlich, die der IT-Nutzer bei der Erstellung und Pflege eines Datenklassifikationsschemas beitragen kann (PO2.3).

Aufgaben in PO3 (Bestimme die technologische Richtung)

Im Hinblick auf PO3 (Bestimme die technologische Richtung) hat der IT-Nutzer an der Überwachung von Trends in der Branche sowie der geschäftlichen und rechtlichen Umwelt mitzuwirken (PO3.3). Weiterhin kann er aufgrund spezifischer Fachkenntnisse das IT-Architekturgremium bei seinen Entscheidungen aus Fachabteilungssicht beraten und unterstützen.

Aufgaben in PO4 (Definiere die IT-Prozesse, Organisation und Beziehungen)

Bei der Definition von IT-Prozessen, Organisation und Beziehungen ist der IT-Nutzer an der Erstellung eines Frameworks für IT-Prozesse zu beteiligen (PO4.1). Außerdem sollte er auch Verantwortung für die Qualitätssicherung von IT-Prozessen übernehmen (PO4.7). Die Eigentümerschaft für Daten und Anwendungen hat nicht in der IT-, sondern in der Fachabteilung zu liegen.[18] Diese Rolle ist von qualifizierten IT-Nutzern zu übernehmen, wobei sie in der Wahrnehmung dieser Verantwortung durch die IT-Abteilung zu unterstützen sind (PO4.9). In Zusammenhang mit der Eigentümerschaft für IT-bezogene Risiken fordert COBIT auch die Zuweisung von Verantwortung für Informationssicherheit, physische Sicherheit und Compliance, also Belange, die durch die Fachabteilung zu steuern sind. Ebenso beinhalten die Festlegung von Rollen, Aufgaben und Verantwortlichkeiten im Rahmen der IT-Organisation immer auch die Dimension der IT-Sicherheit (PO4.8). Zur Förderung einer kooperativen, effizienten Zusammenarbeit zwischen IT-Abteilung und Fachabteilung sollte es definierte Koordinati-

[18] Vgl. *ITGI 2005*, S. 46 ff.

ons-, Kommunikations- und Verbindungsstrukturen geben. Soweit der IT-Nutzer in diese operativ eingebunden ist, sollte er an ihrer Entwicklung teilnehmen und sie aktiv nutzen (PO4.15).

Aufgaben in PO5 (Manage IT-Investitionen)

Beim Management von IT-Investitionen sind Kostenabweichungen in der Fachabteilung möglichst frühzeitig zu identifizieren und führen ggf. im Rahmen des Kostenmanagements zu Anpassungen des Business Case (PO5.4). Die Kontrolle des Wertbeitrages hat sich aber nicht nur auf IT-Projekte, sondern auch auf alle aktuell betriebenen Anwendungen zu beziehen. Der IT-Nutzer sollte gerade bei diesen Systemen kontinuierlich Nutzenmonitoring betreiben und nach Potenzialen für eine Erhöhung des Wertbeitrages suchen und geeignete Aktionen initiieren. Dies ist Inhalt seiner Verantwortung im Rahmen des Nutzenmanagements (PO5.5).

Aufgaben in PO6 (Kommuniziere Ziele und Richtung des Managements)

IT-Richtlinien legen die wesentlichen Leitlinien für Informationsqualität, IT-Sicherheit, Schutz der informationellen Ressourcen etc. fest. Sie bilden eine Basis für die Umsetzung strategischer IT-Planungen. Die Wirksamkeit von Richtlinien hängt von ihrer erfolgreichen Kommunikation ab. Hieran sollte der Nutzer der Fachabteilung teilhaben, sowohl passiv als auch aktiv (bspw. durch Austausch mit Kollegen oder Thematisierung in konkreten Arbeitszusammenhängen) (PO6.4). Gleiches gilt für die Ziele, Strategien und Ausrichtung der IT (PO6.5). Die Kommunikation von Zielen und Ausrichtung der IT umfasst auch die IT-Sicherheit. Hier muss in der Fachabteilung darauf hingewirkt werden, dass ein breites IT-Sicherheitsbewusstsein vorhanden ist – eine Forderung, für deren Erfüllung sich jeder IT-Nutzer einsetzen sollte (PO6.5). Auch wenn jeder Mitarbeiter für IT-Sicherheit verantwortlich sein muss, kann der IT-Nutzer mit gutem Beispiel und beharrlicher Kommunikation das Sicherheitsbewusstsein fördern.

Aufgaben in PO7 (Manage die IT-Human-Ressourcen)

Zur Verbesserung seines IT-Know-hows und zur Entlastung der IT-Abteilung sollten IT-Nutzer regelmäßig an Schulungen und Weiterbildungsmaßnahmen im IT-Bereich teilnehmen (PO7.4). Um sein erworbenes fachspezifisches Wissen für Vertretungen oder Nachfolger zugreifbar zu machen, sollte der IT-Nutzer seine Aufgaben und Verantwortlichkeiten sorgfältig dokumentieren (PO7.5). Im Rahmen der Qualitätssicherung kann er bei der Beurteilung von Lieferanten oder Vertragspartnern unterstützen und so zu einem gleichbleibenden bzw. verbesserten Qualitätsniveau beitragen (PO 7.6). Ein weiterer Qualitätssicherungsaspekt ist die Überprüfung der eigenen Aufgabenbereiche und die dadurch mögliche Optimierung der Aufgabenverteilung (PO7.7).

Aufgaben in PO8 (Manage Qualität)

Ein spezieller Bereich in der Zusammenarbeit mit der IT-Abteilung ist das IT-Qualitätsmanagement. Hierbei ist es wichtig, dass die Praktiken und IT-Standards des IT-Qualitätsmanagements mit den Anforderungen der Fachabteilungen in Einklang stehen. Diesbezüglich kann der IT-Nutzer bei der Erstellung von IT-Qualitätsplänen mitwirken (PO8.1) und außerdem bei der Ermittlung von Anforderungen an IT-Standards eingebunden werden (PO8.4). In diesem Kontext sind ebenso Rollen und Verantwortlichkeiten für eine ggf. erforderliche Konfliktbewältigung festzulegen und wahrzunehmen (PO8.4). Um Qualitätsverbesserungen zu erreichen, ist es notwendig, dass der IT-Nutzer als Multiplikator auftritt. Hierbei kann er durch aktive und passive Kommunikation der IT-Qualitätspläne unterstützen (PO8.5). Ein weiterer Aufgabenbereich ist die Qualitätsbeurteilung, speziell das regelmäßige Überwachen, Messen und Aufzeichnen von Qualitätskriterien, die sich auf anwendungsnahe Elemente des Qualitätsmanagementsystems beziehen (z. B. Systemzugang, Verständlichkeit, Relevanz, Vollständigkeit). Aber auch bei korrektiven oder präventiven Maßnahmen zur Sicherstellung der erforderlichen Qualität sollte der IT-Nutzer einbezogen werden (PO8.6).

Aufgaben in PO9 (Beurteile und Manage IT-Risiken)

Bereits bei den IT-Investitionen war als Aufgabe des Nutzers die Mitwirkung bei der Einschätzung von IT-Risiken im Rahmen der Erstellung von Business Cases genannt worden. Voraussetzung für diese Einschätzung ist die Identifikation von Bedrohungen und Schwachstellen (PO9.3) sowie die Festlegung des Risikokontextes, d. h. die Bestimmung von internen und externen Rahmenbedingungen für die Bewertung sowie die Festlegung der Bewertungsziele und -kriterien (PO9.2). Auf der operativen Ebene hat der Nutzer die Erstellung eines Plans zur Risikobehandlung zu unterstützen und diesen ggf. auch mit umzusetzen (PO9.6). Auch die Bewertung der IT-Risiken ist nach erstmaliger Durchführung im Rahmen der Erstellung von Business Cases eine kontinuierliche Aufgabe, die Bestandteil des Risikocontrollings ist. Soweit diese Risiken anwendungsnah sind, kann der IT-Nutzer die Bewertung von Wahrscheinlichkeit und Auswirkungen eines Schadeneintritts unterstützen (PO9.4). Hiermit hängt auch die Rolle des Risikoeigners zusammen, die für anwendungsnahe IT-Risiken ebenfalls in der Fachabteilung zugeordnet werden sollte. Diese Rolle umfasst auch das Festlegen effektiver Controls, adäquater Risikostrategien (z. B. Vermeidung, Teilung, Akzeptanz) und ggf. zu ergreifender Sicherheitsmaßnahmen. Agiert der IT-Nutzer als Risikoeigner, hat er in dieser Eigenschaft Sicherheitsmaßnahmen zu initiieren und zu steuern, so dass entsprechende Risiken kontinuierlich reduziert werden (PO9.5). Die Umsetzung des Plans zur

Risikobehandlung sowie Maßnahmen zur Risikobehandlung sind zu überwachen und dem vorgesehenen Adressaten (Unternehmensleitung, Risikomanagement) entsprechend zu berichten (PO9.6).

Aufgaben in PO10 (Manage Projekte)

Auch die IT-Projektplanung stellt für den IT-Nutzer potenziell ein umfangreiches Betätigungsfeld dar. Dies betrifft grundlegend die Erstellung und Weiterentwicklung eines hausinternen Projektmanagement-Standards (PO 10.2). Hinsichtlich der Projektorganisation kann der IT-Nutzer an der Einrichtung von Strukturen der Projektsteuerung sowie für die Einbeziehung der Stakeholder mitwirken (PO10.3). Operativ richtet sich die Mitwirkung des Nutzers auf die Mitarbeit an der Projektplanung. Seine planerische Verantwortung erstreckt sich über die Bestimmung der Art und des Umfanges von Projekten (PO10.5), die Abstimmung von Fachabteilungs- und IT-Ressourcen (PO10.7), die Planung von Projektrisiken (PO10.9), Controls und Sicherheitseigenschaften (PO10.12), die Planung von Leistungsindikatoren zur Beurteilung des Projekterfolgs (PO10.13) und die Erstellung eines projektbezogenen Qualitätsmanagementplans (PO10.10). Soweit er im Rahmen des Projektes (als Projektleiter oder Teilprojektleiter) leitend tätig ist, hat er Aufgaben, Verantwortlichkeiten und Befugnisse seiner ihm zugeordneten Projektmitarbeiter zu regeln (PO10.8). Durch die Mitwirkung des IT-Nutzers an der Projektplanung und Projektdurchführung richten sich zahlreiche Aufgaben auch auf die IT-Sicherheit. So sind Sicherheitseigenschaften eines zu entwickelnden oder zu beschaffenden Systems zu planen (PO10.12). Die Aufgaben im IT-Projektcontrolling beziehen sich in erster Linie auf die Projektsteuerung hinsichtlich der Leistungskriterien Umfang, Zeit, Kosten, Qualität und Risiken (PO10.13). Auch an der Erstellung des Projektabschlusses kann der IT-Nutzer mitwirken und bei der Verfassung der Lessons-Learned unterstützen (PO10.14).

3.2 Aufgaben in der Domäne AI

Aufgaben in der Domäne AI

Die Domäne „Acquire and Implement“ (AI) unterstützt die Umsetzung der IT-Strategie durch die Identifizierung, Entwicklung oder Beschaffung und Implementierung von neuen IT-Lösungen für Geschäftsprozesse sowie durch die Anpassung und Wartung bestehender Anwendungen. Die Prozesse dieser Domäne schaffen also die Voraussetzungen für die Nutzung und den Betrieb von Software- und Anwendungen. Hier kann der IT-Nutzer beim Beschaffungsmanagement und beim Changemanagement mitwirken. Tabelle 2 stellt die verschiedenen potenziellen Aufgaben und Verantwortlichkeiten in der Domäne im Überblick dar.

Tab. 2
Aufgaben und Verantwortlichkeiten in der Domäne AI

Lfd. Nr.	Aufgabe / Verantwortlichkeit	Prozess	Con. Obj.
1	Identifizierung, Spezifikation und Priorisierung von funktionalen Anforderungen	Identifiziere automatisierte Lösungen (AI1)	AI1.1
2	Identifizierung, Spezifikation und Priorisierung von Erfordernissen hinsichtlich der IT-Sicherheit		AI1.1
3	Mitwirkung an der Identifizierung und Dokumentation von Risiken		AI1.2
4	Mitwirkung an der Risikoanalyse hinsichtlich IT-Sicherheitsrisiken		AI1.2
5	Unterstützung bei der Beurteilung der wirtschaftlichen Machbarkeit und des Nutzens von IT-Lösungen		AI1.3
6	Mitwirkung an der Feinplanung in Bezug auf Spezifikation und Dokumentation von Anforderungen	Beschaffe und warte Anwendungssoftware (AI2)	AI2.2
7	Mitwirkung an der Feinplanung hinsichtlich Sicherheit und Verfügbarkeit		AI2.2
8	Mitwirken an der Abnahme von Anforderungen und Anpassungen		AI2.2
9	Unterstützung durch das Testen von Anwendungssoftware		AI2.2
10	Mitwirken an der Konzeption von Anwendungskontrollen in Bezug auf Nachvollziehbarkeit		AI2.3
11	Mitwirkung an der Konzeption sicherheitsrelevanter Anwendungskontrollen		AI2.3
12	Mitwirkungen an der kontinuierlichen Überwachung von IT-Sicherheitsrisiken		AI2.4
13	Mitwirkung bei der Durchführung und Dokumentation von Update-Tests		AI2.5
14	Mitwirkung an der Umsetzung von wesentlichen Upgrades		AI2.6

15	Mitwirkung an der Abnahme von Meilensteinen und der Freigabe von Change-Requests		AI2.7
16	Mitwirkung an der Planung für Softwarequalitätssicherung		AI2.8
17	Mitwirkung an Releaseplanung sowie an Reviews		AI2.10
18	Mitwirkung an der Planung der Wartung von Anwendungssoftware		AI2.10
19	Sicherstellung der Berücksichtigung von Sicherheitsanforderungen in der Wartungsplanung		AI2.10
20	Mitwirkung an Reviews zur Wartung der IT-Infrastruktur	Beschaffe und warte technologische Infrastruktur (AI3)	AI3.3
21	Erwerb von Wissen als Voraussetzung für die Übernahme der Verantwortung für die von der Fachabteilung genutzten Daten und Anwendungen	Ermögliche Betrieb und Verwendung (AI4)	AI4.2
22	Erwerb von Wissen zu IT-Sicherheit als Voraussetzung für die Übernahme der Eigentümerschaft für Daten und Anwendungen		AI4.2
23	Mitwirkung an der Sicherstellung des Wissenstransfers in die Fachabteilung		AI4.3
24	Mitwirkung an der Lieferantenbewertung und am Vertragsmanagement (Erstellungs- und Beschaffungsphase)	Beschaffe IT-Ressourcen (AI5)	AI5.2
25	Mitwirkung an der Festlegung von Verantwortlichkeiten bei der Zusammenarbeit mit externen Lieferanten		AI5.2
26	Sicherstellung der Festlegung von Verantwortlichkeiten für IT-Sicherheit bei der Zusammenarbeit mit externen Lieferanten		AI5.2
27	Mitwirkung an der Beurteilung, Priorisierung und Freigabe von Änderungen	Manage Changes	AI6.2

28	Durchführung der Statusverfolgung im Change-Management-Verfahren	(AI6)	AI6.4
29	Mitwirkung an Review-Verfahren zum Abschluss der Änderungen		AI6.5
30	Teilnahme an Schulungen in Folge von Entwicklungs-, Implementierungs- oder Änderungsprojekten	Installiere und akkreditiere Lösungen und Changes (AI7)	AI7.1
31	Mitwirkung an der Erstellung von Testfällen		AI7.2
32	Mitwirkung der zeitlichen Planung des Roll-out		AI7.3
33	Unterstützung durch Bereitstellung von Testdaten für die Testumgebung		AI7.4
34	Mitwirkung an der detaillierten Verifikation einer Anwendung oder eines Systems		AI7.5
35	Mitwirkung an Funktionstests hinsichtlich Performance		AI7.6
36	Mitwirkung an Softwaretests in Bezug auf IT-Sicherheit und Zugriffsrechte		AI7.6
37	Mitwirkung an der Durchführung des Akzeptanztests und der Vorbereitung der Freigabe		AI7.7
38	Mitwirkung am abschließenden Test hinsichtlich der anwendungsbezogenen Sicherheit		AI7.7
39	Mitwirkung an der Überführung in den Produktivbetrieb		AI7.8
40	Mitwirkung an Review-Verfahren zur Sicherstellung von Anforderungserfüllung und Nutzenrealisierung		AI7.12

Aufgaben in AI1 (Identifiziere automatisierte Lösungen)

Nicht nur in Hinsicht auf IT-Projekte, sondern für jede automatisierte Lösung sind funktionale Geschäftsanforderungen von den Fachabteilungen zu identifizieren, zu spezifizieren und zu priorisieren. Die Anforderungen haben nicht nur die unmittelbare Anwendungsfunktionalität abzudecken, sondern ebenso Aspekte wie Kosten, Ergonomie, Verlässlichkeit, Auditierbarkeit, Compliance. Die Festlegung der funktionalen Anforderungen für automatisierte Lösungen hat die Sicherheit neben affinen Aspekten, wie Verfügbarkeit, Zugriffsberechtigungen oder Kontinuität, zu umfassen. Dies

wird ausdrücklich als Verantwortung der Fachabteilung deklariert (AI1.1). Im Rahmen der Anforderungsdefinition hat der IT-Nutzer seinen Blick wiederum auf die Risiken zu richten, die ebenfalls zu identifizieren, zu analysieren und zu dokumentieren sind. Ebenso hat die in diesem Zusammenhang vorzunehmende Risikoanalyse auch Gefährdungen der DateninteGrität, der Sicherheit und des Datenschutzes sowie der Verfügbarkeit zu berücksichtigen (AI1.2). Ebenso ist die Erstellung einer Machbarkeitsstudie ein Betätigungsfeld für den IT-Nutzer, der vor allem zur Beurteilung der wirtschaftlichen Machbarkeit im Sinne von Kosten und Nutzen einen Beitrag leisten kann (AI1.3).

Aufgaben in AI2 (Beschaffe und warte Anwendungssoftware)

Bei der Beschaffung und Wartung von Anwendungssoftware sind viele Aufgaben innerhalb der Feinplanung zu sehen. Diese können sich z. B. auf die Spezifikation und Dokumentation von Anforderungen beziehen. Auch bei der Mitwirkung des IT-Nutzers an der Projektplanung und Projektdurchführung richten sich zahlreiche Aufgaben auf die Feinplanung der IT-Sicherheit. So sind die Sicherheitseigenschaften eines zu entwickelnden oder zu beschaffenden Systems zu planen. Im Rahmen der Entwicklung oder Beschaffung von Anwendungssoftware kann der IT-Nutzer ebenso an der Abnahme von Anforderungen und Anpassungen mitwirken, wenn die definierten Anforderungen durch Änderungen beeinflusst werden. In diesem Zusammenhang sollte er auch am Testen der Softwaresysteme teilnehmen, da so fachspezifische Probleme schneller erkannt werden können (AI2.2). Ebenso sollte der IT-Nutzer an der Konzeption von Anwendungskontrollen beteiligt werden. Bei der Beschaffung und Entwicklung von Anwendungssoftware fallen auch diverse Aufgaben in Bezug auf die IT-Sicherheit an. Dies gilt für die Konzeption sicherheitsrelevanter Anwendungskontrollen, bspw. hinsichtlich Zugriffsschutz oder Backup (AI2.3). Für die kontinuierliche Überwachung von IT-Sicherheitsrisiken werden Zugriffsberechtigungen und Rechtemanagement, der Schutz sensitiver Daten, Authentisierung und Transaktionsintegrität explizit genannt (AI2.4). Im Zusammenhang mit der Implementierung von Software-Updates kann der IT-Nutzer ebenfalls bei der Durchführung und Dokumentation von Update-Tests unterstützen (AI2.5). Bei Upgrades bestehender Systeme, soweit diese mit signifikanten funktionalen Änderungen verbunden sind, kann er an der Abnahme von Anforderungen mitwirken (AI2.6). In der eigentlichen Anwendungsentwicklung sollten die Nutzer bei der Abnahme von Meilensteinen und der Freigabe von Change-Requests beteiligt werden (AI2.7). Auch bei der Planung für die Qualitätssicherung einer Softwarelösung können die

Nutzer durch Spezifikation von Qualitätskriterien mitwirken (AI2.8). Im Rahmen des Betriebs von Anwendungen (der von der IT-Abteilung gegenüber der Fachabteilung als IT-Service erbracht wird) fallen planerische Aufgaben in Zusammenhang mit der Wartung von Anwendungssoftware und künftigen Entwicklungen des Ressourcenbedarfs an. Kommt es bei der Nutzung einer Anwendung zu Problemen, hat der IT-Nutzer im Rahmen der Fehlerbehandlung ggf. Fehler zu melden und die Fehlerbehebung aus Nutzersicht zu bestätigen. Außerdem hat er an Wartungs- und Releaseplanung inhaltlich mitzuwirken (vor allem durch Priorisierung aus Nutzersicht). Auch bei periodischen Reviews der Anwendungssoftware ist seine Beteiligung hinsichtlich der Bewertung von geschäftlichen Anforderungen, Risiken und Sicherheitsanforderungen sinnvoll. In der Betriebsphase von Anwendungssoftware hat der IT-Nutzer sicherzustellen, dass Sicherheitsanforderungen bei der Wartungsplanung ausreichend berücksichtigt werden (AI2.10).

Aufgaben in AI3 (Beschaffe und warte technologische Infrastruktur)

Bei der Beschaffung und Wartung der IT-Infrastruktur kann der Nutzer von IT ebenfalls Aufgaben übernehmen. So kann er beispielsweise an Reviews zur Wartung der Infrastruktur mitwirken und den Service Level beurteilen (AI3.3).

Aufgaben in AI4 (Ermögliche Betrieb und Verwendung)

Die von COBIT geforderte Eigentümerschaft der Fachabteilungen für die von ihnen verwendeten Daten und Anwendungen erfordert die Übernahme der Verantwortung für Leistungserbringung und -qualität, Internal Control und Administrationsprozesse der Anwendung. Der erforderliche Wissenserwerb soll explizit die Bereiche Freigaben für den Zugriff, Rechteverwaltung, Funktionstrennung, automatisierte Geschäftskontrollen, Backup und Recovery, physische Sicherheit und Archivierung von Urbelegen umfassen. Es ist selbstverständlich, dass IT-Nutzer sich in diesen Bereichen qualifizieren müssen. Voraussetzung für das Erlangen eines Sicherheitsbewusstseins ist ein entsprechender Wissenstransfer, der auch Themen der IT-Sicherheit umfassen muss (AI4.2). Zudem kann der IT-Nutzer als Key-User einzelner Anwendungen eine Multiplikator-Funktion einnehmen und als Ansprechpartner für die IT-Abteilung und für Kollegen in der Fachabteilung fungieren. Auch ein weitergehendes Engagement im Wissenstransfer ist denkbar, beispielsweise durch das Mitwirken an der Schulungskonzeption, der Verbesserung von Schulungsmaterialien und Benutzerdokumentationen oder gar Schulungsdurchführung (AI4.3).

Aufgaben in AI5 (Beschaffe IT-Ressourcen)

Die Aufgaben bei der Beschaffung von IT-Ressourcen zielen auf das Lieferantenmanagement. Soweit in der Erstellungs- bzw. Beschaffungsphase sowie während des Betriebs eine Zusammenarbeit mit Lieferanten und externen Dienstleistern erforderlich ist, hat der IT-Nutzer Erfahrungen und Bewertungen dem Lieferantenmanagement zur Verfügung zu stellen. Dies betrifft vor allem vertragliche Aspekte, so dass im Kern das Vertragsmanagement betroffen ist, beschränkt sich aber nicht nur auf diese. Fungiert der IT-Nutzer als Fachzuständiger für die Zusammenarbeit mit externen Lieferanten, hat er an der Zuweisung von Verantwortlichkeiten mitzuwirken. In seiner Zusammenarbeit mit externen Lieferanten hat er dafür zu sorgen, das Verantwortlichkeiten im Hinblick auf die IT-Sicherheit klar definiert sind (AI5.2).

Aufgaben in AI6 (Manage Changes)

Die Beteiligung des IT-Nutzers am Change-Management richtet sich auf die Beurteilung der Auswirkungen von Änderungen auf die Funktionalität sowie die Priorisierung und Freigabe von Änderungen (AI6.2). Im Rahmen der Durchführung des Change-Management-Verfahrens hat der IT-Nutzer den Status zu verfolgen (AI6.4) und an einem evtl. Review-Verfahren mitzuwirken, durch das die vollständige Umsetzung der Änderungen (AI 6.5) gewährleistet werden soll.

Aufgaben in AI7 (Installiere und akkreditiere Lösungen und Changes)

Die Aufgaben bei der Installation und Akkreditierung von Lösungen und Changes beziehen sich auf die Implementierung von Änderungen. Der IT-Nutzer hat an Schulungen in Folge von Entwicklungs-, Implementierungs- oder Änderungsprojekten teilzunehmen (AI7.1). Im Rahmen der Testplanung ist er an der Erstellung von Testfällen beteiligt (AI7.2). Zum Implementierungsplan kann der IT-Nutzer die zeitliche Planung für den Roll-out beisteuern (AI7.3). Zur Durchführung von Tests sind plausible Testdaten notwendig, diese können durch den Nutzer bereitgestellt werden. In einer diesbezüglich erstellten Testumgebung kann er diese anwenden und so die Softwareprüfungen unterstützen (AI7.4). Aufgrund seiner Fachkenntnisse sollte er auch bei einer detaillierten Verifikation einer Anwendung oder eines Systems mitwirken (AI7.5). Auch bei Funktionstests bezüglich der Performance von Softwareanwendungen, der Sicherheit und Zugriffsrechte kann er durchaus unterstützen (AI7.6). Das IT-Projektcontrolling richtet sich vor allem nach den Vorgaben des Projekt-Qualitätssystems und des Change-Management-Verfahrens. Im Rahmen der Testarbeiten kann der IT-Nutzer bei der Durchführung des Akzeptanztests, der Vorbereitung der Freigabe (AI7.7) und der Überführung in den Produktivbetrieb beteiligt sein (AI7.8). Inwieweit der IT-Nutzer tatsächlich in diese Aufgaben einbezogen

ist, hängt vom Umfang seiner Projektmitarbeit ab. Nach Abschluss eines Implementierungsprojektes kann er durch die Mitarbeit an einem Review-Verfahren die Erfüllung der fachlichen Anforderungen und die Realisierung des geplanten Nutzens überprüfen (AI7.12).

3.3 Aufgaben in der Domäne DS

Aufgaben in der Domäne DS

In Domäne „Deliver and Support“ (DS) sind IT-Prozesse zusammengefasst, welche die benötigten IT-Services effizient bereitstellen. Die Aufgaben erstrecken sich u. a. auf das Management von Sicherheit, Kontinuität, Daten und operativem IT-Betrieb sowie auf den Benutzerservice. In dieser Domäne kann der IT-Nutzer an der Definition und am Management von Service Levels mitwirken. Zusätzlich zu den oben genannten Bereichen gehören weitere Aufgaben im Problemmanagement von IT. Tabelle 3 stellt die verschiedenen potenziellen Aufgaben und Verantwortlichkeiten in der Domäne im Überblick dar.

Tab. 3 Aufgaben und Verantwortlichkeiten in der Domäne DS

Lfd. Nr.	Aufgabe / Verantwortlichkeit	Prozess	Con. Obj.
1	Mitwirkung an der Festlegung von Rollen, Aufgaben und Verantwortlichkeiten für das Service-Level-Management	Definiere und manage Service Levels (DS1)	DS1.1
2	Mitwirkung an der Festlegung und Vereinbarung von Service-Level-Agreements		DS1.3
3	Mitwirkung an Berücksichtigung von Sicherheitsbelangen bei der Festlegung und Vereinbarung von Service-Level-Agreements		DS1.3
4	Entgegennahme, Prüfung und Analyse von SLA-Berichten		DS1.5
5	Mitwirkung am Review von Service-Level-Agreements		DS1.6
6	Mitwirkung bei der Festlegung bzw. Kenntnis von Rollen, Aufgaben und Verantwortlichkeiten von IT-Lieferanten	Manage Leistungen von Dritten (DS2)	DS2.1
7	Mitwirkung an der Kontrolle von lieferantenbezogenen IT-Risiken in Bezug auf die IT-Sicherheit		DS2.3

8	Mitwirkung an der Kontrolle von lieferantenbezogenen IT-Risiken in Bezug auf konstante Leistungserbringung		DS2.3
9	Mitwirkung an der Lieferantenüberwachung und -bewertung sowie am Vertragsmanagement (Betriebsphase)		DS2.4
10	Unterstützung durch Information der IT-Abteilung über die aktuelle Performance und Kapazität der IT-Ressourcen	Manage Performance und Kapazität (DS3)	DS3.2
11	Information an IT-Abteilung bezüglich künftigem Bedarf an IT-Ressourcen		DS3.3
12	Mitwirkung an der Erstellung von IT-Kontinuitätsplänen	Stelle den kontinuierlichen Betrieb sicher (DS4)	DS4.2
13	Mitwirkung an der Aktualisierung von IT-Kontinuitätsplänen		DS4.4
14	Teilnahme an Schulungen zum IT-Notfallmanagement		DS4.6
15	Mitwirkung an der Festlegung von Inhalt und Umfang der Backup-Auslagerung		DS4.9
16	Aktive und passive Unterstützung der Kommunikation von IT-Sicherheitsrichtlinien und -verfahren (IT-Sicherheitsplan)	Stelle Security von Systemen sicher (DS5)	DS5.2
17	Mitwirkung an der Ableitung von Benutzerberechtigungen aus Geschäftsanforderungen		DS5.3
18	Mitwirkung am Review von Benutzerkonten und entsprechenden Berechtigungen		DS5.4
19	Mitwirkung am Abgleich von Aufbewahrungszeiträumen und Geschäftsanforderungen im Hinblick auf die Protokollierung		DS5.5
20	Meldung von Security Incidents		DS5.6
21	Mitwirkung an der Beurteilung der Schulungsmaßnahmen	Schule und trainiere User (DS7)	DS7.3
22	Aktive Nutzung des Service Desk zur Meldung von Incidents	Manage den Service Desk	DS8.3

23	Review der Lösungen von Incidents in Bezug auf Zufriedenheit und Useability	und Incidents (DS8)	DS8.4
24	Mitwirkung bei der Identifikation und der Klassifizierung von Problemen	Manage Probleme (DS10)	DS10.1
25	Review zur Problemlösung und Abschluss der Problemaufzeichnungen		DS10.3
26	Mitwirkung an der Identifikation und Definition von Aktivitäten und Verantwortungen	Manage den Betrieb (DS13)	DS13.1

Aufgaben in DS1 (Definiere und manage Service Levels)

Für die Zusammenarbeit zwischen IT-Abteilung und Fachabteilung ist weiterhin ein Service-Level-Management (SLM) von zentraler Bedeutung. An der grundlegenden SLM-Konzeption hat die Fachabteilung mitzuwirken, wenn es um die von ihr wahrzunehmenden Rollen, Aufgaben und Verantwortlichkeiten geht (DS1.1). Im Falle der Vereinbarung einzelner SLAs sind die beiderseitigen Verpflichtungen zu konkretisieren, wobei beiderseitige Unterstützungsanforderungen, Messgrößen etc. zu vereinbaren sind. In der SLA-Vereinbarung sind auch Sicherheitsbelange aus Sicht der Fachabteilung zu berücksichtigen (DS1.3). In der Betriebsphase sind die von der IT-Abteilung zu erbringenden IT-Services innerhalb von Service-Level-Agreements geregelt. Über die regelgerechte Erbringung ihrer Leistung hat die IT-Abteilung Bericht zu erstatten. Die Fachabteilung nimmt diese Berichte als Adressat entgegen, prüft und analysiert sie (DS1.5). Auf Basis dieses kontinuierlichen Monitorings sind die SLAs regelmäßig einem Review zu unterziehen, um sie ggf. an Änderungen der Anforderungen anzupassen (DS1.6).

Aufgaben in DS2 (Manage Leistungen von Dritten)

Soweit externe Lieferanten in die Erbringung von IT-Services integriert sind, sind auch für den externen Partner Rollen, Aufgaben und Verantwortlichkeiten festzulegen. Soweit der IT-Nutzer nicht in die Vereinbarung der beiderseitigen Verpflichtungen involviert ist, muss er die Festlegungen kennen, um in der Zusammenarbeit mit Externen seinen Kontroll- und Bewertungsaufgaben nachkommen zu können (DS2.1). Die gleichen Aufgaben stellen sich auch in der Betriebsphase, allerdings fallen sie hier regelmäßig an (DS2.4). Die lieferantenbezogenen Kontrollaufgaben haben sich auch auf die für die konkrete Lieferantenbeziehung identifizierten Risiken zu richten. Gegebenenfalls hat der IT-Nutzer auch die Aufgabe, Risiken in Bezug auf die IT-Sicherheit in der Zusammenarbeit mit dem Lieferanten zu identifizieren und dem internen Risikomanagement zur Kenntnis zu bringen (DS2.3).

Aufgaben in DS3 (Manage Performance und Kapazität)

Die Aufgaben zielen auf das Management von Performance und Kapazität der IT-Ressourcen. Hierbei ist es wichtig, dass die Fachabteilung zu Planungszwecken den aktuellen Stand zu Ressourcenkapazität und Performance an die IT-Abteilung zurückspiegelt (DS3.2). Rechnet die Fachabteilung mit einem künftigen signifikanten zusätzlichen Bedarf an IT-Ressourcen, hat sie diese Information ebenfalls der IT-Abteilung zur Verfügung zu stellen, damit dort die künftig benötigte Kapazität geplant und zur Verfügung gestellt werden kann (DS3.3).

Aufgaben in DS4 (Stelle den kontinuierlichen Betrieb sicher)

Im Hinblick auf ein Notfallmanagement (auch: betriebliches Kontinuitätsmanagement bzw. Business Continuity) hat der IT-Nutzer ggf. an der Erstellung und Aktualisierung von IT-Kontinuitätsplänen mitzuwirken (DS 4.2 und 4.4), an entsprechenden Schulungen teilzunehmen (DS4.6) und als Adressat für die Verteilung der Planungen zu fungieren. Im Rahmen des Notfallmanagements sollten auch der Inhalt und der Umfang der Backup-Auslagerungen zwischen Fachabteilung und IT-Abteilung durch den Nutzer abgestimmt werden (DS4.9).

Aufgaben in DS5 (Stelle Security von Systemen sicher)

Speziell ist durch den IT-Nutzer die Kommunikation der Inhalte von IT-Sicherheitsrichtlinien und -verfahren zu unterstützen (DS5.2). In der Beachtung der verschiedenen Vorgaben kommt dem IT-Nutzer eine Vorbildfunktion zu (bspw. im Umgang mit Passwörtern, in der Nutzung mobiler Geräte sowie beim Gebrauch von externen Speichermedien). Ein weiteres Gebiet der Zusammenarbeit mit der IT-Abteilung ergibt sich aus der Mitwirkung an der Ableitung von Benutzerberechtigungen aus Geschäftsanforderungen (DS5.3) sowie am Review von Benutzerkonten und entsprechenden Berechtigungen (DS5.4), zumindest soweit diese vom IT-Nutzer selbst benötigt werden. Speziell für die Protokollierung ist dafür zu sorgen, dass Aufbewahrungszeiträume mit den Geschäftsanforderungen korrespondieren (DS5.5). Eine weitere wichtige Verantwortlichkeit ist die sofortige Meldung von Security Incidents, um ein schnelles Gegensteuern und somit eine Verringerung des wirtschaftlichen Schadens zu ermöglichen (DS5.6).

Aufgaben in DS7 (Schule und trainiere User)

Weitere potenzielle Aufgaben und Verantwortlichkeiten beziehen sich auf das Training und die Schulung von Usern. Hier hat der IT-Nutzer die Möglichkeit an der Beurteilung der Schulungsmaßnahmen mitzuwirken, um so zur Verbesserung des IT-Know-hows des Unternehmens beizutragen (DS7.3).

Aufgaben in DS8 (Manage den Service Desk und Incidents)

Beim Management des Service Desks und von Incidents zielen die Verantwortlichkeiten des IT-Nutzers auf die sofortige Meldung von IT-Vorfällen

an das Service Desk in der IT-Abteilung. Durch Rückspiegelung der Akzeptanz der Lösungen kann er zum Abschluss von Incidents beitragen (DS8.4).

Aufgaben in DS10 (Manage Probleme)

Im Hinblick auf das IT-Problemmanagement sollte der IT-Nutzer bei der Identifikation und der Klassifizierung von Problemen mitwirken (DS10.1). Ebenso sollte er sich am Review zur Problemlösung und am Abschluss der Problemaufzeichnungen beteiligen (DS10.3).

Aufgaben in DS13 (Manage den Betrieb)

Zur Sicherstellung des kontinuierlichen IT-Betriebs (DS13.1) sollte auch der IT-Nutzer an der Identifikation und Definition von Aktivitäten und Verantwortungen mitwirken.

3.4 Aufgaben in der Domäne ME

Aufgaben in der Domäne ME

Die IT-Prozesse der Domäne „Monitor and Evaluate“ (ME) dienen der regelmäßigen Überprüfung aller Prozesse auf ihre Qualität und auf die Erreichung der Kontrollziele. Im Fokus steht die Performance-Messung. Weitere Aufgabenbereiche für den IT-Nutzer sind in der Überprüfung der Einhaltung von Vorgaben und in der Unterstützung der IT-Governance zu sehen. Tabelle 4 stellt die verschiedenen potenziellen Aufgaben und Verantwortlichkeiten in der Domäne im Überblick dar.

Tab. 4 Aufgaben und Verantwortlichkeiten in der Domäne ME

Lfd. Nr.	Aufgabe / Verantwortlichkeit	Prozess	Con. Obj.
1	Mitwirkung an der Definition von Vorgaben, Messgrößen, Zielen und Benchmarks für Performance	Monitore und evaluiere IT-Performance (ME1)	ME1.2
2	Mitwirkung an der Beurteilung von Performance		ME1.4
3	Mitwirkung an der Identifikation von Verbesserungsmaßnahmen für Performance		ME1.6
4	Mitwirkung an der Bewertung von IT-Controls	Monitore und evaluiere Internal Controls (ME2)	ME2.1
5	Mitwirkung an der Beurteilung von Controls mit Ausnahmebehandlungen		ME2.3
6	Mitwirkung an der Prüfung von Controls in Bezug auf Vollständigkeit		ME2.5
7	Mitwirkung an der Identifikation von Verbesserungsmaßnahmen für Controls		ME2.7

8	Mitwirkung an der Identifikation von Gesetzen und Vorschriften mit Auswirkungen auf die Unternehmens-IT	Stelle Compliance mit Vorgaben sicher (ME3)	ME3.1
9	Aktive und passive Kommunikation von IT-Richtlinien, Standards und Verfahren, sowie Unterstützung bei der Evaluierung zur Einhaltung dieser		ME3.3
10	Mitwirkung an der Einleitung von Verbesserungsmaßnahmen zur Behandlung von Compliance-Lücken		ME3.4
11	Mitwirkung an der Identifikation und Festlegung von Verantwortlichkeiten und Informationsbedarf	Sorge für IT-Governance (ME4)	ME4.1
12	Mitwirkung an der periodischen Beurteilung der IT-Infrastruktur		ME4.4
13	Aktive Kommunikation der Verantwortlichkeiten und der Unternehmenshaltung zum IT-Risikomanagement		ME4.5

Aufgaben in ME1 (Monitore und evaluiere IT-Performance)

Mit den Control Objectives in der Domäne ME schließt sich der Kreis der Steuerungsmechanismen durch die Bereitstellung von Controls zur Überwachung und Bewertung von IT-Prozessen. Um die Performance der Unternehmens-IT zu halten bzw. zu verbessern, ist es notwendig, Vorgaben, Messgrößen, Ziele und Benchmarks zu definieren. Hierbei kann der IT-Nutzer durch seine fachlichen Erfahrungen unterstützen (ME1.2). Durch sein praktisches Wissen kann er ebenfalls bei der Beurteilung der IT-Performance mitwirken (ME1.4). In diesem Zusammenhang ist es ebenso sinnvoll, ihn bei der Identifikation von Verbesserungsmaßnahmen einzubinden (ME1.6).

Aufgaben in ME2 (Monitore und evaluiere Internal Controls)

Die Verantwortlichkeiten in ME2 beziehen sich auf die Internal Controls. Hier kann der Nutzer an der Bewertung der IT-Controls mitwirken, um Verbesserungsmöglichkeiten zu generieren (ME2.1). In diesem Kontext kann er ebenso an der Beurteilung und Dokumentation für die Ausnahmebehandlung von Controls mitwirken. Als Adressat sollte er die Kommunikation der Ausnahmen in der Fachabteilung übernehmen (ME2.3). Im Rahmen der Bewertung kann er auch an der Prüfung der Controls in Bezug auf ihre

Vollständigkeit mitwirken (ME2.5). Hierbei ist es zusätzlich sinnvoll, ihn an der Identifizierung von Verbesserungsmaßnahmen zu beteiligen (ME2.7).

Aufgaben in ME3 (Stelle Compliance mit Vorgaben sicher)

Auch bei der Sicherstellung von Compliance durch Vorgaben können Aufgaben durch den Nutzer übernommen werden. An der Identifizierung von Gesetzen, Verordnungen und Vorschriften, die Auswirkungen auf die Unternehmens-IT haben, sollte auch die Fachkompetenz beteiligt sein (ME3.1). Als Process-Owner und durch Vorbildfunktion kann der IT-Nutzer die Kommunikation von IT-Richtlinien, -Standards und -Verfahren in seinem Bereich fördern. Ebenso kann er bei der Bewertung und Überwachung ihrer Einhaltung unterstützen (ME3.3). In diesem Zusammenhang kann er zusätzlich an der Einführung von Verbesserungsmaßnahmen zur Behandlung von Compliance-Lücken mitwirken (ME3.4).

Aufgaben in ME4 (Sorge für IT-Governance)

Die detaillierten Controls von ME4 beziehen sich auf die Implementierung von IT-Governance. Im Kontext der Einführung eines IT-Governance-Frameworks kann der IT-Nutzer an der Identifizierung und Festlegung von Verantwortlichkeiten und Informationsbedarf eingebunden werden (ME4.1). Im Hinblick auf das Ressourcenmanagement kann er an einer periodischen Beurteilung der IT-Infrastruktur mitwirken (ME4.4). Weiterhin ist eine aktive Kommunikation der Verantwortlichkeiten und der Unternehmenshaltung zum IT-Risikomanagement denkbar (ME4.5).

4. Vergleich und Bewertung der Aufgaben

Vergleichende Betrachtung in Bezug auf die verschiedenen Domänen

Der Aufgabenbereich in der Domäne „Plan and Organise“ stellt das größte potenzielle Aufgabenspektrum für den IT-Nutzer dar. Je nach Einsatzbreite kann dieser im Rahmen der Planung auch Managementaufgaben bei Projekten übernehmen. Die Prozessgruppe „Deliver and Support“ hat dagegen zwar die meisten detaillierten Controls unter sich vereint, diese sind aber größtenteils sehr IT-spezifisch, so dass viele dieser Aktivitäten, Verantwortlichkeiten und Aufgaben nur von ausgebildetem IT-Personal ausgeführt werden können. Gleiches gilt für die Domäne „Acquire and Implement“. Die Domäne „Monitor and Evaluate“ hat dagegen vergleichsweise weniger Steuerungsvorgaben zu bieten. Die meisten Aktivitäten betreffen dabei die Führungsebene. Der Nutzer kann hier allenfalls unterstützend wirken und den Vorgesetzten berichten. Zusammenfassend gesehen kann der IT-Nutzer in jeder Domäne Aufgaben übernehmen, und so zu einer Verteilung der Aufgabenlast beitragen.

Wertung der Aufgaben und Verantwortlichkeiten des IT-Nutzers

Bei der Aufgabenanalyse haben sich verschiedene Aufgaben- und Verantwortungsformen herauskristallisiert:

1. Mitwirkungsaufgaben und -verantwortlichkeiten
2. Unterstützungsaufgaben
3. Eigenständige Durchführungsaufgaben
4. Vollständige Verantwortungsübernahme
5. Übernahme von Pflichten
6. Beratung

Hierbei ist festzuhalten, dass die eigenständige Durchführung von Aufgaben deutlich höher zu bewerten ist als die Mitwirkung und Unterstützung. Die Analyse hat ergeben, dass der IT-Nutzer im Rahmen seiner Rolle als Fachabteilungsverantwortlicher für IT den Großteil seiner Aufgaben (insgesamt 89) als Mitwirkender und nicht als Hauptverantwortlicher durchführt (vgl. Abbildung 3). Diese Anzahl entspricht etwa 68 Prozent der gesamten möglichen Aufgaben. Unterstützungsaufgaben (insgesamt 16) machen etwa 12 Prozent seiner Tätigkeiten aus. Die eigenständig durchführbaren Aufgaben umfassen, inklusive der vollständigen Verantwortungs- und Pflichtenübernahme sowie der Beratungstätigkeiten, etwa 20 Prozent des gesamten potenziellen Aufgabenbereichs.

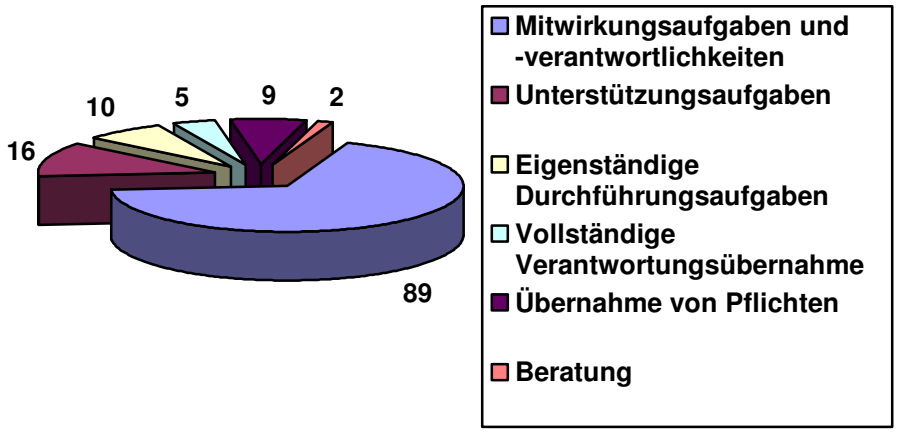

Abbildung 3
Aufgabenverteilung gesamt

5. Fazit

Die Untersuchungen zu möglichen Verantwortlichkeiten und Aufgaben des IT-Nutzers haben gezeigt, dass ihm Mitwirkungsaufgaben sowohl als selbstständig durchführbare als auch als eigenverantwortliche IT-Aufgaben zuge-

wiesen werden können. Beispielsweise kann er im Rahmen von IT-Projekten Planungs- und Organisationsaufgaben übernehmen. Zu seinen möglichen Verantwortungen können ebenfalls Aufgaben aus dem IT-Controlling und -Sicherheitsmanagement gezählt werden. Im IT-Controlling kann und sollte er vor allem ein kontinuierliches Nutzenmonitoring betreiben. Beim IT-Sicherheitsmanagement kann er z. B. die Anforderungen für die IT-Sicherheit definieren und kommunizieren.

Es hat sich im Verlauf der Analysen herausgestellt, dass der IT-Nutzer durch die Übernahme der identifizierten Aufgaben und Verantwortlichkeiten einen wesentlichen Beitrag zur Erfüllung der IT-Ziele leisten kann. Ebenso wurde gezeigt, dass er in der Lage ist, IT-Ressourcen zu unterstützen und Verantwortliche für IT-Governance zu entlasten. Durch die Verteilung der Aufgabenlast und die Einbringung der Fachabteilungssicht und des anwendungsbezogenen Fachwissens wird eine optimale und qualitativ hochwertige Erfüllung der IT-Ziele und somit der Unternehmensanforderungen unterstützt.

In einer Welt, in der sich die Informationstechnologie rasant weiterentwickelt, ist für Unternehmen die Frage der Investition in ständig neue und effektivere Anwendungssoftware elementar geworden. Um mit der Konkurrenz mithalten zu können, muss hierbei kontinuierlich ein zeitgemäßer Standard eingehalten werden. Dazu ist aber auch ein entsprechendes Know-how der Mitarbeiter erforderlich. Für die Unternehmen sollte daher die ständige Weiterbildung der IT-Nutzer oberste Priorität haben. Nur so lassen sich die IT-Aufgaben wirkungsvoll delegieren und damit das aufgezeigte Potenzial ausschöpfen.

Abkürzungsverzeichnis

AI	Domäne: Beschaffe und Implementiere (Acquire and Implement)
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
Con. Obj.	Control Objectives
DS	Domäne: Erbringe und Unterstütze (Deliver and Support)
IM	Informationsmanagement
ISACA	Information Systems Audit and Control Assocaition
ISO	International Organization for Standardization
IT	Information Technology
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
IV	Informationsverarbeitung
KGI	Key Goal Indicator
KPI	Key Performance Indicator
ME	Domäne: Überwache und Evaluiere (Monitor and Evaluate)
PO	Domäne: Plane und Organisiere (Plan and Organise)
RACI	steht für: R=Responsible, A=Accountable, C=Consulted, I= Informed
SLA	Service Level Agreement
SLM	Service Level Management

Literaturangaben

ITGI 2005: IT-Governance Institute (ITGI): COBIT 4.0, Rolling Meadows (USA) 2005; verfügbar unter: http://www.isaca.at/Ressourcen/CobiT%204.0%20Deutsch.pdf; letzter Zugriff am 02.09.2009.

ITGI 2003: IT-Governance Institute (ITGI): IT-Governance für Geschäftsführer und Vorstände, 2. Aufl., verfügbar unter: http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=33261&TEMPLATE=/ContentManagement/ContentDisplay.cfm; letzter Zugriff am 02.09.2009.

Johannsen 2006: Johannsen, W.; Goeken, M.: IT-Governance – neue Aufgaben des IT-Managements. In: Praxis der Wirtschaftsinformatik (HMD 250); dpunkt.verlag, Heidelberg 2006, S. 7-20.

Krause 2003: Krause, M.: Programmierung. In: Disterer, G.; Fels, F.; Hausotter, A. (Hrsg.): Taschenbuch der Wirtschaftsinformatik, 2. Aufl., Carl Hanser Verlag, München-Wien 2003, S. 281-302.

Laudon u. a. 2006: Laudon, K. C.; Laudon, J.; Schoder, D.: Wirtschaftsinformatik – Eine Einführung, Pearson, München 2006.

Meier 2004: Meier, A. (Hrsg.), IT-Servicemanagement, Praxis der Wirtschaftsinformatik (HMD), dpunkt.verlag, Heidelberg 2004.

Meyer 2003: Meyer, M.; Zarnekow, R.; Kolbe, L. M.: IT-Governance – Begriff, Status quo und Bedeutung, Wirtschaftsinformatik 45, 2003; S. 445-448.

Pietsch u. a. 2004: Pietsch, Th.; Martiny, L.; Klotz, M.: Strategisches Informationamanagement - Bedeutung und organisatorische Umsetzung, 4., vollst. überarb. Auflage, Erich Schmidt, Berlin 2004.

Stahlknecht/Hasenkamp 2002: Stahlknecht, Peter; Hasenkamp, Ulrich: Einführung in die Wirtschaftsinformatik, 10. überarb. Aufl., Springer, Berlin u.a . 2002.

Das Stralsund Information Management Team (SIMAT)

Das von Prof. Dr. Michael Klotz geleitete „Stralsund Information Management Team“ (SIMAT) ist am Fachbereich Wirtschaft der FH Stralsund angesiedelt. Es bündelt akademische Lehre und Forschung, Weiterbildungsangebote und Projekte im Themenbereich des betrieblichen Informationsmanagements. Informationsmanagement richtet sich auf die effektive und effiziente Nutzung der informationellen Ressourcen eines Unternehmens. Diese Zielsetzung wird heute von verschiedenen spezialisierten Fachrichtungen in der Informatik, der Wirtschaftsinformatik und der Betriebswirtschaftslehre verfolgt. Das SIMAT arbeitet insofern interdisziplinär, wobei die inhaltlichen Schwerpunkte in Kompetenzzentren (Competence Center) fokussiert werden. Im Rahmen des RD&D-Ansatzes (Research, Development and Demonstration) dienen Labore, die mit aktuellen Tools des Informationsmanagements ausgestattet sind, sowohl der fachlichen Arbeit als auch zu Demonstrationszwecken. Eine intensive Kooperation mit ausgewiesenen Expertinnen und Experten sowie mit privatwirtschaftlichen Unternehmen und die Mitarbeit in anwendungsnahen Fachorganisationen gewährleisten eine praxis- und lösungsorientierte Vorgehensweise. Die Zusammenarbeit mit Lehrstühlen anderer Hochschulen, wissenschaftlichen Einrichtungen und eine umfangreiche Publikationstätigkeit stellen sicher, dass sich das SIMAT am State-of-the-Art des Informationsmanagements orientiert und diesen mitprägt. Auf diese Weise sind die Mitarbeiterinnen und Mitarbeiter des SIMAT in der Lage, anspruchsvolle Konzepte und Lösungen zu konzipieren und zu realisieren.

Das SIMAT versteht sich als Mittler zwischen akademischer Forschung und Lehre auf der einen, und der Wirtschaftspraxis auf der anderen Seite. Diese Transferaufgabe, verankert im Landeshochschulgesetz Mecklenburg-Vorpommerns, bildet den Schwerpunkt der Arbeit des SIMAT. Forschung und Lehre werden nicht als Selbstzweck begriffen, sondern führen zu handlungsrelevanten, innovativen Konzepten und Lösungen, die in die Unternehmenspraxis transferiert werden. Die berufliche Weiterbildung bildet hierbei ein wesentliches Element.

Die anwendungsnahe Forschung am SIMAT ist auf eine ökonomische Verwertung hin orientiert. Es sollen Innovationen entwickelt und in Kooperation mit anderen wissenschaftlichen Einrichtungen, Fach-Institutionen und Unternehmen in eine nachhaltige und profitable Praxis umgesetzt werden. Hierzu werden eigene F&E-Projekte auf dem Gebiet des Informationsmanagements und Innovationsprojekte mit Partnern durchgeführt. Zudem hat sich das SIMAT auf die betriebswirtschaftliche Begleitberatung bei IT-nahen Technologieprojekten spezialisiert. Studierenden und wissenschaftlichen Mitarbeiterinnen und Mitarbeitern wird die Möglichkeit eröffnet, an

der Lösung praktischer Problemstellungen zu arbeiten und sich so optimal auf das spätere Berufsleben vorzubereiten.

Die studentischen Mitarbeiterinnen und Mitarbeiter erhalten im SIMAT Einblick in die Arbeitsmethodik sowohl auf wissenschaftlichem als auch auf wirtschaftlichem Gebiet. Aus den Projekten des SIMAT entstehen zahlreiche Abschlussarbeiten, die den Studierenden der FH Stralsund offen stehen. Das SIMAT bietet zudem eine berufliche Perspektive für Studierende, die sich als wissenschaftliche Mitarbeiter in der anwendungsnahen Forschung qualifizieren wollen.

Das SIMAT beteiligt sich zudem an der Diskussion der wissenschaftlichen Gemeinschaft. Hierzu werden regelmäßig Arbeitspapiere veröffentlicht, die den Stand der Arbeit des SIMAT in die Öffentlichkeit tragen und zur Diskussion anregen sollen. Das SIMAT lädt zudem andere Wissenschaftler, aber auch Referenten aus der Praxis als Vortragende ein. Auf diese Weise lernen die SIMAT-Mitarbeiterinnen und -Mitarbeiter sowie andere interessierte Studierende aktuelle Forschungsergebnisse und praktische Fragestellungen aus erster Hand kennen. Erkenntnisse aus diesen Aktivitäten sowie aus den verschiedenen F&E-Projekten werden systematisch in die Lehre überführt, so dass alle Studierenden von der Forschungsarbeit des SIMAT profitieren können.

Zum Zwecke des ökonomischen Transfers verfolgt das SIMAT den RD&D-Ansatz (Research, Development and Demonstration). Hierzu wird ein Labor als Demonstrationsbereich unterhalten, das einerseits als Testbed, andererseits als Showroom dient.

- Testbed: Im Rahmen des Testbed werden Produkte und Lösungen von Kooperationspartnern des SIMAT in den Bereichen des Informations-, Projekt- und Prozessmanagements betrieben. Auf dieser technischen Grundlage werden im Rahmen von Projekten durch das SIMAT-Team prototypische Lösungen erarbeitet.
- Showroom: Im Showroom werden die erarbeiteten Lösungen und komplexe Nutzungen der verfügbaren Technologie einem Auditorium präsentiert. Hierbei werden sowohl prototypische als auch praktisch erprobte Realisierungen gezeigt.

Kontakt

FH Stralsund • SIMAT • Zur Schwedenschanze 15 • 18435 Stralsund
Ansprechpartner: Prof. Dr. Michael Klotz (Wissenschaftlicher Leiter)
☎ +49 (0)3831 45-6946
✉ michael.klotz@fh-stralsund.de

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance
01-09-002	02.2009	M. Klotz	Von der Informationsgesellschaft zum Informationsarbeiter
01-09-003	09.2009	L. Ramin M. Klotz	Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT