JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL SCHWICKERT

Schwickert, Axel C.; Müller, Laura; Bodenbender, Nicole;
Odermatt, Sven; Brauburger, Dhana

IT-Governance – Reader zur WBT-Serie

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 01/2014
ISSN 1613-6667

Arbeitspapiere WI Nr. 1 / 2014

Autoren: Schwickert, Axel C.; Müller, Laura; Bodenbender, Nicole; Odermatt, Sven; Brauburger, Dhana

Titel: IT-Governance – Reader zur WBT-Serie

Zitation: Schwickert, Axel C.; Müller, Laura; Bodenbender, Nicole; Odermatt, Sven; Brauburger, Dhana: IT-Governance – Reader zur WBT-Serie, in: Arbeitspapiere WI, Nr. 1/2014, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2014, 222 Seiten, ISSN 1613-6667

Kurzfassung: Das vorliegende Arbeitspapier dient als Reader zur WBT-Serie „IT-Governance“, die im E-Campus Wirtschaftsinformatik online zur Verfügung steht.

IT-Governance, als Teilbereich der Corporate Governance, beschreibt den Prozess der verantwortungsvollen Steuerung, Regelung und Kontrolle von Informationstechnologie im Unternehmen. In der WBT-Serie wird zunächst in die Themenbereiche IT-Governance, IT-Performance, Business Impact Management und IT-Compliance eingeführt. Darauf aufbauend wir die Umsetzung der IT-Compliance betrachtet, welche von Fallstudien zu den Standards COBIT und ITIL gefolgt ist. Abschließend folgt die Betrachtung der Norm „ISO/IEC 20000“ aus dem Themenbereich des IT-Service-Management.

Schlüsselwörter: Einführung in IT-Governance, IT-Performance, Business Impact Management, IT-Compliance, Umsetzung der IT-Compliance, Fallstudie COBIT, Fallstudie ITIL, Einführung in ISO/IEC 20000

A Zur Einordnung der WBT-Serie

Die WBT-Serie „IT-Governance“ zu der äquivalenten Master-Veranstaltung „IT-Governance (Vorlesung)“ bildet zusammen mit der WBT-Serie „Einführung in ERP-Systeme - MS Dynamics NAV 2009“ (Übung) das Master-Modul „IT-Governance“. Das Master-Modul „IT-Governance“ wird mit einer 90-minütigen Klausur abgeschlossen. Die Klausur dauert für **alle** Teilnehmer 90 Minuten und umfasst den gesamten Stoff des Master-Moduls "IT-Governance" (bestehend aus der Vorlesung und der Übung "IT-Governance", der WBT-Serie „IT-Governance“ (Vorlesung) und der WBT-Serie „Einführung in ERP-Systeme - MS Dynamics NAV 2009“ (Übung)).

Die Master-Veranstaltung "IT-Governance (Vorlesung)" beinhaltet folgende Stoffe:

- Einführung in IT-Governance
- IT-Performance
- Business Impact Management
- IT-Compliance
- Umsetzung der IT-Compliance
- Fallstudie COBIT
- Fallstudie ITIL
- Einführung in ISO/IEC 20000

Zu den Inhalten der WBT finden Präsenzveranstaltungen statt. Alle WBT zur Vorlesung werden Ihnen auf der Web Site der Professur unter der Rubrik "E-Campus WI" oder direkt bei den Lehrveranstaltungen zur Online-Absolvierung angeboten. Das vorliegende Dokument beschreibt die Inhalte der gesamten WBT-Serie zur Vorlesung. Die Inhalte der WBT sind klausurrelevant - die Studierenden eignen sich die Inhalte im Selbststudium an. Zur Unterstützung bieten wir ein Online-Diskussionsforum und die Direktansprache während der Präsenzveranstaltungen zur Vorlesung an.

Für Ihr Selbststudium per WBT müssen Sie einen Internet-Zugang haben - dies entweder auf Ihren eigenen PCs, auf den PCs im JLU-Hochschulrechenzentrum, in den JLU-Bibliotheken oder dem PC-Pool des Fachbereichs. Bitte beachten Sie, dass Sie sich die erforderlichen Zugangsberechtigungen frühzeitig besorgen.

B Die Web-Based-Trainings zur Übung

Der Lernstoff der Master-Veranstaltung „IT-Governance (Vorlesung)“ wird durch eine Serie von Web-Based-Trainings (WBT) als Äquivalent vermittelt. Die WBT bauen inhaltlich aufeinander auf und sollten daher in der angegeben Reihenfolge und zum vorgesehenen Zeitpunkt absolviert werden. Um bereits im Ablauf der Vorlesungszeit „Klausur-fit“ zu werden, muss jedes WBT mehrfach absolviert werden, bis die jeweiligen Tests in den einzelnen WBT sicher bestanden werden.

WBT-Nr.	WBT-Bezeichnung	Dauer	Bis wann bearbeitet?
1	Einführung in IT-Governance	90 Min.	
2	IT-Performance	90 Min.	
3	Business Impact Management	90 Min.	
4	IT-Compliance	90 Min.	
5	Umsetzung der IT-Compliance	90 Min.	
6	Fallstudie COBIT®	90 Min.	
7	Fallstudie ITIL®	90 Min.	
8	ISO/IEC 20000	45 Min.	

Tab. 1: Übersicht der WBT-Serie

Die Inhalte der einzelnen WBT werden nachfolgend in diesem Dokument gezeigt. Alle WBT stehen Ihnen rund um die Uhr bis zum Ende der Vorlesungszeit online zur Verfügung. Sie können jedes WBT beliebig oft durcharbeiten. In jedem WBT sind enthalten:

- Vermittlung des Lernstoffes,
- interaktive Übungen zum Lernstoff und

abschließende Tests zum Lernstoff.

Inhaltsverzeichnis

Seite

A Zur Einordnung der WBT-Serie I

B Die Web-Based-Trainings zur Übung II

Inhaltsverzeichnis III

Abbildungsverzeichnis X

Tabellenverzeichnis XIV

Abkürzungsverzeichnis XV

1 Einführung in IT-Governance 1

1.1 IT-Präsenz und ihre Risiken 1

1.1.1 Willkommen in der Cronus AG 1

1.1.2 Bedeutungszuwachs und Risiken der IT 1

1.1.3 Deutsche Telekom 1

1.1.4 Swiss Life 2

1.1.5 Deutsche Bahn 2

1.1.6 Entwicklung aus den Ereignissen 2

1.1.7 Bedeutungswandel der IT im Unternehmen 3

1.1.8 Die Wertschöpfungskette der Cronus AG 3

1.1.9 Forderung nach Steuerung, Regulierung und Kontrolle 4

1.2 Zum Begriff IT-Governance 5

1.2.1 Definition von Governance 5

1.2.2 Zusammenhang Corporate Governance – IT-Governance 5

1.2.3 Definitionen von IT-Governance 7

1.2.4 Ziele von IT-Governance 8

1.3 Teilbereiche der IT-Governance 9

1.3.1 Die Teilbereiche der IT-Governance 9

1.3.2 IT-Performance 9

1.3.3 IT-Performance-Messung 10

1.3.4 IT-Compliance 10

1.3.5 Rahmenbedingungen der IT-Compliance 11

1.3.6 IT-Governance als Summe von IT-Performance und IT-Compliance 12

1.3.7 Zusammenfassung und Ausblick 13

1.4 Abschlusstest 14

2 IT-Performance 16
2.1 Der Erfolgsbeitrag der IT 16
2.1.1 Einleitung 16
2.1.2 Definition von Performance 16
2.1.3 Rückblick: Die Teilbereiche der IT-Governance 16
2.1.4 IT-Performance 17
2.1.5 Das Produktivitätsparadoxon der IT 17
2.1.6 IT doesn’t matter!? 18
2.1.7 Business-IT-Alignment 19
2.1.8 Strategic Alignment Model (SAM) 19
2.1.9 Umsetzung eines Business-IT-Alignments 21
2.1.10 Phase 1: Bestandsaufnahme 22
2.1.11 Phase 2: Anpassung mit kritischen Erfolgsfaktoren 23
2.1.12 Phase 2: Anpassung der IT an das Business 23
2.1.13 Phase 3: Messung und IT-Compliance 24
2.2 IT-Performance-Messung 25
2.2.1 Einleitung 25
2.2.2 Kosten und Nutzen von IT-Leistungen 25
2.2.3 Ermittlung der Kosten von IT-Leistungen 26
2.2.4 Ermittlung des Nutzens von IT-Leistungen 27
2.2.5 Verfahren zur Ermittlung des Nutzens von IT-Leistungen 29
2.2.6 Ermittlung des qualitativen Nutzens von IT-Leistungen 30
2.2.7 Übersicht geeigneter qualitativer Verfahren 31
2.2.8 Multifaktorenmethode 32
2.2.9 Mehr-Ebenen-Modell 34
2.2.10 Nutzwertanalyse 35
2.2.11 Argumentebilanz 36
2.2.12 Zusammenfassung I 38
2.2.13 Zusammenfassung II 38
2.3 Abschlusstest 39

3 Business Impact Management 42
3.1 Grundlagen zum Business-Impact-Management 42
3.1.1 Einleitung 42
3.1.2 Problemstellung 42
3.1.3 Steuerung der Ressource "IT" durch das Systems-Management (SM) 44
3.1.4 Business-Impact-Management (BIM) 45
3.1.5 Service Level-Management (SLM) 45

3.1.6 Problemlösung durch BIM ... 46
3.2 Business-Impact-Management - Erwartungen, Funktionen, Nutzen ... 47
3.2.1 Erwartungen an eine BIM-Lösung ... 47
3.2.2 Funktionen von BIM ... 48
3.2.3 Nutzen von BIM ... 48
3.2.4 Entscheidung der Cronus AG ... 49
3.3 Implementierung von BIM in der Cronus AG ... 49
3.3.1 Einleitung ... 49
3.3.2 Implementierungsschritte ... 50
3.3.3 Schritt 1: Geschäftsprozess-Management ... 51
3.3.4 Schritt 2: Systems-Management ... 52
3.3.5 Schritt 3: Service-Level-Management ... 53
3.3.6 Zusammenfassung ... 54
3.4 Abschlusstest ... 55

4 IT-Compliance ... 57
4.1 Zur Notwendigkeit der IT-Compliance ... 57
4.1.1 Bedeutung und Notwendigkeit der IT-Compliance ... 57
4.1.2 Der ENRON-Bankrott 2011 ... 57
4.1.3 WORLDCOM-Betrug 2002 ... 58
4.1.4 FLOWTEX-Betrug 2000 ... 59
4.1.5 Entwicklungen aus den Ereignissen ... 59
4.2 Einordnung der IT-Compliance ... 59
4.2.1 Einleitung ... 59
4.2.2 Business Unit ... 60
4.2.3 Konzeptioneller Rahmen der IT-Compliance ... 60
4.2.4 Einordnung auf konzeptioneller Ebene ... 61
4.2.5 Rückblick. Bereiche der IT-Governance ... 62
4.2.6 Definition der IT-Compliance ... 63
4.2.7 Komponenten der IT-Compliance ... 64
4.2.8 Vorsorge gegen Gesetzesverstöße im IT-Bereich ... 64
4.2.9 Einrichtung eines IT-Risikomanagement ... 66
4.2.10 Persönliche Haftung des Managements ... 66
4.3 Einflussfaktoren auf die IT-Compliance ... 67
4.3.1 Einflussfaktoren der IT-Compliance ... 67
4.3.2 Interessengruppen der IT-Compliance ... 67
4.3.3 Rahmenbedingungen der IT-Compliance ... 69
4.3.4 Standards und Frameworks ... 71
4.3.5 Einordnung der Standards und Frameworks ... 72

4.3.6 Zusammenfassung und Ausblick ... 73
4.4 Abschlusstest ... 74

5 Umsetzung der IT-Compliance ... 77
5.1 Implementierung von IT-Compliance ... 77
5.1.1 Einleitung ... 77
5.1.2 Entwicklung eines Umsetzungsplans von IT-Compliance ... 77
5.1.3 Überblick über den Umsetzungsplan ... 78
5.1.4 Aufbauorganisation in der Cronus AG ... 79
5.1.5 Aufgaben unterschiedlicher Hierarchieebenen ... 80
5.1.6 Der IT-Compliance-Officer ... 81
5.2 Situationsanalyse ... 81
5.2.1 Die Situationsanalyse ... 82
5.2.2 Rückblick: Soll-Analyse aller relevanten Gesetze und Vorgaben ... 82
5.2.3 Soll-Analyse in der Cronus AG ... 85
5.2.4 Die Ist-Situation ... 85
5.2.5 Ist-Situation in der Cronus AG ... 86
5.2.6 Soll-Ist-Vergleich ... 87
5.2.7 Soll-Ist-Vergleich in der Cronus AG ... 89
5.3 Konzeption & Implementierung von Maßnahmen ... 90
5.3.1 Konzeption eigener Maßnahmen ... 90
5.3.2 Konzeption & Implementierung ... 92
5.3.3 Auswahl des "richtigen" Referenzmodells ... 93
5.3.4 COSO®-ERM ... 94
5.3.5 COBIT® ... 96
5.3.6 ITIL® ... 97
5.3.7 ISO-Normen ... 98
5.3.8 Entscheidung für ein Referenzmodell ... 99
5.3.9 Implementierung der Maßnahmen ... 100
5.4 Monitoring & Messung der Wirksamkeit ... 101
5.4.1 Monitoring ... 101
5.4.2 Messung der Wirksamkeit ... 101
5.4.3 Ende des Einführungsprojekts ... 102
5.4.4 Zusammenfassung und Ausblick ... 103
5.5 Abschlusstest ... 104

6 Fallstudie COBIT® ... 107
6.1 Einführung in COBIT® ... 107
6.1.1 Einleitung ... 107

6.1.2 Was ist COBIT®? ... 107
6.1.3 Umsetzung von IT-Governance mit COBIT® ... 109
6.1.4 Komponenten von COBIT® ... 111
6.1.5 Das Prozessreferenzmodell von COBIT® ... 113
6.1.6 Bestandteile des Prozessreferenzmodells von COBIT® ... 114
6.1.7 Was ist ein COBIT®-Prozess? ... 115
6.1.8 Schrittweise COBIT® einführen ... 116
6.2 Umsetzung des COBIT®-Prozesses "BAI06 - Manage Changes" ... 116
6.2.1 Einleitung ... 116
6.2.2 Prozessidentifizierung, -beschreibung und -zweck ... 117
6.2.3 Referenzmaterial ... 118
6.2.4 Prozessziele und Metriken ... 119
6.2.5 Prozessziele der Cronus AG ... 119
6.2.6 IT-bezogene Ziele und Metriken ... 121
6.2.7 IT-Ziele der Cronus AG ... 122
6.2.8 Prozessanforderungen ... 124
6.2.9 Prozessanforderungen der Cronus AG ... 126
6.2.10 Das RACI-Chart ... 127
6.2.11 Das RACI-Chart der Cronus AG ... 128
6.2.12 Prozessaktivitäten ... 131
6.2.13 Prozessaktivitäten der Cronus AG ... 136
6.2.14 Inputs und Outputs ... 137
6.2.15 Projektplanung ... 137
6.2.16 Zusammenfassung und Ausblick ... 138
6.3 Abschlusstest ... 139

7 Fallstudie ITIL® ... 141
7.1 Einführung in ITIL® ... 141
7.1.1 Buongiorno ... 141
7.1.2 Ziele der Cronus AG ... 141
1.1.1 Was ist ITIL®? ... 142
7.1.3 ITIL® steht für IT-Service Management ... 143
7.1.4 Überblick der ITIL®-Version 3 ... 144
7.1.5 Was ist ein Prozess? ... 144
7.1.6 Informationswege zu ITIL® ... 145
7.1.7 Service Lifecycle ... 145
7.2 Die Projektvorbereitungen ... 147
7.2.1 Implementierung von ITIL® in der Cronus AG ... 147
7.2.2 Was ist Incident Management? ... 149

7.2.3 Die ITIL®-Funktionen ... 150
7.2.4 ITIL®-Funktionen: Der Service Desk ... 150
7.2.5 Projektplanung ... 153
7.2.6 Situationsanalyse ... 153
7.2.7 Projektsetup ... 154
7.2.8 Projektnutzen definieren ... 156
7.3 Die Projektdurchführung ... 156
7.3.1 Ausbildung und Training ... 156
7.3.2 Prozessdefinition ... 157
7.3.3 Prozessdefinition: Ausgestaltung des Prozesses I ... 157
7.3.4 Prozessdefinition: Ausgestaltung des Prozesses II ... 159
7.3.5 Prozessdefinition: Definition der Rollen ... 160
7.3.6 Prozessdefinition: Definition der Prozesskennzahlen ... 162
7.3.7 Prozessdefinition: Kriterien des Ticketsystems ... 162
7.3.8 Prozesse etablieren ... 163
7.3.9 Erfolg prüfen ... 164
7.3.10 Zusammenfassung und Ausblick ... 164
7.4 Abschlusstest ... 165

8 ISO/IEC 20000 ... 168
8.1 Grundlagen ... 168
8.1.1 Einleitung ... 168
8.1.2 Was ist ISO/IEC 20000? ... 168
8.1.3 ISO/IEC 20000 und ITIL® ... 169
8.1.4 Ziele der Standardisierung und Zertifizierung ... 170
8.1.5 Vor- und Nachteile der Standardisierung und Zertifizierung ... 171
8.1.6 Das Zertifizierungsverfahren ... 172
8.2 Aufbau der ISO-Norm 20000 ... 173
8.2.1 Einleitung ... 173
8.2.2 Struktur der ISO-Norm ... 173
8.2.3 Bestandteile der ISO-Norm ... 175
8.2.4 ISO/IEC 20000-1: [4]: Das IT-Service-Management-System ... 176
8.2.5 Prozessgruppen ... 177
8.2.6 Ergänzungen von ISO/IEC 20000 ... 178
8.2.7 Zusammenfassung und Ausblick ... 179
8.3 Abschlusstest ... 180

Anhang ... CLXXXIII

Literaturverzeichnis CCIV

Abbildungsverzeichnis

Seite

Abb. 1: Wertschöpfungskette ... 4
Abb. 2: Unternehmensübergreifende Wertschöpfungskette ... 4
Abb. 3: Äußere Einflussfaktoren auf die IT-Governance ... 6
Abb. 4: Innere Einflussfaktoren auf die IT-Governance ... 7
Abb. 5: Strategischer Fit des SAM ... 20
Abb. 6: Das Strategic Alignment Model ... 20
Abb. 7: Planungs- und Umsetzungsschritte zur Umsetzung von Business-IT-Alignment ... 22
Abb. 8: Einmalige Kosten (exemplarisch) von IT-Leistungen ... 26
Abb. 9: Laufende Kosten (exemplarisch) von IT-Leistungen ... 27
Abb. 10: Übersicht qualitativer Verfahren zur Nutzenbewertung ... 31
Abb. 11: Multifaktorenmethode (exemplarisch) ... 33
Abb. 12: Formel zur Berechnung des Nutzenkoeffizients ... 33
Abb. 13: Mehr-Ebenen-Modell (exemplarisch) ... 34
Abb. 14: Nutzwertanalyse (exemplarisch) ... 35
Abb. 15: Bewertungsskala einer Nutzwertanalyse (exemplarisch) ... 36
Abb. 16: Argumentebilanz (exemplarisch) ... 37
Abb. 17: Management-Instrumente des Business-Impact-Management ... 43
Abb. 18: Screenshot eines Systems zur technischen Überwachung der IT-Komponenten im Unternehmen ... 44
Abb. 19: Zusammenhang von Geschäftsprozessen, IT-Services und IT-Ressourcen in der BIM-Pyramide ... 45
Abb. 20: Beispiel für die Zusammenhänge der Bereiche des BIM ... 47
Abb. 21: Vorgehensplan bei der Implementierung einer BIM-Lösung im Unternehmen ... 50
Abb. 22: Modellierung der Geschäftsprozesse der Cronus AG, exemplarische Darstellung eines Teilprozesses ... 51
Abb. 23: Zuordnung der IT-systeme zu dem Teilprozess „After Sales“ ... 52
Abb. 24: Drei-Jahres-Chart der Aktie von ENRON ... 58
Abb. 25: Sieben-Monats-Chart der Aktie von WorldCom ... 58
Abb. 26: Konzeptioneller Rahmen der IT-Compliance ... 61
Abb. 27: Einordnung der IT-Compliance auf konzeptioneller Ebene ... 61
Abb. 28: Komponenten der IT-Compliance ... 64
Abb. 29: IT-Compliance-Risiken ... 66
Abb. 30: Interessengruppen der IT-Compliance ... 67
Abb. 31: Rahmenbedingungen der IT-Compliance ... 70

Abb. 32: Standards und Frameworks 71
Abb. 33: Einordnung der Standards und Frameworks 73
Abb. 34: Umsetzungsplan von IT-Compliance 77
Abb. 35: Aufgaben unterschiedlicher Hierarchieebenen 79
Abb. 36: Die Phasen der Situationsanalyse des Umsetzungsplans 82
Abb. 37: Rahmenbedingungen der IT-Compliance 83
Abb. 38: Soll-Analyse der internen und externen Vorgaben der Cronus AG 85
Abb. 39: Ist-Analyse der internen und externen Vorgaben der Cronus AG 87
Abb. 40: Soll-Ist-Vergleich der internen und externen Vorgaben der Cronus AG 89
Abb. 41: Konzeption eigener Maßnahmen zur Erfüllung der To-Do-Liste 91
Abb. 42: Umsetzungsplan von IT-Compliance: Konzeption und Implementierung 92
Abb. 43: Ansatzpunkte zur Entwicklung von Maßnahmen zur Erreichung von IT-Compliance 93
Abb. 44: Aspekte von Referenzmodellen zur Implementierung von IT-Compliance 94
Abb. 45: Hauptkomponenten von COSO®-ERM 95
Abb. 46: Der COSO®-Würfel 96
Abb. 47: Der COBIT®-Würfel 97
Abb. 48: Übersicht über die 26 ITIL®-Prozesse 98
Abb. 49: Prozess zur Überprüfung der externen und internen Vorgaben 102
Abb. 50: Prozessreferenzmodell von COBIT® 108
Abb. 51: Umsetzungsleitfaden von COBIT® (Schritte) 109
Abb. 52: Schichten des Umsetzungsleitfadens von COBIT® 110
Abb. 53: Der COBIT®-Würfel 112
Abb. 54: Das Prozessreferenzmodell von COBIT® 113
Abb. 55: Die fünf Governance-Prozesse des COBIT®-Prozessreferenzmodells 114
Abb. 56: Die 32 Management-Prozesse des COBIT®-Prozessreferenzmodells 115
Abb. 57: Die Prozesselemente von COBIT®-Prozessen 117
Abb. 58: Prozessidentifizierung, -beschreibung und –zweck des COBIT®-Prozesses BAI06 Manage Changes 118
Abb. 59: Referenzmaterialien für den COBIT®-Prozess BAI06 Manage Changes 118
Abb. 60: Prozessziele und Metriken vom COBIT®-Prozess BAI06 Manage Changes 119
Abb. 61: Prozessziele der Cronus AG für den COBIT®-Prozess 120
Abb. 62: IT-bezogene Ziele und Metriken vom COBIT®-Prozess BAI06 Manage Changes 122
Abb. 63: IT-bezogene Metriken der Cronus AG für den COBIT®-Prozess 123
Abb. 64: IT-bezogene Ziele und Metriken der Cronus AG für den COBIT®-Prozess 123

Abb. 65: Erste Prozessanforderung des Prozesses BAI06 – Manage Changes von COBIT® ... 124
Abb. 66: Zweite Prozessanforderung des Prozesses BAI06 – Manage Changes von COBIT® ... 125
Abb. 67: Dritte Prozessanforderung des Prozesses BAI06 – Manage Changes von COBIT® ... 125
Abb. 68: Vierte Prozessanforderung des Prozesses BAI06 – Manage Changes von COBIT® ... 126
Abb. 69: RACI-.Chart des COBIT®-Prozesses BAI06 – Manage Changes ... 128
Abb. 70: RACI-.Chart der vierten Prozessanforderung des COBIT®-Prozesses BAI06 – Manage Changes ... 129
Abb. 71: Prozessaktivitäten der COBIT®-Prozessanforderung BAI06.01 ... 132
Abb. 72: Prozessaktivitäten der COBIT®-Prozessanforderung BAI06.02 ... 133
Abb. 73: Prozessaktivitäten der COBIT®-Prozessanforderung BAI06.03 ... 134
Abb. 74: Prozessaktivitäten der COBIT®-Prozessanforderung BAI06.04 ... 135
Abb. 75: Inputs und Outputs der COBIT®-Prozessanforderung BAI06.01 ... 137
Abb. 76: Projektplan zur Implementierung des COBIT®-Prozesses BAI06 ... 138
Abb. 77: Logo der „Information Technology Infrastructure Library®“ ... 142
Abb. 78: Übersicht der ITIL®-Prozesse ... 143
Abb. 79: Prozess ... 144
Abb. 80: Service Lifecycle ... 147
Abb. 81: Logo der „Cronus AG“ ... 147
Abb. 82: Der Incident-Management-Prozess ... 149
Abb. 83: Lokaler Service Desk ... 151
Abb. 84: Zentraler Service Desk ... 151
Abb. 85: Virtueller Service Desk ... 152
Abb. 86: Follow the Sun-Service Desk ... 152
Abb. 87: Projektablauf ... 153
Abb. 88: SWOT-Matrix ... 154
Abb. 89: Projektplan „EvI1“ ... 155
Abb. 90: Schritte der Prozessdefinition ... 157
Abb. 91: Vereinfachter Prozessablauf des Incident-Management-Prozesses ... 158
Abb. 92: Originaler ITIL®-Prozessfluss ... 159
Abb. 93: Incident-Priorisierung nach ITIL® ... 160
Abb. 94: Prozesskennzahlen ... 162
Abb. 95: Bestätigte Prozesskennzahlen ... 164
Abb. 96: Logo der ISO ... 169
Abb. 97: Logo der „Information Technology Infrastructure Library®“ ... 169

Abb. 98: ITIL®-Prozesse 170
Abb. 99: Zertifizierungsverfahren 173
Abb. 100: Struktur der ISO-Norm 174
Abb. 101: Bestandteile der ISO-Norm 176
Abb. 102: PDCA-Zyklus 177
Abb. 103: Prozessgruppen 178

Tabellenverzeichnis

Seite

Tab. 1: Übersicht der WBT-Serie II
Tab. 2: Übungsfragen WBT 01 – Einführung in IT-Governance 15
Tab. 3: Übungsfragen WBT 02 –IT-Performance 41
Tab. 4: Übungsfragen WBT 03 –Business-Impact-Management 56
Tab. 5: Übungsfragen WBT 04 – IT-Compliance 76
Tab. 6. Übungsfragen WBT 05 – Umsetzung der IT-Compliance 106
Tab. 7: Übungsfragen WBT 06 –Fallstudie COBIT® 140
Tab. 8: Lösung zu den Übungsfragen WBT 07 – Fallstudie ITIL® 167
Tab. 9: Übungsfragen WBT 08 – ISO/IEC 20000 182
Tab. 10: Lösung zu den Übungsfragen WBT 01 CLXXXIV
Tab. 11: Lösung zu den Übungsfragen WBT 02 CLXXXVII
Tab. 12: Lösung zu den Übungsfragen WBT 03 CLXXXIX
Tab. 13: Lösung zu den Übungsfragen WBT 04 CXCII
Tab. 14: Lösung zu den Übungsfragen WBT 05 CXCV
Tab. 15: Lösung zu den Übungsfragen WBT 06 CXCVII
Tab. 16: Lösung zu den Übungsfragen WBT 07 CC
Tab. 17: Lösung zu den Übungsfragen WBT 08 CCIII

Abkürzungsverzeichnis

AG .....Aktiengesellschaft
AktG .....Aktiengesetz
APO .....Align, Plan and Organise
BAI .....Build, Acquire and Implement
BDSG .....Bundesdatenschutzgesetz
BGB.....Bürgerliches Gesetzbuch
BilMoG.....Bilanzmodernisierungsgesetz
BS .....British Standards
BU .....Business Unit
CCO.....Chief Compliance Officer
CCTA .....Central Computer and Telecommunications Agency
CIO .....Chief Information Officer
CISR .....Center for Information System Research
COBIT.....Control Objectives for Information and related Technology
COSO .....Commitee of Sponsoring Organization of the Treadway Commission
CRM .....Customer-Relationship-Management
DSS.....Deliver, Service and Support
EDM .....Evaluate, Direct and Monitor
ERP.....Enterprise-Ressource-Planning
EvI .....Projekt „Einführung von ITIL®“
EvI1 .....Teilprojekt des Gesamtprojekts „Einführung von ITIL®“
GDPdU .....Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoBS .....Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
IEC .....International Electrotechnical Commission
ISACA.....Information Systems Audit and Control Association
ISMS.....Informationssicherheits-Managementsystem
ISO .....International Organization for Standardization
IT .....Informationstechnologie
ITGI.....IT-Governance Institute
ITIL .....Information Technology Infrastructure Library
ITSM .....Information Technology Service-Management
IuK.....Informations- und Kommunikationstechnologie
KEF .....kritischen Erfolgsfaktoren
KonTraG.....Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
MaRisk .....Mindestanforderungen an das Risikomanagement
MEA .....Monitor, Evaluate and Assess
OECD .....Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

PDCA .....Plan-Do-Check-Act
RACI .....Responsible, Accountable, Consulted, Informed
SAM .....Strategic Alignment Model
SOX.....Sarbanes-Oxley-Act
SRM .....Supplier-Relationship-Management
SWOT.....Strenghts-Weaknesses-Opportunities-Threats
TÜV..... Technischer Überwachungsverein
WBT .....Web-Based-Training

1 Einführung in IT-Governance

1.1 IT-Präsenz und ihre Risiken

1.1.1 Willkommen in der Cronus AG

Hallo! Ich bin Francesco Palla, Chief Information Officer (CIO) in der Cronus AG. Am Beispiel der Cronus AG wird im Laufe dieser WBT-Serie erklärt, was IT-Governance ist und wie die Teilbereiche der IT-Governance in der Cronus AG umgesetzt werden. In diesem ersten WBT wird eine Einführung in IT-Governance gegeben.

Die Cronus AG ist ein mittelständisches Unternehmen der Möbelbranche mit Unternehmensstandort Gießen. Wir stellen Büromöbel her und vertreiben sie direkt an z. B. Möbelhäuser oder an Großhändler. Alle Abteilungen haben die Aufgabe die vorhandenen Ressourcen (z. B. Kapital, Betriebsmittel, Personal etc.) wirtschaftlich sinnvoll einzusetzen. Diese Aufgabe wird durch den Einsatz von Enterprise-Ressource-Planning (ERP)-Systemen unterstützt. Die Cronus AG vertreibt ein solches ERP-System, welches speziell auf die Ansprüche von möbelproduzierenden Unternehmen zugeschnitten ist.

1.1.2 Bedeutungszuwachs und Risiken der IT

Ende des 20. und Anfang des 21. Jahrhunderts gab es einige spektakuläre Fälle, mit denen sich die Bedeutung von IT-Governance-Fragestellungen verdeutlichen lässt. Was damals passiert ist und welche Konsequenzen daraus entstanden sind, soll an folgenden Vorfällen exemplarisch gezeigt werden.

1.1.3 Deutsche Telekom

Die Deutsche Telekom hat 1996 neue Telefontarife eingeführt. Jedoch kam es bei der Ermittlung der Gesprächsgebühren in 550 der insgesamt 8000 Vermittlungsstellen der Telekom zu einem Fehler. Dieser Fehler führte dazu, dass ca. 11 Millionen Kunden überhöhte Gebühren berechnet wurden. Der Schaden pro Kunde belief sich durchschnittlich auf 10 Einheiten, was damals einem Wert von 1,20DM entsprach. Der Gesamtschaden für die Kunden belief sich insgesamt auf ca. 11 Millionen DM.

Der Schaden für die Telekom war jedoch deutlich größer. Um einen anhaltenden Imageschaden zu vermeiden, haben alle betroffenen Kunden 30 Freieinheiten (d. h. 3,60 DM) erhalten. In Summe wurde eine Entschädigung in Höhe von ca. 40 Millionen DM gezahlt. Zusätzlich sind weitere Kosten in Höhe von 40 Millionen DM angefallen. Diese Kosten sind entstanden

durch die Neuinstallation der Software, Presse-Erklärungen sowie die Ermittlung aller betroffenen Kunden. Die Deutsche Telekom hatte im Januar 1996 Mehreinnahmen in Höhe von 11 Mio. DM. Um den Imageschaden zu minimieren, haben sie insgesamt 80 Mio. DM gezahlt. Es ist also insgesamt ein Verlust in Höhe von ca. 69 Mio. DM auf Grund eines Software-Fehlers entstanden.

1.1.4 Swiss Life

Der größte Lebensversicherungskonzern der Schweiz Swiss Life musste 2001 das Jahresergebnis nachträglich um 239 Millionen Franken nach unten korrigieren. Der Grund dafür waren Probleme mit der "Buchhaltungssoftware". Aus einem Reingewinn von rund einer viertel Milliarde Franken wurde ein Verlust in Höhe von einer Million Franken.

Nachdem dieser Fehler ausgemerzt wurde, traten bereits ein halbes Jahr später erneute Probleme mit der "Buchhaltungssoftware" auf. Dieses Mal musste das Ergebnis um 192 Millionen Franken nach unten korrigiert werden. So wurde aus einem Verlust von 386 Millionen Franken ein Verlust in Höhe von 578 Millionen Franken!

1.1.5 Deutsche Bahn

Anfang Mai 2002 hat die **Deutsche Bahn** ihr neues Online-System gestartet, mit dem Bahn-Card-Inhaber bis eine Stunde vor Abfahrt ihre Fahrkarten selbst ausdrucken können. Die Bahn-Server haben jedoch in vielen Fällen Fehler- bzw. überhaupt keine Rückmeldung mehr gegeben. Zwischenzeitlich war sogar das ganze Online-Auskunftssystem "offline". Der Grund dafür war eine Überlastung der Server. Diese kam zu Stande, da es vorab keine ausreichenden Belastungstests für die Server gegeben hat. Nach Aussage der Bahn war man auf viele, aber nicht auf die Menge der Anfragen gefasst.

1.1.6 Entwicklung aus den Ereignissen

Bereits diese wenigen Beispiele zeigen wie die IT zu immensen Wirtschafts- und Image-Schäden führen kann. Die Informations- und Kommunikationstechnologie (IuK - Synonym für IT) durchdringt die gesamte Wertschöpfungskette von jedem Unternehmen. Die gezeigten Beispiele geben klare Hinweise, dass eine verantwortungsvolle Steuerung, Regelung und Kontrolle der IT (IT-Governance) im Unternehmen notwendig ist.

1.1.7 Bedeutungswandel der IT im Unternehmen

Zu Beginn der 50er Jahre bis in die 90er Jahre hinein wurde die Informationstechnologie (IT) als ein Rationalisierungs- und Automatisierungsinstrument betrachtet. Der IT kam zu dieser Zeit keinerlei strategische Bedeutung zu. Mitte der 90er Jahre hat es den ersten großen Bedeutungswandel gegeben. Die IT wurde zu dieser Zeit als strategische Unterstützungs- und Servicefunktion entdeckt. Die strategische Bedeutung der IT spiegelte sich auch in der umfassenden **Präsenz** der IT in allen Unternehmensprozessen wider. Die IT lässt sich seit Mitte der 90er Jahre als eine wesentliche Grundlage der unternehmerischen Tätigkeiten beschreiben. Die Bedeutung der IT im Unternehmen lässt sich aus vier **Perspektiven** beschreiben.

- **IT als Kostenfaktor:** IT kann im Unternehmen als Kostenfaktor betrachtet werden. Dabei hängt die Höhe der IT-bezogenen Kosten von Anteil der Durchdringung der IT in der Wertschöpfungskette eines Unternehmens ab. So haben z. B. Banken eine viel höhere Durchdringung der Wertschöpfungskette mit IT als ein Möbelhersteller und damit auch höhere Kosten.
- **IT als Produktionsfaktor:** Die IT ist heute auch als Produktionsfaktor relevant. Informationen dienen dabei als Input, der in der Prozesskette mit IT-Systemen zu Produkten aus Informationen verarbeitet wird. Die IT als Produktionsfaktor spielt besonders im Dienstleistungsbereich (z. B. Banken, Versicherungen, Medien) eine große Rolle.
- **IT als Wettbewerbsfaktor:** Informationstechnologie wir zunehmend eingesetzt, um Wettbewerbsvorteile zu erzielen und sich so von der Konkurrenz abzusetzen.
- **IT als Risikofaktor:** Je höher der Durchdringungsgrad der IT und umso relevanter die IT als Kosten-, Produktions- und Wettbewerbsfaktor für ein Unternehmen ist, desto abhängiger ist das Unternehmen von der eingesetzten IT. Dieser hohe Einfluss der IT auf dem Unternehmenserfolg führt zu Risiken

1.1.8 Die Wertschöpfungskette der Cronus AG

Heute ist die gesamte Wertschöpfungskette eines Unternehmens von IT durchzogen. Das beginnt bei den primären Aktivitäten der Eingangs-Logistik mit einer automatisierten Lagerhaltung, und geht weiter in der Produktion bis hin zu einer automatisierten Auftragsabwicklung. Gleichermaßen durchzieht die IT die sekundären Aktivitäten der Wertschöpfungskette.

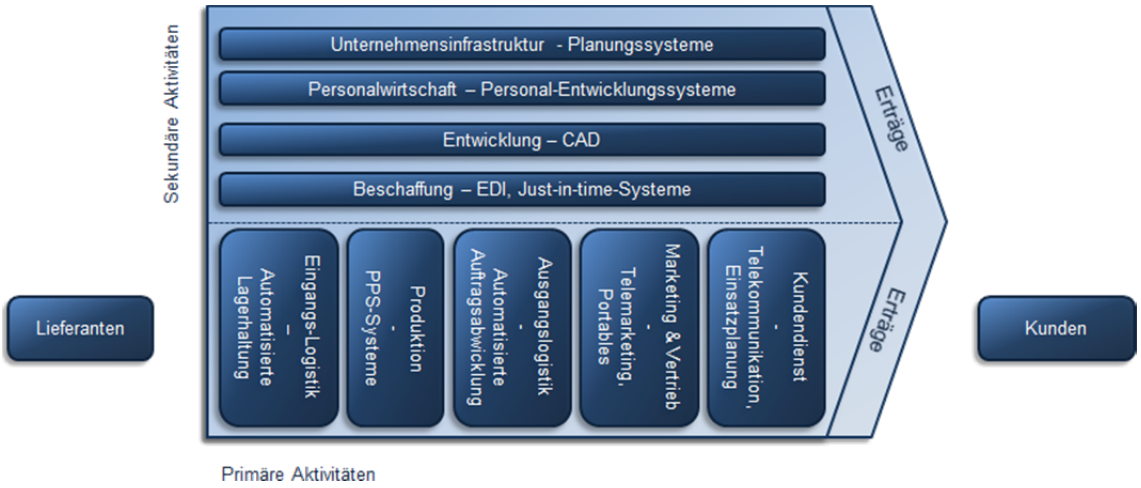


Abb. 1: Wertschöpfungskette

Nach diesem Muster durchdringt die IT die gesamte Wertschöpfungskette, so auch die der Cronus AG. Die Wertschöpfungskette der Cronus AG ist eng mit den Wertschöpfungsketten der vorgelagerten Lieferanten und nachgelagerten Kunden verbunden. Auch diese **unternehmensübergreifende** Wertschöpfungskette wird an den Schnittstellen von IT-Systemen unterstützt. An der Schnittstelle zu den Lieferanten werden sogenannte Supplier-Relationship-Management (SRM)-Systeme eingesetzt. An der Schnittstelle zu den Kunden werden sogenannte Customer-Relationship-Management (CRM)-Systeme eingesetzt.

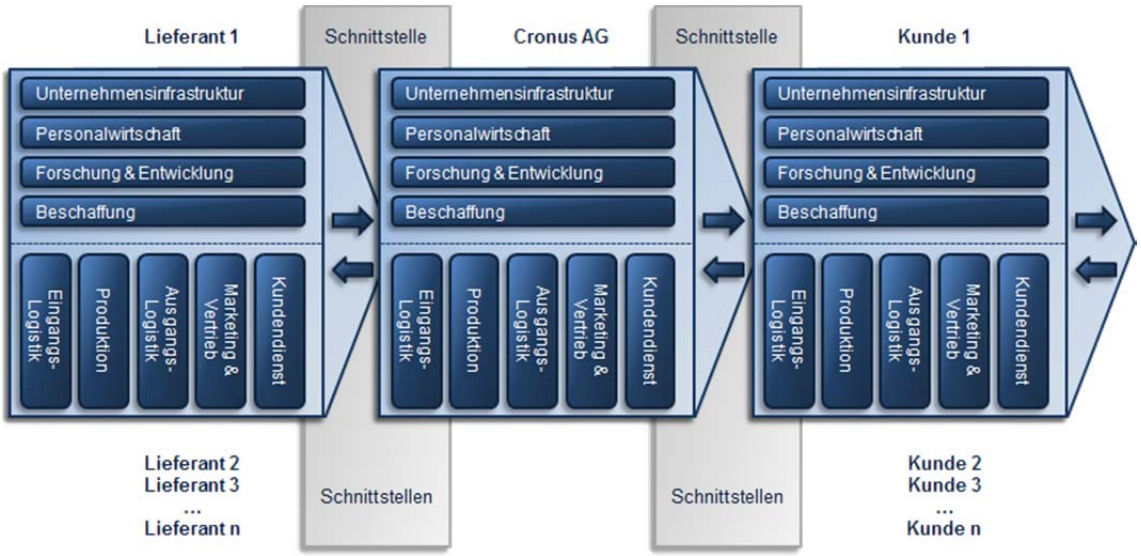


Abb. 2: Unternehmensübergreifende Wertschöpfungskette

1.1.9 Forderung nach Steuerung, Regulierung und Kontrolle

Da sowohl die Wertschöpfungskette der Cronus AG sowie die ihrer Geschäftspartner komplett mit IT durchzogen sind, bestehen hohe IT-Risiken. Die Cronus AG ist also stark vom fehlerfreien Betrieb der IT abhängig. Diese IT-Risiken legen nah, dass eine Regelung, Steue-

rung und Kontrolle der IT notwendig ist, was im Allgemeinen als **IT-Governance** beschrieben werden kann.

1.2 Zum Begriff IT-Governance

1.2.1 Definition von Governance

Der Begriff "Governance" ist abgeleitet aus dem Lateinischen und bedeutet übersetzt steuern, lenken, leiten oder regieren. Bezogen auf den privatwirtschaftlichen Unternehmenssektor kann **Corporate Governance** allgemein als **rechtlicher und faktischer Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens** interpretiert werden.

Definition der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) :

> „Corporate-Governance-Praktiken gehören zu den zentralen Voraussetzungen für die Verbesserung von wirtschaftlicher Effizienz und Wachstum wie auch für die Stärkung des Anlegervertrauens. Sie betreffen das ganze Geflecht der Beziehungen zwischen dem Management eines Unternehmens, dem Aufsichtsorgan, den Aktionären und anderen Unternehmensbeteiligten (Stakeholder). Die Corporate Governance liefert auch den strukturellen Rahmen für die Festlegung der Unternehmensziele, die Identifizierung der Mittel und Wege zu ihrer Umsetzung und die Modalitäten der Erfolgskontrolle.“

Die Definition der OECD betrachtet die **externe Perspektive** der Corporate Governance. Dabei steht das Verhältnis zwischen der Unternehmensführung und den Stakeholdern im Fokus. Studien belegen, dass diese externe Perspektive der Corporate Governance einen positiven Einfluss auf den Unternehmenswert haben kann. Aber auch unternehmensintern spielt die Corporate Governance eine wichtige Rolle. Die **interne Perspektive** der Corporate Governance legt den Fokus auf die Rollen, Kompetenzen, Funktionen und das Zusammenwirken der verschiedenen Unternehmensorgane.

1.2.2 Zusammenhang Corporate Governance – IT-Governance

IT-Governance, als Teilbereich der Corporate Governance, beschreibt den Prozess der verantwortungsvollen Steuerung, Regelung und Kontrolle von Informationstechnologie im Unternehmen. So unterstützt die IT-Governance die Unternehmensführung bezüglich der Beurteilung von Kosten und Nutzen, Chancen und Risiken des IT-Einsatzes im Unternehmen.

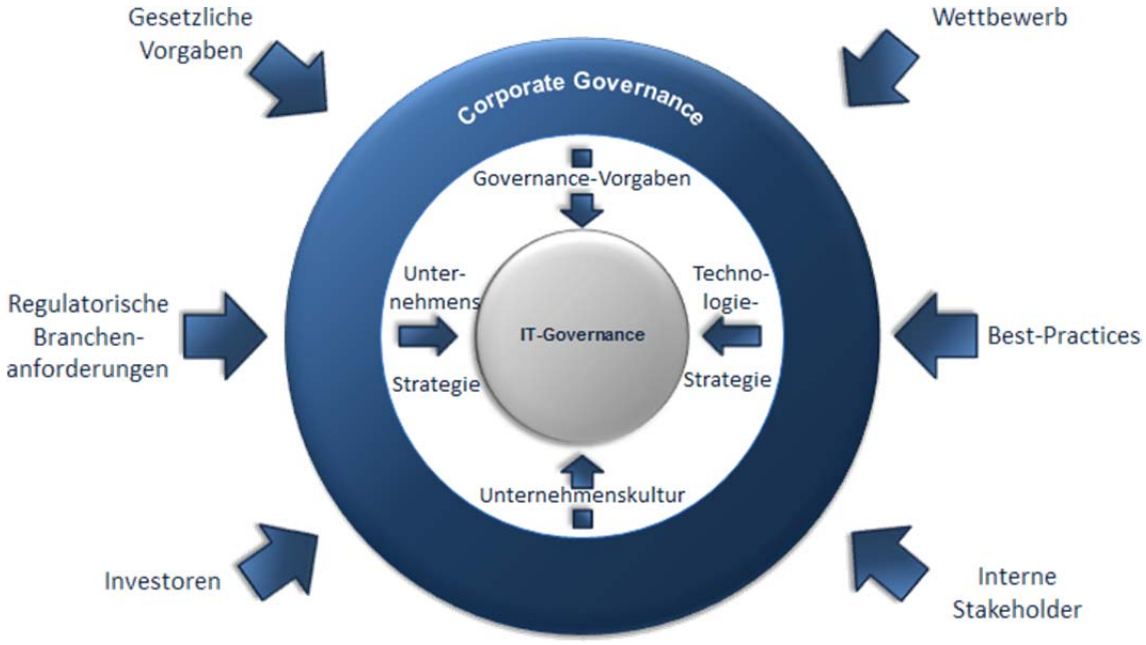


Abb. 3: Äußere Einflussfaktoren auf die IT-Governance

Der innere Kreis "IT-Governance" wird geformt durch die Einflussfaktoren, die aus der Corporate Governance auf den Bereich der IT wirken (vgl. Abb. 3). Auch von innen gibt es Einflussfaktoren auf die IT-Governance (vgl. Abb. 4). So formt die IT selbst die IT-Governance eines Unternehmens, durch die Rolle der IT im Unternehmen, die IT-Strategie, IT-Skills etc.

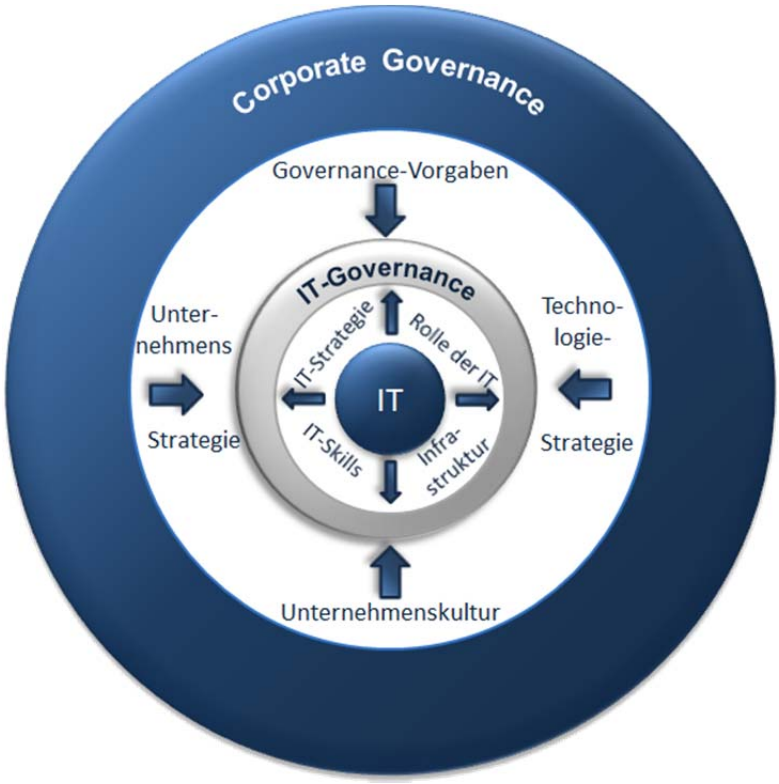


Abb. 4: Innere Einflussfaktoren auf die IT-Governance

1.2.3 Definitionen von IT-Governance

Mit der IT-Governance werden die Prinzipien der Corporate Governance auf den IT-Bereich übertragen. Dabei sind die Inhalte der IT-Governance nicht immer trennscharf von anderen Bereichen der IT abzugrenzen. Demzufolge existieren mehrere unterschiedliche **Begriffsdefinitionen**. Eine einheitliche Definition von IT-Governance hat sich noch nicht herauskristallisiert.

Allgemeines Verständnis von IT-Governance:

- Grundsätze,
- Verfahren und
- Maßnahmen,
- die gewährleisten sollen,
- dass durch den IT-Einsatz
- Unternehmensziele erreicht
- Ressourcen verantwortungsvoll eingesetzt und
- Risiken entsprechend überwacht werden.

Spezielle Definitionen von IT-Governance:

1. Eine der am häufigsten genutzten Definitionen der IT-Governance ist die vom IT-Governance Institute (ITGI) entwickelte:

   "IT-Governance liegt in der Verantwortung des Vorstands und des Managements und ist ein wesentlicher Bestandteil der Unternehmensführung. IT-Governance besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die IT die Unternehmensziele und -strategie unterstützt".

2. Die Information Systems Audit and Control Association (ISACA) definiert IT-Governance als:

   "a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise`s goals by adding value while balancing risk versus return over IT and its processes".

   In dieser Definition spielt "Direction" und "Control" eine wichtige Rolle.

3. Die Definition von IT-Governance, die vom MIT Sloan School of Management Center for Information System Research (CISR) geprägt wurde, zielt auf die Klärung von Rechten und Verantwortlichkeiten ab:

   "specifying the decision rights and accountability framework to encourage desirable behavior in using IT".

Der Vorstand der Cronus AG erhofft sich von der Einführung von IT-Governance eine intensivere Ausrichtung der IT an die Anforderungen der einzelnen Fachabteilungen, die Reduzierung der IT-Kosten, die Erhöhung der IT-Kundenzufriedenheit, eine Risikominimierung und die Einhaltung von regulatorischen und gesetzlichen Anforderungen.

1.2.4 Ziele von IT-Governance

Aus der allgemeinen Definition der IT-Governance müssen unternehmensspezifische Anforderungen und Ziele der IT-Governance abgeleitet werden. Der Chief Information Officer (CIO) der Cronus AG Francesco Palla hat ausgehend von den Zielen der Corporate Governance die **Ziele der IT-Governance** wie folgt festgelegt. Diese Ziele kommuniziert der CIO in seinem wöchentlichen E-Mail-Verteiler an alle Mitarbeiter der IT-Abteilung. Weiterhin hat er einen Beitrag über die Ziele von IT-Governance in der Cronus AG erstellt, der im nächsten Monat im Newsletter der Cronus AG veröffentlicht

wird.

IT-Governance in der Cronus AG soll:

- die Sicherheit der IT-Systeme gewährleisten.
- die Orientierung der IT an den Unternehmenszielen erleichtern.

- den effizienten Einsatz von IT-Ressourcen sicherstellen.
- die Erfüllung der gesetzlichen, vertraglichen und internen Vorgaben gewährleisten.
- einen Beitrag zur Optimierung der IT-Organisation leisten.
- die Transparenz des IT-bereichs erhöhen und so Vertrauen bei den Stakeholdern schaffen

1.3 Teilbereiche der IT-Governance

1.3.1 Die Teilbereiche der IT-Governance

IT-Governance beschreibt den Prozess der verantwortungsvollen Steuerung, Regelung und Kontrolle von IT, sodass die IT die Geschäftsprozesse eines Unternehmens optimal unterstützt. Die in der Literatur zu findenden Definitionen der IT-Governance stellen entweder Performance-Aspekte als innengerichtete Sichtweise der IT-Governance oder Compliance-Aspekte als außengerichtete Sichtweise der IT-Governance in den Vordergrund.

> **IT-Performance:** Bei der IT-Performance als innengerichtete Sichtweise der IT-Governance steht der Wertbeitrag der IT im Vordergrund. Damit sind alle allgemeinen Regelungen, methodische Verfahren und konkrete Maßnahmen des IT-Managements gemeint
>
> **IT-Compliance:** Bei der IT-Compliance, als außengerichtete Sichtweise der IT-Governance, steht das regelkonforme Verhalten in der IT im Vordergrund. Damit ist die Einhaltung aller gesetzlichen, vertraglichen und internen Vorgaben gemeint.

1.3.2 IT-Performance

Die **IT-Performance** als Teilbereich der IT-Governance befasst sich mit der Messung bzw. Bewertung des Wertbeitrags der IT. Die Messung bzw. Bewertung von Kosten und Nutzen birgt jedoch einige **Probleme** in sich.

Häufig fordert die Geschäftsleitung die Generierung von Performance-Kennzahlen. So ist z. B. eine Aufgabe der IT-Leitung Investitionen bzgl. ihrer Kosten und Nutzen gegenüberzustellen. Aber wie soll der zusätzliche Nutzen von Flachbildmonitoren im Vergleich zu den veralteten Röhrenmodellen messbar gemacht werden? Welchen Vorteil hat eine SSD-Karte gegenüber einer Festplatte für die Leistung eines Mitarbeiters der Marketing-Abteilung? Das Problem, dass sich der Produktivitätsbeitrag von IT-Investitionen nicht eindeutig quantifizieren lässt, nennt sich "Produktivitätsparadoxon der IT"

1.3.3 IT-Performance-Messung

Neben der quantitativen Nutzenmessung z. B. Kosteneinsparungen von Personalkosten durch ein neues IT-System spielt auch der qualitative Nutzen z. B. Mitarbeiterzufriedenheit oder -kompetenz eine wichtige Rolle. Um eine vollständige IT-Performance-Messung durchführen zu können, müssen **alle Kosten** mit dem **gesamten Nutzen** verglichen werden.

Zur Ermittlung des quantitativen Nutzens von IT-Leistungen kann z. B. die Rentabilitätsrechnung angewendet werden. Dies ist aber nur möglich, wenn der Nutzen einer IT-Leistung ausschließlich quantitativ ist. In der Regel beschreiben monetäre Werte den Nutzen von IT-Leistungen aber nur sehr beschränkt. Somit muss auch der qualitative Nutzen von IT-Leistungen ermittelt werden, dazu kann z. B. die Nutzwertanalyse angewendet werden. Die einzelnen Verfahren werden detailliert in WBT 02 - IT-Performance betrachtet.

- **Verfahren zur Bestimmung von quantitativem Nutzen**: Quantitative Verfahren berechnen den monetär quantifizierbaren Nutzen von IT-Leistungen. Monetär quantifizierbarer Nutzen ist z. B. die Kosteneinsparung, die durch die Rationalisierung von Personal durch ein neues IT-System entsteht. Dieser Nutzen lässt sich eindeutig quantifizieren. Quantitative Verfahren sind zum Beispiel:
    - Kostenvergleichsrechnung
    - Rentabilitätsrechnung
    - Amortisationsrechnung
    - Kapitalwert-Methode
    - Methode des internen Zinssatzes
- **Verfahren zur Bestimmung von qualitativem Nutzen**: Bei den qualitativen Verfahren wird der nicht-monetär quantifizierbare Nutzen bewertet. Es gibt viele Verfahren, die eine qualitative Bewertung anstreben. Diese Verfahren basieren jedoch durchweg auf subjektiven Einschätzungen. Qualitative Verfahren sind zum Beispiel:
    - Verbale Nutzenbeschreibung
    - Multifaktorenverfahren
    - Nutzwertanalyse
    - Argumentebilanz
    - Mehr-Ebenen-Modell

1.3.4 IT-Compliance

Compliance meint die Konformität mit z. B. **internen Vorgaben**, Gesetzen und **vertraglichen Verpflichtungen**.

In der Cronus AG ist eine **interne Richtlinie** das Vier-Augen-Prinzip. Jeder Mitarbeiter hat wichtige Entscheidungen und Vorgänge durch einen weiteren Mitarbeiter kontrollieren zu lassen.

Eine **vertragliche Verpflichtung** kann z. B. ein Service-Level-Agreement sein. Der Begriff bezeichnet die vertragliche Vereinbarung zwischen einem Auftraggeber und einem Dienstleister für wiederkehrende Dienstleistungen. Vertraglich werden bestimmte Leistungseigenschaften zugesichert wie beispielsweise Leistungsumfang oder das sogenannte Service-Level, welches die vereinbarte Leistungsqualität beschreibt.

Die Aufmerksamkeit für das Thema Compliance hat besonders zu Beginn des 21. Jahrhunderts stark zugenommen. Die hat insbesondere mit den verschiedenen gesetzlichen Vorgaben hinsichtlich des internen Risikomanagements zu tun. Diese Vorgaben wurden im Zuge diverser Bilanzskandale, von den Gesetzgebern erarbeitet. IT-Compliance bezeichnet dabei die Einhaltung und Überwachung der Compliance-Anforderungen **an die IT selbst (IT als Gegenstand)** sowie die Umsetzung der Compliance-Anforderungen mit **IT-Unterstützung (IT als Instrument)**.

- **IT als Gegenstand** der IT-Compliance im Sinne eines Zielobjekts:

  In der IT werden Daten und Informationen verarbeitet. In der Betrachtung von IT als Gegenstand werden konkrete Anforderungen an die Daten- und Informationsverarbeitung direkt gestellt, welche die IT erfüllen muss. Damit sind Ansprüche an die Erhebung, Verarbeitung und Nutzung von diesen Daten und Informationen gemeint. So regelt z. B. das Bundesdatenschutzgesetz die IT-gestützte Verarbeitung personenbezogener Daten.

- **IT als Instrument** der IT-Compliance:

  IT als Instrument wird im Bereich IT-Compliance eingesetzt, um die Einhaltung bestehender Gesetze sicherzustellen. So können Regelverstöße durch IT-Systeme verhindert werden. In der Cronus AG wird beispielsweise das ERP-System "Cronus myERP" genutzt. Innerhalb dieses Systems ist es nicht möglich, nachträglich Rechnungen zu löschen oder zu ändern. So wird durch das ERP-System die IT als Instrument verwendet, um ein regelkonformes Verhalten sicherzustellen. Die IT wird hier als Mittel zur Erfüllung von Compliance-Anforderungen genutzt.

1.3.5 Rahmenbedingungen der IT-Compliance

Zur Umsetzung der zahlreichen Gesetze, internen und externen Vorgaben, vertraglichen Verpflichtungen etc. wurden über die Zeit viele **Frameworks und Best-Practices** (Synonyme Verwendung der Begriffe: Referenzmodell, Framework, Rahmenwerk, Best-Practice-

Sammlung) entwickelt. Diese geben konkrete Anweisungen zur Umsetzung der abstrakten Gesetze und Vorgaben.

- **COSO®-Framework**: Das COSO®-Framework (wird von der Commitee of Sponsoring Organization of the Treadway Commission (COSO®) herausge-geben) ist international anerkannt und lässt sich als Corporate Governance in Regelform beschreiben. Es betrachtet unternehmensübergreifende Aspekte des Risikomanagements und bietet den Unternehmen einen Rahmen zur Einrichtung eines internen Kontrollsystems.
- **Control Objectives for Information and related Technology (COBIT®)**: COBIT® wurde in Anlehnung an COSO® entwickelt. Der Fokus liegt auf der Integration von IT-Governance in die Corporate Governance. COBIT® bietet einen Rahmen für die Ausgestaltung einer IT-Governance, dabei liegt der Fokus auf dem **was** gemacht wird (Zielgrößen werden formuliert) und nicht auf dem **wie**.
- **Information Technology Infrastructure Library (ITIL®)**: ITIL® ist eine Sammlung von Best Practices für die Planung, Überwachung und Steuerung von IT-Leistungen. ITIL® beschreibt dabei **wie** IT-Leistungen erbracht werden, stellt also die Vorgehensweise in den Mittelpunkt.
- **ISO**: ISO 20000 ist die Normierung von ITIL®. Nach dieser Richtlinie können sich die Unternehmen zertifizieren lassen. ISO 2700X sind eine Reihe von Standards zur IT-Sicherheit nach der sich die Unternehmen zertifizieren lassen können.

In den letzten Jahren haben sich eine Vielzahl solcher Frameworks entwickelt. Das COSO®-ERM Framework fokussiert sich auf die Gesamtrisikosteuerung der Unternehmen. Die ISO-Standards 27000 und 20000 beziehen sich auf spezifische technische Aspekte. CobiT® und ITIL® schlagen den Bogen zwischen Technologie und Corporate Governance. Auf die einzelnen Frameworks wird in "WBT 04 - IT-Compliance" detailliert eingegangen.

1.3.6 IT-Governance als Summe von IT-Performance und IT-Compliance

IT-Governance ist die Summe der beiden Teilbereiche IT-Performance und IT-Compliance. Die Definitionen der Teilbereiche legen nah, dass IT-Performance und IT-Compliance inhaltlich überschneidungsfrei voneinander funktionieren. Die Darstellung der Extreme, in denen entweder **nur IT-Performance** beziehungsweise **nur IT-Compliance** umgesetzt werden, verdeutlichen jedoch, wie eng die beiden Bereiche **zusammenhängen.**

- **Nur IT-Performance**: Ein Unternehmen, welches den Wertbeitrag seiner IT-Systeme regelmäßig steigert, aber den Einsatz der IT nicht regelkonform gestaltet, ist wertlos. Das Unternehmen wird Dank der eingesetzten IT einen hohen Umsatz erzielen, jedoch

verstoßen sie gegen geltende Gesetze. So ist der erzielte Umsatz illegal und die Unternehmensleitung muss mit Konsequenzen durch den Rechtsstaat rechnen

- **Nur IT-Compliance**: Ein Unternehmen, welches seine IT-Systeme vollkommen regelkonform einsetzt, aber mit diesen IT-Systemen keinen Wertbeitrag erzielt, schlimmer noch, den Unternehmenserfolg verringert, ist wertlos. Die Manager haben sich zwar einer möglichen Haftbarkeit der IT-Risiken entzogen, erwirtschaften aber keinen Umsatz. Das Unternehmen wäre nach einiger Zeit zwar regelkonform aber insolvent.

Aus Sicht des Managements wird trotz dieser engen Verbindung der **Fokus auf der IT-Performance** liegen. Die Begründung dafür liegt in der Manager-Vergütung, die häufig an ein Bonussystem geknüpft ist. In der Praxis werden die Bonuszahlungen in der Regel an den Einfluss der Abteilung an den Unternehmenserfolg geknüpft. Dieser Einfluss auf den Unternehmenserfolg lässt sich durch die IT-Performance messen. Hingegen gibt es keine Methode festzustellen, ob der Einsatz der IT mehr oder weniger regelkonform gestaltet wurde, als in der vorangegangenen Periode. Das führt dazu, dass die Manager in der Praxis stärker auf eine gute IT-Performance fokussiert sind als auf IT-Compliance. Dieses Wissen über die Relevanz beider Teilbereiche und die unausgewogene Vergütung der Manager, soll der Unternehmensleitung aufzeigen, dass die **Relevanz von IT-Compliance ausreichend stark kommuniziert** werden muss.

1.3.7 Zusammenfassung und Ausblick

In diesem WBT haben Sie gelernt, was IT-Governance bedeutet und wie es in die Corporate Governance einzuordnen ist. Sie haben weiterhin einen ersten Eindruck von den Teilbereichen der IT-Governance erhalten. Die Teilbereiche IT-Performance und IT-Compliance werden im Laufe dieser WBT-Serie detailliert behandelt. Das nächste WBT beschäftigt sich mit der IT-Performance und den Möglichkeiten zur Messung des Wertbeitrags der IT zum Unternehmenserfolg.

1.4 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	Die Informationstechnologie hat in den letzten Jahrzehnten einen starken Bedeutungswandel erlebt. Dabei hat sich die Bedeutung der Informationstechnologie von der Nutzung als Rationalisierungs- und Automatisierungsinstrument hin zur heutigen strategischen Unterstützungs- und Servicefunktion hin entwickelt.		
	Richtig		
	Falsch		
2	Heute ist die gesamte Wertschöpfungskette eines Unternehmens von IT durchzogen.		
	Richtig		
	Falsch		
3	Da die gesamte unternehmensübergreifende Wertschöpfungskette komplett von IT-systemen durchzogen ist, werden Schnittstellen vermieden und somit sinkt das Risiko von IT-Fehlern, wie sie am Beispiel der Deutschen Bahn, Deutschen Telekom und Swiss Life beschrieben sind.		
	Richtig		
	Falsch		
4	Heute lässt sich die IT aus welchen vier Perspektiven beschreiben?		
	IT als Servicefaktor		
	IT als Wettbewerbsfaktor		
	IT als Produktionsfaktor		
	IT als Nutzenfaktor		
	IT als Risikofaktor		
	IT als Kostenfaktor		
5	Bezogen auf den privatwirtschaftlichen Unternehmenssektor kann Corporate Governance allgemein als rechtlicher und faktischer Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens interpretiert werden.		
	Richtig		
	Falsch		

6	Corporate Governance, als Teilbereich der IT-Governance, beschreibt den Prozess der verantwortungsvollen Steuerung von IT im Unternehmen.		
	Richtig		
	Falsch		
7	IT-Governance lässt sich in zwei Teilbereiche aufteilen: IT-Performance und IT-Compliance.		
	Richtig		
	Falsch		
8	Die IT-Performance, als innengerichtete Sichtweise der IT-Governance, beschreibt das regelkonforme Verhalten in der IT. Das meint den Zustand, in dem alle für die Unternehmens-IT relevanten Rechtsnormen (Gesetze und die damit zusammenhängenden Bestimmungen und Verordnungen) sowie Regelwerke nachweislich eingehalten werden.		
	Richtig		
	Falsch		
9	Zur Messung von Performance gibt es allgemein zwei Verfahren: qualitative und quantitative Verfahren der Messung.		
	Richtig		
	Falsch		
10	Eine interne Vorgabe an die man sich der IT-Compliance nach halten soll kann z. B. ein Service-Level-Agreement mit anderen Fachabteilungen sein.		
	Richtig		
	Falsch		

Tab. 2: Übungsfragen WBT 01 – Einführung in IT-Governance

2 IT-Performance

2.1 Der Erfolgsbeitrag der IT

2.1.1 Einleitung

Unternehmensleitungen verfolgen unter anderem das Ziel, Kosten zu senken bzw. auf einem niedrigen Niveau zu halten. So ist es Aufgabe aller Abteilungen in einem Unternehmen ihre Kosten zu senken, und sich für bestehende Kostenblöcke zu rechtfertigen. Neben dem Kostenaspekt muss auch der Nutzenaspekt betrachtet werden. Durch den Vergleich von Kosten und Nutzen lässt sich der Wertbeitrag von z. B. Investitionen oder Abteilungen auf die Unternehmenssituation darstellen.

Auch die IT-Abteilung muss sich mit der Analyse von Kosten und Nutzen beschäftigen. Der Nutzen von einzelnen IT-Leistungen bzw. der gesamten IT-Abteilung lässt sich jedoch schwer quantifizieren. Somit ist auch die Ermittlung des Wertbeitrags der IT auf die Unternehmenssituation nicht einfach.

2.1.2 Definition von Performance

Der Begriff "**Performance**" kann als "**Leistungsfähigkeit**" oder "**Erfolg**" übersetzt werden. Performance wird im Finanzwesen als Maß benutzt, um die Wertentwicklung einer Aktie darzustellen. Über die Wertentwicklung einer Aktie lassen sich Rückschlüsse auf die aktuelle Unternehmenssituation ziehen.

Fordert die Unternehmensleitung eine Aussage über die Performance der IT-Abteilung, müsste streng genommen, der Einfluss der Informationstechnologie auf den Aktienkurs dargestellt werden. Dieser Einfluss ist jedoch nur schwer zu zeigen.

Der Begriff der Performance hat im IT-Bereich eine andere Entwicklung genommen. IT-Performance befasst sich mit dem Vergleich von Kosten und Nutzen. Ist der Nutzen

höher als die Kosten für z. B. die gesamte IT-Abteilung oder ein einzelnes IT-Projekt wird ein positiver Wertbeitrag zur Unternehmenssituation und nicht zum Aktienkurs geleistet. IT-Performance meint also die durch IT-Leistungen erwirtschaftete "Rendite".

2.1.3 Rückblick: Die Teilbereiche der IT-Governance

Wie bereits in "WBT 01 - Einführung in IT-Governance" erläutert wurde, lässt sich die IT-Governance in zwei Teilbereiche aufteilen. Die in der Literatur zu findenden Definitionen der IT-Governance stellen entweder **Performance**-Aspekte, als innengerichtete Sichtweise der

IT-Governance oder **Compliance**-Aspekte, als außengerichtete Sichtweise der IT-Governance, in den Vordergrund.

- **IT-Performance**: Bei der IT-Performance als innengerichtete Sichtweise der IT-Governance steht der Wertbeitrag der IT zur Unternehmenssituation im Vordergrund.
- **IT-Compliance**: Bei der IT-Compliance als außengerichtete Sichtweise der IT-Governance steht die Regelkonformität der IT im Unternehmen im Vordergrund. Damit ist die Einhaltung aller gesetzlichen, vertraglichen und internen Vorgaben gemeint.

2.1.4 IT-Performance

Die **IT-Performance** als Teilbereich der IT-Governance befasst sich mit der Messung bzw. Bewertung des Wertbeitrags der IT zur Unternehmenssituation. Die Messung bzw. Bewertung von Kosten und Nutzen birgt jedoch einige **Probleme** in sich.

Welchen Sinn hat z. B. eine Umstellung des ERP-Systems von einem lokalen Anbieter auf ein großes Unternehmen wie z. B. SAP? Hat der Wechsel des Anbieters einen positiven Einfluss zum Wertbeitrag der IT auf die Unternehmenssituation? Die Umstellung hat dann einen positiven Wertbeitrag, wenn der Nutzen des neuen ERP-Systems größer ist als die anfallenden Kosten. Dann kann man sagen, dass dieses IT-Projekt eine positive IT-Performance hat.

Am Ende einer Periode wird aus der Summe aller IT-Projekte und den Standardaufgaben die Gesamtperformance der IT-Abteilung bestimmt. Ist die Gesamtperformance positiv, dann ist der Gesamtnutzen der IT größer als die angefallenen Kosten.

Das "Produktivitätsparadoxon der IT" besagt jedoch, dass kein empirischer positiver Zusammenhang zwischen Investitionen in die IT und der Produktivität eines Unternehmens besteht. Haben Investitionen in die IT also immer eine negative Performance, da der Nutzen empirisch nicht größer sein kann als die anfallenden Kosten?

2.1.5 Das Produktivitätsparadoxon der IT

Das sogenannte **Produktivitätsparadoxon der IT** ist das Ergebnis einer Reihe von empirischen Studien, die bis Mitte der 90er Jahre durchgeführt wurden. Diese Studien besagen, dass insbesondere im Dienstleistungssektor, kein positiver Zusammenhang zwischen IT-Investitionen und der Produktivität auf unternehmerischer Ebene zu bestehen scheint. Diese fehlende oder sogar negative Steigung der Produktivität trotz hoher IT-Investitionen wird als Produktivitätsparadoxon der IT bezeichnet.

Dieses Paradoxon wurde in der Literatur viel diskutiert, da ohne den Einsatz von IT viele Unternehmen gar nicht wettbewerbsfähig wären. Der IT ist also ein gewisser Nutzen nicht abzusprechen. Es gibt viele Erklärungsansätze, die gegen eine generelle Gültigkeit der Hypothesen sprechen, z. B.:

- Verzögerungen zwischen IT-Einsatz und der Wirkung
- Managementfehler und unzureichende Nutzung der Potentiale beim Einsatz der IT
- Abhängigkeit der IT von Subjektivität (Menschen)
- IT-Erfolge werden durch Defizite anderer Unternehmensbereiche kompensiert.
- IT nur einer von vielen Einflussfaktoren auf den Erfolg eines Unternehmens. Eine isolierte Betrachtung des "Business Impact of IT" ist realitätsfern.

Diese Studien haben eine **bis heute anhaltende Diskussion** um den Beitrag der IT zum Unternehmenserfolg angestoßen.

Im Zusammenhang mit der Diskussion um das Produktivitätsparadoxon der IT, wurde ein kontrovers diskutierter Beitrag namens **"IT doesn't matter"** veröffentlicht. Die daraufhin erneut entbrannte Diskussion hat herausgestellt, dass die IT alleine keinen Wertbeitrag zum Unternehmenserfolg liefert, dass sinnvolle managen hingegen schon.

2.1.6 IT doesn't matter!?

2003 hat Nicholas Carr einen Beitrag mit dem provokanten Namen "**IT doesn't matter**" veröffentlicht. In diesem Beitrag wird die These aufgestellt, dass sich durch den Einsatz von IT aufgrund des hohen Verbreitungsgrades kein Wettbewerbsvorteil erzielen lässt. Dieser Beitrag hat das Produktivitätsparadoxon der IT erneut in den Mittelpunkt vieler Diskussionen gerückt.

IT doesn't matter, IM does

Eine Gegenthese von Hal Varian (2005), die im Rahmen dieser Diskussion erstellt wurde sagt: "**IT doesn't matter, IM does**". Diese Gegenthese gibt der These von Carr dahingehen recht, dass der Einsatz von IT selbst keinen Wert hat. Er behauptet aber, dass die Fähigkeit die IT richtig anzuwenden und einzusetzen sehr wohl zur Schaffung, Erhaltung und Nutzung von Wettbewerbsvorteilen beitragen kann. Gemäß dieser These hängt der Erfolg des IT-Einsatzes vom Management der IT und dessen Ausgestaltung ab.

Diese These hat in der Praxis dazu geführt, dass das effiziente Management der IT und so auch die Messung des Wertbeitrags der IT zum Unternehmenserfolg in den Vordergrund des IT-Managements gerückt ist.

2.1.7 Business-IT-Alignment

IT-Performance ist nur dann relevant, wenn die IT die Unternehmensziele und -strategien unterstützt. Deswegen ist eine fortlaufende Ausrichtung der IT an die Unternehmensziele und -strategie notwendig. Diese Ausrichtung der IT an die Unternehmensziele und -strategie wird Business-IT-Alignment genannt.

Erfolgt **keine Ausrichtung** von der Informationstechnologie an das Business, leistet die IT nicht zwingend einen positiven Wertbeitrag zur Unternehmenssituation.

Ein Teil der Geschäftsstrategie der Cronus AG ist der kundenorientierte Service:

> "Die Cronus AG will auf die Bedürfnisse der Kunden eingehen und diese mit eigenen und fremden Services und Produkten befriedigen."

Um diese Strategie zu verfolgen wurde das Ziel formuliert, dass alle Kundenanfragen innerhalb von drei Werktagen zur Zufriedenheit des Kunden abgearbeitet werden.

Die Mitarbeiter des Kundenservices der Cronus AG haben in letzter Zeit vermehrt die Beschwerde eingereicht, dass sämtliche Kundendaten im CRM-System, die seit über einem Jahr nichts gekauft haben, ins Archiv ausgelagert werden. Aus diesem Grund dauert die Bearbeitung einer Kundenanfrage häufig länger als drei Tage, da die notwendigen Daten erst aus dem Archiv beschafft werden müssen.

In diesem Fall verhindert die eingesetzte IT-Lösung die Erreichung der Unternehmensziele.

2.1.8 Strategic Alignment Model (SAM)

Zur Ausrichtung der IT an der Unternehmensstrategie wurden verschiedene Alignment-Modelle entwickelt, dabei hat das **Strategic Alignment Model (SAM)** eine gewisse Prominenz erlangt. SAM thematisiert dabei zwei Arten der Abstimmung, die im Unternehmen durchgeführt werden sollen: den **strategischen Fit** und die **funktionale Integration**.

Das Strategic Alignment Model zeigt, dass es eine Abstimmungsnotwendigkeit zwischen IT und Business gibt. Dabei werden die verschiedenen Beziehungen zwischen IT und Business dargestellt. Jedoch gibt das Modell keine Hinweise zum speziellen Vorgehen, wie eine solche Abstimmung im Unternehmen erfolgen soll, es erfasst lediglich die analytischen Zusammenhänge.

Strategischer Fit meint die Abstimmung zwischen der Strategie und den Infrastrukturen im Unternehmen:

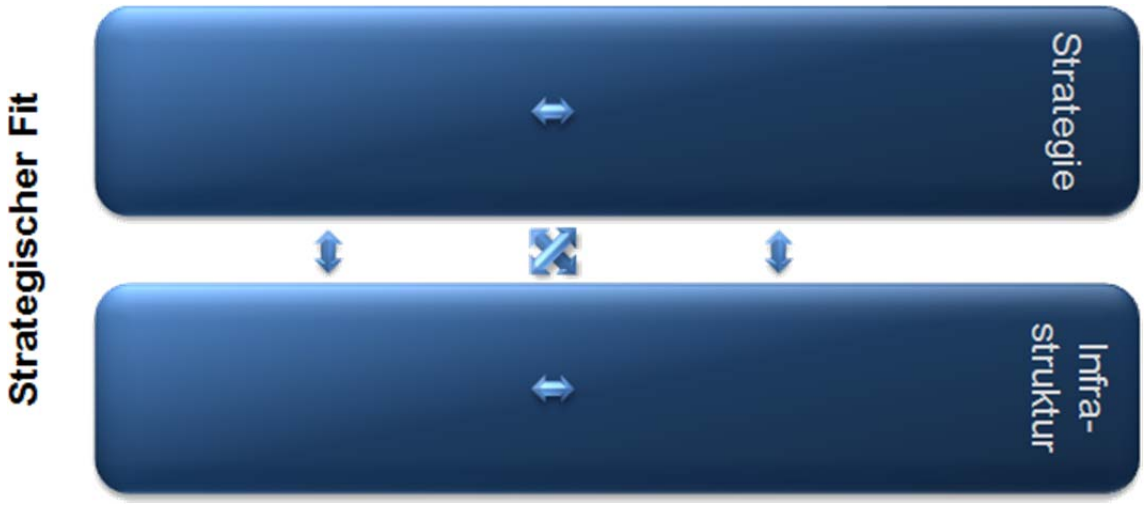


Abb. 5: Strategischer Fit des SAM

Bei der funktionalen Integration wird die geschäftliche Seite mit der IT-Seite eines Unternehmens abgestimmt:

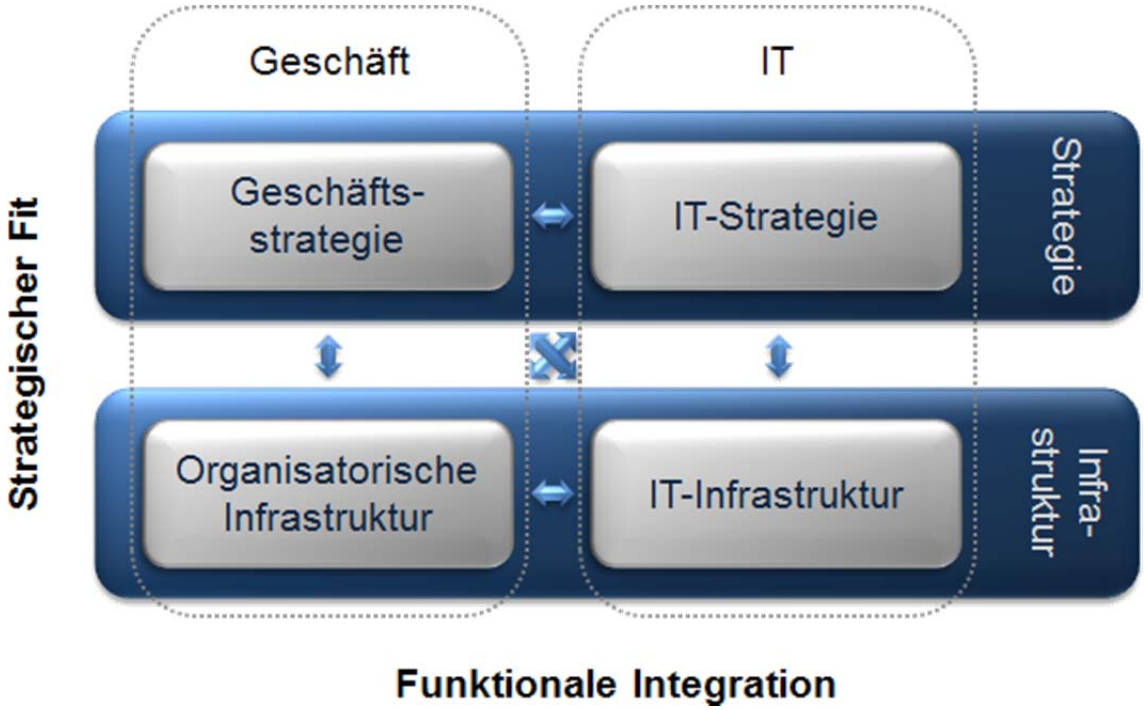


Abb. 6: Das Strategic Alignment Model

Die Zusammenhänge zwischen den einzelnen Bereichen des SAM werden durch die Pfeile dargestellt.

- **Abstimmung: Geschäftsstrategie und IT-Strategie:** Die IT-Strategie kann über das Modell der kritischen Erfolgsfaktoren an den Unternehmensziele und -strategie ausgerichtet werden.
- **Abstimmung: IT-Infrastruktur und IT-Strategie:** Die IT-Infrastruktur ist an der IT-Strategie ausgerichtet. Die IT-Infrastruktur ist z. B. für Systeme und Netze verantwort-

lich, die die IT-Strategie und somit die Ziele und Strategie des Unternehmens unterstützen.

- **Abstimmung: Organisatorische Infrastruktur und IT-Strategie:** Bei der Ausrichtung der IT-Infrastruktur an der organisatorischen Infrastruktur wird die Aufbauorganisation festgelegt. Dabei kann die IT-Abteilung als z. B. Stabsstelle, Linienstelle, Cost Center oder Profit Center organisiert sein.
- **Abstimmung: Organisatorische Infrastruktur und Geschäftsstrategie:** Die Organisatorische Infrastruktur (Verantwortungen, Rollen, Geschäftsprozesse, etc.) wird an der Geschäftsstrategie ausgerichtet.

2.1.9 Umsetzung eines Business-IT-Alignments

Das SAM beschreibt zwar, dass es ein Beziehungskonzept zwischen IT und Business gibt, jedoch werden keine Hinweise gegeben, wie das Business-IT-Alignement umzusetzen ist. Daraus ergibt sich die Frage, wie die IT an die Unternehmensziele und -strategie angepasst werden kann.

Im Folgenden möchte ich Ihnen zeigen, wie die Cronus AG die IT an den übergeordneten Unternehmenszielen und der -strategie ausrichtet. Dazu haben wir den Prozess zur Umsetzung eines Business-IT-Alignments zunächst in drei Phasen unterteilt. Diese Umsetzung kann in anderen Unternehmen von der hier dargestellten Herangehensweise abweichen.

- **Bestandsaufnahme:** In der **ersten Phase** wird eine Bestandsaufnahme von den existierenden Unternehmens- und IT-Strategien im Unternehmen vorgenommen. Bei der Bestandsaufnahme in der Cronus AG haben wir festgestellt, dass wir eine Unternehmensstrategie formuliert haben, jedoch keine davon abgeleitete IT-Strategie. Es bedarf also der Erstellung und Formulierung der IT-Strategie. Diese soll von vorneherein mit der Unternehmensstrategie abgestimmt werden.
- **Anpassung:** Die **zweite Phase** beinhaltet die Anpassung der IT-Strategie an die Unternehmensstrategie. Damit ist die Anpassung von z. B. Systemen, Aktivitäten und Entscheidungsmustern im IT-Bereich an die Unternehmensziele und -Strategien gemeint. Die Angleichung der IT-Strategie an die Unternehmens- und IT-Strategie wird im Unternehmen fortlaufend durch-geführt.

Messung und IT-Compliance: Die **dritte Phase** befasst sich mit der Feststellung und Bewertung der Kosten und Nutzen der erzeugten IT-Leistungen. Die Kosten und Nutzen werden gegenübergestellt, um den Wertbeitrag der IT zur Unternehmenssituation zu bestimmen. Dieser Wertbeitrag der IT zur Unternehmenssituation muss regelkonform sein. Diese Regelkonformität ist Gegenstand der IT-Compliance.

2.1.10 Phase 1: Bestandsaufnahme

Die Ableitung einer IT-Strategie aus der Unternehmensstrategie gehört unter anderem zu den **Aufgabenbereichen** des IT-Managements.

Beispiele für die Aufgabenbereiche des IT-Managements:

- IT-Strategieentwicklung
- IT-Infrastruktur & Anwendungen planen und steuern
- IT-Services definieren
- IT-Lösungen für den täglichen und speziellen Bedarf entwickeln bzw. einführen
- Kosten-und Leistungstransparenz der IT schaffen

Die Entwicklung einer solchen IT-Strategie, sowie die Angleichung an die Unternehmensstrategie, lässt sich in die folgenden vier Planungs- und Umsetzungsschritte unterteilen. Die erste Phase der Bestandsaufnahme beschäftigt sich mit der **Situationsanalyse**.

Abb. 7: Planungs- und Umsetzungsschritte zur Umsetzung von Business- IT-Alignment

Im Rahmen der Situationsanalyse soll die vorhandene strategische Rolle der IT im Unternehmen bestimmt werden. Zunächst ist zu prüfen, ob die IT überhaupt strategisch relevant für die Unternehmenssituation ist.

Da die Cronus AG Software-Hersteller des ERP-Systems "Cronus myERP" ist, dient die IT hier als strategische Waffe. Eine Ausrichtung der IT an der Unternehmensstrategie ist in diesem Fall sehr wichtig. Wäre die Cronus AG hingegen ausschließlich ein Möbelproduzent, wäre eine Ausrichtung der IT an der Unternehmensstrategie nicht so relevant.

2.1.11 Phase 2: Anpassung mit kritischen Erfolgsfaktoren

Die zweite Phase beinhaltet die Anpassung der IT-Strategie an die **Unternehmensziele und -strategie**. Mit der Anpassung ist die Angleichung von z. B. Systemen, Aktivitäten und Entscheidungsmustern im IT-Bereich an die Unternehmensziele und-Strategien gemeint. Die zweite Phase beschäftigt sich mit den Umsetzungsschritten Zielplanung, Strategieentwicklung und Maßnahmenplanung. Um diese Schritte durchführen zu können, wird das Instrument der **kritischen Erfolgsfaktoren (KEF)** angewendet. Mit Hilfe der KEF kann Business-IT-Alignment erreicht werden.

KEF sind die Faktoren, die Einfluss auf den wirtschaftlichen Erfolg eines Unternehmens haben und die strategischen Unternehmensziele unterstützen. Jedes Unternehmen und jeder Bereich eines Unternehmens hat eigene individuelle KEF.

Ein KEF für die Abteilung **Einkauf** ist z. B. die kostengünstige Rohstoffbeschaffung. Ein KEF für die Abteilung **Vertrieb** ist z. B. der gewinnmaximale Umsatz. Auch die **IT-Abteilung** hat solche KEF, die einen direkten Einfluss auf den Erfolg des Unternehmens haben. Ein Beispiel für KEF in der IT-Abteilung ist z. B. ein performantes System, mit dem die Kundendienstleister via z. B. Tablet jederzeit und überall zugreifen können.

2.1.12 Phase 2: Anpassung der IT an das Business

Die zweite Phase beinhaltet die Anpassung der IT-Strategie an die Unternehmensziele und -strategie. Mit der Anpassung ist die Angleichung von z. B. Systemen, Aktivitäten und Entscheidungsmustern im IT-Bereich an die Unternehmensziele und-Strategien gemeint. Diese Phase beschäftigt sich mit den Umsetzungsschritten **Zielplanung, Strategieentwicklung** und **Maßnahmenplanung**. Diese Schritte werden auf Basis der Analyse der unternehmensspezifischen kritischen Erfolgsfaktoren durchgeführt.

- **Zielplanung**: Im Rahmen der Zielplanung werden mit Hilfe der Analyse der kritischen Erfolgsfaktoren die IT-bezogenen KEF identifiziert und gesammelt. Diese KEF bilden die IT-Ziele, welche die Unternehmensziele und -strategie unterstützen.
- **Strategieentwicklung**: Die IT-Ziele werden im Rahmen der Strategieentwicklung mit Kontrollgrößen versehen. Kontrollgrößen von IT-Systemen sind beispielsweise Reaktionszeiten oder Kontaktfrequenzen. Mit Hilfe dieser Kontrollgrößen lässt sich die IT-

Strategie entwickeln, die den Weg und Umfang des zukünftigen Handelns für die Leistung der IT-Abteilung aufzeigt.

Zur Formulierung der IT-Strategie helfen einige exemplarische Fragen:

- Welche Anwendungen (IT-Systeme) werden eingesetzt?
- Wie werden die Anwendungen wo integriert?
- Auf welchen Plattformen und Netzen arbeitet das Unternehmen (IT-Infrastruktur)?
- Welche Services werden wo und wie angeboten?

- **Maßnahmenplanung**: Auf Basis der formulierten Strategie können nun geeignete Maßnahmen geplant und umgesetzt werden, welche die identifizierten KEF unterstützen können.

  Die entwickelte IT-Strategie der Cronus AG beinhaltet nun eine Unterstützung des kundenorientierten Service. Dies wurde als **KEF** der IT-Abteilung identifiziert. Nun werden geeignete Maßnahmen geplant werden, wie die IT-Abteilung der Fachabteilung "Kunden-Services" garantieren kann, dass sämtliche Anfragen systemseitig innerhalb von drei Tagen beantwortbar sind. Dazu schließt die IT-Abteilung einen Service-Vertrag mit der Fachabteilung ab. Als Kontrollgröße dient die Anzahl der Beschwerden der Mitarbeiter der Fachabteilung. Die IT ist nun ausgerichtet auf die Unternehmensziele und -strategie.

2.1.13 Phase 3: Messung und IT-Compliance

Die **dritte Phase** befasst sich mit der Bewertung und dem Gegenüberstellen von Kosten und Nutzen, also der **IT-Performance-Messung**.

Die Mitarbeiter der Cronus AG sind sich im Klaren, dass die Ergebnisse der Ausrichtung der IT an den Unternehmenszielen und -strategie auch gemessen werden müssen. Welche Verfahren sich allgemein zur Messung der IT-Performance anbieten, wird im nächsten Kapitel detailliert erläutert.

Weiterhin werden die Ergebnisse des Business-IT-Alignment auf Regelkonformität (**IT-Compliance**) hin überprüft.

Den Begriff IT-Compliance haben sie bereits in "WBT 01 - Einführung in IT-Governance" als **Teilbereich der IT-Governance** kennengelernt. IT-Compliance hängt dabei eng mit der IT-Performance zusammen. Ein Unternehmen welches bei der IT-Performance den Compliance-Aspekt vernachlässigt, wird durch Einsatz der IT eventuell einen hohen Wertbeitrag erwirtschaften können, berücksichtigt dabei aber nicht die geltenden Gesetze. Dies kann dazu füh-

ren, dass sich das Unternehmen illegal verhält und so mit Konsequenzen durch den Rechtsstaat rechnen muss.

2.2 IT-Performance-Messung

2.2.1 Einleitung

Im Anschluss an die strategische Anpassung von IT an die Unternehmensziele und -strategie, befinden sich in einem Unternehmen im Optimalfall nur noch IT-Leistungen, die den Wertbeitrag zur Unternehmenssituation positiv beeinflussen.

Wie hoch dieser Wertbeitrag ist, muss anhand der IT-Performance-Messung bestimmt werden. Zur Bestimmung der **IT-Performance** werden die Kosten- und Nutzen bestimmt und miteinander vergleichen. Dieses Vorgehen beschreibt man als **Kosten- und Nutzenanalyse**.

2.2.2 Kosten und Nutzen von IT-Leistungen

Um diese Kosten- und Nutzenanalyse auf die IT anzuwenden, muss zunächst überlegt werden, wie die **Kosten** und der **Nutzen** von IT-Leistungen gemessen bzw. bestimmt werden können. Die Messmethoden hängen davon ab, ob es sich um quantitative oder qualitative Kosten- bzw. Nutzenwerte handelt.

Quantitative Werte werden in aller Regel durch Geldbeträge ausgedrückt. **Qual**itative Werte drücken subjektive Werturteile aus.

- Kostenkategorien von IT-Systemen:
    - einmalige Kosten:
    - Personalkosten (z. B. Mitarbeiter zum erstmaligen Entwickeln und Aufsetzen einer Software)
    - Sachkosten (z. B. Anschaffungskosten für Soft- und Hardware)
    - laufende Kosten:
    - Personalkosten (z. B. Mitarbeiter zur kontinuierlichen Pflege und Administration der IT-Systeme)
    - Sachkosten (z. B. Abschreibungen bzw. neue Anschaffung von Soft- und Hardware)

  Bei den Kosten handelt es sich immer um alle Kosten, die im Lebenszeitraum (z. B. Abschreibungszeitraum) einem IT-System zugeordnet werden können, also auch um zukünftige Kosten.

- Nutzenkategorien von IT-Systemen:
    - Kategorie 1: monetär quantifizierbarer Nutzen (berechenbar)

- Quantitativer Nutzen über:
- Gegenwärtige Kosteneinsparungen (direkt quantifizierbar)
- zukünftige Kosteneinsparungen (indirekt quantifizierbar)
- Kategorie 2: nicht-monetär quantifizierbarer Nutzen (schätzbar)
- Qualitativer Nutzen
- Kategorie 3: Strategischer qualifizierbarer Nutzen (entscheidbar)
- strategischer Nutzen

Bei dem Nutzen handelt es sich immer um den gesamten Nutzen, den ein IT-System über seinen gesamten Lebenszeitraum (z. B. Abschreibungszeitraum) erbringt, also auch um zukünftigen Nutzen.

2.2.3 Ermittlung der Kosten von IT-Leistungen

Der erste Schritt einer Kosten- und Nutzenanalyse ist die Auflistung und quantitative Berechnung der Kosten einer IT-Leistung. Dazu werden alle **einmaligen** und **laufenden** Kosten, die in der Cronus AG für die eingesetzte IT anfallen können, aufgelistet.

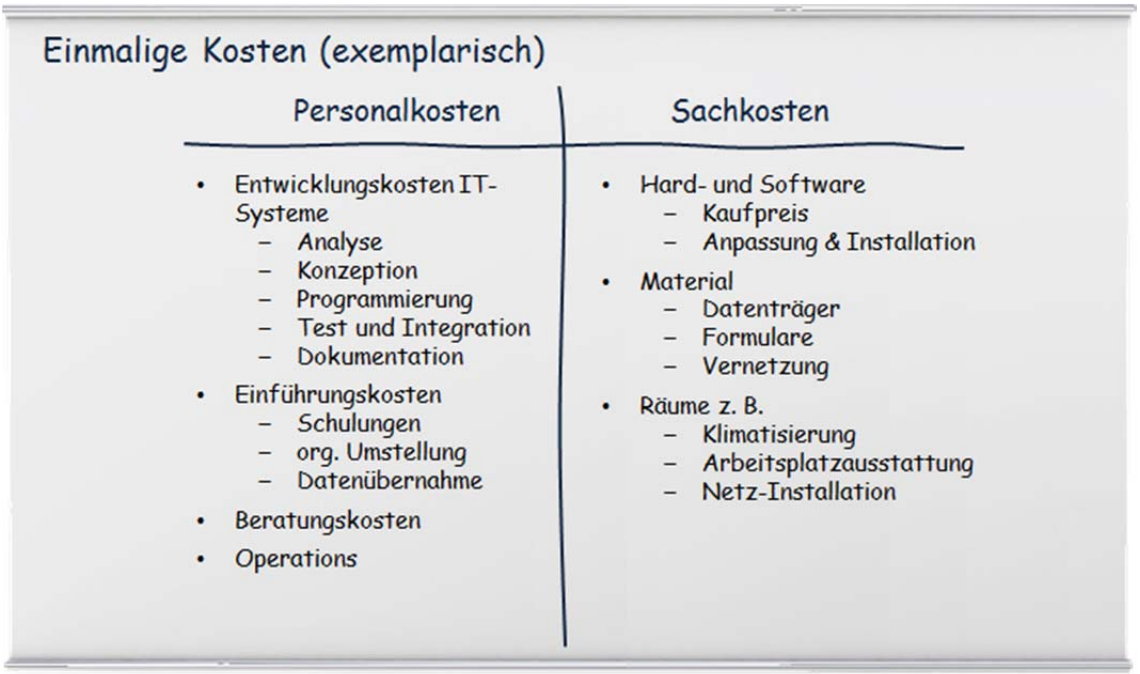


Abb. 8: Einmalige Kosten (exemplarisch) von IT-Leistungen

Abb. 9: Laufende Kosten (exemplarisch) von IT-Leistungen

Die laufenden Kosten setzen sich aus **gegenwärtigen und zukünftigen Kosten** zusammen. Die zukünftig anfallenden Kosten müssen für die Berechnung der Summe aller IT-bezogenen Kosten geschätzt werden. So kommt die Summe dieser Auflistung lediglich einer **Schätzung** gleich, die mit Unsicherheit behaftet ist.

2.2.4 Ermittlung des Nutzens von IT-Leistungen

Der zweite Schritt einer Kosten- und Nutzenanalyse ist die Auflistung und Berechnung des IT-bezogenen Nutzens. Doch bevor wir versuchen den Nutzen von IT-Leistungen zu beziffern, muss verdeutlicht werden, in welche Kategorien der Nutzen von IT-Leistungen eingeteilt werden kann. Dies soll anhand einiger Beispiele verdeutlicht werden.

Die Cronus AG will einen IT-Help-Desk für die Mitarbeiter einrichten, an das sich die Mitarbeiter bei IT-Problemen jederzeit richten können. Die Kosten eines Help-Desk lassen sich direkt quantifizieren durch z. B. die Personalkosten der Help-Desk-Mitarbeiter. Wie hoch ist aber der Nutzen eines Help-Desk? Der Help-Desk hat z. B. den Vorteil, dass nicht mehr alle Mitarbeiter Schulungen besuchen müssen. Die Gesamtkosten für Schulungen sinken also. Dieser Nutzen lässt sich eindeutig durch die Kosteneinsparung quantifizieren. Der Help-Desk hat z. B. auch den Nutzen, dass die Mitarbeiter weniger Vorbehalte (bzw. eine höhere Akzeptanz) im Umgang mit neuen IT-Systemen haben. Dies hat einen direkten Einfluss auf die Zufriedenheit der Mitarbeiter und so auch auf ihre Leistungsbereitschaft. Die Mitarbeiterzufriedenheit ist ein eindeutiger qualitativer Nutzen, den das Help-Desk für die Unternehmenssituation liefern kann. Das Help-Desk liefert neben dem quantitativen also auch einen **qualitativen Nutzen**. Diesem Nutzen stehen klar quantifizierbare Kosten gegenüber. Welchen konkreten Wert misst man den Nutzen des Help-Desk zu?

Auch viele andere IT-Leistungen liefern ausschließlich qualitativen Nutzen. Zum Beispiel können neue Zusatzfunktionen oder eine neue Benutzeroberfläche in einem Release eines IT-Systems verschiedene qualitative Nutzeneffekte liefern.

- Neue Zusatzfunktionen können z. B. dazu führen, dass Mitarbeiter schneller auf Informationen zugreifen können.
- Neue Zusatzfunktionen können auch dazu führen, dass Mitarbeiter Zusammenhänge von Prozessabläufen besser verstehen. Damit wird die Mitarbeiterkompetenz erhöht.
- Eine intuitive Benutzeroberfläche kann die Motivation des Mitarbeiters steigern, da die Usability des IT-Systems verbessert wurde.

Diese IT-Leistungen erbringen alle einen eindeutigen Nutzen. Jedoch kann Mitarbeiterzufriedenheit oder -kompetenz nicht in Geldbeträgen beziffert werden.

2.2.5 Verfahren zur Ermittlung des Nutzens von IT-Leistungen

Anhand dieser Beispiele wird klar, dass neben der quantitativen Nutzenmessung z. B. Kosteneinsparungen von Personalkosten durch ein neues IT-System auch der qualitative Nutzen z. B. Mitarbeiterzufriedenheit oder -kompetenz eine wichtige Rolle spielt. Um eine vollständige Kosten- und Nutzenanalyse durchführen zu können, müssen **alle Kosten** mit dem **gesamten Nutzen** verglichen werden.

Zur Ermittlung des quantitativen Nutzens von IT-Leistungen kann z. B. die Rentabilitätsrechnung angewendet werden. Dies ist aber nur möglich, wenn der Nutzen einer IT-Leistung ausschließlich quantitativ ist. In der Regel beschreiben monetäre Werte den Nutzen von IT-Leistungen aber nur sehr beschränkt. Somit muss auch der qualitative Nutzen von IT-Leistungen ermittelt werden, dazu kann z. B. die Nutzwertanalyse angewendet werden.

- **Verfahren zur Bestimmung von quantitativem Nutzen**: Quantitative Verfahren berechnen den monetär quantifizierbaren Nutzen von IT-Leistungen. Monetär quantifizierbarer Nutzen ist z. B. die Kosteneinsparung, die durch die Rationalisierung von Personal durch ein neues IT-System entsteht. Dieser Nutzen lässt sich eindeutig quantifizieren. Quantitative Verfahren sind zum Beispiel:
    - Kostenvergleichsrechnung
    - Rentabilitätsrechnung
    - Amortisationsrechnung
    - Kapitalwert-Methode
    - Methode des internen Zinssatzes
- **Verfahren zur Bestimmung von qualitativem Nutzen**: Bei den qualitativen Verfahren wird der nicht-monetär quantifizierbare Nutzen bewertet. Es gibt viele Verfahren, die eine qualitative Bewertung anstreben. Diese Verfahren basieren jedoch durchweg auf subjektiven Einschätzungen. Qualitative Verfahren sind zum Beispiel:
    - Verbale Nutzenbeschreibung
    - Multifaktorenverfahren
    - Nutzwertanalyse
    - Argumentebilanz
    - Mehr-Ebenen-Modell

2.2.6 Ermittlung des qualitativen Nutzens von IT-Leistungen

Qualitative Verfahren haben den Nachteil, dass sie stark subjektiv geprägt und somit auch leicht manipulierbar sind. Aus diesem Grund sind qualitative Verfahren als Basis für die Bestimmung des Wertbeitrags zur Unternehmenssituation dem Top-Management gegenüber nur schwierig zu vermitteln.

Wie sollen wir nun in der Cronus AG den Wertbeitrag der IT auf die Unternehmenssituation feststellen? Der Nutzen lässt sich nicht ausreichend quantifizieren und von einer qualitativen Messung versprechen wir uns wenig Akzeptanz im Vorstand. Ich, Francesco Palla habe unsere Unternehmensberatung "KPME" diesbezüglich um **Hilfe** gebeten.

> *Hallo Herr Palla,*
>
> *Um die Subjektivität und Manipulierbarkeit bei der Anwendung von qualitativen Verfahren zur Bestimmung des IT-Nutzens möglichst gering zu halten, hat es sich in der Praxis durchgesetzt, dass* ***mehrere qualitative Verfahren*** *zur Nutzenbestimmung durchgeführt werden. Zusätzlich können die Nutzen-einschätzungen von* ***verschiedenen*** *Personen und Abteilungen durchgeführt werden. Wenn Sie zusätzlich auch* ***pessimistische und optimistische*** *Einschätzungen des Nutzens nebeneinanderstellen, können die qualitativen Verfahren einen realistischen Eindruck über den zukünftigen Nutzen der IT darstellen. Ich bin mir sicher, dass sie mit Hilfe dieser Tipps und einer Kombination von quantitativen und qualitativen Messverfahren die anderen Vorstandsmitglieder der Cronus AG von einer wichtigen IT-Investition überzeugen können.* ***Viel Erfolg dabei!***

2.2.7 Übersicht geeigneter qualitativer Verfahren

In Theorie und Praxis wurden viele qualitative Verfahren zur Nutzenbewertung entwickelt. Einige wichtige dieser qualitativen Verfahren werden diesem Kapitel erläutert.

Abb. 10: Übersicht qualitativer Verfahren zur Nutzenbewertung

- **Verbale Nutzenbeschreibung**: Häufig ist der erste Versuch, den nicht-quantifizierbaren Nutzen **verbal** zu beschreiben. Die alleinige verbale Nutzenbeschreibung sollte jedoch lediglich als Grundlage weiterer Verfahren der Nutzenbewertung dienen, da sie sehr subjektiv ist und so von der Einstellung einzelner Personen abhängt.
- **Multifaktorenverfahren**: Beim Multifaktorenverfahren werden die Nutzen-kriterien (z. B. Qualität, Sicherheit, Transparenz), die für eine IT-Leistung relevant sind, aufgelistet. Diese Kriterien werden anhand verschiedener Faktoren bewertet. Anhand dieser Bewertung lässt sich ein Nutzenkoeffizient bilden. Wesentlich bei der Bewertung ist, dass die Nutzenkriterien nicht individuell für jede Entscheidung neu formuliert werden, sondern dass ein **einheitlicher** Katalog für die Bewertung vorliegt. So lassen sich verschiedene Entscheidungen anhand ihrer Nutzenkoeffizienten vergleichen, ohne

dass eine quantitative monetäre Bewertung notwendig ist. Das Multifaktorenverfahren kann als Vorstufe der **Nutzwertanalyse** genannt werden.

- **Mehr-Ebenen-Modell**: Das **Mehr-Ebenen-Modell** zielt darauf ab, Wirtschaftlichkeits- und Nutzenaspekte der IT auf verschiedene Wirkungs-ebenen - z. B. Arbeitsplatz, Abteilung, Unternehmen - zu veranschaulichen. Die Zuordnung der Nutzeneffekte erstreckt sich auf die verschiedenen Ebenen mit dem Ziel, die einzelnen Nutzeneffekte getrennt voneinander zu untersuchen. Weiterhin soll mit Hilfe der Kosten- Nutzenbeziehung der Ebenen untereinander, ein aussagefähiges Ergebnis über das Nutzenpotential der Informationssysteme in den einzelnen Bereichen erreicht werden.
- **Nutzwertanalyse**: Die **Nutzwertanalyse** ist eins der bekanntesten Verfahren, um qualitativen Nutzen mittels quantitativen Hilfsgrößen auszudrücken. Über einen **Scoring-Ansatz** werden dabei Kriterien von IT-Leistungen bewertet und gewichtet. Ein weiteres Ziel der Nutzwertanalyse ist es, eine Rangfolge der ermittelten Nutzwerte zu entwickeln. Die Bewertung erfolgt anhand einer Skala, die für alle Kriterien und IT-Leistungen immer gleich ist.
- **Argumentebilanzen**: In **Argumentebilanzen** werden alle Vor- und Nachteile, die vorab in den Verfahren gesammelt wurden, verbal gegenübergestellt. Die Bilanzierung des Nutzens stellt eine gute Basis zur Beurteilung vom Nutzen einer IT-Leistung dar. Die Beurteilung kann darüber hinaus durch Eintritts-wahrscheinlichkeiten der Nutzenbeschreibungen ergänzt werden.

2.2.8 Multifaktorenmethode

Beim Multifaktorenverfahren werden die Nutzenkriterien (z. B. Qualität, Sicherheit, Transparenz), die für die Informationstechnologie relevant sind, aufgelistet. Diese Nutzenkriterien werden anhand verschiedener Faktoren bewertet. Anhand dieser Bewertung lässt sich ein **Nutzenkoeffizient** bilden.

Wesentlich bei der Bewertung ist, dass die Nutzenkriterien nicht individuell für jede Bewertung neu formuliert werden, sondern dass ein **einheitlicher Katalog** für die Bewertung vorliegt. So lassen sich verschiedene Entscheidungen anhand ihrer Nutzenkoeffizienten **quantitativ** vergleichen, ohne dass eine monetäre Bewertung notwendig ist.

Nutzenkriterien:	Erfüllungsfaktoren	Vorgabefaktoren	
	A	B	A x B
Kostenreduzierung	1	3	3
Zeitreduzierung	1	3	3
Qualität	3	2	6
Schnelligkeit	0	0	0
Flexibilität	2	3	6
Entscheidungsunterstützung	3	1	3
Auskunftsbereitschaft	3	2	6
Sicherheit	2	2	4
Anwenderfreundlichkeit	3	2	6
Kapazitätsreserve	0	0	0
Transparenz	0	0	0
Summe:		18	37

Abb. 11: Multifaktorenmethode (exemplarisch)

Die Vorgabefaktoren sind festgelegte Zielwerte von z. B. der Unternehmensleitung. Die Adressaten einer IT-Leistung bewerten die Erfüllung der Nutzenkriterien (Erfüllungsfaktoren). Durch die Multiplikation der einzelnen Zeilen "A x B" und das anschließende Teilen der Summe aus "A x B" durch die Summe der Vorgabefaktoren ergibt sich der Nutzenkoeffizient. In diesem Fall hat der Nutzenkoeffizient einen Wert von 2,06.

$$\text{Nutzenkoeffizient} = \frac{\sum A * B}{\sum B}$$

Abb. 12: Formel zur Berechnung des Nutzenkoeffizients

Die Faktorenwerte sind einheitlich zu wählen, um eine Vergleichbarkeit von verschiedenen Informationstechnologien gewährleisten zu können. Hier wurden die Faktorenwerte wie folgt gewählt:

- 3 = erhebliche Veränderung
- 2 = deutliche Veränderung
- 1 = geringe Veränderung
- 0 = keine Veränderung

2.2.9 Mehr-Ebenen-Modell

Das Mehr-Ebenen-Modell zielt darauf ab, Wirtschaftlichkeits- und Nutzenaspekte der IT auf verschiedene Wirkungsebenen - z. B. Arbeitsplatz, Abteilung, Unternehmen - zu veranschaulichen.

Die Zuordnung der Nutzeneffekte erstreckt sich auf die **verschiedenen Ebenen** mit dem Ziel, die einzelnen Nutzenkategorien zu untersuchen. Weiterhin soll mit Hilfe der Kosten- und Nutzenbeziehung der einzelnen Ebenen untereinander, ein aussagefähiges Ergebnis über das Nutzenpotential der IT-Leistungen erreicht werden.

Zuordnung der Effekte / Bewertungsebene	Kosten für Organisation quantitativ/qualitativ	Nutzen für Organisation und Mitarbeiter quantitativ	Nutzen für Organisation und Mitarbeiter qualitativ
Ebene 1: Arbeitsplatz	-Personalkosten -Ausstattungskosten (Technik, Mobiliar, Ergonomie) -Ausbildungskosten -Betriebskosten	-Arbeitsmenge -Bearbeitungszeiten -Abwesenheitszeiten -Koordinationsaufwand -Fehlerquote Belastung Kosteneinsparungen	-Qualität der Leistung -Aufgabenstruktur, z.B. verbesserte Möglichkeiten der Aufgabenintegration -Qualifikations-anforderungen -Arbeitsplatzkomfort
Ebene 2: Arbeitsplatz-verbund	-Kosten der Organisa-tionsanalyse und -gestaltung -Qualifikationskosten -Implementierungskosten -Ausstattungskosten -Betriebskosten -Kosten des innerbe-trieblichen Transports	-Durchlaufzeit -Liege-, Transport- und -Rüstzeiten -Produktivität -Erreichbarkeit -Abstimmungszeit -Bearbeitungsaufwand	-Tätigkeitsvielfalt -Bearbeitungsqualität -Verbundrationali-sierung
Ebene 3: Gesamt-unternehmung	-Infrastrukturen -Personalkosten -Reorganisationskosten -Ausbildungskosten -Beratungskosten	-Reaktionszeiten -Straffung der Abläufe -Führungsaufwand -Konfiguration	-Flexibilität -Verbesserung der Humansituation -Inhaltliche Qualität der Leistung -Innovationsfähigkeit -Entscheidungsqualität -Individualisierung der Marktbedienung
Ebene 4: Unternehmungs-umwelt	negative Auswirkungen bezüglich Aufgaben-umwelt und der generellen Umwelt (Gesellschaft, Arbeits-markt, Konkurrenz, Kunden, etc.)	positive Auswirkungen bezüglich Aufgaben-umwelt und der generellen Umwelt (Gesellschaft, Arbeits-markt, Konkurrenz, Kunden, etc.)	

Abb. 13: Mehr-Ebenen-Modell (exemplarisch)

Im Rahmen des Enterprise Ressource Planning (ERP) bietet dieses Verfahren zur Nutzenbestimmung einen wichtigen Ansatz. Denn die Nutzenwirkung von ERP-Systemen ist auf den unterschiedlichen Wirkungsebenen nicht zwingend gleichverteilt.

Auf diese Weise lassen sich die verschiedenen Wirkungsbereiche eines ERP-Systems differenzierter darstellen. So kann z. B. eine Alternative, die nur den zweiten Rang in der Nutz-

wertanalyse erreicht hat, anhand des Mehr-Ebenen-Modells bevorzugt werden, da dort eine getrennte Untersuchung verschiedener Wirkungsebenen betrachtet wird.

2.2.10 Nutzwertanalyse

Die Nutzwertanalyse ist ein qualitatives Verfahren zur Bewertung von komplexen Entscheidungsalternativen also z. B. von Investitionsentscheidungen. Die Nutzwertanalyse ist ein qualitatives Verfahren, dass in der Praxis aufgrund der einfachen Handhabung eine breite Akzeptanz genießt. Das Ziel einer Nutzwertanalyse ist es, eine Rangfolge der Alternativen aufzustellen. Dazu werden zunächst die relevanten **Kriterien** ermittelt, die im Folgenden **gewichtet** werden. Anschließend werden alle Alternativen hinsichtlich der Kriterien **bewertet**, um so letztlich den **Nutzwert** jeder Alternative berechnen zu können.

		Alternative 1		Alternative 2		...	Alternative 3	
Kriterien	**Gewichtung**	**Bewertung**	**Punktwert**	**Bewertung**	**Punktwert**	**...**	**Bewertung**	**Punktwert**
Kosten-Leistungs-Verhältnis	G_1	$W_{1,1}$	$G_1*W_{1,1}$	$W_{2,1}$	$G_1*W_{2,1}$	...	$W_{3,1}$	$G_1*W_{3,1}$
Bedienung	G_2	$W_{1,2}$	$G_2*W_{1,2}$	$W_{2,2}$	$G_2*W_{2,2}$	...	$W_{3,2}$	$G_2*W_{3,2}$
Anpassungsaufwand	G_3	$W_{1,3}$	$G_3*W_{1,3}$	$W_{2,3}$	$G_3*W_{2,3}$	...	$W_{3,3}$	$G_3*W_{3,3}$
...	...	...	...	...	...	...	...	...
Kriterium n	G_n	$W_{1,n}$	$G_n*W_{1,n}$	$W_{2,n}$	$G_n*W_{2,n}$	...	$W_{3,n}$	$G_n*W_{3,n}$
Nutzwert (Summe der Punktwerte)			$\sum G*W$		$\sum G*W$			$\sum G*W$
Rangfolge		**1**		**3**			**2**	

Abb. 14: Nutzwertanalyse (exemplarisch)

- **Kriterien**: Im ersten Schritt der Nutzwertanalyse werden Kriterien ausgewählt, die für das Unternehmen relevant sind. Für das Beispiel einer IT-Investition in ein neues ERP-System können diese Kriterien z. B. das Kosten-Leistungs-Verhältnis, die einfache Bedienung oder ein notwendiger Anpassungsaufwand der Standardsoftware sein.
- **Gewichtung**: Im zweiten Schritt der Nutzwertanalyse werden die ausgewählten Kriterien gewichtet. Dabei kann z. B. eine prozentuale Gewichtung vorge-nommen werden, bei der die Summe immer 100 entsprechen muss. Dies hat den Nachteil, dass wenn z. B. die Anzahl der Kriterien nachträglich geändert werden soll, müssen alle Gewichtungen neuverteilt werden.

  So hat sich die Cronus AG entschieden, eine ganzzahlige Skala zur Gewichtung der Kriterien vorzunehmen. Dabei werden die Kriterien von 1 bis 10 bewertet, wobei 1 die niedrigste und 10 die höchste Priorität eines Kriteriums widerspiegelt.
- **Bewertung**: Im dritten Schritt der Nutzwertanalyse werden die Investitionsalternativen hinsichtlich der genannten Kriterien bewertet. Dazu muss im Unternehmen eine geeignete **Bewertungsskala** festgelegt werden, um die Subjektivität der Bewertung

möglichst gering zu halten. Anhand dieser Skala werden alle Alternativen hinsichtlich der Kriterien bewertet.

Kriterium	Anpassungsaufwand	Bewertungsskala
Ausprägung	sehr gering	5
	gering	4
	durchschnittlich	3
	hoch	2
	sehr hoch	1

Abb. 15: Bewertungsskala einer Nutzwertanalyse (exemplarisch)

Wurden alle Kriterien gewichtet und alle Alternativen bewertet, kann mit der finalen Auswertung begonnen werden:

Dazu wird zunächst der Punktwert jeder Alternative je Kriterium bewertet, indem die Gewichtung mit der Bewertung multipliziert wird. Die so ermittelten Punktwerte werden je Alternative summiert. Dies ergibt den Nutzwert, den eine Alternative in Abhängigkeit der gewählten Kriterien für das Unternehmen erreicht. Diese Nutzwerte werden final miteinander direkt verglichen. Daraus ergibt sich wiederum eine Rangfolge der Alternativen. Der höchste erreichte Nutzwert spiegelt dabei die zu favorisierende Alternative wider. Ihr wird der Rang "eins" zugeordnet.

Dieses methodische Vorgehen der Nutzwertanalyse suggeriert eine objektive Bewertung des Nutzens. Diese Objektivität ist jedoch nur scheinbar vorhanden, es handelt sich bei der Nutzwertanalyse um ein qualitatives Verfahren zur Nutzenbestimmung. Das heißt, die Nutzwertanalyse basiert auf subjektiven Gewichtungs- und Bewertungsmaßstäben und ist somit als alleiniges Entscheidungsinstrument nicht zu empfehlen. Es sollte durch weitere qualitative und quantitative Verfahren ergänzt werden, um ein möglichst ganzheitliches Bild vom Nutzen der Investitionsalternativen erzeugen zu können.

2.2.11 Argumentebilanz

In Argumentebilanzen werden alle Vor- und Nachteile, die vorab in den Verfahren gesammelt wurden, verbal gegenübergestellt. Die Bilanzierung des Nutzens stellt eine gute Basis zur Beurteilung vom Nutzen einer IT-Leistung dar. Die Beurteilung kann darüber hinaus durch Eintrittswahrscheinlichkeiten der Nutzenbeschreibungen ergänzt werden.

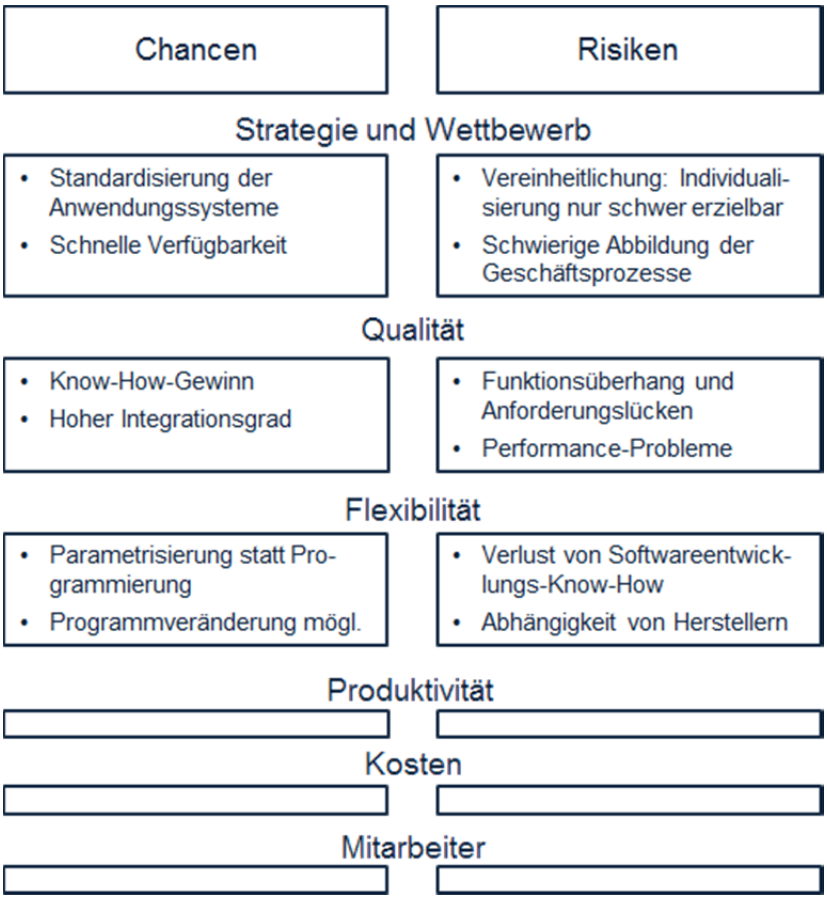


Abb. 16: Argumentebilanz (exemplarisch)

2.2.12 Zusammenfassung I

Die dargestellten **qualitativen Verfahren** haben den **Vorteil**, dass der häufig nur qualitative Nutzen von IT-Leistungen nachvollziehbar beschrieben werden kann.

Ein wichtiger **Nachteil** von qualitativen Verfahren ist, dass sie stark subjektiv geprägt und somit auch leicht manipulierbar sind. Aus diesem Grund sind qualitative Verfahren als Basis für z. B. Investitionsentscheidungen dem Top-Management gegenüber nur schwer zu vermitteln. So hat es sich in der Praxis etabliert, eine **Kombination** aus quantitativen und qualitativen Verfahren bei Entscheidungen oder Bewertungen zu berücksichtigen.

Zeigt der Großteil aller Verfahren in die gleiche Richtung, also z. B. für einen positiven Wertbeitrag eines IT-Systems für die Unternehmenssituation, ist dies die bestmögliche qualitative Rechtfertigung für ein IT-System, die die IT-Abteilung gegenüber der Unternehmensleitung erbringen kann.

2.2.13 Zusammenfassung II

Alle Kosten sind quantifiziert und der qualitative und quantitative Nutzen wurde ermittelt. Diese einzelnen Bestandteile müssen nun gegenübergestellt und **saldiert** werden. Ist der ermittelte Nutzen der IT-Leistung größer als die quantifizierten Kosten dieser, kann die IT-Leistung einen **positiven Wertbeitrag** zur Unternehmenssituation liefern.

Wird hingegen festgestellt, dass die Kosten einer IT-Leistung den Nutzen übertreffen, hat die IT-Leistung eine **negative IT-Performance**. Es sollte über z. B. Outsourcing der IT-Leistung nachgedacht werden.

Ist die Summe aller IT-Leistungen auch positiv, dann hat die IT-Abteilung in der betrachteten Periode eine positive IT-Performance und leistet so einen positiven Beitrag zum Unternehmenserfolg.

2.3 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	IT-Performance befasst sich mit dem Vergleich von Kosten und Nutzen. Ist der Nutzen höher als die Kosten für z. B. die gesamte IT-Abteilung oder ein einzelnes IT-Projekt wird ein negativer Wertbeitrag zur Unternehmenssituation geleistet.		
	Richtig		
	Falsch		
2	Das "Produktivitätsparadoxon der IT" besagt jedoch, dass kein empirischer positiver Zusammenhang zwischen Investitionen in die IT und der Produktivität eines Unternehmens besteht.		
	Richtig		
	Falsch		
3	Im Zusammenhang mit der Diskussion um das Produktivitätsparadoxon der IT, wurde ein kontrovers diskutierter Beitrag namens "IT doesn’t matter" veröffentlicht. Die daraufhin erneut entbrannte Diskussion hat herausgestellt, dass die IT tatsächlich keinen Wertbeitrag zur Unternehmenssituation liefern kann.		
	Richtig		
	Falsch		
4	In der Cronus AG wird die Umsetzung von Business-IT-Alignment in drei Phasen unterteilt. Die drei Phasen sind:		
	Soll- und Ist-Analyse		
	Bestandsaufnahme		
	Messung und IT-Compliance		
	Anpassung		
	Messung der IT-Compliance		
5	Diese Ausrichtung der Unternehmensziele und -strategie an die IT wird Business-IT-Alignment genannt.		
	Richtig		
	Falsch		

6	Mit Hilfe des Strategic Alignment Models (SAM) lässt sich der Zusammenhang zwischen IT und Business theoretisch darstellen. Die einzelnen Pfeile zeigen, wie man das strategische Alignment im Unternehmen umsetzt.		
	Richtig		
	Falsch		
7	Die zweite Phase beinhaltet die Anpassung der IT-Strategie an die Unternehmensstrategie. Damit ist die Anpassung von z. B. Systemen, Aktivitäten und Entscheidungsmustern im IT-Bereich an die Unternehmensziele und -Strategien gemeint.		
	Richtig		
	Falsch		
8	Die erste Phase des Umsetzungsplans von Business-IT-Alignment der Cronus AG ist die Bestandsaufnahme. Im Zuge der Bestandsaufnahme wird eine Situationsanalyse durchgeführt. Die Situationsanalyse soll die vorhandene strategische Rolle der IT im Unternehmen betrachten. Dazu wird das Modell der kritischen Erfolgsfaktoren angewendet.		
	Richtig		
	Falsch		
9	Ein typischer kritischer Erfolgsfaktor (KEF) für die Abteilung „Vertrieb“ ist der gewinnmaximale Umsatz.		
	Richtig		
	Falsch		
10	Die zweite Phase des Umsetzungsplans von Business-IT-Alignment der Cronus AG ist die Anpassung. Im Zuge der Anpassung wird eine Strategie entwickelt. Dazu werden die IT-Ziele mit Kontrollgrößen versehen. Zur Zielplanung wird das Modell der kritischen Erfolgsfaktoren (KEF) angewendet.		
	Richtig		
	Falsch		

11	Kosten von IT-Leistungen lassen sich unterteilen in einmalige und laufende Kosten. Es handelt sich bei Kosten immer um qualitative Werte.		
	Richtig		
	Falsch		
12	Der Nutzen von IT-Leistungen setzt sich in der Regel sowohl aus quantitativen und qualitativen Werten zusammen.		
	Richtig		
	Falsch		
13	Ein typisches Verfahren zur Ermittlung des quantitativen Nutzens ist die Nutzwertanalyse. Dabei werden Kriterien mit Hilfe des Scoring-Ansatzes bewertet und gewichtet.		
	Richtig		
	Falsch		

Tab. 3: Übungsfragen WBT 02 –IT-Performance

3 Business Impact Management

3.1 Grundlagen zum Business-Impact-Management

3.1.1 Einleitung

Bisher wurde die Bewertung von IT-Leistungen auf Basis der Kosten- und Nutzenanalyse durchgeführt (vgl. WBT 02 - IT-Performance). Dies entspricht der klassischen BWL, die die **ressourcenorientierte Sicht** der IT in den Vordergrund stellt. Welchen Einfluss aber z. B. ein einzelnes IT-System auf einen bestimmten Geschäftsprozess hat, kann mit Hilfe der klassischen BWL nicht dargestellt werden.

Die moderne Idee von einer **geschäftsprozessorientierten** Planung, Steuerung und Kontrolle der IT (**Business-Impact-Management of IT**) hat in den letzten Jahren jedoch eine stärkere Bedeutung in den Unternehmen gewonnen. Dabei geht es nicht um eine monetäre Bewertung der einzelnen IT-Ressourcen, sondern um die Relevanz / Bedeutung von IT-Leistungen für einen Geschäftsprozess.

Um die genauen Funktionen und den Nutzen des Business-Impact-Managements (BIM) beschreiben zu können, werden in diesem Kapitel zunächst einige Grundlagen eingeführt.

3.1.2 Problemstellung

Klassisch werden in Unternehmen die IT-Ressourcen über das sogenannte **Systems-Management** technisch überwacht und gesteuert. Die IT-Performance-Messung, die in WBT 02 - IT-Performance vorgestellt wurde, versucht über diese ressourcenorientierte Sichtweise die IT zu messen bzw. zu bewerten.

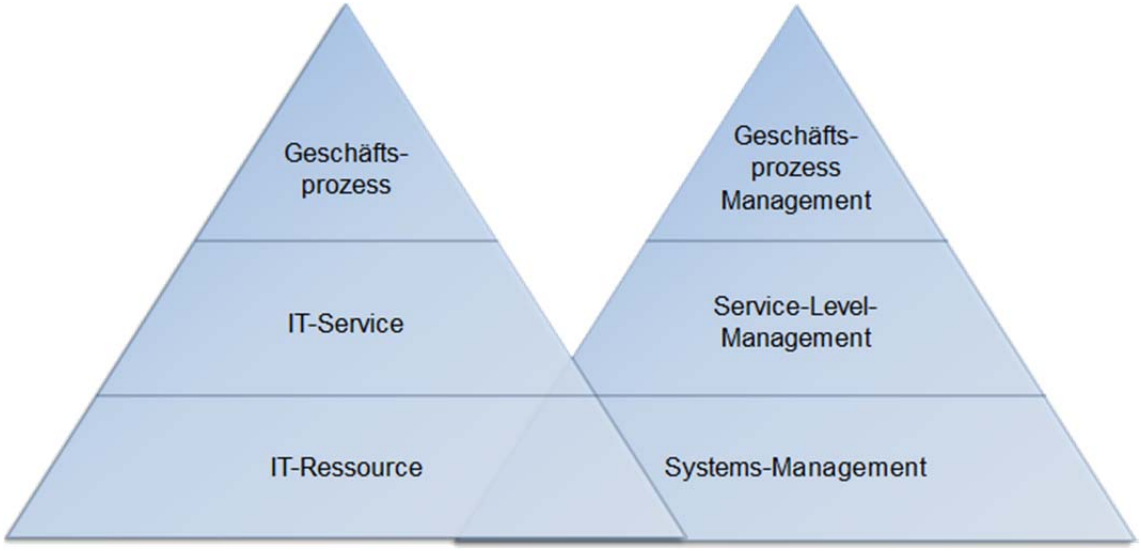


Abb. 17: Management-Instrumente des Business-Impact-Management

Dabei wird jedoch kein Bezug zu den Geschäftsprozessen des Unternehmens hergestellt. Die Geschäftsprozesse eines Unternehmens sind die Determinanten, die den Erfolg eines Unternehmens bestimmen. Um die IT-Ressourcen mit dem Erfolgsfaktor "Geschäftsprozess" in Verbindung zu bringen, kann das **Business-Impact-Management** angewendet werden. Dazu werden **Service-Verträge** zwischen der IT-Abteilung und den Prozesseignern abgeschlossen. Anhand eines **Beispiels** soll gezeigt werden, wie Business-Impact-Management funktioniert.

Wie relevant ist z. B. das CRM-System für den täglichen Betrieb in der Vertriebsabteilung?

Um diese Frage beantworten zu können, werden verschiedene Mitarbeiter der Vertriebsabteilung (Prozesseigener) befragt, wie wichtig dieses IT-System für den täglichen Betrieb auf einer Skala von 1 bis 100 ist. Weiterhin wird abgefragt, wie es sich auf den täglichen Betrieb auswirkt, wenn das IT-System z. B. eine Stunde, einen Tag oder eine Woche ausfällt?

Auf Basis dieser Umfragen kann die IT-Abteilung einen Vertrag (Service-Level-Agreement) mit der Vertriebsabteilung abschließen. In diesem Vertrag sichert die IT-Abteilung z. B. eine 99,997% Verfügbarkeit des CRM-Systems während der Geschäftszeiten zu.

So wird jede Abteilung oder jeder Prozesseigner bzgl. der verwendeten IT-Ressourcen befragt und es ergeben sich verschiedene Service-Level-Agreements. So ist z. B. die Relevanz des E-Mail-Systems für den reibungslosen Ablauf der Geschäftsprozesse in der Vertriebsabteilung nicht genauso wichtig, wie das CRM-System. Das Managen dieser Service-Level-Agreements nennt sich Service-Level-Management.

Im Business-Impact-Management werden die vorab gesammelten Informationen analysiert und Zusammenhänge zwischen den Prozessen und der zugrunde liegenden IT dargestellt. So kann die Unternehmensleitung jederzeit feststellen, welche IT-Ressourcen für einen Ge-

schäftsprozess von Bedeutung ist und welche Prozesse in Folge von Fehlern in der IT gestört sind.

Dieses Beispiel soll die Bedeutung bzw. Wirkung von IT für die Geschäftsprozesse im Unternehmen aufzeigen. Dabei soll klar werden, dass die Bedeutung von IT nicht anhand von IT-Performance-Maßen, wie z. B. der Geschwindigkeit eines Servers oder der Antwortzeit einer Web Site feststellbar ist.

3.1.3 Steuerung der Ressource "IT" durch das Systems-Management (SM)

Das Systems-Management dient als Basis für das Business-Impact-Management. Um das Business-Impact-Management vollständig definieren zu können, muss zunächst das Systems-Management erläutert werden. Das Ziel des Systems-Management ist es, die vorhandenen IT-Ressourcen (Hard- und Software und sonstige IT-Komponenten) möglichst **vollautomatisch technisch** zu überwachen. Das Systems-Management ist die rein technische Sichtweise auf IT-Ressourcen.

Beim Systems-Management werden die einzelnen IT-Ressourcen technisch gesteuert und überwacht. Das Systems-Management kann z. B. feststellen ob eine Festplatte ausgefallen ist. Welche Auswirkungen bzw. Relevanz ein Ausfall einer Festplatte auf die Geschäftsprozesse eines Unternehmens hat, kann das Systems-Management jedoch nicht feststellen. Diese geschäftsprozessorientierte Sicht der IT-Ressourcen soll mit Hilfe des Business-Impact-Managements (BIM) ermöglicht werden.

Auslastung	OK	09-09-2014 10:36:34	443d 10h 6m 16s	1/3	SNMP OK - 54 %
Batterie Kapazitaet	OK	09-09-2014 10:29:04	427d 21h 8m 31s	1/3	SNMP OK - Batterie Kapazitaet 100 %
Batterie wechseln	OK	09-09-2014 10:31:35	52d 13h 6m 43s	1/3	OK - Batterie funktioniert
Batterielaufzeit	OK	09-09-2014 10:34:06	678d 17h 14m 7s	1/3	SNMP OK - Timeticks: (72000) 0:12:00.00
UPS Temperatur	OK	09-09-2014 10:36:36	427d 21h 8m 31s	1/3	SNMP OK - Interne Temperatur 18 Celsius
BackupExec Agent	OK	09-09-2014 10:29:07	7d 2h 25m 2s	1/3	beremote.exe: Running
Betriebssystem	OK	09-09-2014 10:31:37	7d 2h 23m 8s	1/3	OK - Windows Server (R) 2008 Standard 32 Bit
Cursor	OK	09-09-2014 10:34:04	5d 14h 29m 0s	1/3	JBoss_CURSOR-CRM.exe: Running
Firewall	OK	09-09-2014 10:36:35	7d 2h 26m 30s	1/3	MpsSvc: Started
NSClient Log-File	OK	09-09-2014 10:29:06	5d 14h 29m 52s	1/3	OK: C:/Programme/NSClient++/nsclient.log: 45.3K
Open Manage	OK	09-09-2014 10:35:36	4d 1h 1m 7s	1/3	OK - System: 'PowerEdge 2950', SN: '5H0683J', 4 GB ram (4 dimms), 1 logical drives, 5 physical drives
Oracle	OK	09-09-2014 10:34:07	7d 2h 26m 50s	1/3	ORACLE.EXE: Running
Service-Laufzeit	CRITICAL	09-09-2014 08:46:37	236d 17h 53m 15s	3/3	Return code of 255 is out of bounds
Sophos	OK	09-09-2014 10:29:08	7d 2h 25m 1s	1/3	SavService.exe: Running
SysInfo-CPU Load	OK	09-09-2014 10:31:38	7d 2h 23m 21s	1/3	CPU Load 0% (5 min average)

Abb. 18: Screenshot eines Systems zur technischen Überwachung der IT-Komponenten im Unternehmen

3.1.4 Business-Impact-Management (BIM)

Das Business-Impact-Management ist ein Management-Werkzeug, um die Informationstechnologie eines Unternehmens **geschäftsprozessorientiert** zu planen, steuern und zu überwachen.

Mit Hilfe von Business-Impact-Management soll die technische Analyse der IT-Ressourcen des Systems-Managements mit den Geschäftsprozessen eines Unternehmens in Verbindung gebracht werden. Dazu werden als verbindendes Hilfsmittel **IT-Services** zwischen der IT- und den Fachabteilungen abgeschlossen.

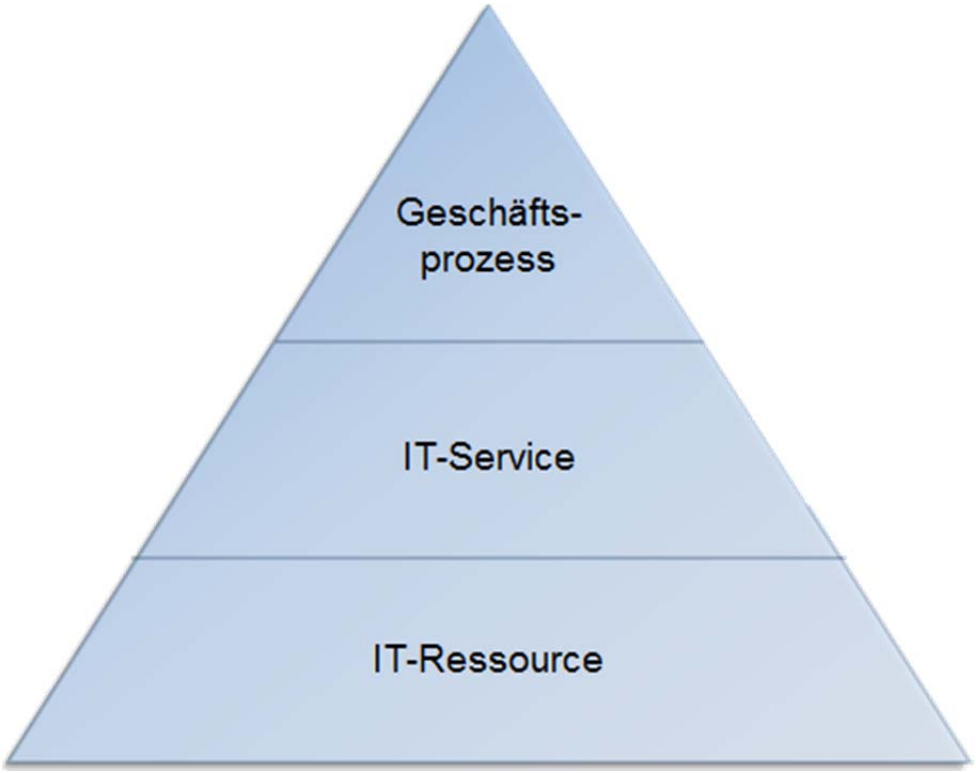


Abb. 19: Zusammenhang von Geschäftsprozessen, IT-Services und IT-Ressourcen in der BIM-Pyramide

3.1.5 Service Level-Management (SLM)

Das Service-Level-Management (SLM) ist das zentrale Hilfsmittel zur **Verbindung zwischen der Technik** (Systems-Management (SM)) **mit den Geschäftsprozessen** im Unternehmen. Um die Verbindung herstellen zu können, müssen Vereinbarungen zwischen dem Prozesseigner mit der IT- Abteilung abgeschlossen werden.

Das Service-Level-Management (SLM) beschäftigt sich mit der Steuerung und Überwachung von Service-Verträgen zwischen der IT-Abteilung und den einzelnen Fachabteilungen über die Leistungsfähigkeit der IT. Diese Service-Verträge werden **Service-Level-Agreements (SLA)** genannt.

Ein SLA wird definiert als die **Vereinbarung** von Indikatoren und deren Abgleich mit festgelegten Richtwerten. Typische Indikatoren sind beispielsweise: Durchsatz, Verfügbarkeitszeiten, Abbruch- und Wiederaufnahmezeiten. Jede dieser Vereinbarungen ist **individuell** auf die Anforderungen der jeweiligen Abteilung zugeschnitten.

Beispiele:

- Ein Beispiel für ein Service-Level-Agreement ist die Nutzung von E-Mails z. B. zur Kommunikation mit Kunden. Die Nutzung von E-Mails ist kein eigener Prozess, sondern ist lediglich eine IT-Komponente, die einen oder mehrere Teilprozesse unterstützt. Trotzdem wird für diese Teilkomponente ein SLA benötigt.

  Bei den Verhandlungen über das Service-Level-Agreement gibt der Abteilungsleiter "Kunden-Service" an, dass die Nutzung eines Telefons zur vollständigen Kommunikation mit den Kunden nicht ausreicht. E-Mails werden z. B. benötigt um Angebote zu verschicken. Aus der Prozessanforderung ergibt sich die Basis für das SLA. Das SLA besteht also u. a. aus einer 100%igen Verfügbarkeit des E-Mail-Dienstes.

- Die Abteilung "Kunden-Service" verspricht ihren Kunden eine Betreuung rund um die Uhr, dazu benötigen Sie ein funktionierendes CRM-System. Die Abteilung Kunden-Service hat somit ein SLA mit der IT-Abteilung abgeschlossen, welches u. a. besagt, dass das CRM-System zu 99,997% der Geschäftszeiten verfügbar sein muss.

  Weiterhin legt das SLA fest, wie auf eine Störung reagiert werden muss und welche Konsequenzen einer Vertragsverletzung folgen. In diesem Beispiel ist der Indikator die Verfügbarkeit und der Richtwert sind 99,997%.

- Die Marketing-Abteilung nutzt das Analysemodul des CRM-Systems zur Analyse des Kaufverhaltens der Kunden. Hier ist die Verfügbarkeit des CRM-Systems nicht so relevant für die Durchführung ihrer Geschäftsprozesse, wie für die Abteilung Kunden-Service.

  So wird das SLA zwischen der Abteilung Marketing und der IT-Abteilung für das gleiche IT-System und den gleichen Indikator (Verfügbarkeit zu den Geschäftszeiten) einen anderen Richtwert (z. B. 90%) haben.

3.1.6 Problemlösung durch BIM

Als oberstes **Unternehmensziel** steht z. B. die Erhöhung der Umsatzrendite. Dieses Ziel wird durch die Umsetzung verschiedener **Geschäftsprozesse,** z. B. der Betreuung der Bestandskunden verfolgt. Die Umsetzung der Geschäftsprozesse wird durch verschiedene Ressourcen, wie z. B. Maschinen, Personal und eben auch durch **IT-Ressourcen** (u. a. E-Mail und CRM-System) unterstützt.

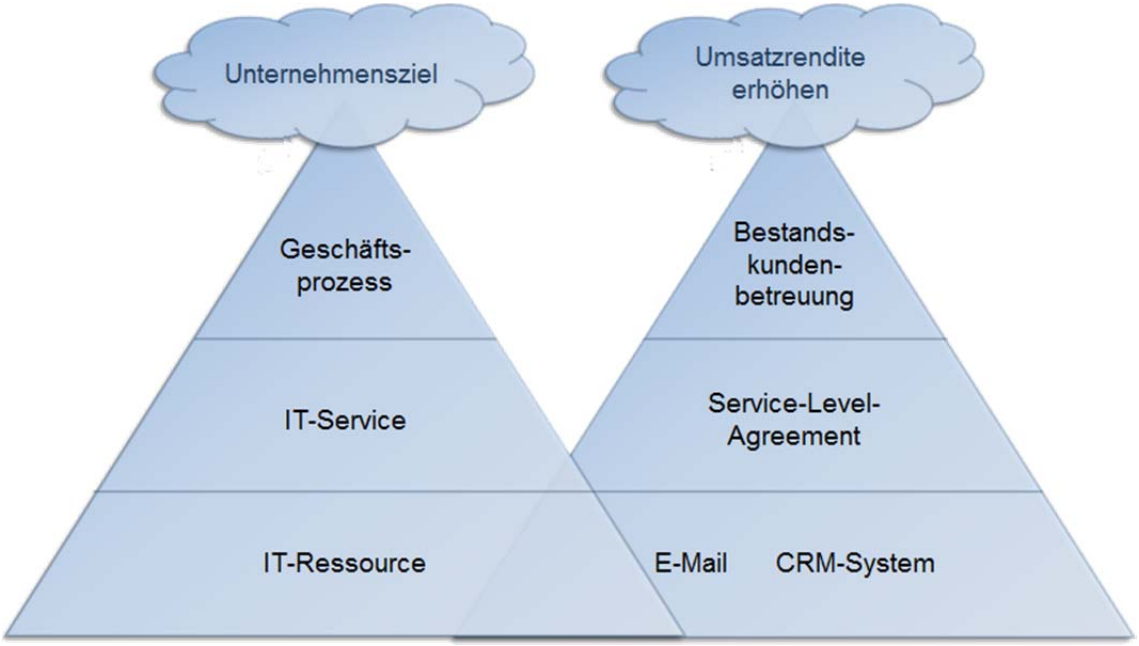


Abb. 20: Beispiel für die Zusammenhänge der Bereiche des BIM

Durch das Business-Impact-Management werden die IT-Ressourcen in eine Beziehung zu den Geschäftsprozessen gebracht. Dazu werden die Anforderungen an alle IT-Ressourcen, die einen Prozess unterstützen, zu je einem IT-Service pro Prozess zusammengefasst. Aus dem IT-Service werden **Service-Level-Agreements** z. B. über die Verfügbarkeit des CRM-Systems zwischen der Fachabteilung und der IT-Abteilung abgeschlossen.

3.2 Business-Impact-Management - Erwartungen, Funktionen, Nutzen

3.2.1 Erwartungen an eine BIM-Lösung

Francesco Palla, der CIO der Cronus AG, erstellt zunächst eine Liste der Erwartungen der Unternehmensleitung an eine BIM-Lösung. Eine solche BIM-Lösung wird nur dann implementiert, wenn es dem Unternehmen auch einen positiven Beitrag zur Unternehmenssituation liefern kann. Die Unternehmensleitung der Cronus AG hat folgende **Erwartungen** an eine BIM-Lösung:

- **Geschäftsprozess**: Eine BIM-Lösung soll die Wirkung der IT-Ressourcen auf einen Geschäftsprozess darstellen.
- **IT-Service**: Eine BIM-Lösung soll alle Service-Level-Agreements, die die IT-Abteilung mit den einzelnen Fachabteilungen abgeschlossen hat, darstellen können.
- **IT-Ressource**: Eine BIM-Lösung soll eine automatische technische Überwachung aller IT-Ressourcen beinhalten.

3.2.2 Funktionen von BIM

Anhand der Erwartungen, welche die Cronus AG an eine BIM-Lösung stellen, können nun **Funktionen** einer BIM-Lösung abgeleitet werden, die die Erwartungen erfüllen sollen.

Weist eine BIM-Lösung diese Funktionen auf, entspricht sie den Erwartungen der Cronus AG und wird voraussichtlich implementiert werden.

- **Geschäftsprozess**: Eine BIM-Lösung soll die Funktion haben, die Unternehmensleistung automatisch bei der Geschäftsprozessmodellierung zu unter-stützen.
- **IT-Service**: Eine BIM-Lösung soll die Funktion bieten, die Geschäftsprozesse automatisch mit den SLA zu verbinden. Weiterhin müssen die SLA und die dafür veranschlagten Preise (Preis den die Fachabteilung an die IT-Abteilung für Erbringung des IT-Services zahlt) administriert werden.
- **IT-Ressource**: Eine BIM-Lösung soll eine automatische technische Überwachung aller IT-Ressourcen beinhalten, sowie versuchen, Störungen automatisch zu verhindern. Ist dies nicht möglich muss das System automatisch den Prozesseigner sowie die IT-Abteilung informieren, um die Auswirkungen der Störung auf den Geschäftsprozess möglichst gering zu halten.

3.2.3 Nutzen von BIM

Bevor ein Unternehmen in ein neues System investiert wird zunächst geprüft, ob die Implementierung von einem BIM-System eine positive IT-Performance hat. Wie sie bereits in "WBT 02 - IT-Performance" gelernt haben, bedeutet eine **positive IT-Performance**, dass der Nutzen größer als die Kosten einer IT-Leistung sein muss.

Es stellt sich also für die Cronus AG die Frage, welchen **Nutzen** Business-Impact-Management liefern kann.

Der wichtigste Nutzen von BIM liegt darin, die IT mit der Erfolgsdeterminante "Geschäftsprozess" in Verbindung zu bringen, ohne dass eine quantitative Bewertung von IT-Ressourcen notwendig ist. Sie haben bereits in "WBT 02 - IT-Performance" Verfahren zur Bewertung qualitativer Werte kennengelernt, deren Ziel war es jedoch primär, qualitative Werte z. B. durch Scoring quantitativ darstellbar zu machen. Dieses Ziel verfolgt das BIM nicht.

Diese qualitative Nutzenbewertung durch das BIM kann mit quantitativen Bewertungen des Nutzens (z. B. Kosteneinsparungen) kombiniert werden.

Diese Kombination ermöglicht eine bestmögliche Bewertung der Wirkung von IT auf die Geschäftsprozesse und somit auf den Unternehmenserfolg.

3.2.4 Entscheidung der Cronus AG

Die dargestellten Funktionen und Nutzen einer BIM-Lösung entsprechenden Erwartungen der Unternehmensleitung der Cronus AG.

Wir haben somit entschieden, eine BIM-Lösung in der Cronus AG zu implementieren. Mit der Umsetzung dieses Projektes wurde ich als CIO beauftragt. Wie die Implementierung von BIM in der Cronus AG geplant und umgesetzt wird, soll im nächsten Kapitel exemplarisch dargestellt werden.

3.3 Implementierung von BIM in der Cronus AG

3.3.1 Einleitung

Hallo, ich Francesco Palla bin als CIO der Cronus AG verantwortlich für die Planung, Steuerung und Überwachung der IT-Ressourcen und somit auch für das Business-Impact-Management der Cronus AG.

Die Unternehmensleitung der Cronus AG hat sich dazu entschieden, eine BIM-Lösung in der Cronus AG zu implementieren. Wie dabei **vorgegangen** wird, soll im Folgenden gezeigt werden.

Das BIM stellt die IT-bezogene Sicht auf die Geschäftsprozesse in den Vordergrund und nicht die isolierte Betrachtung von IT-Systemen.

Francesco Palla hat sich für ein praxisnahes Vorgehen zur Implementierung entscheiden. Damit ist gemeint, dass zunächst die Geschäftsprozesse identifiziert werden und zeitgleich die IT-Ressourcen über das Systems-Management überwacht und gesteuert werden. Erst im Anschluss wird versucht die beiden Bereiche durch Service-Level-Agreements miteinander zu verbinden.

3.3.2 Implementierungsschritte

Die Einführung von BIM in der Cronus AG geschieht entlang der dargestellten Pyramide. Das Vorgehen kann dabei in **drei Schritte** unterteilt werden, wobei die Schritte zeitlich nicht trennscharf abgrenzbar sind.

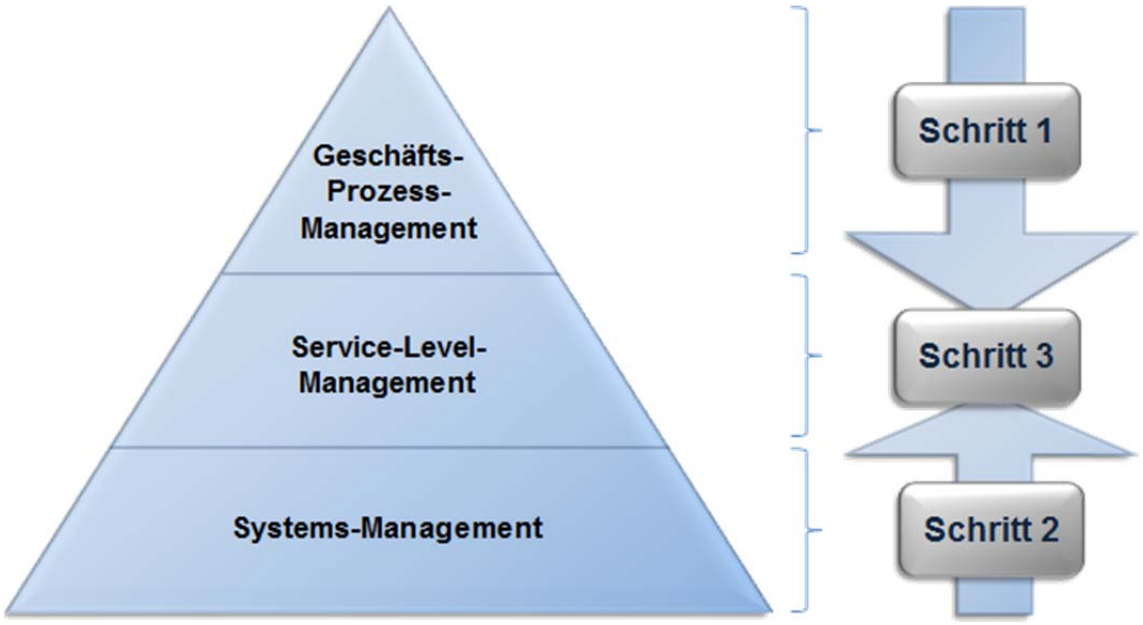


Abb. 21: Vorgehensplan bei der Implementierung einer BIM-Lösung im Unternehmen

- **Geschäftsprozess-Management**: Das Geschäftsprozess-Management ist der erste Schritt der Implementierung von Business-Impact-Management in der Cronus AG. Dabei werden alle Geschäftsprozesse der Cronus AG durch die Unternehmensleitung identifiziert und modelliert.
- **Service-Level-Management**: Das Service-Level-Management als dritter Schritt der Implementierung von BIM in der Cronus AG verbindet das Systems-Management mit dem Geschäftsprozess-Management. Dafür werden Verträge über die Leistungsziele der IT, gemeinsam von der Unternehmensleitung, den Fachabteilungen und der IT-Abteilung festgelegt
- **Systems-Management**: Das Systems-Management ist der zweite Schritt zur Implementierung von BIM in der Cronus AG. Das Systems-Management meint dabei die Überwachung der IT-Ressourcen und wird durch die IT-Abteilung umgesetzt. Der zweite Schritt läuft zeitlich parallel zu dem Management der Geschäftsprozesse (Schritt 1).

3.3.3 Schritt 1: Geschäftsprozess-Management

Im ersten Schritt der Implementierung von BIM in der Cronus AG liegt der Fokus auf den **Geschäftsprozessen** der Cronus AG. So wird das Ziel verfolgt, nach der Implementierung den Zustand eines Geschäftsprozesses anhand der zugeordneten Service-Levels beurteilen zu können. Anhand von einem Geschäftsprozess der Cronus AG soll exemplarisch gezeigt werden, wie dieser erste Schritt umgesetzt werden kann. Zunächst werden die Geschäftsprozesse der Cronus AG identifiziert, im Anschluss die zugehörigen IT-Systeme.

- **Geschäftsprozesse identifizieren**: Die Geschäftsprozesse der Cronus AG müssen identifiziert und modelliert werden.

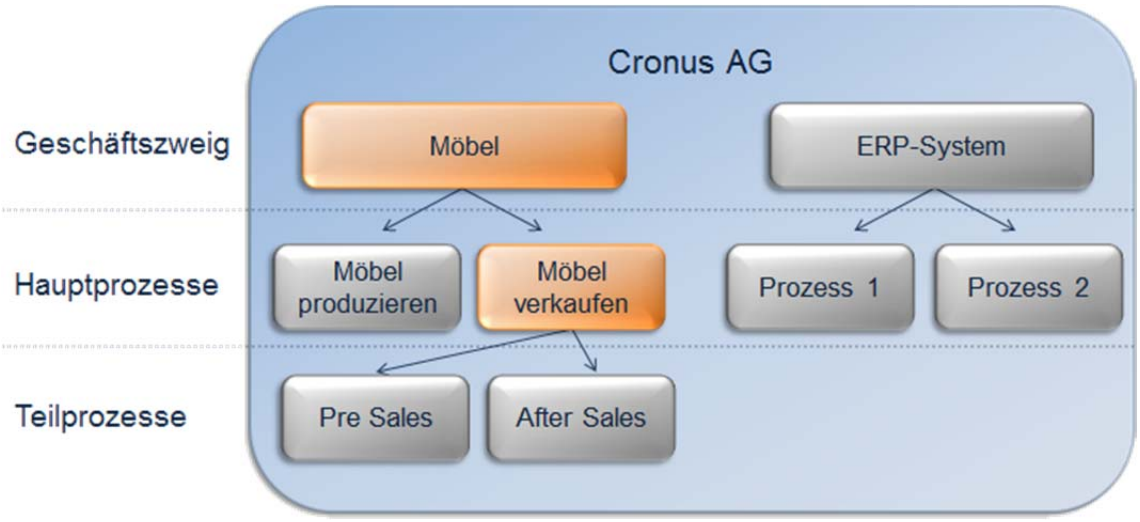


Abb. 22: Modellierung der Geschäftsprozesse der Cronus AG, exemplarische Darstellung eines Teilprozesses

Die Cronus AG lässt sich in zwei Hauptgeschäftszweige unterteilen. Der Geschäftszweig Möbel besteht aus zwei Hauptprozessen. Der Hauptprozess "Möbel verkaufen" lässt sich wiederrum in zwei Teilprozesse aufteilen. Für alle Teilprozesse müssen die IT-Systeme identifiziert werden, die den Teilprozess unterstützen.

- **Identifikation der IT-Systeme**: Für alle Teilprozesse müssen die IT-Systeme identifiziert werden, die den Teilprozess unterstützen.

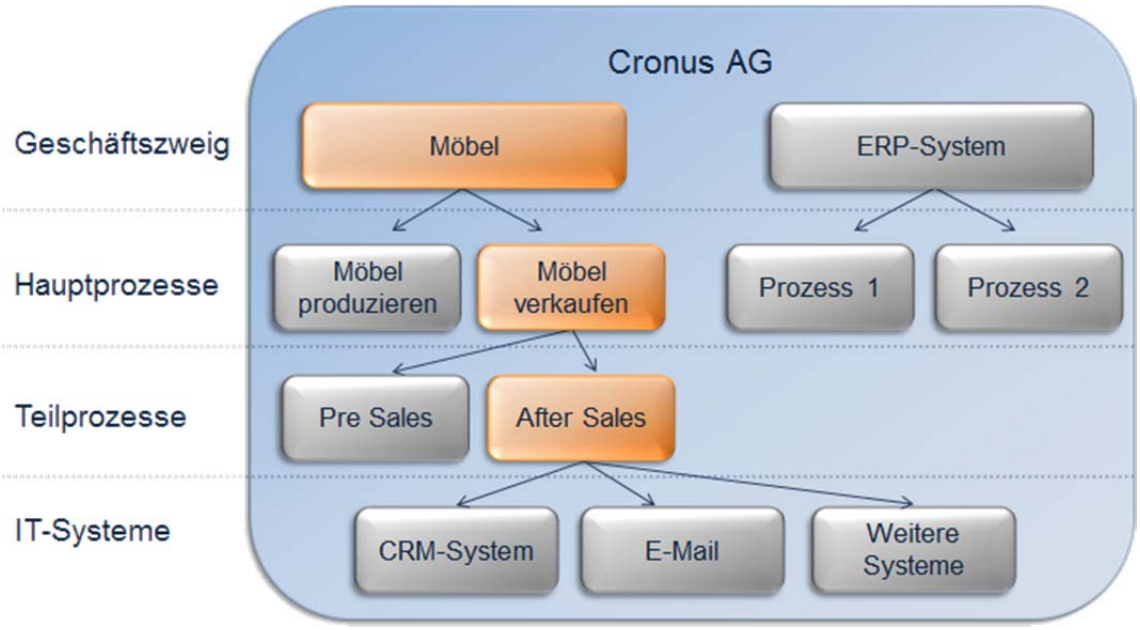


Abb. 23: Zuordnung der IT-systeme zu dem Teilprozess „After Sales“

Der Teilprozess After Sales wird unter anderem durch die IT-Systeme "CRM-System" und "E-Mail" unterstützt. Anhand dieser Modellierung der Geschäftsprozesse wird eine Verbindung zwischen den marktorientierten Zielen eines Geschäftsprozesses (z. B. Auftragsabwicklungszeit, 24/7 Verfügbarkeit der Abteilung Kunden-Service) und den zugrunde liegenden IT-Systemen hergestellt.

3.3.4 Schritt 2: Systems-Management

Im Zuge des zweiten Schrittes werden die IT-Systeme auf Basis des Systems-Managements geplant und überwacht.

Dazu wird in der BIM-Lösung die Funktion zur Planung, Steuerung und Überwachung auf die Anforderungen der einzelnen IT-Systeme eingestellt.

Damit z. B. das CRM-System den Teilprozess "After Sales" unterstützen kann, muss das System zu den Geschäftszeiten verfügbar sein. Um dies umzusetzen zu können, muss die Systems-Management-Funktion im BIM alle, dem CRM-System zugrundeliegenden IT-Komponenten (z. B. Server, Festplatten, Software), überwachen. Tritt bei einer der IT-Komponenten eine Störung auf, muss festgelegt werden, wie diese automatisch behoben werden soll, bzw. wer informiert wird, wenn es einer manuellen Lösung der Störung bedarf.

Diese Einstellungen müssen für alle IT-Komponenten und IT-Services vorgenommen werden, die die Geschäftsprozesse der Cronus AG unterstützen.

3.3.5 Schritt 3: Service-Level-Management

Es wurden bereits die IT-Services identifiziert und den Geschäftsprozessen zugeordnet. Weiterhin wurde das Systems-Management der BIM-Lösung auf die Planung, Überwachung und Steuerung der IT-Komponenten eingestellt.

Nun im letzten Schritt werden die **IT-Services** definiert und Service-Level-Agreements über sie abgeschlossen. Dieser letzte Schritt verbindet somit die Geschäftsprozesse mit den zugrundeliegenden IT-Komponenten und bildet somit den wichtigsten Schritt des Business-Impact-Managements.

- **Definition von IT-Services**: Alle IT-Services, die einem Geschäftsprozess zugeordnet werden können, werden zu einem IT-Service zusammengefasst.

  Am Beispiel des Geschäftsprozesses "After Sales" werden alle Anforderungen, die die Mitarbeiter an die IT-Systeme stellen, zu dem IT-Service "After Sales" zusammengefasst.

- **Abschluss von SLA**: Über den definierten IT-Service schließt die IT-Abteilung ein Service-Level-Agreement (SLA) mit der Fachabteilung ab, in welchem die Ziele und Anforderungen an den IT-Service verankert sind.

  Über den IT-Service "After Sales" wird ein SLA abgeschlossen. In dem ist z. B. festgelegt, dass das CRM-System eine Verfügbarkeit von 99,997% während der Geschäftszeiten haben muss.

- **Funktionsgrad eines IT-Services**: Der Funktionsgrad eines IT-Service soll in eine quantitative Beziehung mit dem Geschäftsprozess gesetzt werden. Dazu wird als Kennzahl der Erreichungsgrad der Service-Level-Ziele angewendet. Werden alle Service-Level-Ziele eines IT-Services eingehalten, so ist der IT-Service zu 100% Funktionstüchtig.

  Der Funktionsgrad wird genutzt, um den Verantwortlichen jederzeit anzeigen zu können, in welchen Zustand sich ein Prozess derzeit befindet.

3.3.6 Zusammenfassung

Das Business-Impact-Management bietet eine Möglichkeit, die IT-Komponenten auf die Geschäftsprozesse abzubilden, dies ist einer der wichtigsten Vorteile, den das BIM einem Unternehmen liefern kann. Denn so kann der **Wertbeitrag der IT-Komponenten** auf die Unternehmenssituation dargestellt werden.

Neben diesem Vorteil ist das Bim auch ein gutes **Management-Instrument** zur Planung, Überwachung und Steuerung der IT, z. B. durch die automatisierte Steuerung und proaktive Verhinderung von Störungen.

3.4 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	Aus welchen Bestandteilen besteht die Business-Impact-Management-Pyramide?		
	Systems-Management		
	Geschäftsprozess-Management		
	IT-Performance-Management		
	Service-Level-Management		
2	Das Business-Impact-Management verbindet die IT-Ressourcen mit den Geschäftsprozessen eines Unternehmens. So kann mit Hilfe des BIM eine Aussage über den Wertbeitrag der IT zum Unternehmenserfolg getätigt werden.		
	Richtig		
	Falsch		
3	Das Systems-Management hat zum Ziel, die vorhandenen IT-Ressourcen technisch zu überwachen.		
	Richtig		
	Falsch		
4	Ein Service-Level-Agreement beschreibt einen Vertrag zwischen der IT-Abteilung und der jeweiligen Fachabteilung. Ein Beispiel für ein SLA ist ein Vertrag über die Verfügbarkeit von dem CRM-System. Über eine kleine IT-Komponente wie z. B. Drucker werden kein SLA abgeschlossen.		
	Richtig		
	Falsch		
5	Ziel vom Business-Impact-Management ist es, IT-Services mit den Geschäftsprozessen in Verbindung zu bringen.		
	Richtig		
	Falsch		
6	Auf Grund der zahlreichen Vorteile, die eine BIM-Lösung hat, lohnt es sich auch für kleine Unternehmen eine BIM zu implementieren.		
	Richtig		
	Falsch		

7	Das Geschäftsprozess-Management ist der erste Schritt der Implementierung von Business-Impact-Management in der Cronus AG. Dabei werden alle Geschäftsprozesse der Cronus AG durch die Unternehmensleitung identifiziert und modelliert.		
	Richtig		
	Falsch		
8	Das Systems-Management ist der dritte Schritt zur Implementierung von BIM in der Cronus AG. Das Systems-Management meint dabei die Überwachung der Service-Level-Agreements.		
	Richtig		
	Falsch		
9	SLA ist die Abkürzung für …		
	Systems-Level-Management		
	Service-Level-Management		
	Software-Level-Management		

Tab. 4: Übungsfragen WBT 03 –Business-Impact-Management

4 IT-Compliance

4.1 Zur Notwendigkeit der IT-Compliance

4.1.1 Bedeutung und Notwendigkeit der IT-Compliance

Anfang des 21. Jahrhunderts gab es einige **spektakuläre Unternehmenspleiten**, mit denen sich der Bedeutungsgewinn von Governance- und Compliance-Fragestellungen verdeutlichen lässt.

4.1.2 Der ENRON-Bankrott 2011

ENRON gehörte zu einem der größten Energiekonzerne der USA. Das Gasunter- nehmen erlitt Ende der 90er Jahre starke Verluste durch die Expansion in den Telekommunikationsbereich und dem Absinken der Energiepreise. Diese Verluste wurden verschleiert durch die Verflechtung der Unternehmensbeteiligungen, Nichtausweis von Verbindlichkeiten und die Vortäuschung von Gewinnen.

Eine solche Bilanzverschleierung war nur möglich, da interne Kontrollsysteme unzureichend und die Handlungsspielräume der Manager sehr groß waren. Unterstützt wurden die Manager dabei von der Prüfungsgesellschaft **Arthur Andersen**. Nach Anmeldung der Insolvenz im Dezember 2001 wurde bekannt, dass rund 500 ENRON-Manager kurz vor der Pleite ihres Konzerns hohe Bonuszahlungen erhalten haben. So ließ sich der Gründer und CEO Kenneth Lay eine Abfindung in Höhe von 300 Millionen US-Dollar auszahlen.

Arthur Anderson war eine der Big-Five-Prüfungsgesellschaften und bot Leistungen im Bereich Wirtschaftsprüfung, Steuer- und Unternehmensberatung an. Im ENRON-Skandal haben Mitarbeiter Unterlagen des ENRON-Konzerns vernichtet, obwohl die Aufnahme des Verfahrens gegen ENRON bereits bekannt war. Arthur Anderson wurde durch die Verstrickung in diesen Skandal 2002 zerschlagen.

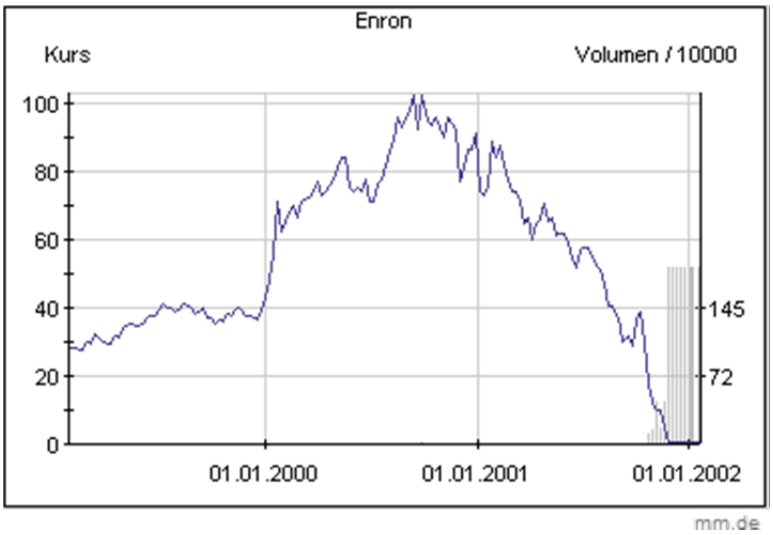


Abb. 24: Drei-Jahres-Chart der Aktie von ENRON

4.1.3 WORLDCOM-Betrug 2002

Die Telefongesellschaft WORLDCOM hatte 2001 20.000 Mitarbeiter und einen Jahresumsatz in Höhe von 21,3 Milliarden US-Dollar. Sie zählte zu den drei größten Telefongesellschaften der Welt. Das Unternehmen erlitt hohe Verluste aus Fehlinvestitionen, der allgemeinen Konjunkturkrise, dem starken Konkurrenzdruck und durch hohe Zinsbelastungen. Diese Verluste wurden verschleiert und ein Bilanzbetrug durch Falschausweis von 3,85 Milliarden $ und Fehlbuchungen von 11 Milliarden $ festgestellt.

Eine solche Bilanzverschleierung war nur möglich, da interne Kontrollsysteme unzureichend und die Handlungsspielräume der Manager sehr groß waren. WorldCom meldete 2002 Insolvenz an. Der Gründer und damaliger CEO wurde zu 25 Jahren, der Chef der Finanzen und Buchhaltung zu 5 Jahren Gefängnis verurteilt. Der Aktienkurs ist von 60 $ auf 35 Cent gefallen.

Abb. 25: Sieben-Monats-Chart der Aktie von WorldCom

4.1.4 FLOWTEX-Betrug 2000

Der FlowTex-Betrug beschreibt den schwersten Fall an Wirtschaftskriminalität in der deutschen Geschichte. Zwischen 1994 und 1999 verkaufte FlowTex Horizontalbohrmaschinen für Strom-, Gas- und Telekommunikationsleitungen und leaste sie im Anschluss zurück. FlowTex verkaufte 3.142 Bohrmaschinen zu einem Stückpreis von rund 1,5 Mio. DM, dem gegenüber stehen jedoch nur 270 reale Bohrmaschinen. So bestanden weit über 90% der Bohrmaschinen nur auf dem Papier. Der auf betrügerische Weise erlangte Gewinn belief sich auf 1,6 Mrd. DM.

In diesem Zeitraum sind reale Geschäftsausgaben in Höhe von ca. 1 Mrd. DM entstanden. Die verbliebenen 616 Mio. DM flossen zum Großteil an die damaligen Geschäftsführer von FlowTex. Der Haupttäter Manfred Schmider wurde zu 12 Jahren Haft verurteilt.

4.1.5 Entwicklungen aus den Ereignissen

Die Bilanzfälschungen, die von Managern bei FlowTex, WORLDCOM und ENRON durchgeführt wurden, haben Anfang des 21. Jhd. zu einem großen Aufruhr auf den Märkten geführt. Die Skandale waren nur möglich, da den Managern ein sehr großer Handlungsspielraum in Verbindung mit fehlenden **internen Kontrollen** ermöglicht wurde.

Die Unternehmenspleiten waren Auslöser für die Diskussion um die Notwendigkeit einer Corporate Governance in den Unternehmen. Als Reaktion auf diese Diskussion wurden von Gesetzgebern und Aufsichtsbehörden Vorgaben entwickelt, die die Unternehmen zu einem transparenten Verhalten zwingen. Dies soll dazu führen, dass die Anleger wieder in die Märkte vertrauen können. Die Erfüllung von verschiedenen Anforderungen wird als **Compliance** bezeichnet. Die Cronus AG musste sich zu Beginn des 21. Jahrhunderts zunächst mit dem Begriff im Allgemeinen auseinandersetzen.

4.2 Einordnung der IT-Compliance

4.2.1 Einleitung

Als Reaktion auf die zahlreichen Skandale hatte der Vorstand der Cronus AG entschieden, dass auch wir eine Corporate Governance benötigen. Dies hatte zur Folge, dass ich, Francesco Palla, als Chief Information Officer der Cronus AG diesen langen Prozess der Umstellung leiten durfte.

Da es zu diesem Zeitpunkt kein ERP-System gab, welches möbelproduzierende Unternehmen bei der Umsetzung von Corporate Governance ausreichend unterstützt, hat unsere IT-Abteilung ein eigenes ERP-System entwickelt. Heute sind wir Hersteller und Vertreiber des

ERP-Systems **"Cronus myERP"**, welches speziell auf die Ansprüche der möbelproduzierenden Branche zugeschnitten ist. "Cronus myERP" wird intern bei uns und unseren Lieferanten genutzt. Zusätzlich vertreiben wir das ERP-System an andere Unternehmen in der Möbelbranche. So konnten wir die **IT-Abteilung als eigenständige Business Unit** in der Cronus AG etablieren.

4.2.2 Business Unit

Eine Business Unit (BU) lässt sich als eigenständiges Unternehmen innerhalb eines Unternehmens beschreiben. Bei der Cronus AG sind die Bereiche "Möbel" und "IT" je eine eigenständige Business Unit.

Die Unit "IT" arbeitet der Unit "Möbel" als interner Dienstleister zu. Zusätzlich dazu betreut die Unit "IT" externe Kunden im Zuge der Implementierung und anschließenden Kundenberatung des ERP-Systems "Cronus myERP" Für die Unit "IT" ist diese externe Dienstleistung das umsatzrelevante Geschäft.

Im Zuge der Entwicklung von "Cronus myERP" musste zunächst geklärt werden, in welchen Bereichen das ERP-System bei der Umsetzung von Corporate Governance, besonders von IT-Compliance, die Cronus AG unterstützen kann. Was IT-Compliance bedeutet, wie es definiert und eingeordnet werden kann, wird im Laufe dieses WBT erklärt.

4.2.3 Konzeptioneller Rahmen der IT-Compliance

Der auf der Abbildung 7 dargestellte konzeptionelle Rahmen hilft uns bei der Erklärung und Positionierung von IT-Compliance in der Cronus AG. Im Laufe dieses WBT wird dieser konzeptionelle Rahmen erläutert.

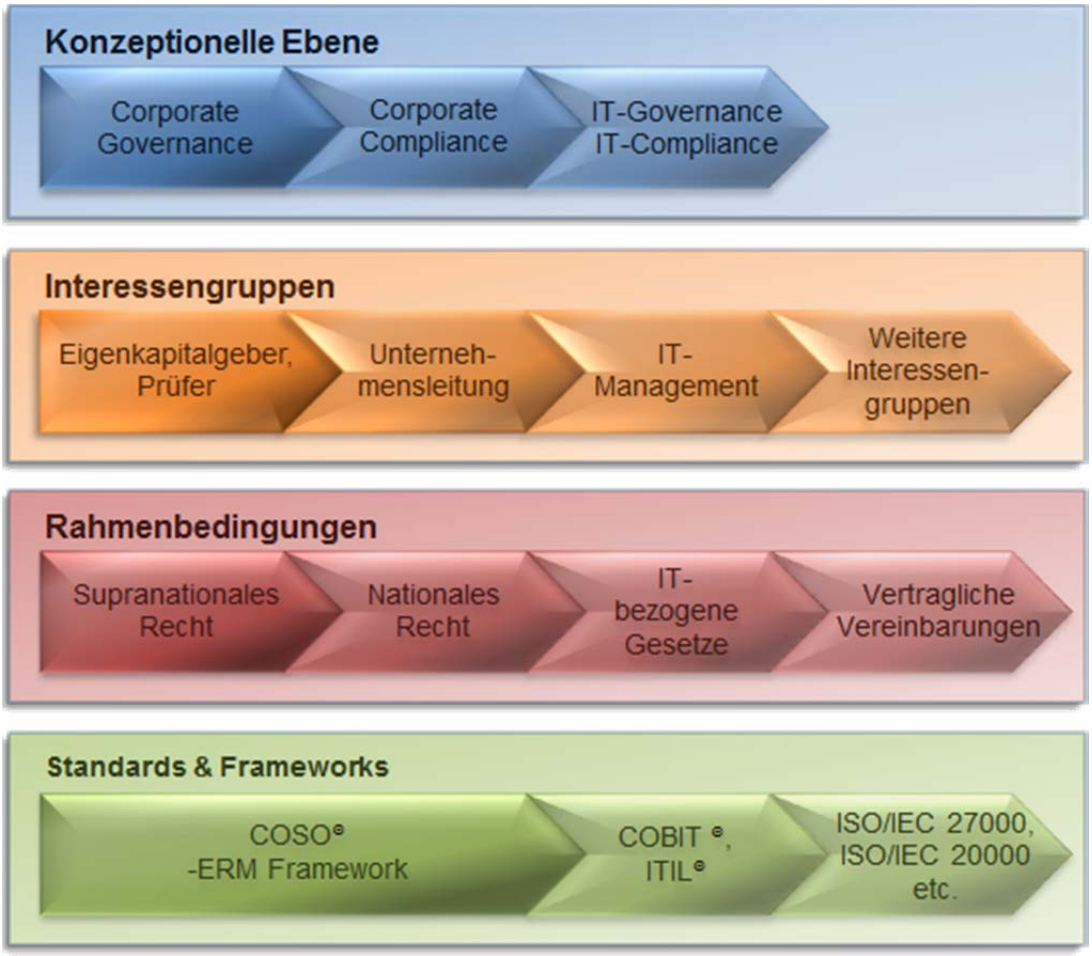


Abb. 26: Konzeptioneller Rahmen der IT-Compliance

4.2.4 Einordnung auf konzeptioneller Ebene

Unter Corporate Governance versteht man die Gesamtheit aller Regeln zur Steuerung und Überwachung des Unternehmens. Nur ein Teil der Corporate Governance ist die Compliance. Compliance meint dabei den Teil, der sich mit der Einhaltung von Regeln befasst. Diese Regeln können das Unternehmen sowohl von intern als auch von extern betreffen.

Abb. 27: Einordnung der IT-Compliance auf konzeptioneller Ebene

- **Corporate Governance**: Hätte es bei Flowtex einen Corporate-Governance-Kodex gegeben, wären die Unternehmenspleiten eventuell vermeidbar gewesen. Ein Corporate-Governance-Kodex kann Fehlverhalten und regelkonformes Verhalten im Unternehmen vermeiden. In diesem Kodex werden Empfehlungen gegeben, wie eine gute Unternehmensführung möglich ist.

- **Corporate Compliance**: Das folgende Beispiel soll den Unterschied zwischen Compliance und Governance verdeutlichen: Besonders in der Textilindustrie ist die Fertigung von Kleidung für Europa durch Kinderarbeit in Asien gängig. Wenn das bekannt wird, haben die europäischen Unternehmen häufig Image-Probleme. Diese fallen in den Bereich Governance. Trotzdem sind die Unternehmen **compliant**, da Kinderarbeit in den asiatischen Ländern nicht verboten ist.
- Während Compliance also die Einhaltung von internen und externen Regeln eines Unternehmens meint, so umfasst Governance allgemein eher, inwieweit Regeln zur Steuerung und Überwachung im Unternehmen beitragen.
- **IT-Governance/IT-Compliance:** So wie Corporate Compliance ein Teil der Corporate Governance ist, so ist auf Ebene der IT die IT-Compliance ein Teilbereich der IT-Governance.

Auf konzeptioneller Ebene ist der Begriff Compliance der Governance nachgeordnet. Corporate Governance betrachtet dabei das ganze Unternehmen, Corporate Compliance zielt hingegen auf die Regeleinhaltung im gesamten Unternehmen ab. Compliance meint die Einhaltung externer Gesetzte und Normen (gesetzliche Compliance), vertraglicher Pflichten (kommerzielle Compliance) und die Einhaltung von eigenen Qualitäts- bzw. Wertmaßstäben des Unternehmens.

4.2.5 Rückblick. Bereiche der IT-Governance

IT-Governance beschreibt den Prozess der verantwortungsvollen Steuerung, Regelung und Kontrolle von IT, sodass die IT die Geschäftsprozesse eines Unternehmens optimal unterstützt. Die in der Literatur zu findenden Definitionen der IT-Governance stellen entweder Performance-Aspekte als innengerichtete Sichtweise der IT-Governance oder Compliance-Aspekte als außengerichtete Sichtweise der IT-Governance in den Vordergrund.

- **IT-Performance**: Bei der IT-Performance als innengerichtete Sichtweise der IT-Governance steht der Wertbeitrag der IT im Vordergrund. Damit sind alle allgemeinen Regelungen, methodische Verfahren und konkrete Maßnahmen des IT-Managements gemeint.
- **IT-Compliance**: Bei der IT-Compliance, als außengerichtete Sichtweise der IT-Governance, steht das regelkonforme Verhalten in der IT im Vordergrund. Damit ist die Einhaltung aller gesetzlichen, vertraglichen und internen Vorgaben gemeint.

4.2.6 Definition der IT-Compliance

Compliance meint die Konformität mit z. B. **internen Vorgaben**, Gesetzen und **vertraglichen Verpflichtungen**.

In der Cronus AG ist eine **interne Richtlinie** das Vier-Augen-Prinzip. Jeder Mitarbeiter hat wichtige Entscheidungen und Vorgänge durch einen weiteren Mitarbeiter kontrollieren zu lassen.

Eine **vertragliche Verpflichtung** kann z. B. ein Service-Level-Agreement sein. Der Begriff bezeichnet die vertragliche Vereinbarung zwischen einem Auftraggeber und einem Dienstleister für wiederkehrende Dienstleistungen. Vertraglich werden bestimmte Leistungseigenschaften zugesichert wie beispielsweise Leistungsumfang oder das sogenannte Service-Level, welches die vereinbarte Leistungsqualität beschreibt.

Die Aufmerksamkeit für das Thema Compliance hat besonders zu Beginn des 21. Jahrhunderts stark zugenommen. Die hat insbesondere mit den verschiedenen gesetzlichen Vorgaben hinsichtlich des internen Risikomanagements zu tun. Diese Vorgaben wurden im Zuge diverser Bilanzskandale, von den Gesetzgebern erarbeitet. IT-Compliance bezeichnet dabei die Einhaltung und Überwachung der Compliance-Anforderungen **an die IT selbst (IT als Gegenstand)** sowie die Umsetzung der Compliance-Anforderungen mit **IT-Unterstützung (IT als Instrument)**.

- **IT als Gegenstand** der IT-Compliance im Sinne eines Zielobjekts:

  In der IT werden Daten und Informationen verarbeitet. In der Betrachtung von IT als Gegenstand werden konkrete Anforderungen an die Daten- und Informationsverarbeitung direkt gestellt, welche die IT erfüllen muss. Damit sind Ansprüche an die Erhebung, Verarbeitung und Nutzung von diesen Daten und Informationen gemeint. So regelt z. B. das Bundesdatenschutzgesetz die IT-gestützte Verarbeitung personenbezogener Daten.

- **IT als Instrument** der IT-Compliance:

  IT als Instrument wird im Bereich IT-Compliance eingesetzt, um die Einhaltung bestehender Gesetze sicherzustellen. So können Regelverstöße durch IT-Systeme verhindert werden. In der Cronus AG wird beispielsweise das ERP-System "Cronus myERP" genutzt. Innerhalb dieses Systems ist es nicht möglich, nachträglich Rechnungen zu löschen oder zu ändern. So wird durch das ERP-System die IT als Instrument verwendet, um ein regelkonformes Verhalten sicherzustellen. Die IT wird hier als Mittel zur Erfüllung von Compliance-Anforderungen genutzt.

4.2.7 Komponenten der IT-Compliance

Der Begriff IT-Compliance lässt sich durch eine einzelne Definition nicht vollständig abgrenzen. In Theorie und Praxis haben sich folgende drei Komponenten der IT-Compliance durchgesetzt. Mit deren Hilfe kann gezeigt werden, welche Bereiche der Begriff IT-Compliance abdeckt.

Abb. 28: Komponenten der IT-Compliance

- **Vorsorge gegen Regelverstöße**: Vorsorge meint die Verpflichtung der Unternehmen entsprechende Maßnahmen für die Vermeidung von Verstößen gegen gesetzliche Regelungen zu treffen.
- **Einrichtung eines Risikomanagement**: Für das frühzeitige Erkennen und Entgegenwirken von Risiken, müssen Unternehmen ein Risikofrühwarnsystem verpflichtend einrichten.
- **Strafmaß bei strafbarem Verhalten**: Das Management muss persönlich haften, wenn es gegen Compliance-Vorgaben im Unternehmen verstößt.

4.2.8 Vorsorge gegen Gesetzesverstöße im IT-Bereich

Um eine entsprechende **Vorsorge gegen Regelverstöße** sicherstellen zu können, bedarf es zunächst einer Analyse, welche der bestehenden Gesetze für die Cronus AG relevant sind. Weiterhin muss eine unternehmensinterne Analyse erfolgen, welche vertraglichen Vereinbarungen und internen Regeln beachtet werden müssen. Die Unternehmensleitung muss dann

organisatorische und technische Maßnahmen treffen, um Verstöße gegen geltende Gesetze zu vermeiden.

Die relevanten Gesetze lassen sich in zwei Typen unterscheiden. Gesetze...

- …die, die IT direkt **als Gegenstand** betrachten.
    - Bundesdatenschutzgesetz (BDSG):
    - Hier wird die IT-gestützte Verarbeitung personenbezogener Daten geregelt. Das BDSG umfasst die Erhebung, Verarbeitung und Nutzung dieser Daten
    - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen **(GDPdU):**
    - Die Grundsätze befassen sich mit der korrekten Aufbewahrung digitaler Unterlagen.
    - Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme **(GoBS):**
    - Die GoBS befassen sich mit dem Umgang von aufbewah-rungspflichtigen Daten in elektronischen Buchführungssystemen.
    - Bürgerliches Gesetzbuch (**BGB, allg. Vertragsrecht**)
- …bei welchen die IT **als Instrument** zur Umsetzung von IT- Compliance betrachtet wird.
    - Sarbanes-Oxley-Act **(SOX)**:
    - Fördert Korrektheit und Zuverlässigkeit der Berichterstattung.
    - Aktiengesetz **(AktG)**
    - Bilanzmodernisierungsgesetz **(BilMoG)**:
    - Aktualisierung des Handelsbilanzrechts.
    - Mindestanforderungen an das Risikomanagement **(MaRisk)**:
    - Vorgaben zur Gestaltung eines Risikomanagements.
    - Basel II, Solvency II:
    - Vorschriften zur Vorhaltung bestimmter Eigenkapitalquoten für Banken und Versicherungen.

4.2.9 Einrichtung eines IT-Risikomanagement

Um existenzbedrohende Risiken frühzeitig erkennen zu können, muss ein Risikofrüherkennungs- und Überwachungssystem eingerichtet werden. Dabei ist das IT-Risikomanagement ein Teil des unternehmensweiten Risikomanagements.

Abb. 29: IT-Compliance-Risiken

Die Einrichtung eines IT-Risikomanagementsystems als Komponente der IT-Compliance betrachtet die speziellen **IT-Risiken** und allgemein die **Risiken, die durch Regelverstöße** entstehen.

- **IT-Risiken**: Mit den IT-Risiken sind Risiken gemeint, wie z. B. der Ausfall eines Servers. Diese Risiken lassen sich bewerten und absichern, z. B. über einen zweiten redundanten Server.
- **Risiken durch Regelverstöße**: Bewusste oder unbewusste Regelverstöße durch die Mitarbeiter eines Unternehmens bergen Risiken. Solche Regelverstöße können z. B. Verstöße gegen ein Service-Level-Agreement sein. Mitarbeiter können für diese Verstöße haftbar gemacht werden.

Die Schnittmenge dieser Risikokomponenten sind die IT-Compliance-Risiken. Damit sind Risiken gemeint, die aus den Informations- und Kommunikationssystemen (IuK-Systeme) eines Unternehmens entstehen. Mögliche IT-Compliance-Risiken sind schlecht organisierte, nicht verfügbare oder manipulierbare IT-Systeme, die dazu führen, dass gesetzliche Vorgaben, interne Richtlinien oder vertragliche Verpflichtungen nicht eingehalten werden können.

4.2.10 Persönliche Haftung des Managements

Um der Unternehmensleitung einen Anreiz gegen strafbare Handlungen zu geben, wird der Verstoß gegen Compliance-Vorgaben mit persönlichen Folgen verbunden. Das bedeutet, dass die Unternehmensleitung im Schadensfall (z. B. Schaden eingetreten in Folge eines IT-Systeme-Ausfalls) durch Gerichte persönlich **haftbar** gemacht werden kann.

Die Unternehmensskandale, die Anfang des 21. Jahrhunderts zu beobachten waren, wurden meist durch strafbares Verhalten in der Unternehmensleitung hervorgerufen. Als Reaktion auf

dieses Verhalten haben die Eigenkapitalgeber den Anstoß für verschiedene interne Kontrollsysteme in der Cronus AG gegeben. Das Ziel dieser Maßnahmen, wie z. B. dem vier-Augen-Prinzip, ist die Vermeidung von Fehlverhalten.

Um als Manager nicht haftbar gemacht werden zu können, müssen sie nachweisen können, dass sie sich nach bestem Wissen und Gewissen verhalten haben. Den Nachweis können sie erbringen, indem sie sich z. B. an IT-Compliance-Vorgaben halten.

4.3 Einflussfaktoren auf die IT-Compliance

4.3.1 Einflussfaktoren der IT-Compliance

Mit dem Begriff Einflussfaktoren sind die Ebenen des konzeptionellen Rahmens der IT-Compliance gemeint.

Wenn alle relevanten Einflussfaktoren betrachtet werden sollen, ist eine **isolierte** Betrachtung des Bereichs IT nicht ausreichend. Die Betrachtung von IT-Compliance sollte also **unternehmensübergreifend** sein und alle relevanten **inneren und äußeren** Einflussfaktoren und möglichen Verflechtungen berücksichtigen.

Ob und inwieweit die Mitarbeiter der Cronus AG wissen, dass sie sich an Datenschutzrichtlinien halten müssen, ist ein Beispiel für typische innere Einflussfaktoren. Typische äußere Einflussfaktoren sind Gesetze. Dabei stellt sich die Frage, welche Gesetze für die Cronus AG relevant sind.

4.3.2 Interessengruppen der IT-Compliance

Die Ausgestaltung der IT-Compliance orientiert sich bezüglich der internen Einflussfaktoren an den verschiedenen **Interessengruppen** der Cronus AG. Im Mittelpunkt stehen dabei verschiedene Maßnahmen in einem internen Kontrollsystem zur Reduzierung von unternehmensgefährdenden Risiken.

Abb. 30: Interessengruppen der IT-Compliance

- **Eigenkapitalgeber, Prüfer**: Das Hauptinteresse des Eigenkapitalgebers liegt in der Erwirtschaftung einer möglichst hohen Rendite. Besteht die Gefahr, dass Manager

durch nicht regelkonformes Verhalten das Unternehmen in Skandale oder gar eine Pleite manövrieren, sind die Interessen der Eigenkapitalgeber verletzt.

Darauf folgend haben die Eigenkapitalgeber der Cronus AG verschiedene interne Kontrollsysteme eingeführt. So muss z. B. jede wichtige Entscheidung durch das vier-Augen- Prinzip kontrolliert werden. Die Interessenvertreter der Eigenkapitalgeber - die Wirtschaftsprüfer - bewerten neben der Vermögens-, Finanz- und Ertragslage auch den Zustand der Compliance. Auf diesem Weg kann die Wirksamkeit der internen Kontrollsysteme kontrolliert werden.

Investitionen in die IT-Compliance sollen somit das Risiko von strafbarem Fehlverhalten in der IT im Unternehmen senken.

- **Unternehmensleitung**: Die Unternehmensleitung wird durch die internen Kontrollsysteme angehalten, sich an die Rahmenbedingungen der Cronus AG zu halten. Die Rahmenbedingungen sind ein Bündel aus gesetzlichen und nicht-gesetzlichen Regelungen, die für ein Unternehmen / eine Abteilung gelten.

  Ein Hauptinteresse der Manager an der Compliance ist es, eine möglichst hohe Vergütung zu erzielen und für möglichst wenig haftbar gemacht zu werden. Werden also bestimmte Maßnahmen durchgeführt (z. B. 4-Augen-Prinzip), die bekannte Risiken (z. B. Veruntreuung) vorbeugen, so kann der Manager nachweisen, dass er stets nach bestem Wissen und Gewissen gehandelt hat und sich so der Haftbarkeit entziehen.

  Investitionen in IT-Compliance dienen den Managern dazu, sich an regulatorische Vorgaben zu halten. Zusätzlich erfüllen die Investitionen auch Anforderungen ansteigende Qualität, Leistungsfähigkeit und strategischer Ausrichtung der IT.

- **IT-Management**: Hauptfokus des IT-Managements liegt historisch auf dem Managen von typischen IT-Risiken, also z. B. dem Implementieren von technischen Schutzmaßnahmen wie Firewalls und Virenscannern.

  Die Durchdringung der IT im gesamten Unternehmen führt zu einer höheren Risikoanfälligkeit im IT-Bereich. Das führt dazu, dass das IT-Management für die Entwicklung und Gestaltung eines IT-Compliance-Systems für die Cronus AG verantwortlich gemacht wird.

  Investitionen in IT-Compliance durch das IT-Management haben den Zweck, interne Kontrollsysteme durch IT-Systeme einzurichten und so effektive interne Kontrollen durch IT-Systeme durchzuführen. Die Herausforderung dabei ist, dass die IT-Effizienz unter der Einhaltung der Rahmenbedingungen nicht leiden darf.

Interne Kontrollmaßnahmen durch IT-Systeme werden z. B. durch das Access-Management sichergestellt. So werden Mitarbeitern nur diejenigen Informa-tionen zur Verfügung gestellt, die sie für Ihre Arbeit auch wirklich brauchen.

- **Weitere Interessengruppen**: Weitere Interessengruppen sind z. B. die Mitar-beiter der Cronus AG, Fremdkapitalgeber, Lieferanten und Kunden. Ihr Interesse an IT-Compliance lässt sich häufig aus vertraglichen Vereinbarungen oder gesetzlichen Grundlagen ableiten.

  Besonders der Betriebsrat, als Vertretung der Mitarbeiter eines Unternehmens, stellt eine wichtige Interessengruppe im Bereich IT-Compliance dar. Die Mitarbeiter sind direkt von den internen Kontrollsystemen betroffen und wollen ihre Privatsphäre schützen. Arbeitsrechtliche Regelungen begrenzen die Mög-lichkeit zur internen Kontrolle der Unternehmensleitung, da die Privatsphäre der Mitarbeiter sowie ihre Persönlichkeitsrechte durch gesetzliche Grundlagen geschützt sind.

  Die Kontrolle der Geschwindigkeit von Klicks der einzelnen Mitarbeiter im ERP-System durch die Unternehmensleitung, wäre beispielsweise ein Eingriff in die Privatsphäre der Mitarbeiter.

4.3.3 Rahmenbedingungen der IT-Compliance

Die regulatorischen Rahmenbedingungen der IT-Compliance sind ein Bündel aus internen, externen und vertraglichen Regelungen, die für ein Unternehmen bzw. eine Abteilung gelten. Diese Regelungen sind typische äußere Einflussfaktoren der IT-Compliance.

Die Cronus AG muss dabei supranationale und nationale Gesetze beachten, sowie vertragliche Vereinbarungen, die mit den weiteren Interessengruppen (z. B. Kunden, Lieferanten, Mitarbeiter) vereinbart wurden.

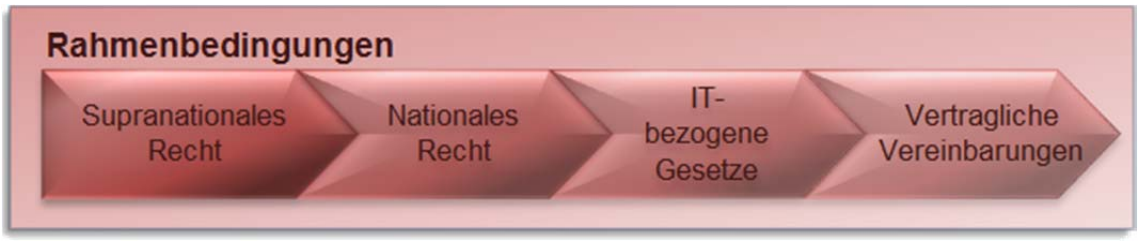


Abb. 31: Rahmenbedingungen der IT-Compliance

- **Supranationales Recht**: Supranationales Recht meint die relevanten Gesetze, die eine Ebene über nationalem Recht stehen. Damit sind z. B. Richtlinien der EU gemeint.

  Allgemein fordern auf supranationaler Ebene die **8. EU Richtlinie** und der Sarbanes-Oxley-Act (SOX) Transparenz und Kontrolle von Abläufen im Unternehmen. Die 8. EU-Richtlinie soll gewährleisten, dass sich Investoren und andere Interessengruppen auf die Korrektheit der geprüften Unternehmens-abschlüsse verlassen können. So wird z. B. der Abschlussprüfer vor unzulässigem Druck von Seiten der Manager geschützt.

  Die Reaktion der USA auf die zahlreichen Bilanzskandale ist die Einführung von SOX im Jahr 2002 als einheitliche Richtlinie für die Prüfung von z. B. Finanzabschlüssen. Dabei wurde das Ziel verfolgt, eine korrekte und zuverlässige Berichterstattung zu gewährleisten, um den Anlegern das Vertrauen in den Markt zurückgeben zu können. Der Sarbanes-Oxlex-Act gilt als Vorreiter aller folgenden Regelwerke im Bereich der Corporate Governance.

- **Nationales Recht:** Auf nationaler Ebene werden SOX und die 8. EU-Richtlinie durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) und das Bilanzmodernisierungsgesetz (BilMoG) umgesetzt.

  Diese gesetzlichen Regelungen auf nationaler und supranationaler Ebene enthalten keine konkreten Anforderungen an die IT, sondern richten sich allgemein an das Risikomanagement im Unternehmen. Da sich aber die IT durch die gesamte Wertschöpfungskette und somit auch durch die Prozesse der Unternehmen zieht, sind diese Gesetze indirekt auf die IT anzuwenden.

  Diese Gesetze beziehen sich nicht direkt auf die IT als Gegenstand der Richt-linien. Jedoch müssen für die IT als Instrument Werkzeuge wie z. B. bestimmte Kontrollmechanismen eingeführt werden.

- **IT-bezogene Gesetze**: Neben den allgemeinen Gesetzen, welche die IT eher als Instrument betrachten und auf Abläufe im Unternehmen abzielen, gibt es auch Gesetze, die sich direkt auf die IT als Gegenstand beziehen. Das deutsche Datenschutzrecht im Bundesdatenschutzgesetz (BDSG) fordert z. B. eine Firewall zur Vermeidung von Zugriffen von Unberechtigten auf Unternehmensdaten.

- **Vertragliche Vereinbarung:** Zuletzt runden die vertraglichen Vereinbarungen des Unternehmens mit den weiteren Interessengruppen die Rahmenbedingungen ab. Dabei werden unter anderem der Umgang mit Daten und Geheimhaltungsbestimmungen oder die Wartung von IT-Systemen geregelt.

  Die IT-Abteilung der Cronus AG hat einen Service-Vertrag mit den anderen Fachabteilungen der Cronus AG. In diesem Service-Vertrag garantiert die IT-Abteilung eine 99,997%-Verfügbarkeit des ERP-Systems "Cronus NAV", während der Geschäftszeiten. Hält sich die IT-Abteilung nicht an diese Zusage, dann haben die Fachabteilungen die Möglichkeit den internen Verrechnungssatz um 10% zu kürzen.

4.3.4 Standards und Frameworks

Auf Ebene der Rahmenbedingungen sind an erster Stelle abstrakt formulierte, allgemeine Anforderungen zu finden. Zur Umsetzung dieser abstrakten Gesetze in konkrete Anweisungen sind eine Reihe von **Standards und Frameworks** entwickelt worden.

Abb. 32: Standards und Frameworks

- **COSO®-Framework**: Das COSO®-Framework ist international anerkannt und lässt sich als Corporate Governance in Regelform beschreiben. Es betrachtet unternehmensübergreifende Aspekte des Risiko-managements und bietet den Unternehmen einen Rahmen zur Einrichtung eines internen Kontrollsystems.
- **Control Objectives for Information and related Technology (COBIT®)**: COBIT® wurde in Anlehnung an COSO® entwickelt. Der Fokus liegt auf der Integration von IT-Governance in die Corporate Governance. COBIT® bietet einen Rahmen für die Ausgestaltung einer IT-Governance, dabei liegt der Fokus auf dem **was** gemacht wird (Zielgrößen werden formuliert) und nicht auf dem **wie**.
- **Information Technology Infrastructure Library (ITIL®)**: ITIL® ist eine Sammlung von Best Practices für die Planung, Überwachung und Steuerung von IT-Leistungen. ITIL® beschreibt dabei **wie** IT-Leistungen erbracht werden, stellt also die Vorgehensweise in den Mittelpunkt.

- **ISO**: ISO 20000 ist die Normierung von ITIL®. Nach dieser Richtlinie können sich die Unternehmen zertifizieren lassen. ISO 2700X sind eine Reihe von Standards zur IT-Sicherheit nach der sich die Unternehmen zertifizieren lassen können.

In den letzten Jahren haben sich eine Vielzahl solcher Frameworks entwickelt. Das COSO®-Framework ("Die Mutter der Regelwerke") fokussiert sich auf die Gesamtrisikosteuerung der Unternehmen. Die ISO-Standards 27000 und 20000 beziehen sich auf spezifische technische Aspekte. CobiT® und ITIL® schlagen den Bogen zwischen Technologie und Corporate Governance.

4.3.5 Einordnung der Standards und Frameworks

Um sich in den zahlreichen Standards und Frameworks zurecht zu finden, kann man sie zusätzlich zum Anwendungsgebiet, auch nach der Reichweite im Unternehmen einordnen. All diese Standards können von der Unternehmensleitung eingesetzt werden, um die gesetzlichen Vorgaben zu erfüllen.

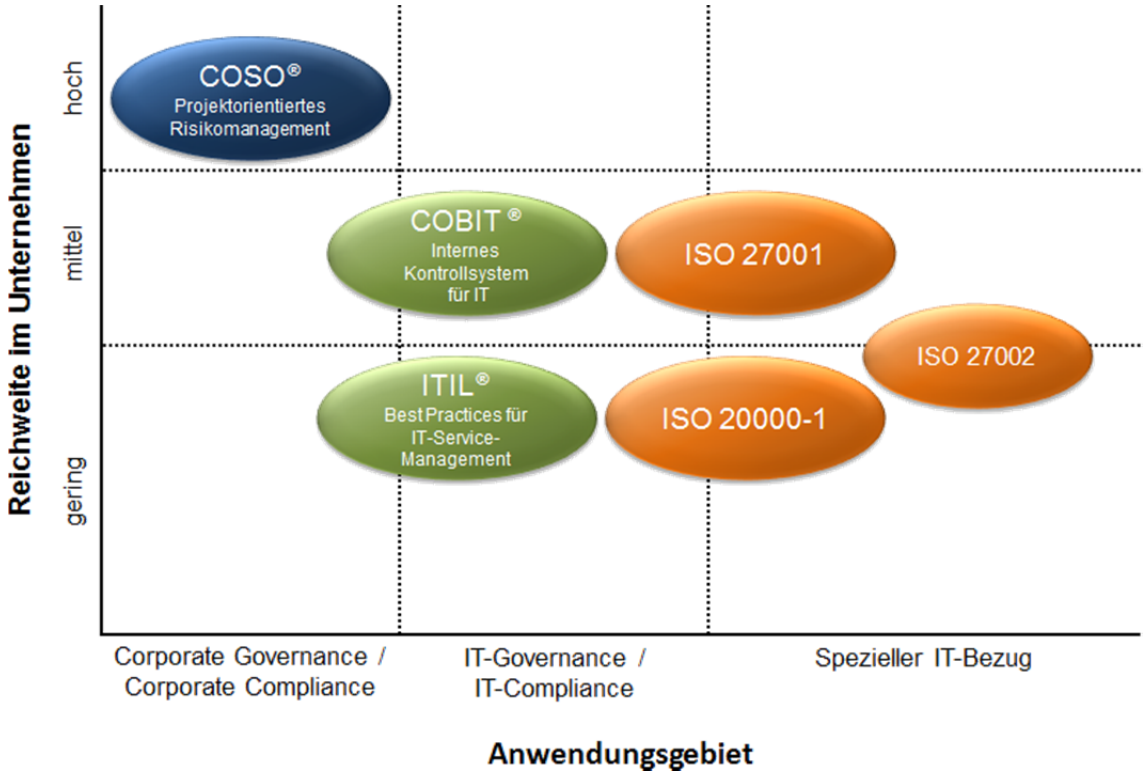


Abb. 33: Einordnung der Standards und Frameworks

4.3.6 Zusammenfassung und Ausblick

Mit Hilfe des konzeptionellen Rahmens konnten wir IT-Compliance erklären. Dabei lässt sich mit Hilfe der ersten konzeptionellen Ebene IT-Compliance einordnen und ein Zusammenhang zu Governance und Compliance herstellen. Die anderen drei Ebenen beschreiben die inneren und äußeren Einflüsse, die auf die IT-Compliance wirken. Im nächsten WBT....

Im nächsten WBT werde ich, Francesco Palla, erklären, wie die IT-Compliance in der Cronus AG umgesetzt wurde und wie der Implementierungsprozess abläuft. In den folgenden WBT werden wir uns Projekte ansehen, bei denen Standards (COBIT® und ITIL®) in der Cronus AG etabliert werden. Abschließend kann mit Hilfe der ISO-Normen eine Zertifizierung der Cronus AG erreicht werden.

4.4 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	Die Unternehmenspleite von ENRON ist zurückzuführen auf…		
	Unzureichende interne Kontrollsysteme.		
	Große Freiheitsgrade der Manager.		
	Eine schlechte Konjunkturlage.		
2	Die Skandale zu Beginn des 21ten Jahrhunderts hatten keinen Einfluss auf das Vertrauen der Anleger.		
	Richtig		
	Falsch		
3	Die Erfüllung von regulatorischen Anforderungen wird als Governance bezeichnet. Die entwickelten Gesetze und Regelwerke sollen Unternehmen zu einem transparenten Verhalten zwingen.		
	Richtig		
	Falsch		
4	Die Business Unit „IT“ setzt sich aus den Mitarbeitern der sekundären IT-Abteilungen aller Business Units zusammen.		
	Richtig		
	Falsch		
5	Die zentrale IT-Unit versteht sich als Dienstleister für die sekundären IT-Abteilungen der anderen Units.		
	Richtig		
	Falsch		
6	In welche Unterbereiche lässt sich IT-Governance unterteilen?		
	IT-Management		
	IT-Performance		
	IT-Compliance		
	IT-Controlling		
7	In der Betrachtung - IT als Instrument – werden konkrete Anforderungen an die Daten und Informationsverarbeitung gestellt. Die IT ist der Träger von Compliance Anforderungen.		
	Richtig		
	Falsch		

8	In welche Komponenten lässt sich IT-Compliance unterteilen?		
	Vorsorge gegen Gesetzesverstöße		
	Einrichtung eines Risikomanagement		
	Implementierung eines internen Kontrollsystems		
	Persönliche Haftung des Managements		
9	Welche Aussage ist richtig?		
	Manager können von der persönlichen Haftung nicht entbunden werden.		
	IT-Risikomanagement beschreibt die Schnittmenge aus IT-Risiken und Risiken aus Regelverstößen. Diese Schnittmenge wird als IT-Compliance-Risiken bezeichnet.		
10	Eine isolierte Betrachtung von IT-Compliance stellt sicher, dass alle Einflussfaktoren der IT auf ein Unternehmen berücksichtigt werden.		
	Richtig		
	Falsch		
11	Welche Aussagen sind richtig?		
	Das Hauptinteresse der Eigenkapitalgeber liegt in der Erwirtschaftung einer möglichst hohen Rendite.		
	Der Hauptfokus des IT-Managements liegt zukünftig auf dem Managen von typischen IT-Risiken (z. B. Firewalls).		
	Die Unternehmensleitung wird durch interne Kontrollsysteme verpflichtet, sich an die Rahmenbedingungen der Cronus AG zu halten.		
	Mitarbeiter sind keine relevante Anspruchsgruppe im Bereich der IT-Compliance		
12	Zur Umsetzung der Gesetze, die sich an die IT-Compliance im Unternehmen richten, sind eine Reihe von Rahmenwerken und Best-Practices entwickelt worden.		
	Richtig		
	Falsch		

13	Welche Synonyme für den Begriff Standards kennen Sie?		
	Framework		
	Rahmenwerk		
	Referenzmodell		
	Regelwerk		

Tab. 5: Übungsfragen WBT 04 – IT-Compliance

5 Umsetzung der IT-Compliance

5.1 Implementierung von IT-Compliance

5.1.1 Einleitung

Im letzten WBT haben wir IT-Compliance und seine Komponenten kennengelernt. Auch wissen wir, warum es notwendig ist, Compliance im Allgemeinen und IT-Compliance im Speziellen umzusetzen.

Wie IT-Compliance in der Cronus AG umgesetzt wird, soll in diesem WBT betrachtet werden. Dazu werden wir einen Vorgehensplan zur Implementierung entwerfen und die verschiedenen Referenzmodelle betrachten, die zur Umsetzung benötigt werden.

Als Treiber für die Einführung von IT-Compliance im Unternehmen ist besonders die starke Zunahme an externen (Gesetzen und regulatorischen Anforderungen) und internen Normen (IT-Governance-Richtlinien) zu nennen. Durch die großen Unternehmenspleiten zu Beginn des 21. Jahrhunderts steht das Thema stärker in der Öffentlichkeit und wird so vermehrt von den Stakeholdern der Unternehmen gefordert.

5.1.2 Entwicklung eines Umsetzungsplans von IT-Compliance

Zur Implementierung von IT-Compliance in der Cronus AG haben wir einen Umsetzungsplan entwickelt. Es ist wichtig, die Umsetzung von IT-Compliance strukturiert und detailliert zu planen, da an den Unternehmensprozessen tiefgreifende Änderungen vorgenommen werden.

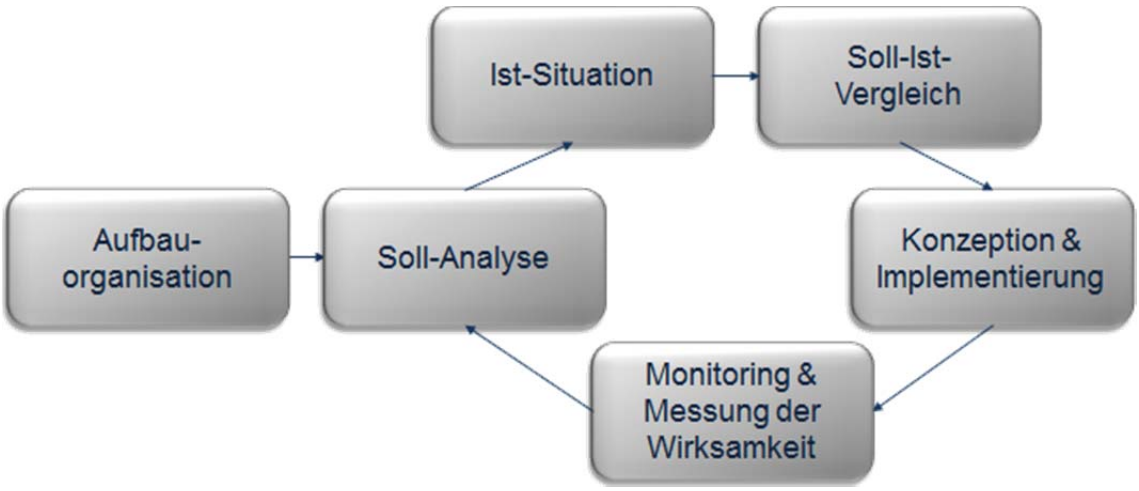


Abb. 34: Umsetzungsplan von IT-Compliance

Durch die ständige Weiterentwicklung der Bereiche Governance und Compliance ist es notwendig, den oben genannten Prozess der Umsetzung in regelmäßigen Abständen zu wieder-

holen. Ganz besonders bei der Ersteinführung von IT-Compliance muss beachtet werden, dass die Umsetzung von IT-Compliance keine kurzfristige, einmalige Aktion ist, sondern ein langfristiger Plan mit mehreren Phasen und Wiederholungen.

5.1.3 Überblick über den Umsetzungsplan

- **Aufbauorganisation**: Mit der Aufbauorganisation sind an dieser Stelle die compliance-spezifischen Bereiche der Aufbauorganisation gemeint. Diese compliance-spezifischen Bereiche müssen initial und zeitstabil in der Cronus AG installiert werden.

  IT-Compliance ist eine Führungsaufgabe, damit ist die Verantwortung in der obersten Führungsebene zu sehen. Zur Umsetzung und Kontrolle der IT-Compliance ist jedoch die Zusammenarbeit von Mitarbeitern verschiedener Hierarchieebenen notwendig.

- **Soll-Analyse**: In dieser Phase findet eine Soll-Analyse der Regeln statt, die der Einhaltung von IT-Compliance in der Cronus AG dienen sollen. Denn erst, wenn man weiß, an welche Vorgaben man sich halten soll, kann man sie auch umsetzen und einhalten.

- **Ist-Situation**: Nachdem festgestellt wurde, an welche externen und internen Regularien man sich halten muss, kann im Rahmen der Ist-Analyse geprüft werden, welche Vorgaben bereits umgesetzt werden. In diesem Fall wird geprüft, welche Maßnahmen zur Erzielung von regelkonformem Verhalten in der Cronus AG gelebt werden.

- **Soll-Ist-Vergleich**: Nachdem nun eine Soll- und Ist-Analyse der IT-Compliance in der Cronus AG erstellt wurde, müssen diese beiden Situationen miteinander verglichen werden. Das Ergebnis dieser Analyse ist eine Menge von Vorgaben, die noch nicht, bzw. noch nicht ausreichend in der Cronus AG umgesetzt worden sind. Mit der Menge an Vorgaben kann eine To-Do-Liste für die Konzeption der Maßnahmen erstellt werden.

- **Konzeption und Implementierung**: In der Phase der Konzeption & Implementierung werden Maßnahmen zur Beseitigung der Compliance-Defizite (vgl. Soll-Ist-Vergleich) festgelegt und umgesetzt. Die Cronus AG wird zur Unterstützung auf die Hilfe von Standards und Frameworks zurückgreifen. Diese geben Hilfestellungen bei der Umsetzung von IT-Compliance in der Cronus AG.

- **Monitoring und Messung der Wirksamkeit**: Monitoring von Maßnahmen zur Umsetzung von IT-Compliance meint einerseits die Überwachung, ob die entwickelten Maßnahmen so durchgeführt werden, wie es vorgeschrieben wurde. Andererseits meint Monitoring auch die Überwachung der Maßnahmen hinsichtlich der Erfüllung

der Anforderungen (Effektivität). Unterstützt die gesetzte Maßnahme überhaupt regelkonformes Verhalten in der Cronus AG? Diese Maßnahmen werden sowohl von internen als auch externen Prüfern regelmäßig auf ihre Wirksamkeit hin geprüft.

Im Anschluss an die Phase Monitoring & Performancemessung steht wieder die Soll-Analyse. Häufig ist ein Unternehmen nach einem Durchlauf des Implementierungsplans noch nicht "compliant" mit allen externen und internen Vorgaben. Ist ein Unternehmen "compliant" mit allen externen und internen Vorgaben, so muss regelmäßig geprüft werden, ob sich diese Vorgaben geändert haben.

5.1.4 Aufbauorganisation in der Cronus AG

An erster Stelle des Umsetzungsplans zur IT-Compliance in der Cronus AG steht die compliance-spezifische Aufbauorganisation der Cronus AG. In der Praxis wird die Umsetzung und Steuerung von IT-Compliance häufig in der IT-Abteilung oder der Rechtsabteilung eingegliedert. Damit allein ist es aber nicht getan!

Die Verantwortung für Compliance im Allgemeinen, aber auch für IT-Compliance im Speziellen liegt in der obersten Führungsebene. Die Unternehmensleitung trägt somit auch die Folgen, die aus einer Nichterfüllung der IT-Compliance resultieren können.

IT-Compliance ist nur durch eine enge Zusammenarbeit von den verschiedenen Hierarchieebenen der Cronus AG sinnvoll umsetzbar.

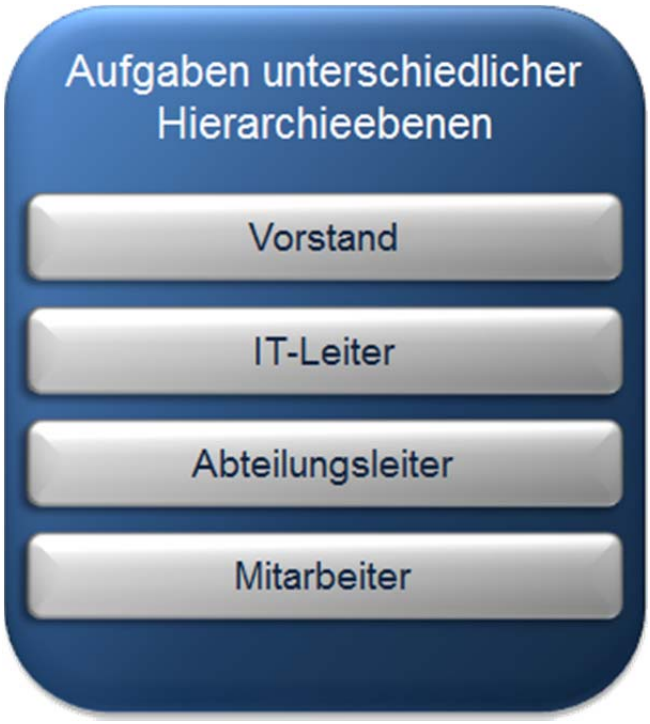


Abb. 35: Aufgaben unterschiedlicher Hierarchieebenen

Manager können für Verstöße gegen Compliance-Vorgaben persönlich haftbar gemacht werden. Somit muss die Verantwortung bei der Umsetzung von IT-Compliance in der Unternehmensleitung angesiedelt sein.

5.1.5 Aufgaben unterschiedlicher Hierarchieebenen

Den verschiedenen Hierarchieebenen der Cronus AG fallen bei der Implementierung von IT-Compliance unterschiedliche Aufgabenbereiche zu. Wie bei allen hierarchieübergreifenden Aufgaben, ist bei der Implementierung von IT-Compliance eine enge Zusammenarbeit von Vorstand und nachgelagerten Hierarchieebenen unerlässlich.

- **Vorstand**: Der Vorstand wirkt aktiv bei der Analyse der Soll- und Ist-Situation mit. Zusätzlich wird der Vorstand regelmäßig über den aktuellen Stand der Compliance und der IT-Compliance durch den Chief Compliance Officer (CCO) informiert.

  Die Cronus AG hat einen Chief-Compliance-Officer (CCO) eingestellt. Sein Aufgabengebiet liegt in der Kontrolle und Überwachung von regulatorischen und unternehmensinternen Anforderungen der Compliance (Monitoring & Performancemessung. Der CCO ist direkt dem Vorstandsvorsitzenden unterstellt und nur ihm gegenüber berichtspflichtig. So können Probleme, die durch Moral Hazard entstehen, vermieden werden.

- **IT-Leiter**: Der IT-Leiter ist verantwortlich für die gesamte IT im Unternehmen. Er stellt sicher, dass die IT-Strategie stets geschäftsorientiert umgesetzt wird.

  In der Cronus AG ist der Leiter der IT der Chief Information Officer (CIO) Francesco Palla. Der CIO leitet den Implementierungsplan und anschließenden Prozess der IT-Compliance in der Cronus AG. Dabei leitet er alle Phasen der Umsetzung, außer die Phase des Monitoring. Beim Monitoring arbeitet Francesco Palla jedoch eng mit dem IT-Compliance-Officer zusammen.

- **Abteilungsleiter**: Alle Abteilungsleiter müssen in den Implementierungsprozess der IT-Compliance mit einbezogen werden. Dabei können sie einerseits mit Know How bzgl. der internen und externen Vorgaben helfen. Andererseits sind die Abteilungen Objekt der Maßnahmen. Die Abteilungen müssen sich auf die neuen Anforderungen der IT-Compliance einstellen.

  Die unternehmensinterne Rechtsabteilung ist z. B. für die Einhaltung von rechtlichen Vorgaben in der Cronus AG verantwortlich. So ist bei der Implementierung von IT-Compliance eine enge Zusammenarbeit mit den anderen Bereichen der Cronus AG notwendig.

- **Mitarbeiter**: Zuletzt muss jeder Mitarbeiter in den Prozess der Umsetzung von IT-Compliance einbezogen werden. Durch Schulungen sollen die Mitarbeiter für die Anforderungen, z. B. des Datenschutzes, sensibilisiert werden.

  Die Mitarbeiter der Cronus AG müssen z. B. das Datenschutzrecht in der Praxis leben und die relevanten Voraussetzungen kennen, unter denen Daten verarbeitet werden dürfen.

5.1.6 Der IT-Compliance-Officer

Durch die gestiegene Relevanz von Compliance im Generellen und IT-Compliance im Speziellen, haben sich in der Praxis neue Berufe entwickelt. Wie bereits vorgestellt, ist der **Chief-Compliance-Officer** auf Vorstandsebene anzusiedeln. Er ist allgemein für die Einhaltung von Compliance in einem Unternehmen verantwortlich.

Bei der Daimler-Benz AG ist der CCO zum Stand 2014 eine ehemalige Richterin des Landgerichts und ehemalige Justiz- bzw. Wissenschaftsministerin des Landes Hessen. Eine juristische Ausbildung ist bei Mitarbeitern im Bereich Compliance häufig zu finden.

Für den Bereich IT hat sich die Berufsbezeichnung **IT-Compliance-Officer** entwickelt. In der Praxis hat sich noch keine gefestigte Position für den Beruf in den Unternehmen herauskristallisiert. In der Cronus AG ist der IT-Compliance-Officer dem CCO direkt unterstellt und arbeitet Hand in Hand mit dem CIO. er ist nicht dem CIO unterstellt, da er sonst seinen Vorgesetzten kontrollieren müsste, dies führt zu Moral-Hazard-Problemen.

Die Hauptaufgabe des IT-Compliance-Officers ist die Beratung des CCO in allen relevanten IT-Compliance-Bereichen. Dazu zählt die Gestaltung, Weiterentwicklung und Umsetzung von IT-Compliance im Unternehmen essentiell. Der IT-Compliance-Officer ist die Schnittstelle zwischen Compliance und IT. So berät er z. B. die Mitarbeiter der IT-Abteilung bei der Systementwicklung und -überarbeitung hinsichtlich der Compliance-Fragestellungen.

Eine Ausbildung zum IT-Compliance-Officer im traditionellen Sinne gibt es nicht. Kenntnisse von IT und rechtlichen Fragestellungen sind mindestens erforderlich, um die Anforderungen erfüllen zu können.

Die Rolle des IT-Compliance-Officers lässt sich anhand seiner Aufgaben zusammenfassen als beratende, initiierende und steuernde Position innerhalb der Unternehmens-Compliance. So muss er sich z. B. gemeinsam mit dem Vorstand und COO, für ein oder mehrere Referenzmodelle entscheiden, um die relevanten Normen umzusetzen und "compliant" zu sein.

5.2 Situationsanalyse

5.2.1 Die Situationsanalyse

Die Situationsanalyse umfasst die Phasen: Vorgaben identifizieren, Ist-Situation und

Soll-Ist-Vergleich.

Als erster Erfolg ist zu verbuchen, dass ein Plan für die Umsetzung einer IT-Compliance gefasst wurde. In konservativen Unternehmensleitungen wird nicht zwingend verstanden, dass die **IT ein unverzichtbares Bindeglied** zwischen allen Bestandteilen von Geschäftsprozessen darstellt.

Durch die zunehmende Anzahl von externen Gesetzen und Vorgaben, sowie Unternehmenspleiten wie z. B. ENRON, ist die Sensibilität allerdings für den häufig verkannten Produktionsfaktor IT in den letzten Jahren stark angestiegen.

Nach einem geglückten Projektsetup werden sich die Mitarbeiter der IT-Abteilung nun an die Situationsanalyse der IT-Compliance begeben.

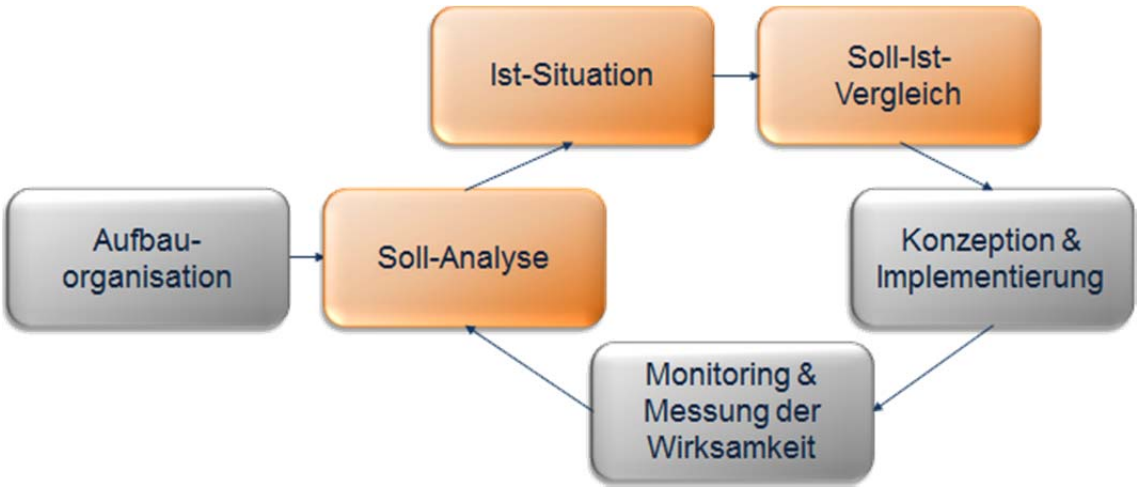


Abb. 36: Die Phasen der Situationsanalyse des Umsetzungsplans

5.2.2 Rückblick: Soll-Analyse aller relevanten Gesetze und Vorgaben

Als erster Schritt der Situationsanalyse wird eine Soll-Analyse durchgeführt. Ziel dieser Analyse ist es, alle relevanten externen und internen Vorgaben zu identifizieren, welche die Cronus AG befolgen soll.

Welche compliance-relevanten **Rahmenbedingungen** für die Implementierung von IT-Compliance relevant sein können, wurde bereits in "WBT 04 - IT-Compliance" dargestellt und an dieser Stelle wiederholt.

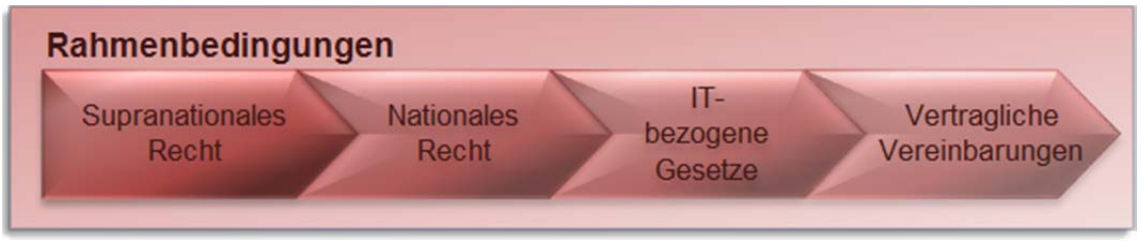


Abb. 37: Rahmenbedingungen der IT-Compliance

- **Supranationales Recht**: Supranationales Recht meint die relevanten Gesetze, die eine Ebene über nationalem Recht stehen. Damit sind z. B. Richtlinien der EU gemeint.

  Allgemein fordern auf supranationaler Ebene die **8. EU Richtlinie** und der Sarbanes-Oxley-Act (SOX) Transparenz und Kontrolle von Abläufen im Unternehmen. Die 8. EU-Richtlinie soll gewährleisten, dass sich Investoren und andere Interessengruppen auf die Korrektheit der geprüften Unternehmens-abschlüsse verlassen können. So wird z. B. der Abschlussprüfer vor unzulässigem Druck von Seiten der Manager geschützt.

  Die Reaktion der USA auf die zahlreichen Bilanzskandale ist die Einführung von SOX im Jahr 2002 als einheitliche Richtlinie für die Prüfung von z. B. Finanzabschlüssen. Dabei wurde das Ziel verfolgt, eine korrekte und zuverlässige Berichterstattung zu gewährleisten, um den Anlegern das Vertrauen in den Markt zurückgeben zu können. Der Sarbanes-Oxlex-Act gilt als Vorreiter aller folgenden Regelwerke im Bereich der Corporate Governance.

- **Nationales Recht:** Auf nationaler Ebene werden SOX und die 8. EU-Richtlinie durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) und das Bilanzmodernisierungsgesetz (BilMoG) umgesetzt.

  Diese gesetzlichen Regelungen auf nationaler und supranationaler Ebene enthalten keine konkreten Anforderungen an die IT, sondern richten sich allge-mein an das Risikomanagement im Unternehmen. Da sich aber die IT durch die gesamte Wertschöpfungskette und somit auch durch die Prozesse der Unterneh-men zieht, sind diese Gesetze indirekt auf die IT anzuwenden.

  Diese Gesetze beziehen sich nicht direkt auf die IT als Gegenstand der Richt-linien. Jedoch müssen für die IT als Instrument Werkzeuge wie z. B. bestimmte Kontrollmechanismen eingeführt werden.

- **IT-bezogene Gesetze**: Neben den allgemeinen Gesetzen, welche die IT eher als Instrument betrachten und auf Abläufe im Unternehmen abzielen, gibt es auch Gesetze, die sich direkt auf die IT als Gegenstand beziehen. Das deutsche Datenschutzrecht im Bundesdatenschutzgesetz (BDSG) fordert z. B. eine Firewall zur Vermeidung von Zugriffen von Unberechtigten auf Unternehmensdaten.

- **Vertragliche Vereinbarung:** Zuletzt runden die vertraglichen Vereinbarungen des Unternehmens mit den weiteren Interessengruppen die Rahmenbedingungen ab. Dabei werden unter anderem der Umgang mit Daten und Geheimhaltungsbestimmungen oder die Wartung von IT-Systemen geregelt.

  Die IT-Abteilung der Cronus AG hat einen Service-Vertrag mit den anderen Fachabteilungen der Cronus AG. In diesem Service-Vertrag garantiert die IT-Abteilung eine 99,997%-Verfügbarkeit des ERP-Systems "Cronus NAV", während der Geschäftszeiten. Hält sich die IT-Abteilung nicht an diese Zusage, dann haben die Fachabteilungen die Möglichkeit den internen Verrechnungssatz um 10% zu kürzen.

5.2.3 Soll-Analyse in der Cronus AG

Der IT-Compliance-Officer der Cronus AG hat eine Excel-Tabelle erstellt, mit dessen Hilfe die relevanten internen und externen Vorgaben aufgelistet werden. Hier dargestellt ist ein Ausschnitt dieser **Soll-Analyse**.

	A	B
1	**Soll-Ist-Analyse**	
2		
3	**Analyse der Soll-Situation**	
4		
5	**externe Vorgaben**	
6	**BDSG**	
7	§ 5	"Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort."
8	§ 28	Datenerhebung und -speicherung für eigene Geschäftszwecke
9	§ 29	Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung
10	...	
11	**KonTraG** (Präzision und Erweiterung des HGB und AktG)	
12	§ 91 Abs. 2 AktG	"Der Vorstand ist verpflichtet, geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."
13	...	
14	**BilMoG**	
15	...	
16	**8. EU-Richtlinie**	
17	...	
18	**...**	
19	interne Vorgaben	
20	**Service-Vertrag**	Verfügbarkeit ERP-System
21		Verfügbarkeit CRM-System
22		...
23	**Wartungs-Vertrag**	Software
24		Hardware
25		...
26	...	

Abb. 38: Soll-Analyse der internen und externen Vorgaben der Cronus AG

Diese Excel-Tabelle ist lediglich eine beispielhafte Darstellung. Es ist hervorzuheben, dass eine solche Soll-Analyse extrem umfangreich ist und besonderer Fähigkeiten bedarf! Welche Vorgaben für eine solche Analyse zuletzt ausgewählt werden, ist unternehmensindividuell und sehr komplex.

5.2.4 Die Ist-Situation

Im dieser Phase des Umsetzungsplans wird die Ist-Situation der IT-Compliance in der Cronus AG analysiert. Im Zuge dieser Bestandsaufnahme wird geprüft, in wieweit bereits Maßnahmen eingeleitet oder umgesetzt wurden, die bereits das Ziel von regelkonformem Verhalten verfolgen.

Diese Maßnahmen können sich mit Vorgaben aus **externen** Regularien oder **unternehmensinternen** Verträgen / Regularien befassen.

- **Externe Regularien**: Der Schutz von personenbezogenen Daten wird geregelt über §9 des Bundesdatenschutzgesetzes Dieser verlangt einen Schutz vor unberechtigten Zugriff auf diese Daten. Die Cronus AG hat Zugriffskontrollen eingerichtet, sodass nur die berechtigten Mitarbeiter auf diese Daten zugreifen können.
- **Unternehmensinterne Verträge**: Die IT-Abteilung der Cronus AG hat einen Service-Vertrag mit den anderen Fachabteilungen der Cronus AG. In diesem Service-Vertrag garantiert die IT-Abteilung eine 99,997%-Verfügbarkeit des ERP-Systems "Cronus MyERP", während der Geschäftszeiten. Hält sich die IT-Abteilung nicht an diese Zusage, dann haben die Fachabteilungen die Möglichkeit, den internen Verrechnungssatz um 10% zu kürzen.

5.2.5 Ist-Situation in der Cronus AG

Der IT-Compliance-Officer der Cronus AG hat die Excel-Tabelle der Soll-Analyse um die Ist-Situation erweitert. Dabei hat er mit Hilfe von Ampelfarben, den Erfüllungsgrad der internen und externen Vorgaben markiert. Für die Vorgaben die einen Erfüllungsgrad "nicht erfüllt" zugeordnet bekommen, sind als erstes Maßnahmen zu entwickeln. Hier dargestellt ist ein Ausschnitt dieser Ist-Analyse.

	A	B	C
1	**Soll-Ist-Analyse**		
2			
3	**Analyse der Soll-Situation**		**Analyse der Ist-Situation**
4			
5	**externe Vorgaben**		Erfüllungsgrad
6	**BDSG**		
7	§ 5	"Den bei der Datenverarbeitung beschäftigten Personen ist	zum Teil erfüllt
8	§ 28	Datenerhebung und -speicherung für eigene	nicht erfüllt
9	§ 29	Geschäftsmäßige	zum Teil erfüllt
10	…		
11	**KonTraG** (Präzision und Erweiterung des HGB und AktG)		
12	§ 91 Abs. 2 AktG	"Der Vorstand ist verpflichtet, geeignete Maßnahmen zu	zum Teil erfüllt
13	…		
14	**BilMoG**		nicht erfüllt
15	…		
16	**8. EU-Richtlinie**		nicht erfüllt
17	…		
18	**…**		
19	interne Vorgaben		
20	**Service-Vertrag**	Verfügbarkeit ERP-System	zum Teil erfüllt
21		Verfügbarkeit CRM-System	nicht erfüllt
22		…	
23	**Wartungs-Vertrag**	Software	nicht erfüllt
24		Hardware	erfüllt
25		…	
26	**…**		

Abb. 39: Ist-Analyse der internen und externen Vorgaben der Cronus AG

5.2.6 Soll-Ist-Vergleich

Der IT-Compliance-Officer hat auf Basis des Soll-Ist-Vergleichs eine To-Do-Liste für die Cronus AG erstellt. Dabei wurde festgestellt, dass die Cronus AG bereits einige Maßnahmen eingeleitet hat, die das Ziel der IT-Compliance verfolgen. Diese sind jedoch noch nicht ausreichend effizient und effektiv. Allgemein kann das Ergebnis des Soll-Ist-Vergleichs für eine Maßnahme drei verschiedene Ausprägungen haben.

1. Die Ist-Analyse hat ergeben, dass bis dato keine Maßnahme zur Erreichung einer IT-Compliance-Vorgabe eingeleitet wurde.
2. Die Ist-Analyse hat ergeben, dass die eingeführte Maßnahme zur Erreichung von IT-Compliance nicht **effizient/ effektiv** ist.

3. Die Ist-Analyse hat ergeben, dass wir eine Maßnahme die Vorgaben für eine vollständige IT-Compliance erfüllt haben. Diese ist effizient und effektiv. Es besteht zunächst kein weiterer Handlungsbedarf.

Das Ergebnis des Soll-Ist-Vergleichs hat ergeben, dass die Cronus AG die internen und externen Vorgaben **noch nicht bzw. noch nicht ausreichend** umgesetzt hat.

- **Maßnahme für eine interne Vorgabe**: Die IT-Abteilung der Cronus AG hat einen Service-Vertrag mit den anderen Fachabteilungen der Cronus AG. In diesem Service-Vertrag garantiert die IT-Abteilung eine 99,997%-Verfügbarkeit des ERP-Systems "Cronus NAV", während der Geschäftszeiten. Die IT-Abteilung prüft die Verfügbarkeit des ERP-Systems lediglich einmal am Tag. Um die Verfügbarkeit zu gewährleisten, müsste z. B. eine automatisierte minütliche Kontrolle erfolgen.
- **Maßnahme für eine externe Vorgabe**: Die Cronus AG hat Zugriffskontrollen eingerichtet, sodass nur die berechtigten Mitarbeiter auf diese Daten zugreifen können. Die zugriffsberechtigten Mitarbeiter nutzen aber alle einen unpersönlichen Administratorenzugang, um auf die Daten zuzugreifen. Hier müssen individuelle Schlüssel eingerichtet werden, um den Schutz der Daten gewährleisten zu können.

Auf der nächsten Seite wird anhand der Soll-Ist-Analyse eine To-Do-Liste entwickelt. Mit Hilfe dieser Liste, werden in der Konzeptionsphase Maßnahmen entwickelt, mit denen IT-Compliance erreicht werden soll.

5.2.7 Soll-Ist-Vergleich in der Cronus AG

Der IT-Compliance-Officer hat auf Basis des Soll-Ist-Vergleichs eine To-Do-Liste für die Cronus AG erstellt. Hier dargestellt ist ein Ausschnitt dieser To-Do-Liste.

	A	B	C	D
1	**Soll-Ist-Analyse**			
2				
3	**Soll-Situation**		**Ist-Situation**	**To-Do-Liste**
4				
5	**externe Vorgaben**		**Erfüllungsgrad**	
6	**BDSG**			
7	§ 5	"Den bei der Datenverarbeitung beschäftigten Personen ist untersagt,	zum Teil erfüllt	Zugriffskontrollen von Mitarbeitern auf personenbezogene Daten verstärken.
8	§ 28	Datenerhebung und -speicherung für eigene Geschäftszwecke	nicht erfüllt	Prüfung der Voraussetzungen, inwieweit eine Datenerhebung bzw. -speicherung der Daten zulässig ist.
9	§ 29	Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung	zum Teil erfüllt	Prüfung der Voraussetzungen, inwieweit eine Datenerhebung bzw. -speicherung der Daten zulässig ist.
10				
11	**KonTraG** (Präzision			
12	§ 91 Abs. 2 AktG	"Der Vorstand ist verpflichtet, geeignete Maßnahmen zu treffen,	zum Teil erfüllt	Einrichtung eines zeitkonsistenten Governance- und Compliance-Managements.
13	...			
18	**...**			
19	**interne Vorgaben**			
20	**Service-Vertrag**	Verfügbarkeit ERP-Systen	zum Teil erfüllt	Regelmäßige Prüfung der Verfügbarkeit des ERP-Systems.
21		Verfügbarkeit CRM-Syster	nicht erfüllt	Regelmäßige Prüfung der Verfügbarkeit des CRM-Systems.
22		...		
23	**Wartungs-Vertrag**	Software	nicht erfüllt	Regelmäßige Prüfung der Software-Nutzung und -Aktualität.
24		Hardware	erfüllt	Kein To-Do erforderlich
25		...		

Abb. 40: Soll-Ist-Vergleich der internen und externen Vorgaben der Cronus AG

5.3 Konzeption & Implementierung von Maßnahmen

5.3.1 Konzeption eigener Maßnahmen

Der IT-Compliance-Officer hat auf Basis der erstellten To-Do-Liste einige Maßnahmen zur Erreichung von regelkonformem Verhalten entwickelt. Leider hat er schnell gemerkt, dass diese Arbeit extrem aufwendig ist, und am Ende trotzdem unklar bleibt, ob diese Maßnahmen regelkonformes Verhalten unterstützen.

	A	B	C	D	E
1	**Soll-Ist-Analyse**				
2					
3		**Soll-Situation**	**Ist-Situation**	**To-Do-Liste**	**geplante Maßnahmen**
4					
5		externe Vorgaben	Erfüllungsgrad		
6	**BDSG**				
7		§ 5 "Den bei der Datenverarbeitung	zum Teil erfüllt	Zugriffskontrollen von Mitarbeitern auf personenbezogene Daten verstärken.	Einrichtung individueller Zugangsschlüssel für die berechtigten Mitarbeiter.
8		§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke	nicht erfüllt	Prüfung der Voraussetzungen, inwieweit eine Datenerhebung bzw. -speicherung der Daten zulässig ist.	Erstelle Prozess, zur ständigen Prüfung der erhobenen und gespeicherten Daten. Richte eine Wiederspruchsmöglichkeit für Betroffene ein.
9		§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck	zum Teil erfüllt	Prüfung der Voraussetzungen, inwieweit eine Datenerhebung bzw. -speicherung der Daten zulässig ist.	Erstelle Prozess, zur ständigen Prüfung der erhobenen und gespeicherten Daten. Richte eine Wiederspruchsmöglichkeit für Betroffene ein.
10		...			
11	**KonTraG** (Präzision				
12		§ 91 Abs. 2 AktG "Der Vorstand ist verpflichtet, geeignete Maßnahmen zu treffen,	zum Teil erfüllt	Einrichtung eines zeitkonsistenten Governance- und Compliance-Managements.	Führe eine Soll-Ist-Analyse durch und schließe die Lücke zwischen Soll und Ist durch geeignete Maßnahmen. Prüfe die Maßnahmen regelmäßig auf Wirksamkeit.
13		...			
18		...			
19		interne Vorgaben			
		Service-Vertrag			
20		Verfügbarkeit ERP-System	zum Teil erfüllt	Regelmäßige Prüfung der Verfügbarkeit des ERP-Systems.	Einrichtung einer minütlichen automatisierten Prüfung der Verfügbarkeit. Richte ein Notfallplan ein, für den fall eines Ausfalls.
21		Verfügbarkeit CRM-System	nicht erfüllt	Regelmäßige Prüfung der Verfügbarkeit des CRM-Systems.	Einrichtung einer minütlichen automatisierten Prüfung der Verfügbarkeit. Richte ein Notfallplan ein, für den fall eines Ausfalls.
22		...			
		Wartungs-Vertrag			
23		Software	nicht erfüllt	Regelmäßige Prüfung der Software-Nutzung und -Aktualität.	Beauftragung eines Verantwortlichen für die Unternehmens-Software.
		Hardware	erfüllt	Kein To-Do erforderlich	Keine Maßnahme erforderlich. Erneute Prüfung auf regelkonforme Einhaltung der Vorgabe in der nächsten Periode.
24					
25		...			

Abb. 41: Konzeption eigener Maßnahmen zur Erfüllung der To-Do-Liste

5.3.2 Konzeption & Implementierung

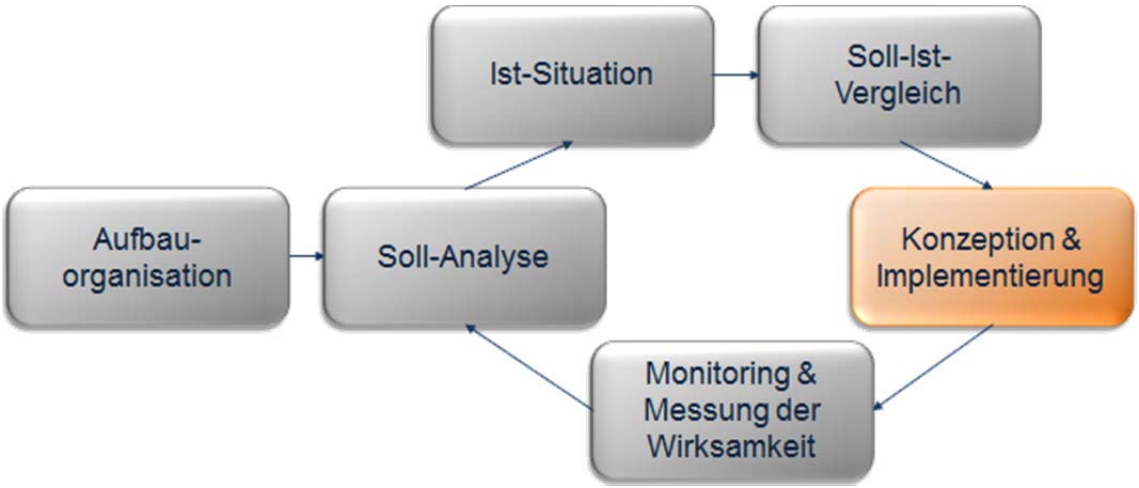
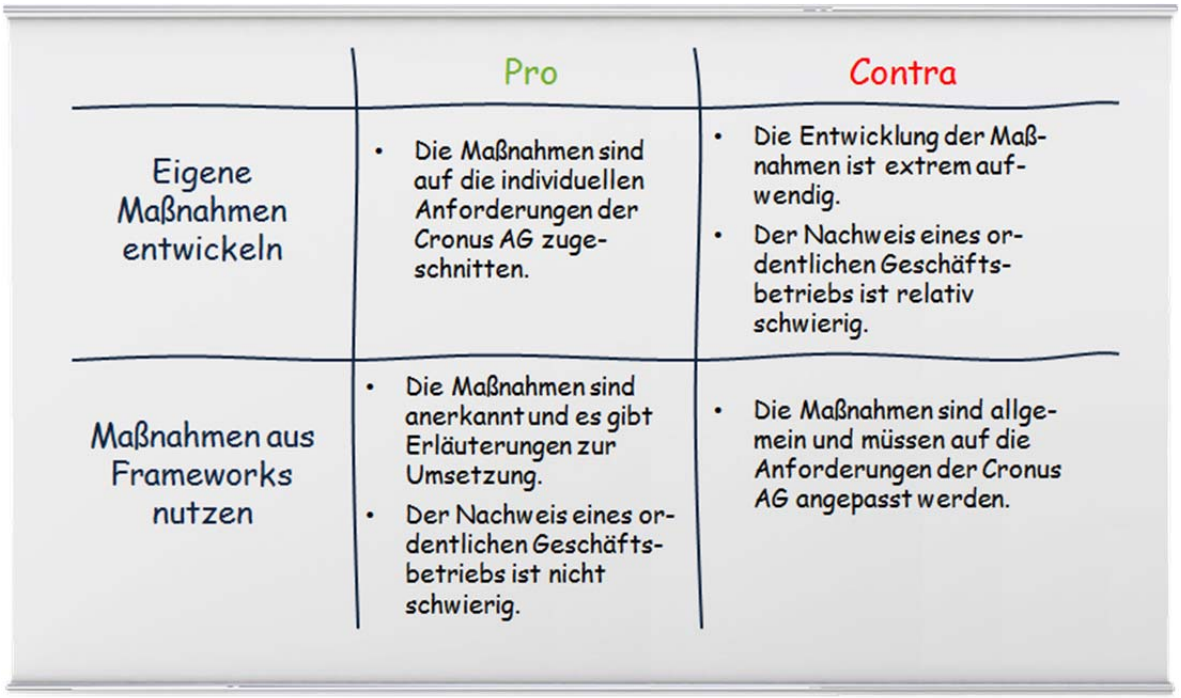


Abb. 42: Umsetzungsplan von IT-Compliance: Konzeption und Implementierung

Die Entwicklung von Maßnahmen zur Erreichung von IT-Compliance können grundsätzlich **zwei** verschiedene **Ansatzpunkte** haben, wie die Entwicklung und Umsetzung. Die Umsetzung der gültigen Gesetze kann entweder durch selbst entwickelte Maßnahmen erfolgen oder aber, in dem man sich an einem der gängigen Referenzmodelle oder Best-Practices richtet. In der Praxis werden in der Regel etablierte Referenzmodelle genutzt, welche auf die spezifischen Unternehmensanforderungen angepasst werden.



	Pro	Contra
Eigene Maßnahmen entwickeln	• Die Maßnahmen sind auf die individuellen Anforderungen der Cronus AG zugeschnitten.	• Die Entwicklung der Maßnahmen ist extrem aufwendig. • Der Nachweis eines ordentlichen Geschäftsbetriebs ist relativ schwierig.
Maßnahmen aus Frameworks nutzen	• Die Maßnahmen sind anerkannt und es gibt Erläuterungen zur Umsetzung. • Der Nachweis eines ordentlichen Geschäftsbetriebs ist nicht schwierig.	• Die Maßnahmen sind allgemein und müssen auf die Anforderungen der Cronus AG angepasst werden.

Abb. 43: Ansatzpunkte zur Entwicklung von Maßnahmen zur Erreichung von IT-Compliance

Die Ausrichtung an etablierten Best-Practices ist aus zwei Gründen empfehlenswert: Einerseits kann die Anwendung den Enthaftungsbeweis für die Unternehmensleitung liefern, andererseits liefern Best-Practices auch einfache Hinweise zur konkreten Umsetzung von Compliance-Vorgaben.

Die etablierten Referenzmodelle passen im Normalfall gut zu den Anforderungen, die ein "normales" Unternehmen an die IT-Compliance stellt. Auch die die Cronus AG hat sich im Zuge der Implementierung der IT-Compliance dazu entscheiden, sich an den bestehenden und etablierten Referenzmodellen zu orientieren.

5.3.3 Auswahl des "richtigen" Referenzmodells

In "WBT 04 - IT-Compliance" wurde eine **Auswahl** von bekannten Referenzmodelle, Standards und Best-Practices im Bereich IT-Governance und IT-Compliance vorgestellt.

Diese **Referenzmodelle** werden wir im Laufe des Kapitels detaillierter betrachten und versuchen eine Entscheidung zu treffen, ob und wenn ja welche/s Referenzmodell/e uns bei der Implementierung von IT-Governance und IT-Compliance in der Cronus AG unterstützen kann/ können.

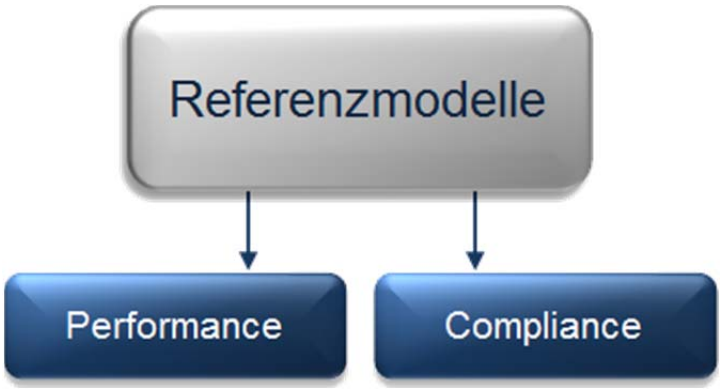


Abb. 44: Aspekte von Referenzmodellen zur Implementierung von IT-Compliance

Einige Referenzmodelle beschäftigen sich primär mit dem Performance-Aspekt der IT-Governance / IT-Compliance. Andere Referenzmodelle betrachten primär den Compliance-Aspekt der IT-Governance / IT-Compliance. Diese Zuordnung ist nicht immer eindeutig, die Referenzmodelle haben immer Aspekte, die auf beide Sichtweisen zutreffen.

Die Referenzmodelle sind:

- COSO®
- COBIT®
- ITIL®
- ISO 20000
- ISO 27001
- ISO 27002

ITIL® befasst sich mit dem IT-Service-Management, dieser Aspekt betrifft die Performance-Sichtweise. Andererseits beschreibt ITIL® auch Service-Level-Agreements, welche die Compliance-Sichtweise betreffen.

Ein gutes Referenzmodell fördert den Output (Performance) und ist regelkonform (Compliance). Das trifft auf die hier vorgestellten etablierten Referenzmodelle zu.

5.3.4 COSO®-ERM

Das Referenzmodell der Commitee of Sponsoring Organization of the Treadway Commission (COSO®-ERM) befasst sich allgemein mit Corporate Governance und hat keinen speziellen IT-Bezug. Das COSO®-ERM-Referenzmodell kann dazu verwendet werden, das Gesetz **SOX** (Sarbanes-Oxley-Act) umzusetzen (Konformität).

- **SOX**: SOX wurde als Folge auf die Unternehmensskandale wie z. B. ENRON entwickelt. Damit werden die gesetzlichen Bestimmungen für die Bilanzierung von Unternehmen, die in den USA börsennotiert sind, verschärft.

Neben der Erfüllung von Konformität mit SOX und der Einführung eines internen Kontrollsystems, sollte ein weiteres Ziel der Implementierung von COSO®-ERM die Unterstützung der Unternehmensleitung bei der Umsetzung von Prozessen und deren Performancesteigerung sein. Das COSO®-ERM-Framework fordert mindestens **5 Hauptkomponenten** als Bestandteil eines internen Kontrollsystems.

Abb. 45: Hauptkomponenten von COSO®-ERM

Die Komponenten sind dabei eng miteinander verbunden. Die verfolgten Ziele lassen sich in drei Bereiche einteilen: Betrieb, Berichtswesen und Compliance. Alle möglichen Zusammenhänge von Komponenten und Zielen können mit den Geschäftsbereichen und Aktivitäten eines Unternehmens zu dem **COSO®-Würfel** zusammengefasst werden.

Abb. 46: Der COSO®-Würfel

5.3.5 COBIT®

Das Referenzmodell Control Objectives for Information and Related Technology (COBIT®) bietet den Unternehmen Unterstützung, um die IT-Ressourcen im Unternehmen **effizienter** und **effektiver** zu managen. Eine wesentliche Komponente von COBIT® ist das Prozessmodell, welches alle Prozesse im Unternehmen darstellt, die für jegliche IT-Aktivitäten benötigt werden. Durch diese Hilfestellung zum Aufbau eines effizienten Prozessmodells, lässt sich COBIT® den performanceorientierten Referenzmodellen zuordnen.

Das COBIT®-Framework richtet sich konkret an die IT und unterstützt bei der Implementierung von IT-Governance in die Corporate Governance eines Unternehmens. Dazu nutzt das COBIT®-Framework die Komponenten von COSO®-ERM als Basis der COBIT®-Komponenten. Durch diese Integration entsteht ein **ganzheitlicher Ansatz** für die Ausgestaltung von IT-Governance im Unternehmen.

Wie der Begriff „ganzheitlicher Ansatz“ bereits sagt, ist COBIT® ein extrem umfangreiches Werk. Zur Umsetzung ist ein **Totalplanungsansatz** nötig, welcher extrem viel Zeit und Geld beansprucht. Ein weiteres Problem von COBIT® besteht in dem methodischen Ansatz. So werden lediglich beschränkte Handlungsempfehlungen gegeben, und hauptsächlich Hinweise, was zu tun ist und nicht im Detail wie etwas umzusetzen ist.

Auch COBIT® lässt sich als Würfel darstellen. Dabei stellen die IT- Ressourcen den Input für die 37 Prozesse dar, um die IT-Ziele zu erreichen, die wiederum aus den Geschäftsanforderungen resultieren.

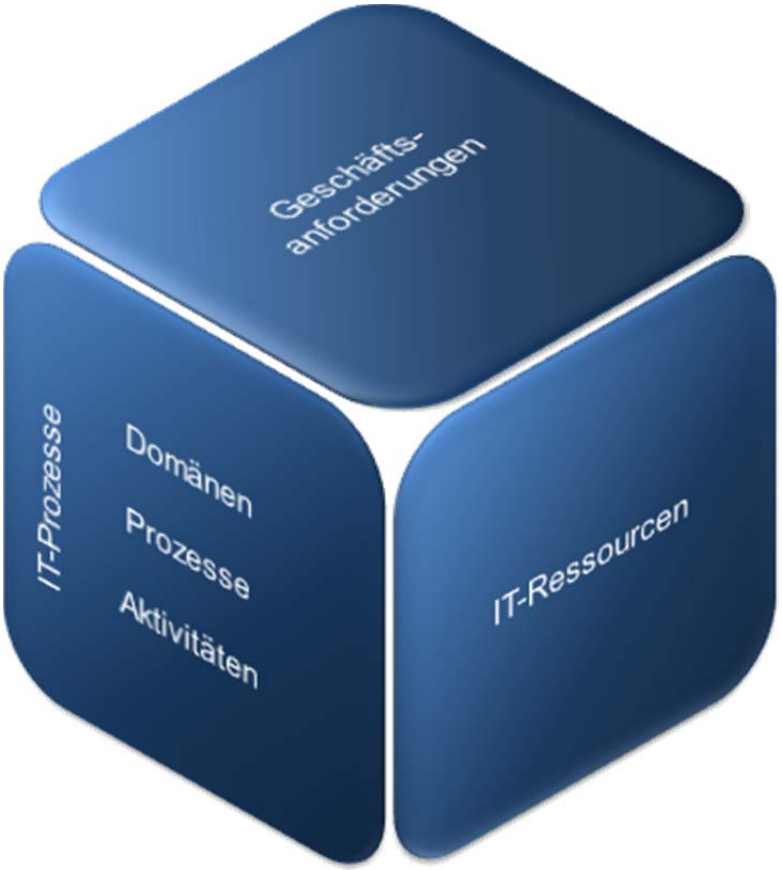


Abb. 47: Der COBIT®-Würfel

5.3.6 ITIL®

Eine britische Regierungsbehörde gab 1989 den Startschuss zur Entwicklung der Information Technology Infrastructure Library (ITIL®), da eingekaufte IT-Dienstleistungen stets eine mangelhafte Qualität aufwiesen.

Seitdem umfasst ITIL® eine Sammlung von Erfahrungen (Best-Practices) aus der Welt des IT-Service-Managements, die in Form von Best-Practice-Leitlinien niedergeschrieben wurden. Inhaltlich befassen sich diese Leitlinien mit der Planung, Überwachung und Steuerung von IT-Leistungen.

Mithilfe von fünf ITIL®-Handbüchern, die insgesamt **26 Prozesse** umfassen, ist es den IT-Mitarbeitern möglich, aus den Erfahrungen anderer zu lernen. ITIL® hat im Rahmen der ITIL®-Handbücher eine Vielzahl von **Anweisungen** formuliert. Diese helfen bei der Organisation und Definition von **Leistungserbringung** in der IT.

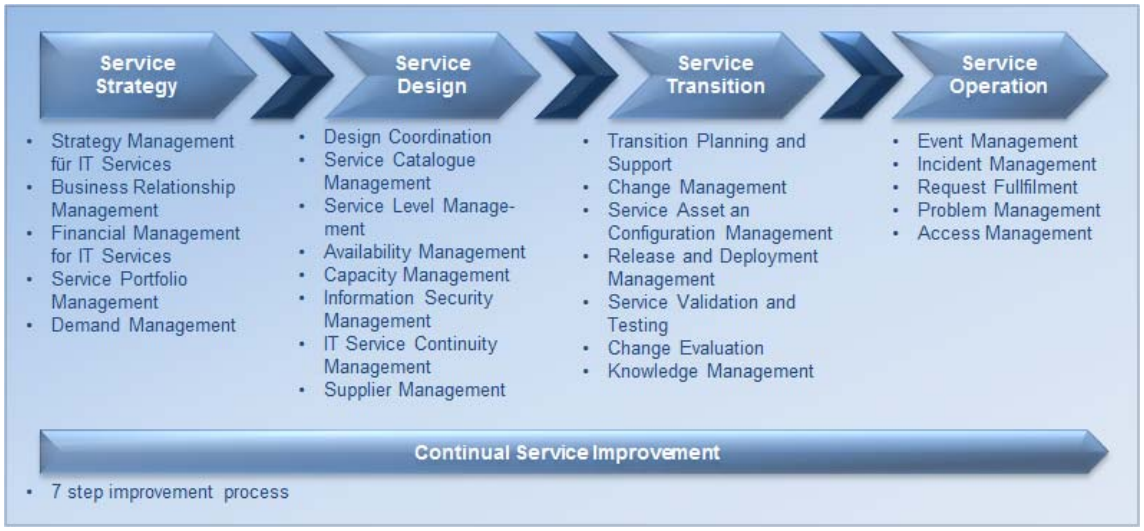


Abb. 48: Übersicht über die 26 ITIL®-Prozesse

- **Anweisungen**: Der IT-Mitarbeiter bekommt Anweisungen, **welche** Prozesse und Funktionen im Unternehmen **wie** umgesetzt werden sollen. So gibt es beispielsweise den umfangreichen Prozess "Access Management", mit dessen Hilfe Zugang auf unternehmensinterne IT-Ressourcen gewährt, beschränkt oder entzogen werden kann.
- **Leistungserbringung**: ITIL® formuliert dabei vielzählige Anforderungen an das Servicemanagement. Z. B. fordert ITIL® die Bereitstellung eines Service Desks um beispielsweise Kundenanfragen zu bearbeiten. Wie dieses Service Desk konkret einzurichten ist, formuliert ITIL® nur beschränkt.

5.3.7 ISO-Normen

Die internationalen ISO-Normen werden von der International Organisation for Standardization herausgegeben. Diese Normen versuchen zu standardisierende Sachverhalte vergleichbar und somit transparenter zu gestalten. Das Institut deckt dabei eine extrem hohe Bandbreite an zu standardisierenden Sachverhalten ab, beispielsweise die Normung der Drehrichtung von Garnen bei der Textilverarbeitung oder die Normung des IT-Sicherheits-Managements.

- **ISO 20000:** ISO 20000 enthält Prozesse, die zugehörigen Zielsetzungen und Steuerungsmaßnahmen für das IT-Service-Management. Die Cronus AG kann sich ihr IT-Service-Management nach ISO 20000 zertifizieren lassen.

  ITIL® bietet als Best Practice Hilfestellung bei der Umsetzung von ISO 20000.

  Bei einer Zertifizierung wird ein bestimmter Qualitätsstandard gemessen und eine Bescheinigung darüber ausgestellt, dass man das "Richtige" tut. Die Qualität von IT-Services (ISO 20000) oder IT-Sicherheit-Management (ISO 27001) kann mit Hilfe der Zertifizierung sichtbarer dokumentiert werden.

Es gibt verschiedene Gründe, warum ein Unternehmen das "Richtige" tun möchte. Eine Zertifizierung kann zu einem Wettbewerbsvorteil führen, da der Kunde durch eine Zertifizierung ein höheres Vertrauen an das Unternehmen hat. Bei der Umsetzung der Anforderungen aus ISO 20000 kann man auf die Best-Practice-Empfehlungen von ITIL® zurückgreifen. Wendet ein Unternehmen ITIL® an, um sich regelkonform zu Verhalten, so kann es sich durch eine Zertifizierung von ISO 20000 bescheinigen lassen, dass es tatsächlich regelkonform verhält.

- **ISO 27001**: ISO 27001 enthält Anforderungen an ein Informationssicherheits-Managementsystem (ISMS). Die Cronus AG hat die Möglichkeit sich dieses nach ISO 27001 zertifizieren zu lassen.

  ISO 27002 konkretisiert ISO 27001 und ergänzt ihn um eine Übersicht von in der Praxis erprobten Maßnahmen zur Schaffung von IT-Sicherheit.

  Die Cronus AG verfolgt mit ISO 27001 die Implementierung, Prüfung, Instandhaltung und Verbesserung eines ISMS. Als Grundlage zur Erreichung von Informationssicherheit dient dabei der PDCA-Zyklus. Dieser funktioniert im Sinne einer kontinuierlichen Verbesserung: Plan, Do, Check und Act.

5.3.8 Entscheidung für ein Referenzmodell

Bis heute wurde kein Referenzmodell von der Gesetzgebung als das "Richtige" Modell identifiziert, um mit den Anforderungen der IT-Compliance regelkonform zu sein. So muss jedes Unternehmen individuell entscheiden, welche(s) der verschiedenen Referenzmodelle eingeführt werden soll(en). Dabei ist zu bedenken, dass die Referenzmodelle dem Unternehmen individuell angepasst und in der Regel durch eigene Maßnahmen ergänzt werden müssen. Für die Cronus AG wählen wir zwischen den Frameworks und Normen aus, die in diesem Kapitel vorgestellt wurden.

- **COSO®**: Das COSO®-Framework richtet sich an die Umsetzung von Corporate Governance und hat keinen speziellen IT-Bezug. Zur Umsetzung von IT-Compliance ist es somit nur bedingt geeignet.
- **COBIT®**: Das COBIT®-Framework richtet sich allgemein an die IT-Governance und ist daher geeignet.
- **ITIL®:** ITIL® setzt das IT-Service-Management um und deckt somit einen Teilbereich der notwendigen IT-Compliance im Unternehmen ab.
- **ISO:** Mit Hilfe der vorgestellten ISO-Normen lässt sich das IT-Sicherheitsmanagement sowie der IT-Service-Management zertifizieren und dient so der IT-Compliance.

Da sich die Cronus AG durch die Zertifizierung nach **ISO 20000** einen Wettbewerbsvorteil für den Vertrieb von "Cronus MyERP" erhoffen, hat sich die Unternehmensleitung für eine Implementierung von ITIL® bzgl. des IT-Service-Managements in der Cronus AG entschieden. Für viele andere Bereiche der Cronus AG wird zusätzlich **COBIT®** benötigt, um "compliant" zu sein. Deswegen werden **ITIL® und COBIT®** in der Cronus AG implementiert. Die Umsetzung von beiden Referenzmodellen werden anhand von Teilprojekten der Gesamtimplementierung exemplarisch in den nächsten beiden WBT dargestellt. Anschließend wird im letzten WBT eine **Zertifizierung** nach ISO 20000 angestrebt.

Nachdem sich die Unternehmensleitung für die genannten Referenzmodelle entschieden hat, können diese nun in einem langwierigen Prozess umgesetzt werden. Im folgenden Kapitel wird gezeigt, wie die umgesetzten Maßnahmen überwacht und gemessen werden.

5.3.9 Implementierung der Maßnahmen

Nachdem sich die Unternehmensleitung für die genannten Referenzmodelle entschieden hat, können die Referenzmodelle in den relevanten Teilen umgesetzt werden. Es ratsam, die Prozessüberarbeitung schrittweise in Teilprojekten zu planen. Das **gesamte Projekt** zur Umsetzung der Maßnahmen, mit dem Ziel der Erreichung von IT-Compliance, kann sich dabei über mehrere Jahre ziehen und ist sehr teuer.

Zur Erinnerung ist an dieser Stelle zu betonen, dass die Umsetzung der IT-Compliance nur einen Teilbereich der Umsetzung von IT-Governance darstellt.

Die Umsetzung der IT-Governance ist wiederum lediglich ein Teilprojekt der Corporate Governance. Die Umsetzung dieser Projekte ist nicht zu unterschätzen, weder bzgl. der zeitlichen, fachlichen noch der finanziellen Belastung!

5.4 Monitoring & Messung der Wirksamkeit

5.4.1 Monitoring

Monitoring von Maßnahmen meint die Erfassung, Beobachtung und Überwachung der entwickelten Maßnahmen. Dabei wird die Einhaltung diese Maßnahmen sowohl von internen als auch externen Prüfern regelmäßig überprüft.

Die **interne Prüfung** wird **laufend** durch interne Audits durchgeführt. **Externe Prüfungen** sind hingegen punktuell bzw. **zeitpunktbezogen** und werden in der Regel von Wirtschaftsprüfern durchgeführt.

- **Interne Prüfungen**: Audits sind allgemein Untersuchungsverfahren, bei denen Maßnahmen hinsichtlich ihrer Erfüllung und Regelkonformität überprüft werden. Bei den internen Audits in der Cronus AG werden die eingeführten IT-Compliance-Maßnahmen also hinsichtlich ihrer Effektivität und Effizienz geprüft. Diese Prüfung kann entweder manuell durch Mitarbeiter der internen Revision oder automatisch durch IT-Systeme erfolgen.
- **Externe Prüfungen**: Angesichts der hohen Bedeutung von IT-Systemen für die Cronus AG, werden im Rahmen der Jahresabschlussprüfung auch die IT-Systeme durch externe Prüfer beurteilt. Besonderer Fokus liegt dabei auf der Ordnungsmäßigkeit der IT-gestützten Buchführung und der Wirksamkeit der IT-bezogenen Kontrollen. Die IT-Prüfung ist ein integraler Bestandteil der Jahresabschlussprüfung.

5.4.2 Messung der Wirksamkeit

Um abschließend die Wirksamkeit der umgesetzten Maßnahmen und die Minimierung der IT-Risiken intern zu überprüfen, müssen die Ergebnisse gemessen werden. Für eine Messung der Wirksamkeit der umgesetzten Maßnahmen gibt es jedoch keine Formel.

Wendet ein Unternehmen z. B. die Best Practices aus ITIL® zur Umsetzung der gesetzlichen und vertraglichen Anforderungen an, so kann es sich nach ISO 20000 zertifizieren lassen. Damit kann sich das Unternehmen zertifizieren lassen, dass die umgesetzten Maßnahmen wirksam sind.

Aber ISO bietet kaum weiteren Normen, die andere Referenzmodelle oder sonstige Maßnahmen zur Umsetzung der IT-Compliance zertifizieren. So bleibt den Unternehmen häufig nur die
Hoffnung, dass alles richtig gemacht wird und stets bemüht zu sein die Lücke zwischen der Soll- und Ist-Analyse weitgehend zu schließen.
Im Rahmen der Messung der Wirksamkeit der Maßnahmen wird Vollständigkeit der Umsetzung von IT-Compliance festgestellt. Da an dieser Stelle in der Regel keine vollständige Im-

plementierung von IT-Compliance festzustellen ist, muss eine erneute Soll-Analyse erfolgen. Dort wird geprüft, ob sich die Vorgaben (Gesetze, Verträge etc.) verändert haben. Der Prozess der Implementierung von IT-Compliance ist kein einmaliges, sondern ein mehrstufiges Projekt. Dieser Zyklus im Umsetzungsplan schärft das Bewusstsein innerhalb der Cronus AG für die Bedeutung von IT-Compliance und führt zu einer kontinuierlichen Verbesserung.

5.4.3 Ende des Einführungsprojekts

Das Einführungsprojekt "Umsetzung von IT-Compliance" in der Cronus AG kann mit der Phase "Monitoring & Messung der Wirksamkeit" abgeschlossen werden. Jedoch ist an dieser Stelle die Umsetzung noch lange nicht abgeschlossen. Die Umsetzung von IT-Compliance ist nun ein Prozess, der kontinuierlich durchgeführt werden muss. Nur so kann die Cronus AG langfristig **regelkonform** mit den internen und externen Vorgaben sein.

Da wir während der Ist-Analyse festgestellt haben, dass die Cronus AG noch nicht regelkonform mit allen internen und externen Vorgaben ist, muss im Anschluss an das Projektende eine erneute Situationsanalyse erfolgen. Erst wenn die Situationsanalyse ergibt, dass wir uns regelkonform verhalten, wird ein neuer Prozess gestartet. Dieser Prozess enthält eine periodische Überprüfung der internen und externen Vorgaben, ob sich die relevanten Gesetze, Verträge, Referenzmodelle etc. der Soll-Analyse geändert haben.

Abb. 49: Prozess zur Überprüfung der externen und internen Vorgaben

5.4.4 Zusammenfassung und Ausblick

In diesem WBT haben wir die verschiedenen Phasen eines beispielhaften Plans zur Implementierung von IT-Compliance kennengelernt. Der in diesem WBT vorgestellte Zyklus ist nicht als Standardvorgehen zu verstehen, sondern bietet eine mögliche Herangehensweise an. Wichtiger Bestandteil eines jeden Plans zur Umsetzung von IT-Compliance, ist das Unternehmen von einer periodischen Überarbeitung zu überzeugen, um eine stetige Verbesserung erreichen zu können.

In den nächsten zwei WBT wird die Umsetzung von ITIL® und COBIT® anhand von beispielhaften Teilprojekten der Gesamtimplementierung in der Cronus AG dargestellt. Anschließend wird im letzten WBT eine Zertifizierung nach ISO 20000 angestrebt.

5.5 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	Wie werden die Phasen der Situationsanalyse in der Cronus AG genannt?		
	Soll-Analyse		
	Vorgaben identifizieren		
	Ist-Situation		
	Konzeption & Implementierung		
	Soll-Ist-Vergleich		
2	Eine regelmäßige Wiederholung aller Prozessschritte ist nötig, um eine kontinuierliche Verbesserung zu erreichen.		
	Richtig		
	Falsch		
3	In der Phase „Soll-Analyse“ wird geprüft, welche Vorgaben bereits umgesetzt wurden.		
	Richtig		
	Falsch		
4	„Umsetzung der IT-Compliance“ lässt sich nur durchführen, wenn das Projekt in der obersten Führungsebene angesiedelt ist und alle Betroffenen zusammenarbeiten.		
	Richtig		
	Falsch		
5	IT-Compliance ist ein einmaliger, langfristiger Prozess.		
	Richtig		
	Falsch		
6	Der IT-Compliance-Officer ist die Schnittstelle zwischen Compliance und IT. So berät er z. B. die Mitarbeiter der IT-Abteilung bei der Systementwicklung und –überarbeitung hinsichtlich der Compliance-Fragestellungen.		
	Richtig		
	Falsch		

7	Das Ergebnis eines Soll-Ist-Vergleichs kann drei verschiedene Ausprägungen haben:		
	Die Ist-Analyse hat ergeben, dass bis dato einige Maßnahmen zur Erreichung von IT-Compliance eingeleitet worden sind, diese sind aber nicht effizient/ effektiv.		
	Die Ist-Analyse hat ergeben, dass wir alle Maßnahmen für eine vollständige IT-Compliance etabliert haben. Diese sind effizient und effektiv. Es besteht zunächst kein weiterer Handlungsbedarf.		
	Die Soll-Analyse hat ergeben, dass bis dato keine Maßnahmen zur Erreichung von IT-Compliance eingeleitet worden sind.		
	Die Ist-Analyse hat ergeben, dass bis dato keine Maßnahmen zur Erreichung von IT-Compliance eingeleitet worden sind.		
8	Mit Hilfe der entwickelten To-Do-Liste werden in der Konzeptionsphase Maßnahmen entwickelt, mit denen IT-Compliance erreicht werden soll.		
	Richtig		
	Falsch		
9	Die Ausrichtung der IT-Compliance an etablierten gesetzlichen Vorgaben ist aus zwei Gründen empfehlenswert: Einerseits kann die Anwendung den Enthaftungsbeweis für die Unternehmensleitung liefern, andererseits liefern Best-Practices auch einfache Hinweise zur konkreten Umsetzung von Compliance-Vorgaben.		
	Richtig		
	Falsch		

10	Welche Aussagen sind richtig?		
	Eigene selbstentwickelte Maßnahmen haben unter anderem den Vorteil, dass der Nachweis eines ordentlichen Geschäftsbetriebs wenig aufwendig ist.		
	Ein Nachteil eigener Maßnahmen ist, dass die Entwicklung dieser Maßnahmen extrem aufwendig ist.		
	Ein Vorteil von Maßnahmen aus Frameworks ist, dass die Maßnahmen anerkannt sind und Erläuterungen zur Umsetzung enthalten.		
	Ein Nachteil von Maßnahmen aus Frameworks ist, dass die Maßnahmen allgemein formuliert sind und noch auf die speziellen Anforderungen der Cronus AG angepasst werden müssen.		
11	ITIL® ist ein typisches Referenzmodell, welches ausschließlich der Performancesichtweise zuzuordnen ist.		
	Richtig		
	Falsch		
12	Hält man sich an COSO®-ERM-Referenzmodell, so ist man gesetzeskonform mit SOX.		
	Richtig		
	Falsch		
13	Das COBIT®-Framework hilft bei der Umsetzung von Corporate Governance in die IT-Governance.		
	Richtig		
	Falsch		
14	ITIL® kann als Best Practice bei der Erfüllung der Anforderungen von ISO/IEC 20000 helfen.		
	Richtig		
	Falsch		
15	Im Rahmen des Monitoring der entwickelten Maßnahmen werden regelmäßige Prüfungen durchgeführt. Prüfungen können durch welche Prüfer durchgeführt werden?		
	Den Betriebsrat		
	Externe Wirtschaftsprüfer		
	Interne Wirtschaftsprüfer		
	Interne Audits		

Tab. 6. Übungsfragen WBT 05 – Umsetzung der IT-Compliance

6 Fallstudie COBIT®

6.1 Einführung in COBIT®

6.1.1 Einleitung

Ich, Francesco Palla, bin der CIO der Cronus AG. Gemeinsam mit unserem IT-Compliance-Officer bin ich für die Umsetzung von IT-Compliance in der Cronus AG verantwortlich. Im letzten WBT haben wir uns für eine Implementierung mit Hilfe der Referenzmodelle COBIT® und ITIL® entschieden.

Wie COBIT® in der Cronus AG umgesetzt wird, soll an einem beispielhaften Teilprojekt im Laufe von diesem WBT gezeigt werden.

6.1.2 Was ist COBIT®?

"Control Objectives for Information and Related Technology®" (COBIT®) bietet den Unternehmen Unterstützung, um die IT-Ressourcen im Unternehmen **effizienter** und **effektiver** zu managen. Eine wesentliche Komponente von COBIT® ist das **Prozessreferenzmodell**, welches alle relevanten IT-Prozesse im Unternehmen darstellt. Dieses Prozessreferenzmodell dient als Hilfestellung zur effizienten **Prozessumsetzung** innerhalb eines Unternehmens.

Das COBIT®-Prozessreferenzmodell stellt die 37 COBIT®-Prozesse dar:

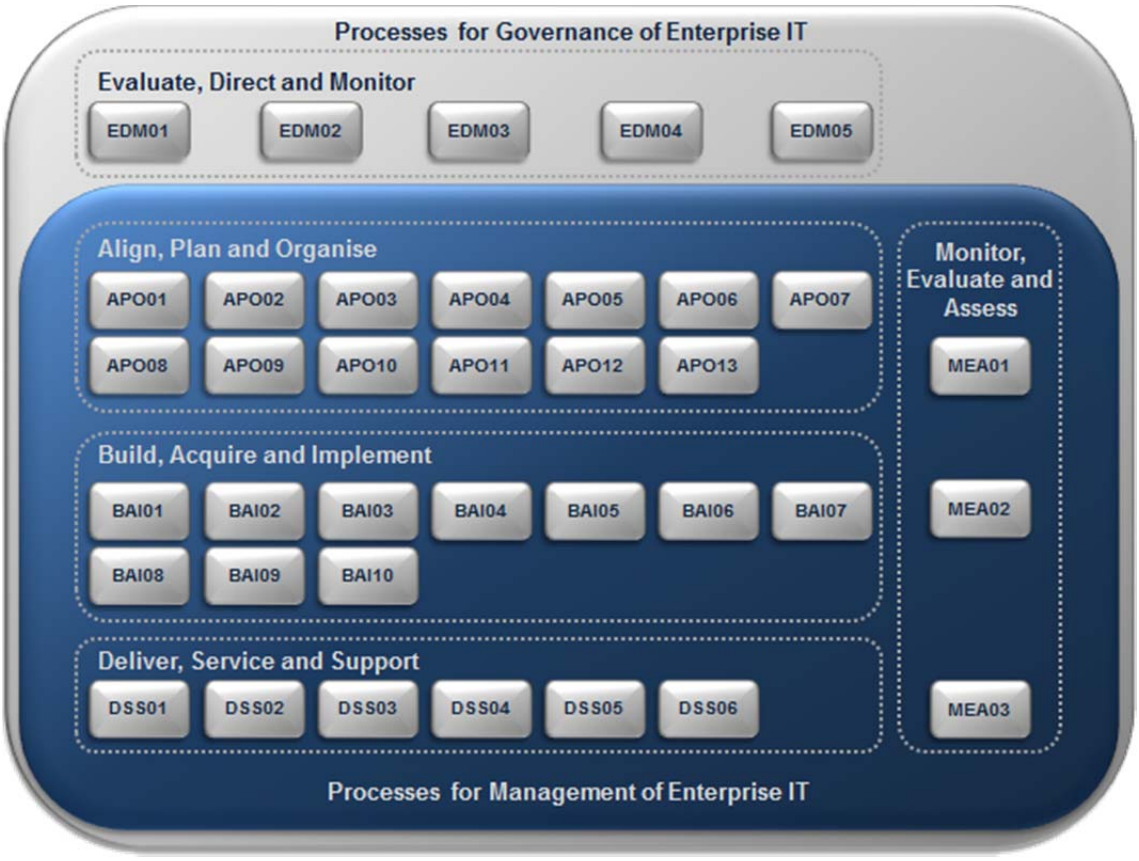


Abb. 50: Prozessreferenzmodell von COBIT®

Die vollständige Umsetzung von COBIT® beansprucht extrem viel Zeit und Geld. Aus diesem Grund wird COBIT® schrittweise umgesetzt.

Ein weiteres Problem von COBIT® besteht in dem methodischen Ansatz. So werden lediglich beschränkte Handlungsempfehlungen gegeben, die hauptsächlich Hinweise darüber beinhalten, was zu tun ist und nicht im Detail wie etwas umzusetzen ist.

6.1.3 Umsetzung von IT-Governance mit COBIT®

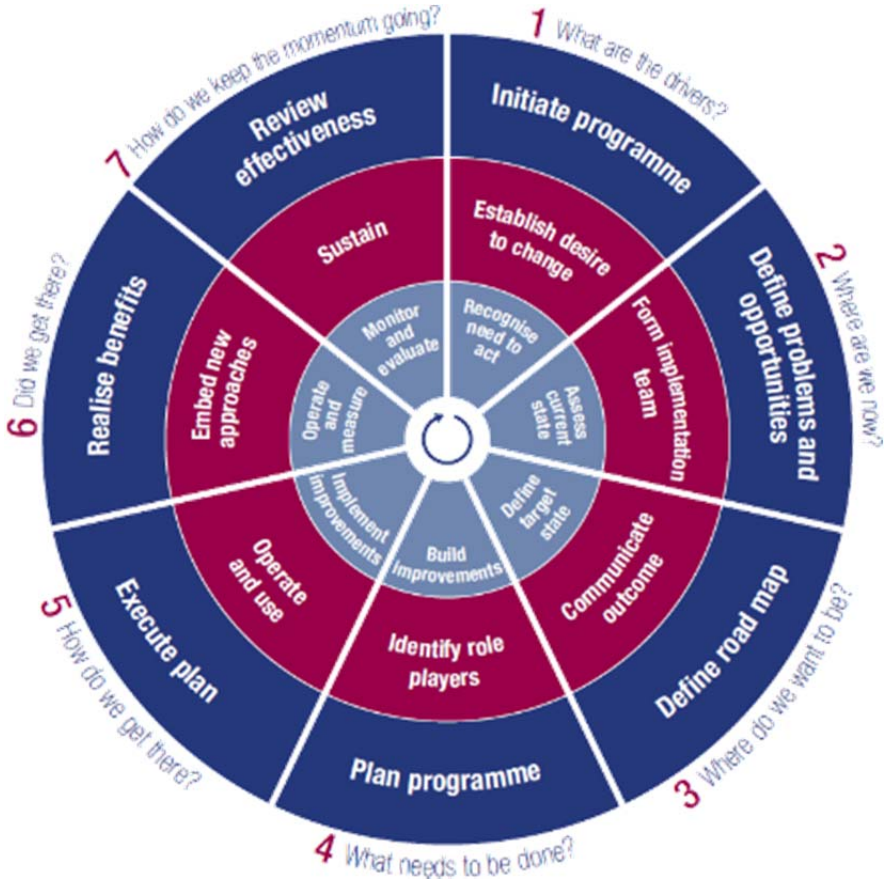


Abb. 51: Umsetzungsleitfaden von COBIT® (Schritte)

Der hier dargestellte Umsetzungsleitfaden soll als Hilfestellung bei der komplexen Umsetzung von IT-Governance mit COBIT® dienen. Dazu werden bewährte Verfahren zur Umsetzung von Großprojekten in Form eines Zyklus dargestellt. Die Verfahren werden unterteilt in **Schichten** und **Schritte**.

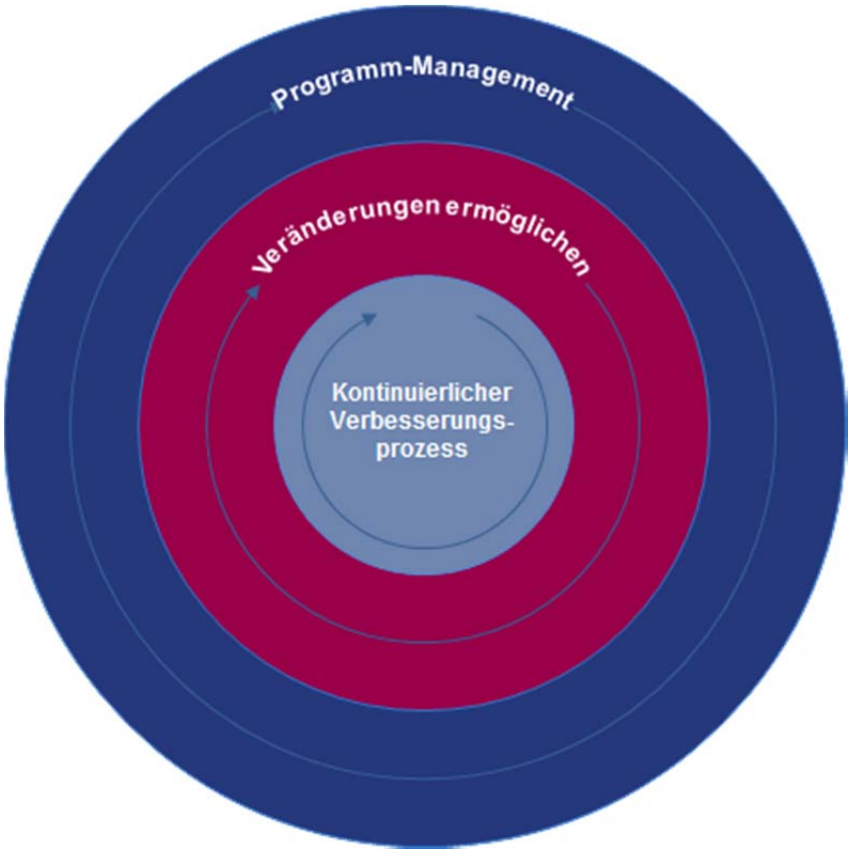


Abb. 52: Schichten des Umsetzungsleitfadens von COBIT®

Die drei Schichten bestehen aus dem Programmmanagement, Änderungsmanagement und kontinuierlichen Verbesserungsmanagement. Jeder der sieben Schritte umfasst die drei Schichten sowie Handlungsanweisungen.

- **Schritt 1: Welche Treiber gibt es?** Im ersten Schritt geht es darum, den Handlungsbedarf für die Umsetzung von IT-Governance mit Hilfe von COBIT® zu erkennen, das Programm zu initiieren und im Management den Wunsch nach Veränderung zu schaffen. Dieser Wunsch nach Veränderung ist in der Cronus AG bereits vorhanden. Wie und warum das bereits geschehen ist, haben Sie in "WBT 05 - IT-Compliance" gelernt.
- **Schritt 2: Wo befinden wir uns jetzt?** Im zweiten Schritt wird der gegenwärtige Zustand der IT-Governance beurteilt. In der Cronus AG haben wir eine Analyse der Ist- und Soll-Situation erstellt (vgl. "WBT 05 - IT-Compliance") mit dem Ergebnis, dass viele Anforderungen von IT-Compliance und IT-Governance noch nicht erfüllt sind. Es wird ein Implementierungsteam zur Umsetzung von COBIT® in der Cronus AG zusammengestellt.
- **Schritt 3: Wo möchten wir stehen?** Ziel des dritten Schritts ist die Ausarbeitung eines detaillierten Plans, wie COBIT® in der Cronus AG umgesetzt werden soll. Das Management der Cronus AG hat sich entschieden, COBIT® schrittweise einzuführen.

Als Pilotprozess soll der COBIT®-Prozess "BAI06 - Manage Changes" eingeführt werden. Dieses Ergebnis wird schnellstmöglich an alle beteiligten Mitarbeiter kommuniziert.

- **Schritt 4: Was muss getan werden?** Im vierten Schritt werden die Verantwortlichkeiten für die Umsetzung von IT-Governance mit Hilfe von COBIT® festgelegt. Einige der nun verantwortlichen Mitarbeiter müssen zunächst eine Schulung zu COBIT® durchlaufen. Weiterhin sollen kurzfristig erreichbare Nutzen identifiziert werden, um den Anspruchsgruppen zeigen zu können, dass man auf dem richtigen Weg ist. Weiterhin wird hier ein Plan zur Umsetzung einzelner Projekte bzw. Prozesse erstellt.
- **Schritt 5: Wie kommen wir dorthin?** Im fünften Schritt des Vorgehensmodells wird nun der vorab erstellte Umsetzungsplan und der damit verbundene Nutzen aus dem vierten Schritte realisiert.
- **Schritt 6: Sind wir angekommen?** Im sechsten Schritt des Umsetzungsleitfadens wird nun überprüft, ob die Ziele erreicht sind und wo es noch Verbesserungspotentiale gibt. Was in Rahmen der Umsetzung gelernt wurde, soll dokumentiert werden.
- **Schritt 7: Wie erhalten wir die Dynamik aufrecht?** Der siebte Schritt legt den Fokus darauf, wie ein Anstoß gegeben werden kann, dass der Zyklus erneut durchlaufen wird und so eine kontinuierliche Verbesserung erreicht werden kann. Dazu wird die Effektivität des vorangegangenen Durchlaufs beurteilt und geprüft ob ein Lerneffekt eingetreten ist.

Der Zyklus ist als Hilfestellung zu interpretieren, um bei komplexen Großprojekten nicht das Große und Ganze aus dem Blick zu verlieren. Jedes Unternehmen kann die Umsetzung von IT-Governance mit COBIT® alternativ auch völlig frei gestalten.

6.1.4 Komponenten von COBIT®

COBIT® ist ein sehr komplexes und umfangreiches Framework, das versucht sowohl für die IT-Spezialisten als auch für das Management verständlich zu sein. Der COBIT®-Würfel zeigt die damit verbundenen Dimensionen.

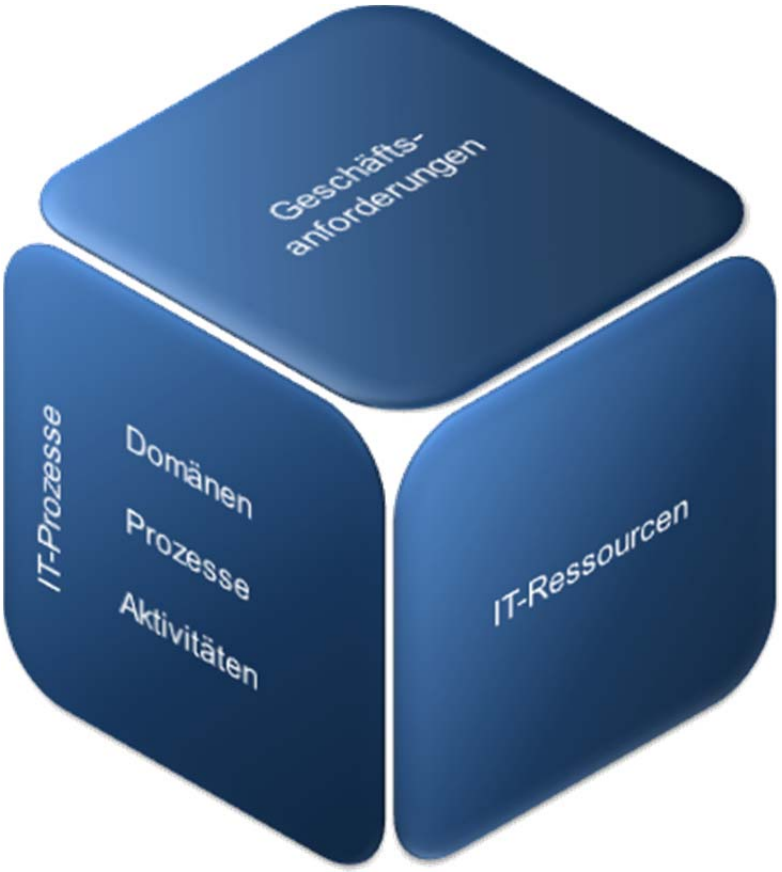


Abb. 53: Der COBIT®-Würfel

COBIT® lässt sich aus drei verschiedenen Sichtweisen betrachten. Die **Geschäftsanforderungen** sind als Ausgangspunkt zu sehen. Aus ihnen werden die **IT-Ressourcen** abgeleitet, die benötigt werden, um die **IT-Prozesse** umzusetzen.

- **Geschäftsanforderungen**: Die verschiedenen Fachbereiche der Cronus AG geben die Geschäftsanforderungen vor. Diese Anforderungen müssen von der IT-Abteilung durch den Einsatz von IT umgesetzt werden. Dabei sind folgende Kriterien zu erfüllen: Effektivität, Effizienz, Vertraulichkeit, Integrität, Verfügbarkeit, Compliance und Zuverlässigkeit.
- Der Fachbereich Vertrieb stellt beispielsweise die Anforderung an die IT-Abteilung, dass die Vertriebs-Mitarbeiter außer Haus stets eine Anbindung an die unternehmenszentralen Datenbestände haben sollen. So können Sie beim Kunden Informationen über Kosten, Lieferzeiten, Rabatt etc. für alle Möbel der Cronus AG weitergeben.
- **IT-Ressourcen**: Zur Realisierung der Geschäftsanforderungen werden verschiedene IT-Ressourcen als Hilfsmittel zur Umsetzung benötigt. IT-Ressourcen nach COBIT® sind: Mitarbeiter, Anwendungen, Informationen / Daten, Infrastruktur / Technologie.
- Um die Geschäftsanforderungen der Vertriebs-Abteilung erfüllen zu können, werden IT-Ressourcen benötigt. Es wird ein Mitarbeiter der IT-Abteilung benötigt, der für die

Bereitstellung der Daten verantwortlich ist. Weiterhin muss dem Mitarbeiter der Vertriebsabteilung ein Laptop mit Anbindung an ein mobiles Netzwerk zur Verfügung gestellt werden.

- **IT-Prozesse**: Jeder der 37 COBIT®-Referenzprozesse wird durch verkettete Aktivitäten ausgeführt. Die Prozesse lassen sich inhaltlich zu fünf Domänen gruppieren. Die Domänen sind: Evaluate, Direct and Monitor (EDM); Align, Plan and Organise (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); Monitor, Evaluate and Assess (MEA).
- Die Geschäftsanforderung, dass die Mitarbeiter der Vertriebsabteilung jederzeit und außer Haus auf die unternehmenszentralen Datenbestände zugreifen können, lässt sich der Domäne APO zuweisen.

6.1.5 Das Prozessreferenzmodell von COBIT®

Im **COBIT®-Prozessreferenzmodell** werden alle typischen Governance- und Managementprozesse vollständig und umfassend definiert. Jedes Unternehmen muss die COBIT®-Prozesse den unternehmensindividuellen Anforderungen anpassen.

Die **37 COBIT®-Prozesse** werden, wie in der Grafik dargestellt, zu **5 Domänen** gruppiert.

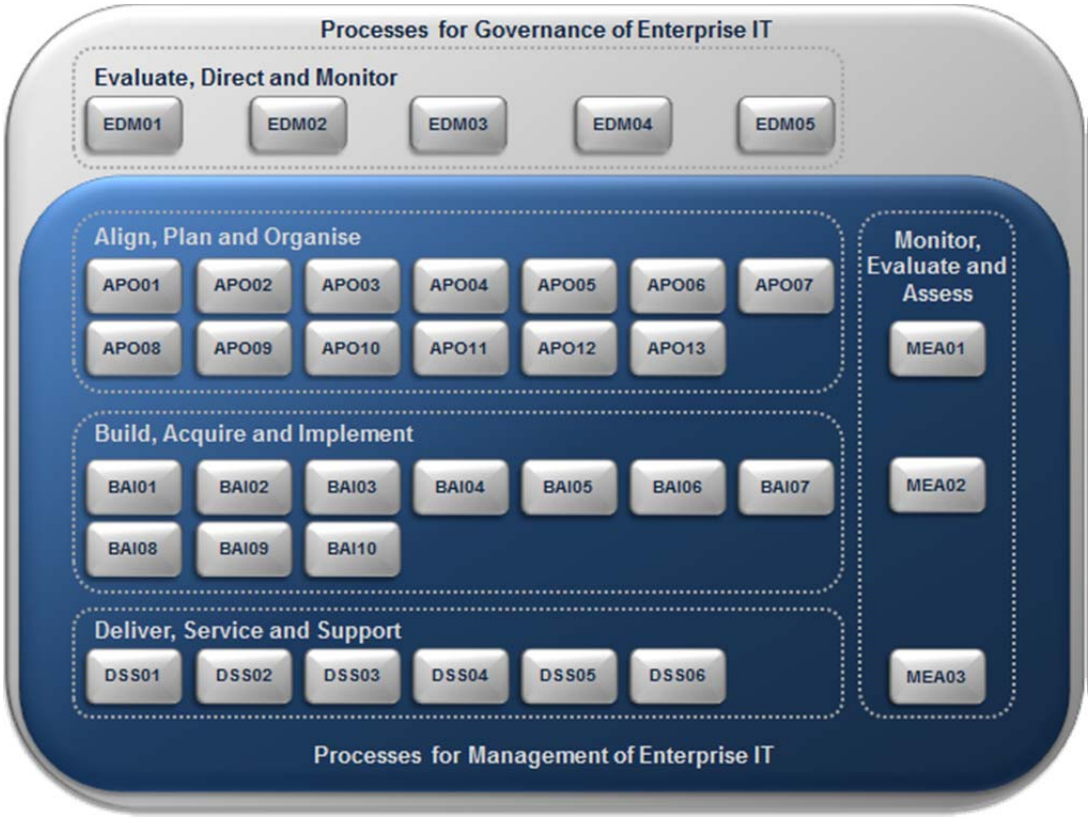


Abb. 54: Das Prozessreferenzmodell von COBIT®

6.1.6 Bestandteile des Prozessreferenzmodells von COBIT®

Das COBIT®-Prozessreferenzmodell umfasst **fünf Governance-Prozesse** (Domäne: Evaluate, Direct and Monitor) und **32 Management-Prozesse**.

- **Die fünf Governance-Prozesse**: Die fünf übergeordneten Governance-Prozesse stellen sicher, dass die Anforderungen, Rahmenbedingungen und Möglichkeiten der Anspruchsgruppen evaluiert werden, um die Unternehmensziele zu erreichen. Die Governance-Prozesse lassen sich zu der Domäne "Evaluate, Direct and Monitor (EDM)" zusammenfassen. Die Governance-Prozesse sind:
    - EDM01 Ensure Governance Framework Setting and Maintenance
    - EDM02 Ensure Benefits Delivery
    - EDM03 Ensure Risk Optimisation
    - EDM04 Ensure Resource Optimisation
    - EDM05 Ensure Stakeholder Transparency

Abb. 55: Die fünf Governance-Prozesse des COBIT®-Prozessreferenzmodells

- **Die 32 Management-Prozesse**: Die Management-Prozesse befassen sich primär mit der Planung, Entwicklung, dem Betrieb und der Überwachung der IT-Ressourcen im Rahmen der von der Governance vorgegebenen Richtung, um die Unternehmensziele zu erreichen. Beispiele dafür sind:

- APO12 Manage Risk
- BAI06 Manage Changes
- DSS05 Manage Security Services

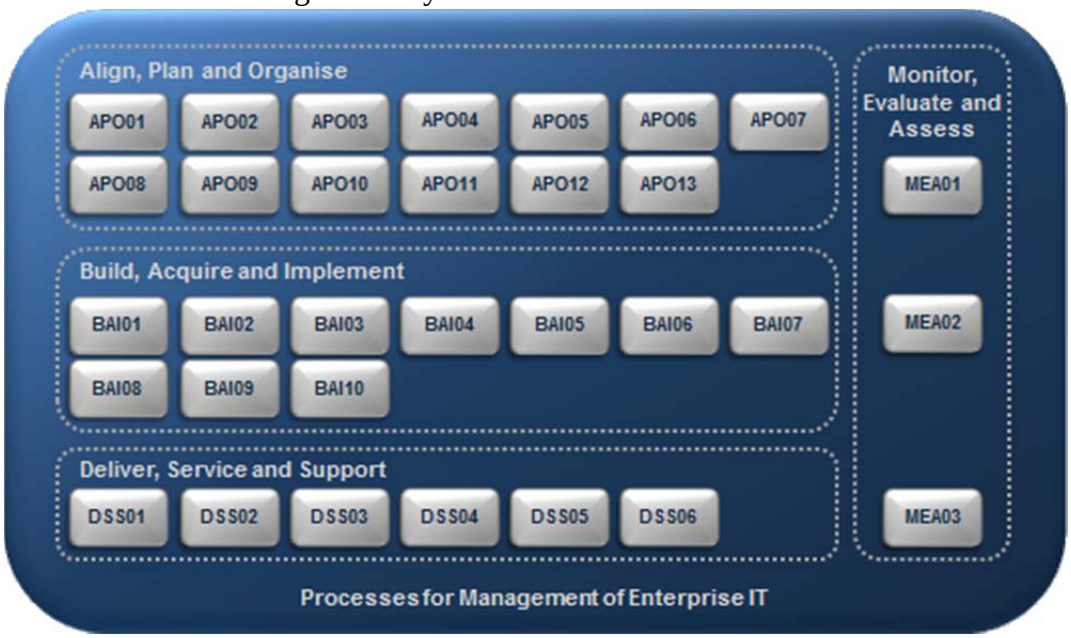


Abb. 56: Die 32 Management-Prozesse des COBIT®-Prozessreferenzmodells

6.1.7 Was ist ein COBIT®-Prozess?

COBIT® umfasst insgesamt **37 Referenzprozesse**, die einzelnen Prozesse bestehen aus einer Verkettung von Aktivitäten. Der Fokus der Aktivitätsbeschreibungen liegt auf dem "Was" getan werden muss, nicht "wie" die Aktivitäten konkret im Unternehmen umzusetzen sind.

Die Aktivitäten der **COBIT®-Prozesse** dienen der Cronus AG als Referenz, was umgesetzt werden muss, um COBIT®-konform zu sein. Die Referenzprozesse und -aktivitäten müssen an die spezifischen Anforderungen der Cronus AG angepasst werden.

Ein COBIT®-Prozess setzt sich aus folgenden Elementen zusammen:

- Prozessidentifizierung
- Prozessbeschreibung und -zweck
- IT-bezogene und Prozessziele
- RACI-Chart
- Prozessanforderungen
- Inputs und Outputs
- Prozessaktivitäten
- Referenzmaterial

Auf die einzelnen Prozesselemente wird in diesem WBT detailliert eingegangen.

6.1.8 Schrittweise COBIT® einführen

Die vollständige Umsetzung von COBIT® beansprucht extrem viel Zeit und Geld. Aus diesem Grund wird COBIT® schrittweise in der Cronus AG umgesetzt. Im ersten Schritt soll zunächst ein Pilotprozess in der Cronus AG umgesetzt werden. Als Pilotprozess wurde das Change Management ausgewählt, da ich, Francesco Palla vermute, dass die Anpassung des Prozesses an die Vorschläge von COBIT® der Cronus AG einen hohen Nutzen bringt.

6.2 Umsetzung des COBIT®-Prozesses "BAI06 - Manage Changes"

6.2.1 Einleitung

Als CIO der Cronus AG leite ich das Projekt der Implementierung von COBIT®. In diesem Kapitel werde ich mich damit auseinandersetzen, wie an IT-Lösungen COBIT®-konforme Änderungen vollzogen werden. Wie in den vorherigen WBT bereits berichtet, nutzt die Cronus AG das ERP-System "Cronus myERP". Die Entwicklungsabteilung hat ein Release (neu veröffentlichte Version der Software) für das intern genutzte ERP-System entwickelt. Dieses neue Release beinhält die Umstellung der Kontodaten auf das SEPA-Verfahren. Die Einführung des neuen Releases ist eine Änderung, die den Change-Management-Prozess betrifft. Diese Einführung des Releases soll COBIT®-konform realisiert werden. Dazu werden die bereits erwähnten Prozesselemente von COBIT®-Prozesses detailliert am Beispiel des Prozesses "BAI06 - Manage Changes" betrachtet.

Die Grafik zeigt den Aufbau der Prozesselemente von COBIT®-Prozessen in COBIT®. Die Inhalte der Elemente sind prozessindividuell. Anhand des COBIT®-Prozesses "BAI06 - Manage Changes" wird gezeigt, welche Inhalte hinter den Prozesselementen stehen.

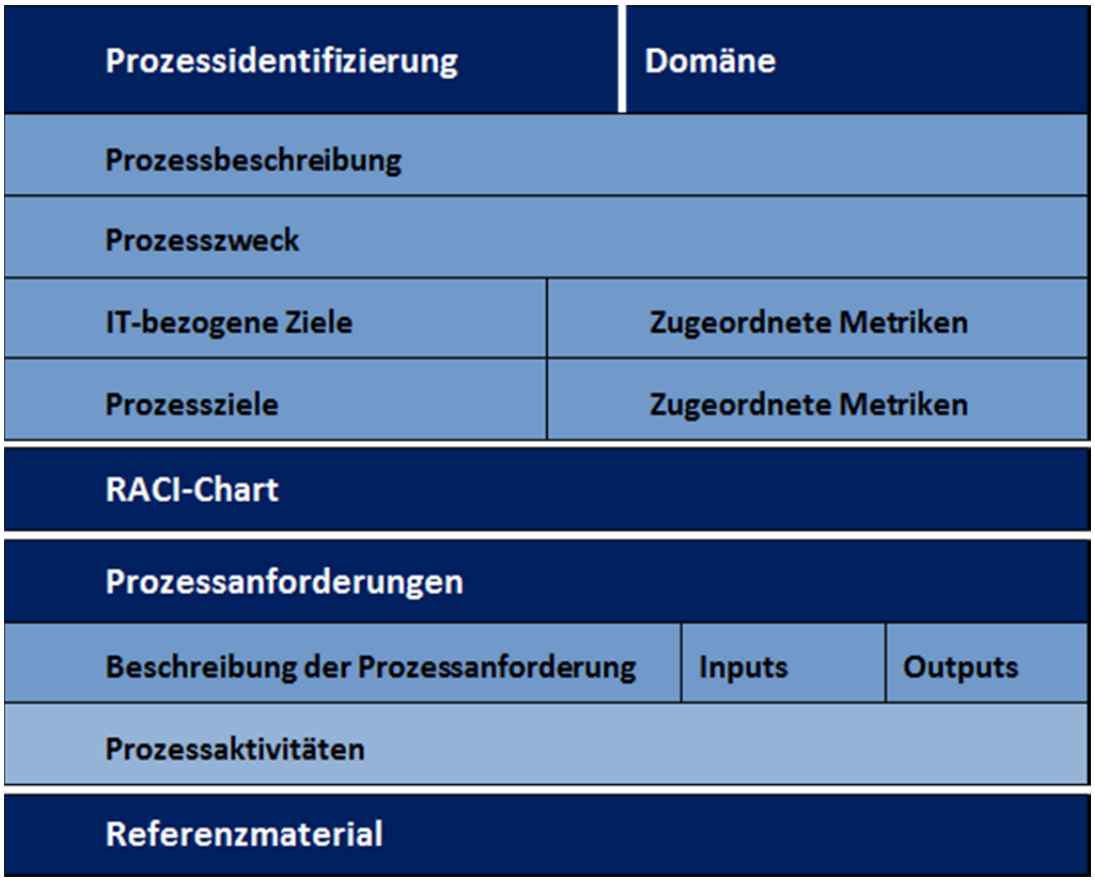


Abb. 57: Die Prozesselemente von COBIT®-Prozessen

6.2.2 Prozessidentifizierung, -beschreibung und -zweck

Jeder COBIT®-Prozess hat eine eindeutige **Prozessidentifizierung**. Diese besteht aus den Initialen der **Domäne**, also EDM, APO, BAI, DSS und MEA, gefolgt von einer **Prozessnummer**, sowie einem eindeutigen **Namen**, der das Hauptthema des Prozesses beschreibt.

Der Prozess "BAI06 - Manage Changes" wird der Domäne "Build, Acquire and Implement", also "**BAI**", zugeordnet und hat die Prozessnummer "**06**" erhalten. Der Prozess BAI06 befasst sich mit dem Managen von Änderungen und erhält somit den Namen: "Manage Changes".

Neben der Prozessidentifizierung formuliert COBIT® für jeden Prozess eine **Beschreibung und den Zweck**.

BAI06 Manage Changes	Area: Management Domain: Build, Acquire and Implement
Prozessbeschreibung Managen sämtlicher Änderungen in einer kontrollierten Art und Weise, einschließlich Standardänderungen und dringender Wartungsmaßnahmen in Bezug auf Geschäftsprozesse, Anwendungen und Infrastruktur. Damit verbunden sind außerdem Änderungsstandards und –verfahren, die Beurteilung von Auswirkungen, Priorisierung und Genehmigung, dringende Änderungen, Rückverfolgung, Berichterstattung, Abschluss und Dokumentation.	
Prozesszweck Ermöglichung einer schnellen und zuverlässigen Bereitstellung von Änderungen für den Geschäftsbetrieb sowie Minderung des Risikos, was die Beeinträchtigung der Stabilität und Integrität in der geänderten Umgebung anbelangt.	

Abb. 58: Prozessidentifizierung, -beschreibung und –zweck des COBIT®-Prozesses BAI06 Manage Changes

6.2.3 Referenzmaterial

Nahezu jeder COBIT®-Prozess verweist auf weitere Standards, gute Praktiken und Rahmenwerke, die zusätzlich Orientierung bzw. Informationen zu dem jeweiligen Prozess bieten. Der COBIT®-Prozess "BAI06 - Manage Changes" verweist auf die Norm ISO/IEC 20000 und das ITIL®-Framework.

Bei der Umsetzung von jedem Prozesselement sollen die beteiligten Mitarbeiter der Cronus AG ständig die Referenzmaterialien prüfen. Die Prüfung empfiehlt sich, da sich die Referenzmaterialien in diesem Fall viel detaillierter mit dem Change Management auseinandersetzen. Der Prozess wird in COBIT® auf drei Seiten beschrieben, ITIL® hingegen befasst sich mit diesem Prozess auf ca. 30 Seiten.

So kann durch die regelmäßige Prüfung der Referenzen die Wahrscheinlichkeit gesteigert werden, dass die beste Lösung für die Prozessumsetzung gefunden wird.

BAI06 Related Guidance	
Related Standard	**Detailed Reference**
ISO/IEC 20000	9.2 Change management
ITIL V3 2011	13. Change Management

Abb. 59: Referenzmaterialien für den COBIT®-Prozess BAI06 Manage Changes

6.2.4 Prozessziele und Metriken

Jeder COBIT®-Prozess unterstützen verschiedene Ziele. Diese sind prozessspezifisch und werden durch die Aktivitäten eines Prozesses erreicht. Der COBIT®-Prozess "BAI06 - Manage Changes" hat vier **Prozessziele**.

Die Prozessziele für den Prozess "BAI06 - Manage Changes" sind:

- Genehmigte Änderungen erfolgen rechtzeitig und nahezu fehlerfrei.
- Die Beurteilung von Auswirkungen (Folgenabschätzung) zeigt die Auswirkungen der Änderung auf alle betroffenen Komponenten.
- Bei ad hoc durchgeführten Notfalländerungen wird die Änderungen erst im Anschluss überprüft und genehmigt.
- Relevante Anspruchsgruppen werden über alle Aspekte der Änderung auf dem Laufenden gehalten.

COBIT® ordnet den Prozesszielen **Metriken** zu, die Hinweise zur Messung des Erreichungsgrades der Ziele geben sollen. Jedes Unternehmen muss die vorgeschlagenen Metriken prüfen und sich für die individuell relevanten und erreichbaren Metriken entscheiden.

Mit Hilfe der definierten Ziele und Metriken kann überprüft werden, ob der Prozess optimiert wurde oder durch die Änderung keine Verbesserung erfolgen konnte.

Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Authorised changes are made in a timely manner and with minimal errors.	• Amount of rework caused by failed changes • Reduced time and effort required to make changes • Number and age of backlogged change requests
2. Impact assessments reveal the effect of the change on all affected components.	• Percent of unsuccessful changes due to inadequate impact assessments
3. All emergency changes are reviewed and authorised after the change.	• Percent of total changes that are emergency fixes • Number of emergency changes not authorised after the change
4. Key stakeholders are kept informed of all aspects of the change.	• Stakeholder feedback ratings on satisfaction with communications

Abb. 60: Prozessziele und Metriken vom COBIT®-Prozess BAI06 Manage Changes

6.2.5 Prozessziele der Cronus AG

Jeder COBIT®-Prozess hat das Ziel verschiedene Ziele zu erreichen. "BAI06 - Manage Changes" verfolgt vier **prozessspezifische Ziele**. Die Ziele werden auf die unternehmensspezifischen Anforderungen der Cronus AG geprüft und eventuell anzupassen.

Die von COBIT® vorgeschlagenen Prozessziele, wurden vom CIO kritisch geprüft. Am Beispiel der Einführung des Releases unserer intern genutzten ERP-Software "Cronus myERP" ist ihm aufgefallen, dass die Prozessziele den Anforderungen der Cronus AG nicht genügen.

Denn die Prüfung des Referenzmaterials hat ergeben, dass bei einem umfangreichen Release von "Cronus myERP" das System jederzeit auf den letzten korrekten **Zustand zurücksetzbar** sein sollte.

Z. B. kann bei nachträglich festgestellten Fehlern das System auf den letzten korrekten Zustand zurückgesetzt werden. So kann das bisherige Service-Level (99,997% Verfügbarkeit während der Geschäftszeiten) durch die Reaktivierung des veralteten Releases eingehalten werden.

So wird die Liste der von COBIT® vorgeschlagenen Prozessziele um das Ziel aus der ISO-Norm 20000 (Abschnitt 9.2 - Change Management) erweitert.

Daraus ergibt sich für die Cronus AG folgende **Liste der Prozessziele und Metriken**.

Prozessziele	Zugeordnete Metriken
Genehmigte Änderungen erfolgen rechtzeitig und nahezu fehlerfrei.	- Umfang der Nacharbeit wegen fehlerhaften Änderungen - Änderungen werden schneller und mit wenig Aufwand durchgeführt. - Anzahl und Alter der aufgelaufenen Änderungsanträge.
Die Beurteilung von Auswirkungen (Folgenabschätzung) zeigen die Auswirkungen der Änderung auf alle betroffenen Komponenten.	- Anteil der erfolglosen Änderungen, die auf eine inadäquate Beurteilung der Auswirkungen zurückzuführen sind
Alle Notfalländerungen werden im Anschluss an die Änderungen überprüft und genehmigt.	- Anteil der dringenden Änderungen bezogen auf die Gesamtzahl der Änderungen - Anzahl der dringenden Änderungen, die im Anschluss an die Änderung nicht genehmigt werden.
Relevante Anspruchsgruppen werden über alle Aspekte der Änderung auf dem Laufenden gehalten.	- Beurteilung der Zufriedenheit mit der Kommunikation in Rückmeldung der Anspruchsgruppen
Rücksetzbarkeit der Änderungen auf den letzten korrekten Zustand.	- Anzahl der Rücksetzungen auf den letzten korrekten Zustand.

Abb. 61: Prozessziele der Cronus AG für den COBIT®-Prozess

6.2.6 IT-bezogene Ziele und Metriken

Die Prozessziele leisten einen Beitrag zu den **IT-bezogenen Zielen**. Diese IT-bezogenen Ziele werden von COBIT® vorgeschlagen und sind nicht prozessspezifisch. Ein IT-bezogenes Ziel kann einerseits durch mehrere COBIT®-Prozesse unterstützt werden, andererseits kann ein Prozess mehrere IT-Ziele unterstützen. Es handelt sich also um eine n:m-Beziehung. COBIT® schlägt insgesamt 17 IT-Ziele vor.

Der Prozess "BAI06 - Manage Changes" unterstützt primär **drei der insgesamt 17 IT-Ziele**. Die 17 IT-bezogenen Ziele werden von COBIT® vorgeschlagen, müssen aber unternehmensspezifisch angepasst werden.

Diese drei, von COBIT® vorgeschlagenen IT-bezogenen Ziele, werden durch den Prozess "BAI06 - Manage Changes" unterstützt:

- **Management der**, mit der IT verbundenen, **Geschäftsrisiken**:

  Das Managen der, mit der IT verbundenen Geschäftsrisiken, wird unter anderem durch das Prozessziel, dass mögliche Auswirkungen von Änderungen beurteilt werden sollen, unterstützt. Wenn Risiken bei geplanten Änderungen nicht gesteuert werden, kann es zu Fehlern kommen (vgl. WBT 1 - Einführung in IT-Governance), die einen negativen Einfluss auf das Image und die Wirtschaftsleistung eines Unternehmens haben können.

- **Bereitstellen von IT-Services**, die sich mit den Geschäftsanforderungen decken:

  Das Bereitstellen von IT-Services im Einklang mit den Geschäftsanforderungen, wird z. B. durch das Prozessziel, dass die relevanten Anspruchsgruppen über alle Aspekte einer Änderung auf dem Laufenden gehalten werden sollen, unterstützt. So kann vermieden werden, dass eine Änderung nicht mit den übergeordneten Unternehmenszielen konform ist.

- **Gewährleisten der Sicherheit** von Informationen, Prozessinfrastruktur und Anwendungen:

  Das Gewährleisten der Sicherheit von Informationen, Prozessinfrastruktur und Anwendungen wird z. B. durch das ISO-Prozessziel, dass die Änderung jederzeit auf den letzten korrekten Zustand zurücksetzbar sein soll, unterstützt. So kann vermieden werden, dass eine fehlerhafte Änderung zu Problemen führt (vgl. WBT 1 - Einführung in IT-Governance), die einen negativen Einfluss auf das Image und die Wirtschaftsleistung eines Unternehmens haben.

COBIT® ordnet den IT-bezogenen Zielen sogenannte **Metriken** zu. Sie sollen Hinweise zur Messung des Erreichungsgrades der Ziele geben. Jedes Unternehmen muss die vorgeschlagenen Metriken prüfen und sich für die individuell relevanten und erreichbaren Metriken ent-

scheiden. Zu Beginn der Implementierung von "BAI06 - Manage Changes" muss der aktuelle Stand der Zielerreichung definiert werden, um später eine Veränderung messen zu können.

The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines

Abb. 62: IT-bezogene Ziele und Metriken vom COBIT®-Prozess BAI06 Manage Changes

6.2.7 IT-Ziele der Cronus AG

Der Prozess "BAI06 - Manage Changes" unterstützt primär **drei der insgesamt 17 IT-Ziele**. Die 17 IT-bezogenen Ziele werden von COBIT® vorgeschlagen, wir werden sie aber auf die unternehmensspezifischen Anforderungen der Cronus AG hin prüfen und eventuell anzupassen.

Die von COBIT® vorgeschlagenen IT-bezogenen Ziele, die vom Prozess "BAI06 - Manage Changes" unterstützt werden, stimmen mit den IT-bezogenen Zielen der Cronus AG überein. Die IT-bezogenen Ziele müssen somit nicht zusätzlich angepasst werden. Auch die Metriken werden vom CIO **kritisch geprüft**. Zwei Metriken hat die Cronus AG nicht von COBIT® übernommen.

Die beiden gestrichenen Metriken (vgl. Abb. 37) wurden nicht übernommen, da sie nicht zu den Anforderungen der Cronus AG an den Prozess "BAI06 - Manage Changes" passen.

The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines

Abb. 63: IT-bezogene Metriken der Cronus AG für den COBIT®-Prozess

Daraus ergibt sich folgende **Auflistung** der IT-Ziele und Metriken für den Prozess "BAI06 - Manage Changes" in der Cronus AG.

IT-bezogene Ziele	Zugeordnete Metriken
Management der, mit der IT verbundenen, Geschäftsrisiken.	- Anteil der kritischen Geschäftsprozesse, IT-Services und IT-gestützten Geschäftsprogramme, die von der Risikobeurteilung abgedeckt werden. - Anzahl der gravierenden IT-bezogenen Störungen, die nicht im Rahmen der Risikobeurteilung identifiziert wurden. - Anteil der Risikobeurteilungen des Unternehmens, einschließlich IT-bezogener Risiken.
Bereitstellen von IT-Services, die sich mit den Geschäftsanforderungen decken.	- Anzahl der Geschäftsunterbrechungen aufgrund von IT-Servicestörungen. - Anteil der Benutzer, die mit der Qualität der IT-Servicebereitstellung zufrieden sind.
Sicherheit von Informationen, Prozessinfrastruktur und Anwendungen gewährleisten.	- Anzahl der Sicherheitsvorfälle, die zu finanziellen Verlusten, zur Unterbrechung der Geschäftstätigkeit oder zu öffentlichen Unannehmlichkeiten führen. - Anzahl der IT-Services mit ausstehenden Sicherheitsanforderungen. - Häufigkeit von Sicherheitsbeurteilungen nach neuesten Standards und Leitlinien.

Abb. 64: IT-bezogene Ziele und Metriken der Cronus AG für den COBIT®-Prozess

6.2.8 Prozessanforderungen

Für jeden der COBIT®-Prozesse sind zwischen drei und 15 Prozessanforderungen (Management Practices) definiert. Prozessanforderungen beschreiben den Soll-Zustand eines COBIT®-Prozesses, der beim Management eines Prozesses zur Steuerung und Überwachung der IT-Ressourcen und Ziele berücksichtigt werden sollen. Jeder Prozessanforderung werden Aktivitäten zugeordnet, die Maßnahmen beschreiben, wie die Anforderungen erreicht werden können. Der COBIT®-Prozess "BAI06 - Manage Changes" besteht aus vier **Prozessanforderungen**.

- **BAI06.01** Evaluieren, Priorisieren und Genehmigen von Änderungs-anträgen:

  Änderungsanfragen werden bewertet, um mögliche Auswirkungen auf den betroffenen Prozess und die IT-Dienstleistungen zu identifizieren. Nach der Bewertung muss gewährleistet werden, dass die Änderungen protokolliert, priorisiert, kategorisiert, bewertet, genehmigt, geplant und eingeplant werden.

BAI06 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
BAI06.01 Evaluate, prioritise and authorise change requests. Evaluate all requests for change to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled.	**From**	**Description**	**Description**	**To**
	BAI03.05	Integrated and configured solution components	Impact assessments	Internal
	DSS02.03	Approved service requests	Approved requests for change	BAI07.01
	DSS03.03	Proposed solutions to known errors		
	DSS03.05	Identified sustainable solutions	Change plan and schedule	BAI07.01
	DSS04.08	Approved changes to the plans		
	DSS06.01	Root cause analyses and recommendations		
Activities				
1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process.				
2. Categorise all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items.				
3. Prioritise all requested changes based on the business and technical requirements, resources required, and the legal, regulatory and contractual reasons for the requested change.				
4. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies amongst changes. Involve business process owners in the assessment process, as appropriate.				
5. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.				
6. Plan and schedule all approved changes.				
7. Consider the impact of contracted services providers (e.g., of outsourced business processing, infrastructure, application development and shared services) on the change management process, including integration of organisational change management processes with change management processes of service providers and the impact on contractual terms and SLAs.				

Abb. 65: Erste Prozessanforderung des Prozesses BAI06 – Manage Changes von COBIT®

- **BAI06.02** Managen von Notfalländerungen:

  Notfalländerungen müssen sorgfältig verwaltet und gesteuert werden, um schlimmere Ereignisse zu vermeiden. Es soll ein Prozess formuliert werden, wie typischerweise bei einer Notfalländerung vorzugehen ist.

Management Practice	Inputs		Outputs	
BAI06.02 Manage emergency changes. Carefully manage emergency changes to minimise further incidents and make sure the change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorised after the change.	**From**	**Description**	**Description**	**To**
			Post-implementation review of emergency changes	Internal
Activities				
1. Ensure that a documented procedure exists to declare, assess, give preliminary approval, authorise after the change and record an emergency change.				
2. Verify that all emergency access arrangements for changes are appropriately authorised, documented and revoked after the change has been applied.				
3. Monitor all emergency changes, and conduct post-implementation reviews involving all concerned parties. The review should consider and initiate corrective actions based on root causes such as problems with business process, application system development and maintenance, development and test environments, documentation and manuals, and data integrity.				
4. Define what constitutes an emergency change.				

Abb. 66: Zweite Prozessanforderung des Prozesses BAI06 – Manage Changes von COBIT®

- **BAI06.03** Verfolgen und Berichten des Änderungsstatus:

  Ein Nachverfolgungs- und Berichterstattungssystem muss gepflegt werden, um abgelehnte Änderungsanträge zu dokumentieren und den Status der genehmigten Änderungsanfragen nachverfolgen zu können. So kann sichergestellt werden, dass genehmigte Anfragen wie geplant umgesetzt wurden.

BAI06 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
BAI06.03 Track and report change status. Maintain a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned.	**From**	**Description**	**Description**	**To**
	BAI03.09	Record of all approved and applied change requests	Change request status reports	BAI01.06 BAI10.03
Activities				
1. Categorise change requests in the tracking process (e.g., rejected, approved but not yet initiated, approved and in process, and closed).				
2. Implement change status reports with performance metrics to enable management review and monitoring of both the detailed status of changes and the overall state (e.g., aged analysis of change requests). Ensure that status reports form an audit trail so changes can subsequently be tracked from inception to eventual disposition.				
3. Monitor open changes to ensure that all approved changes are closed in a timely fashion, depending on priority.				
4. Maintain a tracking and reporting system for all change requests.				

Abb. 67: Dritte Prozessanforderung des Prozesses BAI06 – Manage Changes von COBIT®

- **BAI06.04** Abschließen und Dokumentieren der Änderungen:

  Alle, von einer Veränderung betroffenen Prozesse, müssen nach Implementierung der Änderung der IT-Ressourcen dementsprechend angepasst werden. Was wie geändert

wurde, muss genau dokumentiert werden. Sofern betroffen müssen auch Benutzerhandbücher erstellt, bzw. angepasst werden.

Management Practice	Inputs		Outputs	
BAI06.04 Close and document the changes. Whenever changes are implemented, update accordingly the solution and user documentation and the procedures affected by the change.	**From**	**Description**	**Description**	**To**
			Change documentation	Internal
Activities				
1. Include changes to documentation (e.g., business and IT operational procedures, business continuity and disaster recovery documentation, configuration information, application documentation, help screens, and training materials) within the change management procedure as an integral part of the change.				
2. Define an appropriate retention period for change documentation and pre- and post-change system and user documentation.				
3. Subject documentation to the same level of review as the actual change.				

Abb. 68: Vierte Prozessanforderung des Prozesses BAI06 – Manage Changes von COBIT®

6.2.9 Prozessanforderungen der Cronus AG

Prozessanforderungen beschreiben den Soll-Zustand eines COBIT®-Prozesses, die beim Management eines Prozesses zur Steuerung und Überwachung der IT-Ressourcen und Ziele berücksichtigt werden sollen.

Für den COBIT®-Prozess "BAI06 - Manage Changes" schlägt COBIT® vier **Prozessanforderungen** vor. Diese hat Francesco Palla, der CIO der Cronus AG, den Gegebenheiten der Cronus AG angepasst.

- **BAI06.01** Evaluieren, Priorisieren und Genehmigen von Änderungs-anträgen:

  Für die Einführung des Releases für "Cronus myERP" muss zunächst eine schriftliche Anfrage von einem verantwortlichen Mitarbeiter der IT-Abteilung geprüft, geplant und genehmigt werden. Eine Evaluierung der Anfrage ist nicht notwendig, da es sich um eine notwendige Änderung handelt, ohne die Bankgeschäfte nicht mehr möglich sind. Aufgrund der Dringlichkeit der Änderung wird sie auf höchster Stufe priorisiert. Erst im Anschluss wird der verantwortliche Mitarbeiter der IT-Abteilung den Auftrag zur Einführung des Releases freigeben.

- **BAI06.02** Managen von Notfalländerungen:

  Bei der Einführung des SEPA-Verfahrens in „Cronus myERP" handelt es sich nicht um eine Notfalländerung. Aufgabe der IT-Abteilung ist es, einen Prozess für das Vorgehen bei Notfalländerungen zu definieren. Als relevanten Inhalt dieses Prozesses hat der CIO festgelegt, dass berechtigte Mitarbeiter die Möglichkeit haben, eine Notfalländerung durchzuführen, ohne diese vorab genehmigt zu bekommen. Nur so können Notfalländerungen jederzeit schnell umgesetzt werden. Im Anschluss an jede Notfal-

länderung soll von den Verantwortlichen geprüft werden, ob die Notfalländerung gerechtfertigt war.

- **BAI06.03** Verfolgen und Berichten des Änderungsstatus:

  In der Cronus AG gibt es zu diesem Zeitpunkt kein System, in dem die zuständigen Mitarbeiter den Status von Änderungen nachverfolgen können. Dies muss eingerichtet werden. Der Status einer Änderungsanfrage kann sein: abgelehnt; genehmigt, aber noch nicht eingeleitet; genehmigt und in Bearbeitung; abgeschlossen. Dieser Status muss für den verantwortlichen Mitarbeiter jederzeit einsehbar sein.

- **BAI06.04** Abschließen und Dokumentieren der Änderungen:

  Zu jedem Prozess gibt es in der Cronus AG eine Prozessformulierung, in welcher Abläufe, Ressourcen und Problemlösungen definiert sind. Diese Prozessformulierungen sind nach einer Änderung zu prüfen und gegebenenfalls anzupassen.

6.2.10 Das RACI-Chart

Das **RACI-Chart** zeigt auf, wer innerhalb einer Organisation zuständig oder verantwortlich für die Prozessanforderungen ist, bzw. wer konsultiert oder informiert wird. RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert). Die im RACI-Chart zugeordneten Rollen und Organisationseinheiten werden von COBIT® vorgeschlagen und sollen zur Veranschaulichung dienen, müssen aber unternehmensindividuell angepasst werden.

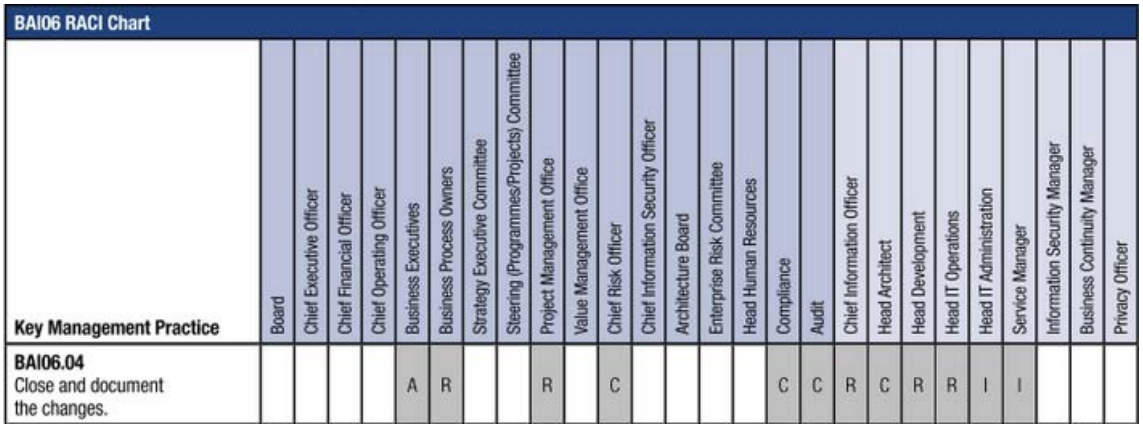
BAI06 RACI Chart																									
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.01 Evaluate, prioritise and authorise change requests.					A	R			C		C					C	C	R	C	R	R	C	R	C		
BAI06.02 Manage emergency changes.					A	I					C					C	C	R	I	R	R		I	C		
BAI06.03 Track and report change status.					C	R			C									A		R	R		R			
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C	R	R	I	I			

Abb. 69: RACI-.Chart des COBIT®-Prozesses BAI06 – Manage Changes

- **Responsible, zuständig**: Als Responsible wird gekennzeichnet, wer zuständig für die erfolgreiche Durchführung der Prozessanforderungen ist.
- **Accountable, verantwortlich:** Als Accountable wird gekennzeichnet, wer gesamtverantwortlich für den Prozesserfolg ist. Aufgrund der Haftbarkeit darf nur eine Rolle je Prozessanforderung als Accountable zugewiesen werden.
- **Consulted, konsultiert:** Als Consulted wird gekennzeichnet, wer beratend zu einer Prozessanforderung hinzugezogen wird oder wer Informationen von anderen (z. B. externen Partnern) beschaffen soll.
- **Informed, informiert:** Als Informed wird gekennzeichnet, wer über Ergebnisse oder/ und Leistungen der Prozessanforderungen informiert werden soll.

6.2.11 Das RACI-Chart der Cronus AG

Am Beispiel der **vierten Prozessanforderung** des COBIT®-Prozesses "BAI06 - Manage Changes", wird gezeigt, wer in der Cronus AG zuständig oder verantwortlich für die Prozessanforderungen ist, bzw. wer konsultiert oder informiert wird.



BAI06 RACI Chart																									
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
BAI06.04 Close and document the changes.					A	R			R		C					C	C	R	C	R	R	I	I			

Abb. 70: RACI-.Chart der vierten Prozessanforderung des COBIT®-Prozesses BAI06 – Manage Changes

- **Accountable**: COBIT® schlägt als verantwortliche (Accountable) Rolle den Bereichsleiter (**Business Executive**) vor.
    - Verantwortlich für die Umsetzung des COBIT®-Pilotprozesses, sowie für zukünftige COBIT®-Projekte in der Cronus AG, ist der **IT-Compliance Officer** (vgl. WBT 5). Seine Aufgabe ist die Gestaltung, Entwicklung und Umsetzung von IT-Compliance und somit auch COBIT® in der Cronus AG.
- **Responsible**: COBIT® schlägt als zuständige (Responsible) Rollen und Organisationseinheiten den Business Process Owner, Project Management Office, Chief Information Officer, Head Developement und Head of IT Operations vor.
    - **Business Process Owner**: In der Cronus AG ist der Prozesseigner für den Prozess des Change Managements, Mitarbeiter der IT-Abteilung. Er ist ab sofort verantwortlich für die Realisierung der gesetzten Ziele und für die Genehmigung von Änderungsanträgen.
    - **Project Management Office**: In der Cronus AG gibt es eine Abteilung, die sich allgemein mit der Projektplanung befasst. Zu Beginn der Planung der Umsetzung von COBIT® wurde innerhalb dieser Abteilung ein Spezial-Team für COBIT®-Projekte zusammengestellt.
    - **CIO**: Der CIO der Cronus AG, Francesco Palla, ist verantwortlich für die Planung, Ressourcenbereitstellung und das Management von IT-Diensten und -Lösungen zur Unterstützung der IT- und Unternehmens-ziele. Er ist Hauptverantwortlich für dieses Pilotprojekt und die weitere Umsetzung von COBIT® in der Cronus AG.
    - **Head Developement**: Bei dem Prozess "Manage Changes" muss auch der Abteilungsleiter der Entwicklungsabteilung als verantwortlich zugeordnet werden. Die Änderungen werden in der Entwicklungs-abteilung umgesetzt. So ist Auf-

gabe des Abteilungsleiters der Entwicklungsabteilung zu entscheiden, was wie umgesetzt werden kann.

- **Head of IT Operations**: In der Cronus AG hat der CIO die Aufgaben des, von COBIT® beschriebenen Head of IT Operations inne. Er ist für den Betrieb der IT-Infrastruktur verantwortlich und so auch für die ERP-Software "Cronus myERP".

- **Consulted**: COBIT® schlägt vor den Chief Risk Officer, Compliance, Audit, Head Architect beratend zu konsultieren (Consulted).
  - **Chief Risk Officer**: Der Abteilungsleiter der Risikoabteilung ist verantwortlich für sämtliche Aspekte des Risikomanagements in der Cronus AG. Er wird als Berater hinzugezogen, sodass mögliche Risiken, die durch die Angleichung der Prozesse an COBIT® entstehen können, geplant und wenn möglich vermieden werden.
  - **Compliance**: Der Chief Compliance Officer ist verantwortlich für die Sicherstellung der Einhaltung von rechtlichen und vertraglichen Anforderungen. Er wird als Berater hinzugezogen, damit die Umsetzung von COBIT® regelkonform umgesetzt wird.
  - **Audit**: Der interne Audit wird in der Cronus AG durch die Mitarbeiter des Qualitätsmanagements durchgeführt. Sie sind verantwortlich für die Qualität der Prozesse. Bei der Umsetzung von COBIT® unterstützen die Mitarbeiter beratend, um die Qualität der Prozesse weiterhin sicherzustellen.
  - **Head Architect**: Die Verantwortung für die IT-Architektur hat ebenfalls der CIO inne. Das beinhält die Organisation der IT-Infrastruktur (also auch die Organisation der ERP-Software) und das zugehörige Management der IT-Ressourcen und der Schnittstellen.

- **Informed**: COBIT® schlägt vor den Head IT Administration und den Service Manager über Ergebnisse der Prozesspraktiken zu informieren.
  - **Head IT Administration**: Der leitende **Administrator** der IT-Abteilung ist verantwortlich für die IT-bezogene Verwaltung zuständig. So muss er z. B. für die einwandfreie Funktion des ERP-System "Cronus myERP" nach dem Release sorgen.
  - **Service Manager**: Der Service Manager muss informiert werden, wenn Produkte oder Dienstleistungen für einen Kunden oder eine Kundengruppe geändert werden. Da die Änderung von "Cronus myERP" zunächst nur intern implementiert werden soll, muss er in diesem Fall nicht über die Ergebnisse der Änderung informiert werden.

6.2.12 Prozessaktivitäten

COBIT® definiert für jede Prozessanforderung jeweils zwischen drei und 15 Aktivitäten, die bei der Umsetzung der Prozessanforderungen als Hilfestellung dienen sollen. Durch die Verkettung aller Prozessaktivitäten wird der gesamte Prozess abgebildet.

Prozessaktivitäten beschreiben, was wie für die einzelnen Prozessanforderungen realisiert werden soll, um die IT-Leistung COBIT®-konform zu gestalten. Die Prozessaktivitäten sind als Anleitung zur Umsetzung der Prozessanforderungen zu verstehen.

- **BAI06.01** Evaluieren, Priorisieren und Genehmigen von Änderungs-anträgen:

  Für BAI06.01 schlägt COBIT® **sieben Aktivitäten** vor. Diese fordern eine formale Änderungsanfrage, um diese später zu kategorisieren, priorisieren und zu planen. Weiterhin müssen alle Änderungsanfragen vom Prozesseigner formal genehmigt werden, bevor sie umgesetzt werden dürfen.

1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process.
2. Categorise all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items.
3. Prioritise all requested changes based on the business and technical requirements, resources required, and the legal, regulatory and contractual reasons for the requested change.
4. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies amongst changes. Involve business process owners in the assessment process, as appropriate.
5. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.
6. Plan and schedule all approved changes.
7. Consider the impact of contracted services providers (e.g., of outsourced business processing, infrastructure, application development and shared services) on the change management process, including integration of organisational change management processes with change management processes of service providers and the impact on contractual terms and SLAs.

Abb. 71: Prozessaktivitäten der COBIT®-Prozessanforderung BAI06.01

- **BAI06.02** Managen von Notfalländerungen:

  Für BAI06.02 schlägt COBIT® **vier Aktivitäten** vor**.** Es soll ein dokumentiertes Verfahren existieren, um die Notfalländerung zu definieren, erklären, dokumentieren, bewerten und zu autorisieren. Eine Notfalländerung muss besonders stark überwacht werden.

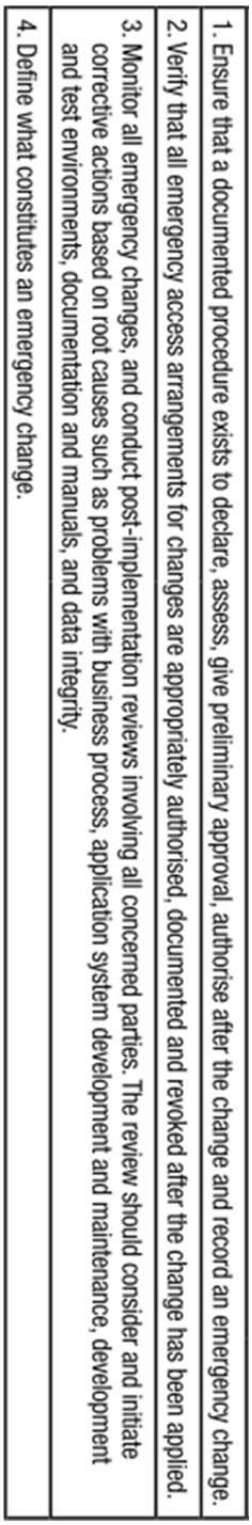


Abb. 72: Prozessaktivitäten der COBIT®-Prozessanforderung BAI06.02

- **BAI06.03** Verfolgen und Berichten des Änderungsstatus:

  Für BAI06.03 schlägt COBIT® **vier Aktivitäten** vor. Es soll eine Kategorisierung (z. B. abgelehnt; genehmigt, aber noch nicht eingeleitet; genehmigt und in Bearbeitung; abgeschlossen) des Fortschritts einer Änderungsanfrage existieren. Zu diesen Kategorien müssen Statusberichte erstellt werden.

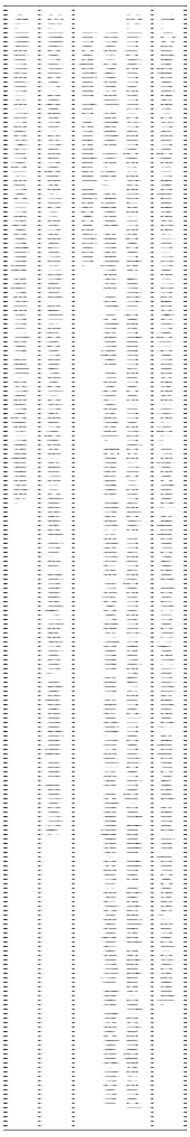


Abb. 73: Prozessaktivitäten der COBIT®-Prozessanforderung BAI06.03

- **BAI06.04** Abschließen und Dokumentieren der Änderungen:

  Für BAI06.04 schlägt COBIT® **drei Aktivitäten** vor. Die Änderungen sollen dokumentiert und es soll eine angemessene Aufbewahrungszeit der Dokumentation festgelegt werden.

Abb. 74: Prozessaktivitäten der COBIT®-Prozessanforderung BAI06.04

6.2.13 Prozessaktivitäten der Cronus AG

Prozessaktivitäten beschreiben, was wie für die einzelnen Prozessanforderungen realisiert werden soll, um die IT-Leistung COBIT®-konform zu gestalten. Die Prozessaktivitäten sind als Anleitung zur Umsetzung der Prozessanforderungen zu verstehen.

- **BAI06.01** Evaluieren, Priorisieren und Genehmigen von Änderungs-anträgen:

  Die Änderungsanfrage wird, bis ein laufendes Ticket-System ("WBT 07 - Fallstudie ITIL®") etabliert wurde, via E-Mail und über eine zentrale Excel-Tabelle vom Prozesseigner dokumentiert, evaluiert, priorisiert und genehmigt.

- **BAI06.02** Managen von Notfalländerungen:

  Um Notfalländerungen schnellst möglichst und effizient zu lösen, wird in der Cronus AG ein Notfallausschuss gebildet. dieser besteht aus dem Prozesseigner und einem erfahrenen Mitarbeiter der IT-Abteilung. Zu den Geschäftszeiten muss immer mindestens ein Mitglied aus dem Notfallausschuss verfügbar und verantwortlich sein. Nur so können Notfalländerungen jederzeit schnell umgesetzt werden. Erst im Anschluss einer jeden Notfalländerung wird von den Verantwortlichen geprüft, ob die Notfalländerung gerechtfertigt war.

- **BAI06.03** Verfolgen und Berichten des Änderungsstatus:

  Um den Status von Änderungsanträgen verfolgen zu können, wurde die Entwicklungsabteilung beauftragt, eine Anwendung für das geplante Ticket-System (vgl. "WBT 07 - Fallstudie ITIL®") zu entwickeln. Anforderung an die Anwendung ist es, dass jeder berechtigte Mitarbeiter den aktuellen Status der Änderung einsehen und aktualisieren kann. Um die Überwachung sicherzustellen, soll die Anwendung Analysen der Änderungsanträge erstellen können, z. B. eine grafische Aufbereitung, ob die Änderungsanträge der Priorität nach bearbeitet und zeitgerecht abgeschlossen wurden.

- **BAI06.04** Abschließen und Dokumentieren der Änderungen:

  Um die Dokumentation zu standardisieren, hat ein Mitarbeiter der IT-Abteilung Checklisten entwickelt, in denen das Vorgehen der Änderungen auf wichtige Punkte hin überprüft wird. Diese Checklisten müssen nach jeder durchgeführten oder abgelehnten Änderung ausgefüllt werden und nach dem Vier-Augen-Prinzip von einem Vorgesetzten geprüft werden. Erst im Anschluss daran kann eine Änderung abgeschlossen werden.

6.2.14 Inputs und Outputs

Jeder COBIT®-Prozessanforderung sind **Inputs und Outputs** zugeordnet, die für die Ausführung eines Prozesses von COBIT® als erforderlich betrachtet werden.

Mit **Inputs** meint COBIT® die Ressourcen oder/und Informationen eines Prozesses, die zur Umsetzung und Anwendung eines Prozesses benötigt werden. Inputs können dabei Outputs anderer COBIT®-Prozesse oder externe Ressourcen bzw. Informationen sein. **Outputs** sind Arbeitsprodukte des Prozesses, die entweder innerhalb des gleichen Prozesses wiederverwendet werden (intern) oder Inputs für andere COBIT®-Prozesse darstellen.

Die Inputs für den COBIT®-Prozesses "BAI06 - Manage Changes" sind Outputs anderer COBIT®-Prozesse. Die Outputs werden sowohl intern für den Prozess selber oder auch für andere COBIT®-Prozesse genutzt.

BAI06 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
	From	Description	Description	To
BAI06.01 Evaluate, prioritise and authorise change requests. Evaluate all requests for change to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled.	BAI03.05	Integrated and configured solution components	Impact assessments	Internal
	DSS02.03	Approved service requests	Approved requests for change	BAI07.01
	DSS03.03	Proposed solutions to known errors		
	DSS03.05	Identified sustainable solutions	Change plan and schedule	BAI07.01
	DSS04.08	Approved changes to the plans		
	DSS06.01	Root cause analyses and recommendations		

Abb. 75: Inputs und Outputs der COBIT®-Prozessanforderung BAI06.01

6.2.15 Projektplanung

Alle Prozesselemente des COBIT®-Prozesses "BAI06 - Manage Changes" sind in der Cronus AG umgesetzt worden. Anhand der gesammelten Erfahrungen hat der IT-Compliance-Officer nachträglichen einen Projektplan erstellt. Dieser soll zukünftig bei der Umsetzung von weiteren COBIT®-Prozessen in der Cronus AG als Hilfestellung dienen. Insgesamt hat die Umsetzung des Pilotprozesses zehn Wochen gedauert.

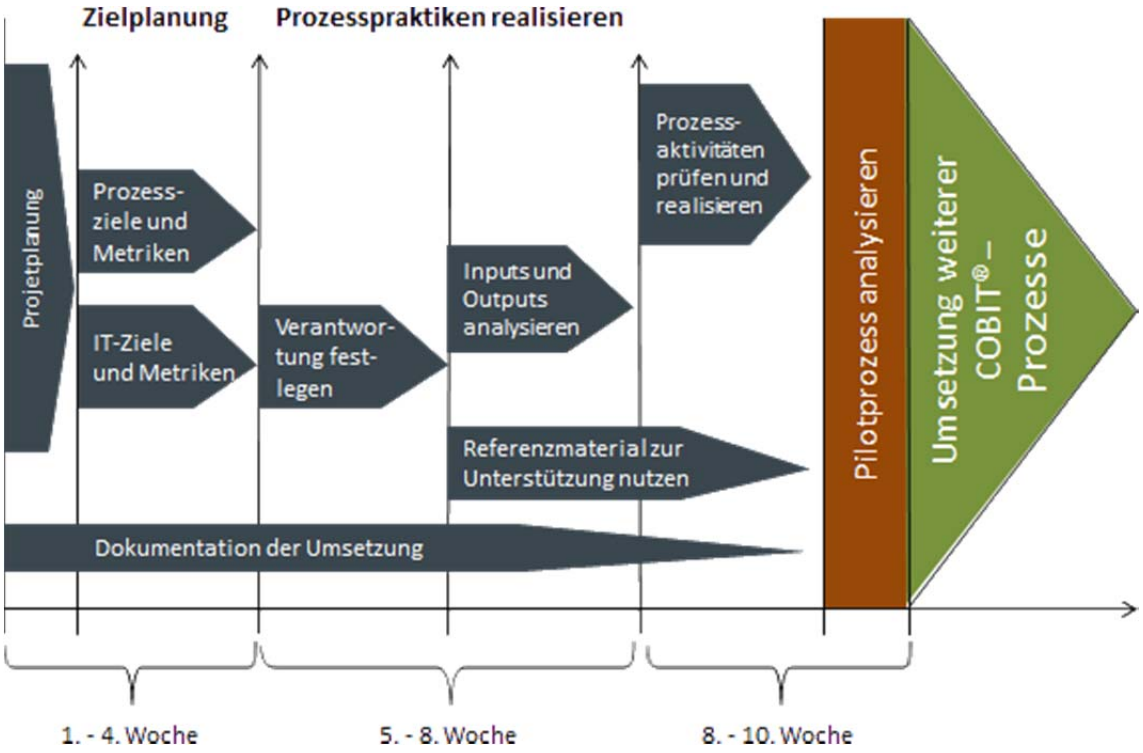


Abb. 76: Projektplan zur Implementierung des COBIT®-Prozesses BAI06

6.2.16 Zusammenfassung und Ausblick

Der Pilotprozess zur Umsetzung von COBIT® wurde erfolgreich in der Cronus AG implementiert. Die Änderung der Kontodaten im ERP-System "Cronus myERP" wurde ebenfalls erfolgreich abgeschlossen. Das Pilotprojekt zur Implementierung von COBIT® in der Cronus AG ist als voller Erfolg zu betrachten. Im nächsten Schritt kann das weitere Vorgehen zur Implementierung der verbleibenden 36 COBIT®-Prozesse geplant werden.

Bis die Prozesse der Cronus AG COBIT®-konform sind, ist also noch ein langer Weg zu bestreiten. Die reine Umsetzung von COBIT® stellt jedoch nicht sicher, dass die Cronus AG regelkonform im Sinne der IT-Compliance ist. Um diese Wahrscheinlichkeit zu erhöhen, wurde in "WBT 05 - IT-Compliance" entschieden, neben COBIT® auch ITIL® in der Cronus AG einzuführen.

Im nächsten WBT werden Sie sich mit der Implementierung eines Pilotprozesses von ITIL® auseinandersetzen.

6.3 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	COBIT® ist ein Referenzmodell, welches sich konkret an die IT eines Unternehmens richtet. Weiterhin unterstützt COBIT® bei der Implementierung von IT-Governance in die Corporate Governance eines Unternehmens.		
	Richtig		
	Falsch		
2	Ein Problem von COBIT® besteht im methodischen Ansatz des Referenzmodells. Damit ist gemeint, dass hauptsächlich beschrieben wird was zu tun ist, die Handlungsempfehlungen jedoch beschränkt sind.		
	Richtig		
	Falsch		
3	Die 37 COBIT®-Prozesse sind standardisiert und können theoretisch von jedem Unternehmen als Referenzmodell genutzt werden, lediglich bedarf es unternehmensindividueller Anpassungen.		
	Richtig		
	Falsch		
4	Aus welchen Hauptbestandteilen besteht der COBIT®-Würfel?		
	IT-Prozesse (Domänen, Prozesse, Reifegrad)		
	IT-Ressourcen		
	Geschäftsanforderungen		
	Anforderungen der einzelnen Fachbereiche		
	IT-Prozesse (Domänen, Prozesse, Aktivitäten)		
5	Die Geschäftsanforderungen sind als Ausgangspunkt zu sehen. Aus ihnen werden die IT-Ressourcen abgeleitet, die benötigt werden, um die IT-Prozesse umzusetzen.		
	Richtig		
	Falsch		

6	Die gleichzeitige Umsetzung aller COBIT®-Prozesse ist sinnvoll, da dies für die Unternehmen am ökonomischsten ist.		
	Richtig		
	Falsch		
7	Die IT-Ziele sind prozessspezifisch und werden durch die Aktivitäten eines Prozesses erreicht. Jedem IT-Ziel werden Metriken zugeordnet.		
	Richtig		
	Falsch		
8	Der Prozess „BAI06 – Manage Changes“ lässt sich in vier Prozessanforderungen unterteilen. Den einzelnen Prozessanforderungen werden mit Hilfe des RACI-Charts die verantwortlichen Abteilungen und Führungspositionen zugeordnet.		
	Richtig		
	Falsch		

Tab. 7: Übungsfragen WBT 06 –Fallstudie COBIT®

7 Fallstudie ITIL®

7.1 Einführung in ITIL®

7.1.1 Buongiorno

Buongiorno! Ich bin Francesco Palla, der CIO der Cronus AG.

Heute beschäftigen wir uns mit dem ITIL®-Framework, das von Unternehmen weltweit eingesetzt wird, um Fähigkeiten im Bereich von IT-Service-Management zu entwickeln und zu verbessern.

Neben zahlreichen internen IT-Service-Angeboten, wie z. B. einem E-Mail-Service, bietet die Cronus AG das ERP-System "Cronus myERP" für andere Möbelhersteller an. Um diese externen Leistungen der Cronus AG weiter ausbauen zu können, möchten wir die ISO/IEC 20000-Zertifizierung erhalten. Doch das ist gar nicht so einfach!

ISO/IEC 20000 stellt abstrakte Regeln auf, was in der Cronus AG alles implementiert sein soll. Die Norm zeigt uns dabei jedoch lediglich die Ziele auf, die wir erreichen müssen. Wie wir diese Ziele allerdings erreichen, wird dabei nicht weiter aufgegriffen. An dieser Stelle hilft uns das ITIL®-Framework. ITIL® bietet konkrete Leitlinien, die zum Verständnis der Norm beitragen und uns genau beschreiben, was wir zu tun haben.

Wir freuen uns, dass Sie uns auf dem langen Weg zur Zertifizierung begleiten!

7.1.2 Ziele der Cronus AG

Um einen Nutzen aus unserer IT ziehen zu können, haben wir uns in der Cronus AG einige Ziele gesetzt, die wir mit Hilfe von ITIL® (Abb. 1) in unserem Unternehmen umsetzen möchten:

- **Anforderungsgerecht**: IT-Services sollten die Geschäftsprozesse und Ziele des Unternehmens bestmöglich unterstützen.

  Ein E-Mail-Service wird beispielsweise anforderungsgerecht betreut, wenn das Support-Team die Probleme der Mitarbeiter werktags 24 Stunden bearbeitet, da die Mitarbeiter in dieser Zeit durchgängig erreichbar sein müssen.

  Am Wochenende hingegen ist dies nicht erforderlich, da die Mitarbeiter nicht auf den E-Mail-Service angewiesen sind.

- **Wirtschaftlich**: Das IT-Service-Management sollte in der Lage sein, die vereinbarten Ergebnisse effektiv und effizient abliefern zu können und nötige Aktivitäten permanent zu verbessern.

Im Hinblick auf wirtschaftliches Verhalten ist es sinnvoll, wenn der E-Mail-Service der Cronus AG nur von der benötigten Anzahl an Mitarbeitern betreut wird. Zudem ist es aus wirtschaftlicher Sicht sinnvoll, dass keine überdimensionierten E-Mail-Postfächer bereitgestellt werden.

- **Benutzerfreundlich**: Services sollten nicht nur hochwertig, sondern auch durch den Benutzer einfach anzuwenden sein. Dadurch entwickeln sie sich nicht zu einer Last für den Benutzer.

Ein benutzerfreundlicher E-Mail-Service ermöglicht es beispielsweise dem User, sich mit Hilfe von umfangreichen Hilfsdokumenten und einer einfachen Einrichtung des Postfachs schnell alleine zurechtzufinden.

Abb. 77: Logo der „Information Technology Infrastructure Library®“

1.1.1 Was ist ITIL®?

Meine Mitarbeiter und ich haben ein wenig recherchiert und die wichtigsten Informationen zu ITIL® zusammengetragen. Diese Grundlagen werden uns später helfen, einen ersten ITIL®-Prozess in der Cronus AG einzuführen.

Die britische Regierungsbehörde Central Computer and Telecommunications Agency (CCTA) gab 1989 den Startschuss zur Entwicklung der Information Technology Infrastructure Library (ITIL®), da eingekaufte IT-Dienstleistungen stets eine mangelhafte Qualität aufwiesen.

Seitdem umfasst ITIL® eine Sammlung von Erfahrungen aus der Welt des IT-Service-Managements, die in Form von Best-Practice-Leitlinien niedergeschrieben wurden.

Mithilfe von fünf ITIL®-Handbüchern, die insgesamt 26 Prozesse umfassen, ist es den IT-Mitarbeitern möglich, aus den Erfahrungen anderer zu lernen.

Der IT-Mitarbeiter bekommt Empfehlungen, welche Aspekte bei der Gestaltung der IT-Services besonders wichtig sind und, wie diese am effizientesten gestaltet werden.

Der IT-Mitarbeiter bekommt Empfehlungen, welche Prozesse und Funktionen im Unternehmen eingeführt werden sollten.

So gibt es beispielsweise den standardisierten Prozess "Incident Management" mit dessen Hilfe Störungen im Betriebsablauf möglichst schnell behoben werden.

In den fünf Handbüchern Service Strategy, Service Design, Service Transition, Service Operation und Continual Service Improvement werden 26 Prozesse ausführlich auf über 500 Seiten beschrieben (Abb. 2). Was Prozesse sind und um was es in den einzelnen Handbüchern geht, werden wir im Laufe dieses WBT-Kapitels gemeinsam erarbeiten.

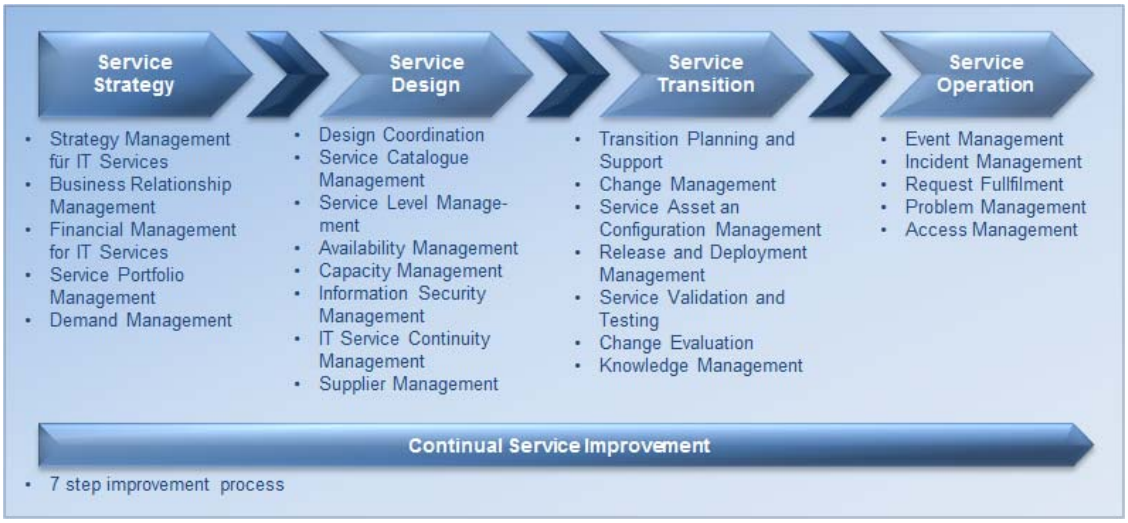


Abb. 78: Übersicht der ITIL®-Prozesse

7.1.3 ITIL® steht für IT-Service Management

Hallo! Ich bin Valérie Environ, die Assistentin von Herrn Palla.

Im Rahmen der Recherchen habe ich mich mit dem Thema IT-Service-Management beschäftigt. IT-Service-Management umfasst die Planung, Steuerung und Kontrolle von IT-Dienstleistungen.

Im Rahmen von ITIL® werden IT-Dienstleistungen mithilfe der ITIL®-Prozesse abgebildet. Im Fokus steht dabei die Umwandlung von vorhandenen Ressourcen in einen "wertvollen" Service für den Servicekunden.

Ein Telefon, ein Tisch und eine Mitarbeiterin alleine stellen für unsere Servicekunden keine Hilfe dar. Wir werden daher geschult, sodass wir Kundenanfragen beantworten können und unsere Kunden an entsprechende Mitarbeiter weiterleiten können.

So klärt sich das Anliegen unseres Servicekunden schnell und er zieht einen Nutzen daraus.

7.1.4 Überblick der ITIL®-Version 3

Die britische Regierungsbehörde Central Computer and Telecommunications Agency (CCTA) gab 1989 den Startschuss zur Entwicklung von ITIL®, da eingekaufte IT-Dienstleistungen stets eine mangelhafte Qualität aufwiesen. Heute wird die Herausgeberschaft von ITIL® durch das Cabinet Office geregelt. Seit dem Entwicklungsstart 1989 wird ITIL® stetig überarbeitet und weiterentwickelt.

Im Zeitablauf entstanden dadurch drei verschiedene ITIL®-Versionen. Wir in der Cronus AG möchten natürlich immer auf dem neusten Stand sein, deswegen werden wir in Zukunft mit dem Update "ITIL® 2011" der Version 3 arbeiten.

Um die schlechte Qualität der IT-Dienstleistungen nachhaltig zu verbessern und zeitgleich die Kosten zu senken, wurde ITIL® von der britischen Regierungsbehörde CCTA entwickelt.

Eine IT-Innovation durch den Auftrag einer staatlichen Institution stellt im Hinblick auf das meist rückschrittliche Verhalten staatlicher Institutionen eine besondere Seltenheit dar.

7.1.5 Was ist ein Prozess?

ITIL® umfasst insgesamt 26 standardisierte Prozesse. ITIL® gibt hierbei eine Empfehlung, wie die Prozesse ablaufen können. Diese Empfehlung kann übernommen oder spezifisch an die Anforderungen des Unternehmens angepasst werden.

Die verschiedenen ITIL®-Prozesse werden in den fünf ITIL®-Handbüchern erläutert.

Ein Prozess (Abb. 3) ist ein Handlungsleitfaden, der abläuft, um Nutzen für einen Kunden zu schaffen. Im Rahmen eines Prozesses ist es so z. B. möglich, die Kapazität eines E-Mail-Postfaches zu erweitern.

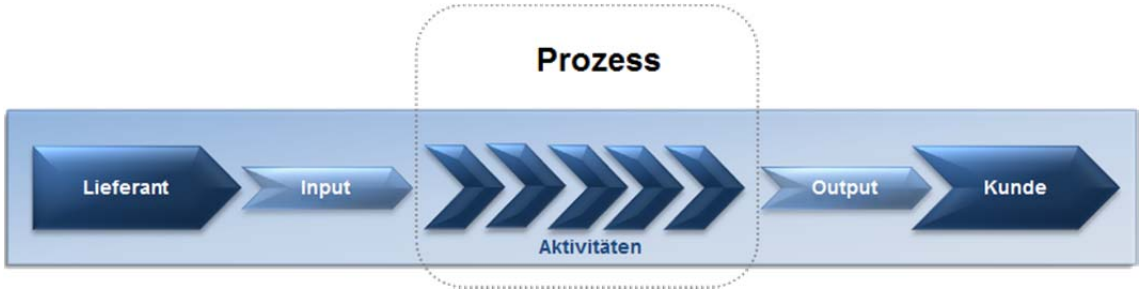


Abb. 79: Prozess

Der Prozessablauf ist zwar durch ITIL® standardisiert, jedoch haben die Unternehmen einen Handlungsspielraum und können die einzelnen Prozesse auf die individuellen Bedürfnisse ihres Unternehmens anpassen.

7.1.6 Informationswege zu ITIL®

Dem ITIL®-Nutzer stehen drei Informationswege zur Verfügung, um sich einen umfassenden Überblick über ITIL® zu verschaffen.

Hauptrelevanz haben dabei die fünf Kernpublikationen. Zusätzlich gibt es zudem ergänzende Literatur, mit der wir uns aber nicht intensiver beschäftigen werden.

In ITIL® dreht sich alles um den zu liefernden Dienst. Im Rahmen des Service Lifecycle werden die fünf, von ITIL® definierten, IT-Service-Kernbereiche in einen Lebenszyklus eingebettet. Mit diesem Lebenszyklus werden wir uns auf der nächsten WBT-Seite beschäftigen.

Die drei Informationswege zu ITIL® sind:

- **ITIL® Kernpublikationen**: Die ITIL® Kernpublikationen umfassen Best Practice Leitlinien, die in allen Unternehmenstypen eingesetzt werden können, die Services für ein Business bereitstellen möchten.

  Die Kernliteratur besteht aus den 5 Handbüchern:

  Service Strategy, Service Design, Service Transition, Service Operation und Continual Service Improvement (Service Lifecycle).

- **ITIL® Complementary Guidance**: Bei dem ITIL® Complementary Guidance handelt es sich um ergänzende ITIL®-Veröffentlichungen.

  Im Rahmen dieser zusätzlichen Publikationen werden ergänzende Leitlinien für bestimmte Branchen, Betriebsmodelle, Technologiearchitekturen und Unternehmenstypen veröffentlicht.

- **ITIL® Web Support Services**: Im Zuge des ITIL® Web Support Services werden online interaktive Services bereitgestellt.

Diese Plattform ermöglicht es dem ITIL®-Nutzer in Kontakt zu Experten zu treten und ergänzende Inhalte wie Templates und Fallstudien herunterzuladen.

7.1.7 Service Lifecycle

Alle ITIL®-Prozesse werden im Service Lifecycle (Abb. 4) eingebettet, um zum Ausdruck zu bringen, dass IT-Services stetig überprüft und ggf. weiterentwickelt werden sollten. Im weiteren Verlauf des WBT werden wir uns mit dem Prozess "Incident Management" aus dem Handbuch "Service Operation" befassen.

ITIL® umfasst fünf Handbücher:

- **Service Strategy**: Der Band "Service Strategy" konzentriert sich auf die strategische Einordnung der IT-Services und eine dichtere Verflechtung von Geschäfts- und IT-Strategie.
- **Service Design**: Der Band "Service Design" konzentriert sich auf die Entwicklung von Servicelösungen und die Gestaltung von Service-Management-Prozessen.
- **Service Transition**: Der Band "Service Transition" umfasst Leitlinien zur Entwicklung und Implementierung von neuen oder geänderten IT-Services.
- **Service Operation**: Der Band "Service Operation" befasst sich mit Prozessen, die für die effiziente und effektive Service-Bereitstellung und Service-Erbringung von Bedeutung sind.
- **Continual Service Improvement**: Der Band "Continual Service Improvement" umfasst instrumentelle Leitlinien zum Erhalt und zur Verbesserung der Servicequalität, in Bezug auf alle ITIL®-Leitlinien.

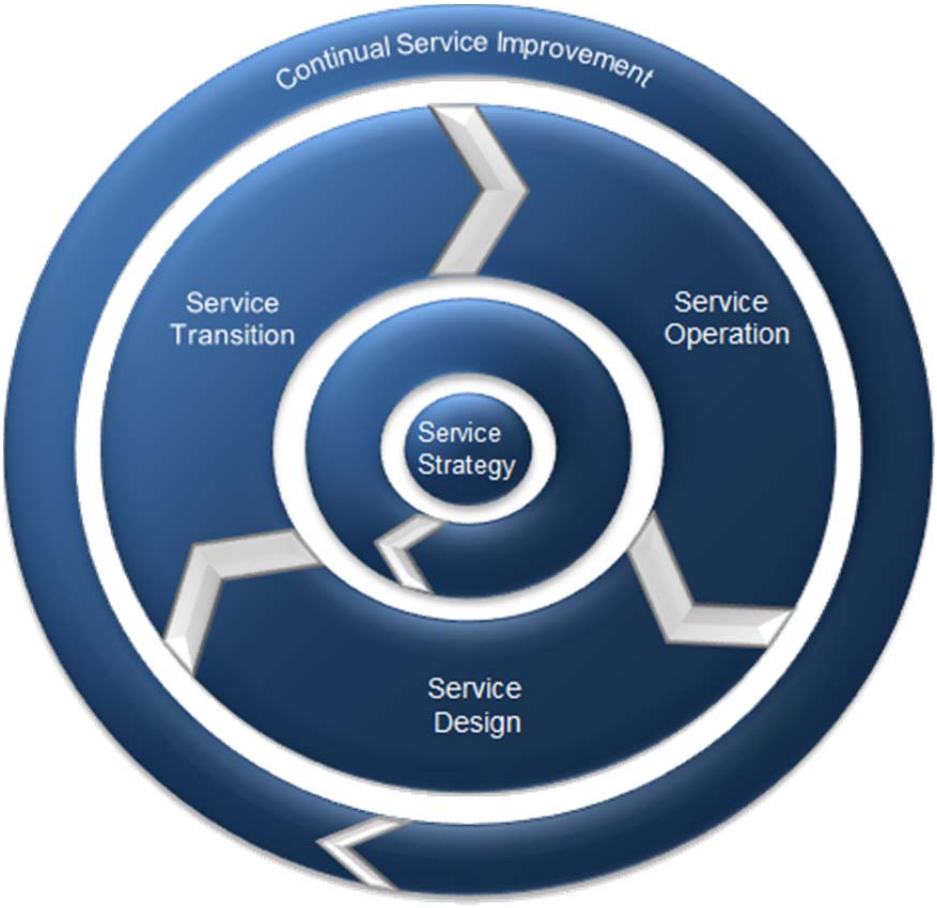


Abb. 80: Service Lifecycle

7.2 Die Projektvorbereitungen

7.2.1 Implementierung von ITIL® in der Cronus AG

In der Cronus AG (Abb. 5) haben wir uns nach reichlicher Recherche dafür entschieden, das ITIL®-Framework in unserem Unternehmen zu etablieren. ITIL® bietet uns die Möglichkeit uns nach ISO/IEC 20000 zertifizieren zu lassen, da die Norm an den ITIL®-Prozessbeschreibungen ausgerichtet ist.

Abb. 81: Logo der „Cronus AG“

Bei der Überlegung, welchen Prozess wir in der Cronus AG als Erstes einführen sollen, sind wir in der ITIL®-Publikation "Service Operation" fündig geworden. Hier wird beschrieben, dass der Prozess "Incident Management" häufig einer der ersten Prozesse ist, die in IT-Service-Management-Projekten implementiert werden. Dieser Prozess zeigt besonders stark, in welchen Bereichen eines IT-Service Management noch große Defizite zu finden sind und hat einen großen Einfluss auf die direkte Beziehung zum Kunden.

Um den Incident-Management-Prozess bestmöglich in der Cronus AG einzuführen, haben wir zunächst einige Informationen über den Prozess und dessen Ziele eingeholt...

Die internationale Norm ISO/IEC 20000 bietet der Cronus AG die Möglichkeit, weltweit Marktpartnern und potenziellen Kunden zu demonstrieren, dass ihr IT- Service-Management international anerkannt organsiert ist.

Im Rahmen des Incident-Management-Prozesses dreht sich alles rund um die Behebung von Störungen. Dieser Prozess wird häufig als einer der ersten Prozesse eingeführt, da er im täglichen Geschäft des Unternehmens besonders stark wahrgenommen wird.

7.2.2 Was ist Incident Management?

Der Prozess Incident Management (aus dem Band "Service Operation") ist einer der 26 standardisierten ITIL®-Prozesse (Abb. 6). Das Incident Management konzentriert sich auf die schnellstmögliche Wiederherstellung des "normalen" Betriebs und die Behebung von Incidents.

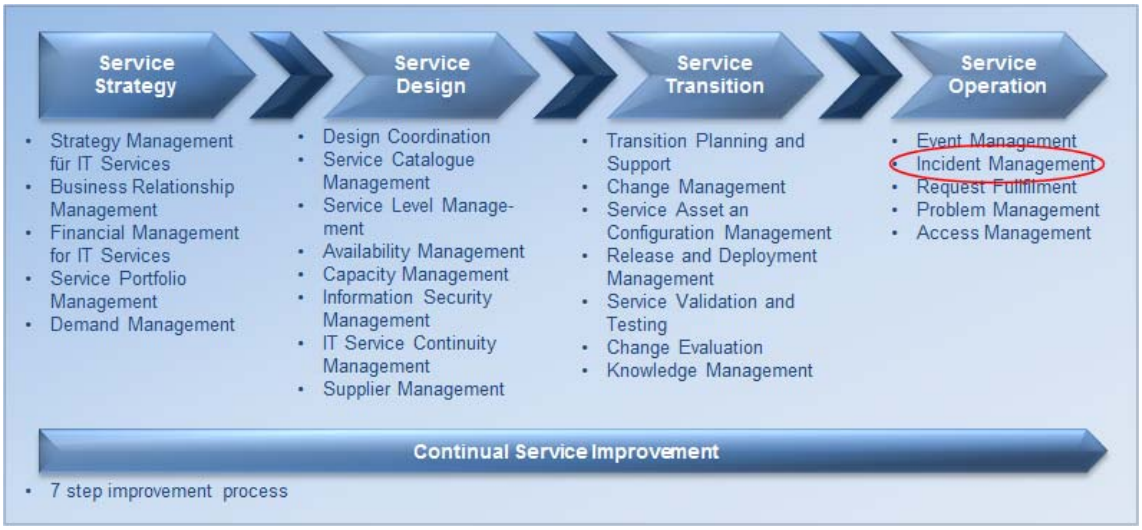


Abb. 82: Der Incident-Management-Prozess

ITIL® definiert einen Incident als eine nicht geplante Unterbrechung eines IT-Service oder eine Qualitätsminderung eines IT- Services.

Im Rahmen des Incident Managements soll möglichst schnell der normale Servicebetrieb wiederhergestellt werden, um negative Auswirkungen, wie zum Beispiel Umsatzverluste durch eine PC-Funktionsstörung, möglichst klein zu halten. Es werden dabei alle Ereignisse berücksichtigt, die einen Service tatsächlich unterbrechen, aber auch alle Ereignisse, die einen Service auch nur unterbrechen könnten.

In Zukunft wird die Behandlung einer Störung in der Cronus AG dann beispielsweise so aussehen: Einer unserer Mitarbeiter meldet einen Systemabsturz bei dem Versuch, eine Datei abzuspeichern. Durch das Gespräch mit einem Service-Techniker stellt sich heraus, dass die Festplatte des PCs defekt ist. Der Servicetechniker der Cronus AG veranlasst den Austausch der Festplatte und nach dieser Reparatur und einem Funktionstest wird das Ticket geschlossen.

Als Ticket wird die elektronische Form eines Anliegens an den Service Desk eines Unternehmens bezeichnet. Dabei kann es sich um eine Störung oder ein anderes Anliegen wie z. B. eine Informationsanfrage oder einen Änderungswunsch handeln.

7.2.3 Die ITIL®-Funktionen

In ITIL® werden 4 Funktionen benannt:

- **Service Desk**: Der Service Desk dient als erste Kontaktstelle für die Anwender, wenn sie Service-Unterbrechungen melden möchten. Zudem dient er als interne Koordinationsstelle für mehrere IT-Prozesse.
- **Technical Management**: Das Technical Management beschäftigt sich mit der Planung, Implementierung und dem Betrieb einer stabilen IT-Infrastruktur. Das Technical Management stellt dazu das nötige technische Wissen und die entsprechenden Ressourcen bereit.
- **Application Management**: Das Application Management kümmert sich um die Steuerung von IT-Anwendungen. Ziel des Application Management ist es, mit Hilfe der IT-Anwendungen die Geschäftsprozesse der Cronus AG zu unterstützen.
- **IT Operations Management**: Im Rahmen des IT Operations Management wird die IT-Infrastruktur gepflegt und die IT-Services verwaltet. In den Aufgabenbereich dieser Funktion fällt dabei auch die kontinuierliche Verbesserung der IT-Services.

Die Funktionen werden durch einzelne Mitarbeiter oder Abteilungen übernommen, die einen stabilen Zustand der Betriebs-IT aufrechterhalten. Zudem ist es möglich, dass z. B. ein Mitarbeiter mehrere Funktionen abdeckt.

7.2.4 ITIL®-Funktionen: Der Service Desk

Die IT-Mitarbeiter des Service Desk werden als Erstes von Anwendern kontaktiert, wenn es zu Service-Unterbrechungen (Incidents) kommt. Die Incidents werden schließlich von den Service Desk-Mitarbeitern bearbeitet oder an andere IT-Mitarbeiter weitergegeben.

Je nach Größe, Struktur, Sprache etc. kann der Service Desk unterschiedlich organisiert werden.

Grundsätzlich werden vier Service-Desk-Strukturen unterschieden:

- **Lokaler Service Desk**: Bei einem lokalen Service Desk hat jeder Standort eines Unternehmens seinen eigenen lokalen Service Desk direkt bei den Anwendern vor Ort (Abb. 7).

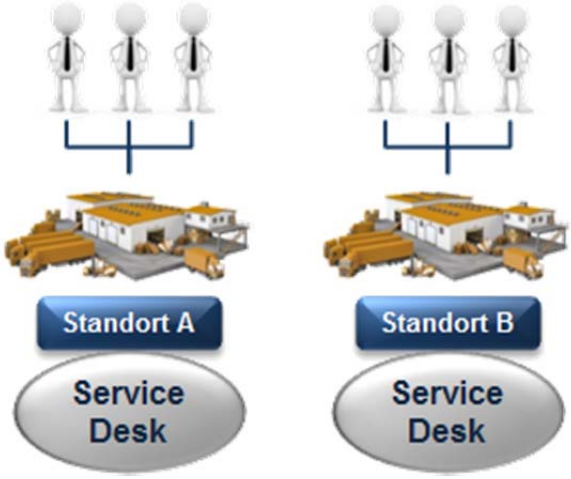


Abb. 83: Lokaler Service Desk

- **Zentraler Service Desk**: Bei der "zentralen" Organisationsstruktur gibt es einen einzigen Service Desk, der für alle Unternehmensstandorte zuständig ist (Abb. 8).

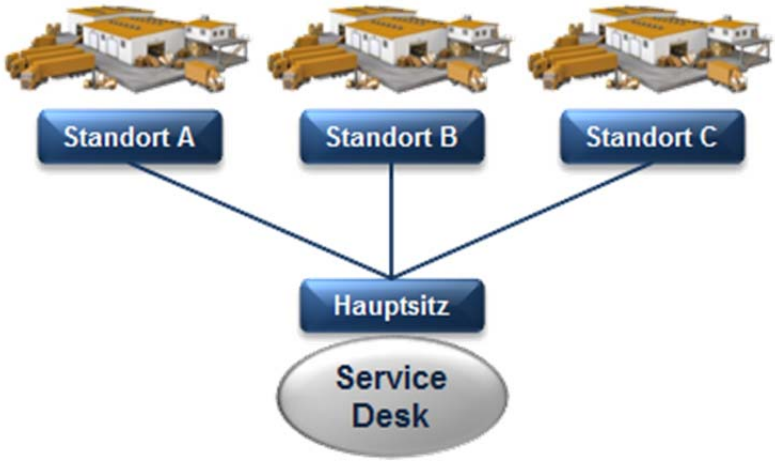


Abb. 84: Zentraler Service Desk

- **Virtueller Service Desk**: Bei einem virtuellen Service Desk sind die Service Desks zwar auf unterschiedliche Orte verteilt, aber alle zentral über einen einzigen Kontakt für den Anwender zu erreichen (Abb. 9).

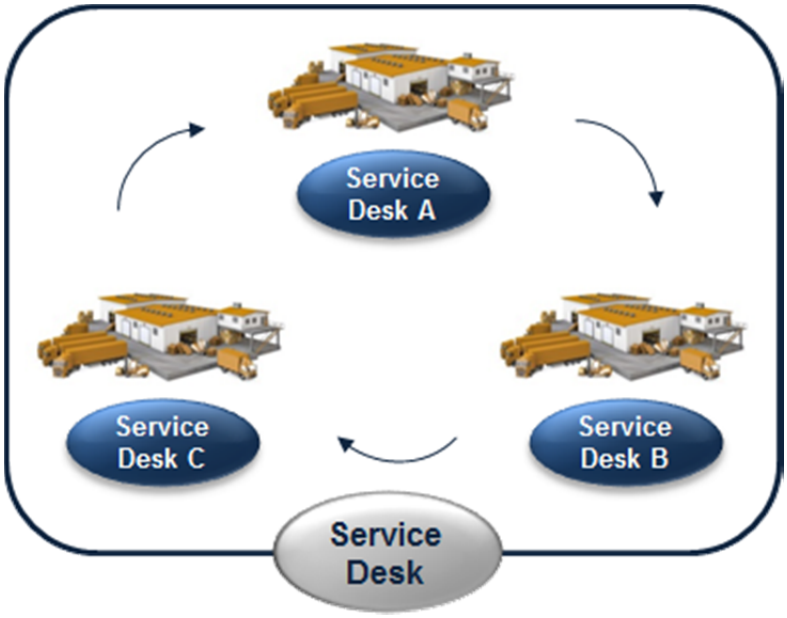


Abb. 85: Virtueller Service Desk

- **Follow the Sun-Service Desk**: Bei der "Follow the Sun"- Organisationsstruktur handelt es sich um eine spezielle Form des virtuellen Service Desks. Über verschiedene Zeitzonen hinweg wird eine durchgängige Erreichbarkeit und Aktivität des Service Desks sichergestellt. Dadurch ist es möglich eine durchgängige Verfügbarkeit des Service Desks im Rahmen von "normalen" Arbeitszeiten der Mitarbeiter zu gewährleisten (Abb. 10).

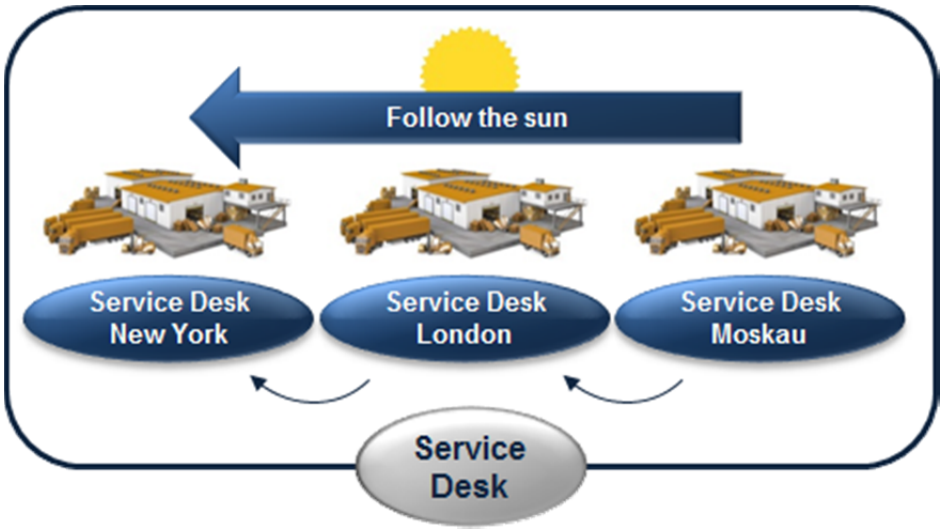


Abb. 86: Follow the Sun-Service Desk

7.2.5 Projektplanung

In der Cronus AG haben wir bereits vor einiger Zeit einen zentralen Service Desk eingeführt. Das heißt, wir können uns jetzt voll und ganz auf die Einführung von ITIL® konzentrieren.

Im Rahmen unseres Gesamtprojekts befassen wir uns mit der Einführung von ITIL®. Exemplarisch werden wir hier nur einen kleinen Bruchteil dieses Gesamtprojekts durchführen: Die Einführung des Prozesses "Incident Management".

Unser Teilprojekt haben wir in sieben Projektschritte unterteilt, wie sie in der Literatur beschrieben werden (Abb. 11). Diese Schritte werden wir nun nach und nach abarbeiten.

Abb. 87: Projektablauf

7.2.6 Situationsanalyse

In einem ersten Schritt habe ich mich damit beschäftigt, in welcher Situation sich die Cronus AG aktuell befindet. Meine Beobachtungen zeigen, dass wir großen Nutzen aus dem Projekt schöpfen können.

Meine Beobachtungen habe ich für Sie in einer SWOT-Matrix zusammengefasst (Abb. 12).

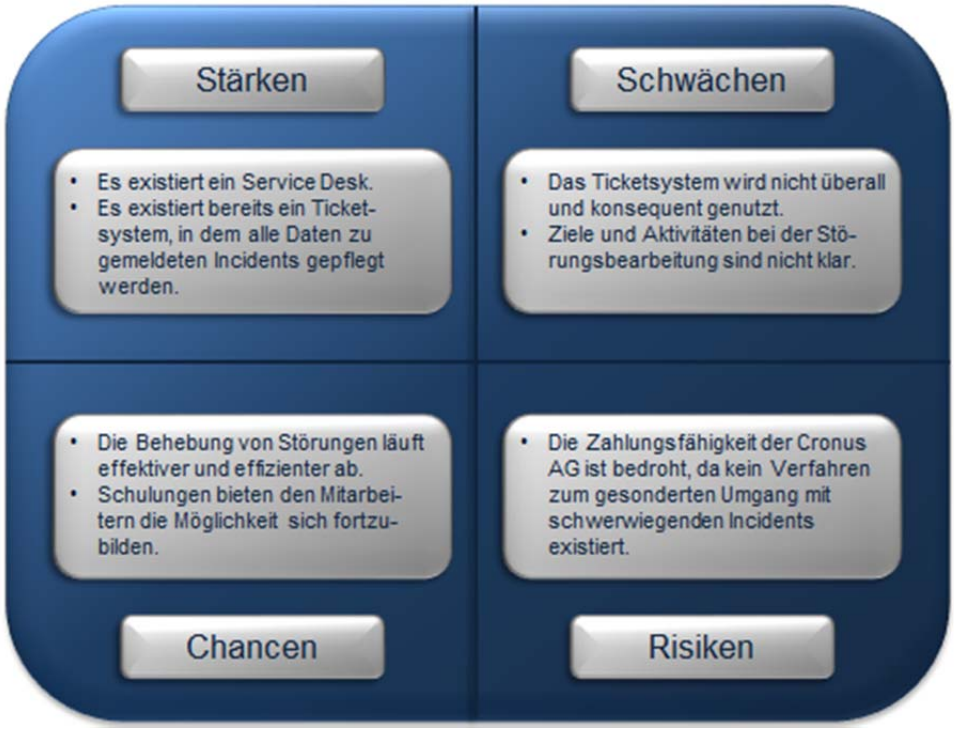


Abb. 88: SWOT-Matrix

7.2.7 Projektsetup

Im ersten Schritt unseres Projekts, dem Projektsetup, haben wir zunächst einige Eckdaten zu unserem Projekt festgelegt, die ich Ihnen nun kurz erläutern möchte.

- **Projektnamen festlegen**: Gemeinsam haben wir uns darauf geeinigt unser Projekt EvI (Einführung von ITIL®) zu nennen. Mit Hilfe dieses Namens können wir in einer späteren Phase Projektmarketing betreiben.

  Dieser Projektname verspricht alles, was wir brauchen: Er ist leicht zu merken, aussagekräftig und motivierend für unsere Mitarbeiter.

- **Projektscope definieren**: Um unsere Mitarbeiter nicht mit einer zu großen Menge an Veränderungen auf einmal zu überfordern, werden wir uns zunächst nur mit der Einführung des Incident Managements befassen. Dadurch wird es uns möglich sein, Störungen schneller zu bearbeiten und die Effizienz unserer IT zu verbessern.

  Das Incident Management ist somit die erste Phase in unserem großen Gesamtprojekt und wird daher den Projektnamen EvI1 erhalten, um immer vor Augen zu haben, dass es sich dabei nur um einen kleinen Teil des Gesamtprojekts handelt.

- **Verantwortungen klären**: Es gibt einige Positionen, die in unserem Projekt auf jeden Fall besetzt sein sollten. Wir haben hierbei besonders darauf geachtet, dass diese Mitarbeiter neben der fachlichen Qualifikation auch genügend Zeit zur Verfügung haben.

So sind verantwortlichen Mitarbeiter in der Lage Fehlentwicklungen des Projekts frühzeitig zu erkennen und entsprechende Maßnahmen einzuleiten.

In unserem Projekt haben wir hierfür einen Auftraggeber, einen Projektleiter und einen Lenkungsausschuss festgelegt.

- **Grobplanung festlegen**: Den voraussichtlichen Zieltermin haben wir mit Hilfe einer Grobplanung bereits bestimmt:

  T - Projektstart

  T+3 Wochen - Abschluss Situationsanalyse

  T+5 Wochen - Abschluss Projektsetup

  T+10 Wochen - Abschluss Prozessnutzendefinition

  T+18 Wochen - Abschluss Prozessdefinition

  T+28 Wochen - Abschluss Prozesse etablieren

  T+32 Wochen - Erfolg prüfen

  Parallel zu den ersten beiden Phasen findet die Ausbildung der Mitarbeiter statt.

Unseren Grobplan haben wir durch einen Projektplan verdeutlicht (Abb. 13).

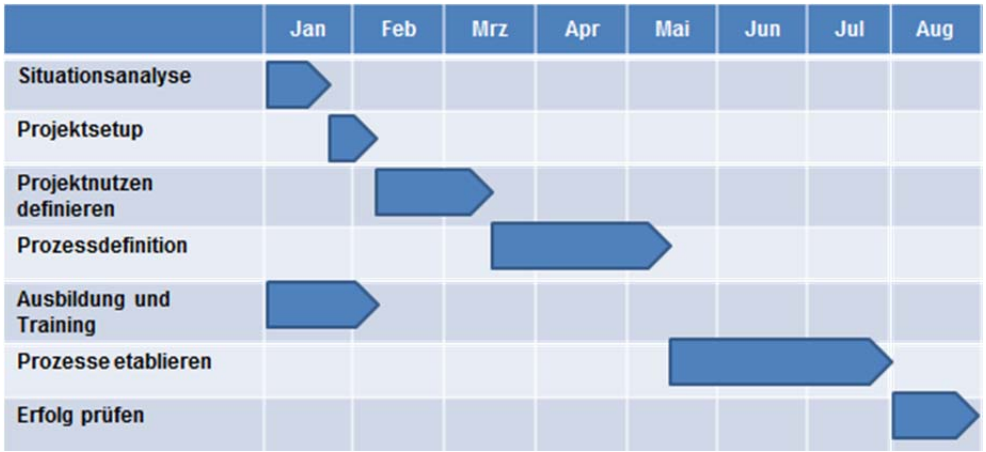


Abb. 89: Projektplan „EvI1“

7.2.8 Projektnutzen definieren

Nachdem wir das Projekt bereits grob durchgeplant haben, müssen wir uns überlegen, wo genau unser Projekt hinführen soll. Dafür haben wir zusammen mit unserem Projektteam in einem zweiten Projektschritt den Nutzen unseres Projekts erarbeitet.

Mit Hilfe von Brainstormings haben wir Aspekte gefunden, die uns besonders wichtig sind. Diese Aspekte haben wir schließlich geordnet und konnten so zwei Hauptaspekte für unser Projekt definieren, die wir mithilfe von ITIL® umsetzen möchten.

- **Minimierung der Supportkosten:**
    - Die Störungsbehebung erfolgt ohne Verzögerung.
    - Anteile von Tickets mit falscher Kategorie werden reduziert.
    - Eine Wissensdatenbank wird aktiv genutzt und gepflegt.
- **Höhere Kundenzufriedenheit:**
    - Die Anwender sind zufrieden.
    - Die vereinbarten Wiederherstellungszeiten werden eingehalten.
    - Beschwerden bezüglich der Lösungsqualität von Incidents nehmen ab.

7.3 Die Projektdurchführung

7.3.1 Ausbildung und Training

Parallel zu den ersten beiden Projektphasen, nahmen unsere IT-Mitarbeiter an zwei Schulungen teil. In der ITIL®-Schulung haben sie zunächst ein Grundverständnis von unserem Projekt EvI1 erlangt. Die Software-Schulung diente dazu, dass unsere IT-Mitarbeiter die Ticketsoftware effektiv und effizient nutzen. Zurzeit verwenden unsere IT-Mitarbeiter diese Software selten oder gar nicht. Das soll sich mit der Einführung des Incident Managements ändern. Unsere IT-Mitarbeiter sind nun mit uns auf einem gemeinsamen Wissensstand und zusammen können wir im nächsten Projektschritt den Incident Management-Prozess für die Cronus AG definieren.

- **ITIL®-Schulung**: Im Rahmen dieser Schulung werden erste Grundlagen zum Thema IT-Service-Management, ITIL® und insbesondere zu dem Prozess "Incident Management" vermittelt. Die Mitarbeiter bekommen einen Überblick darüber, welchen Nutzen die Einführung von ITIL® der Cronus AG bringt und mit welchen Veränderungen sie im täglichen Arbeitsleben rechnen müssen.
- **Software-Schulung**: Im Rahmen ihrer Arbeit werden die Mitarbeiter in Zukunft kontinuierlich mit unserer Ticketsoftware arbeiten. Damit unsere Mitarbeiter die Software

auch beständig im Alltag nutzen, haben wir bereits erste praktische Übungen mit ihnen gemacht und ihnen so den Nutzen der Software vermittelt.

7.3.2 Prozessdefinition

Nachdem nun die Ausgangssituation geklärt ist, können wir die konkrete Definition des Incident Managements starten. Dabei möchten wir unsere Mitarbeiter aktiv einbinden, um Erfahrungswerte direkt in den Prozess einfließen zu lassen.

Diese Projektphase ist besonders wichtig, da hier entschieden wird, wie der spätere Arbeitsalltag unserer Mitarbeiter aussehen wird. Anhand von vier Schritten werden wir auf den folgenden Seiten unseren Incident Management-Prozess genau definieren (Abb. 14).

Abb. 90: Schritte der Prozessdefinition

7.3.3 Prozessdefinition: Ausgestaltung des Prozesses I

Bei der Ausgestaltung des Incident-Management-Prozesses bestimmen wir neben den konkreten Prozessaktivitäten im Fall einer Störung, auch Outputs und Inputs der Cronus AG. In den Prozess gehen zunächst Inputs ein. Diese werden im Rahmen der Prozessaktivitäten zu Outputs verarbeitet.

- Inputs für die Cronus AG sind unter anderem: Informationen zu den Geschäftsprozessen, Informationen zu den vereinbarten Wiederherstellungszeiten, bekannte Fehler und Rückmeldungen von den Anwendern.
- Outputs für die Cronus AG sind unter anderem minimierte Supportkosten, eine höhere Kundenzufriedenheit und vereinbarungsgemäß wiederhergestellte Services.

Ein vereinfachter Prozessablauf (Abb. 15) hilft uns dabei zu verstehen, welche Prozessaktivitäten nacheinander ablaufen müssen.

Abb. 91: Vereinfachter Prozessablauf des Incident-Management-Prozesses

ITIL® gibt uns an dieser Stelle eine Empfehlung, wie der Prozessablauf genau aussehen kann (Abb. 16).

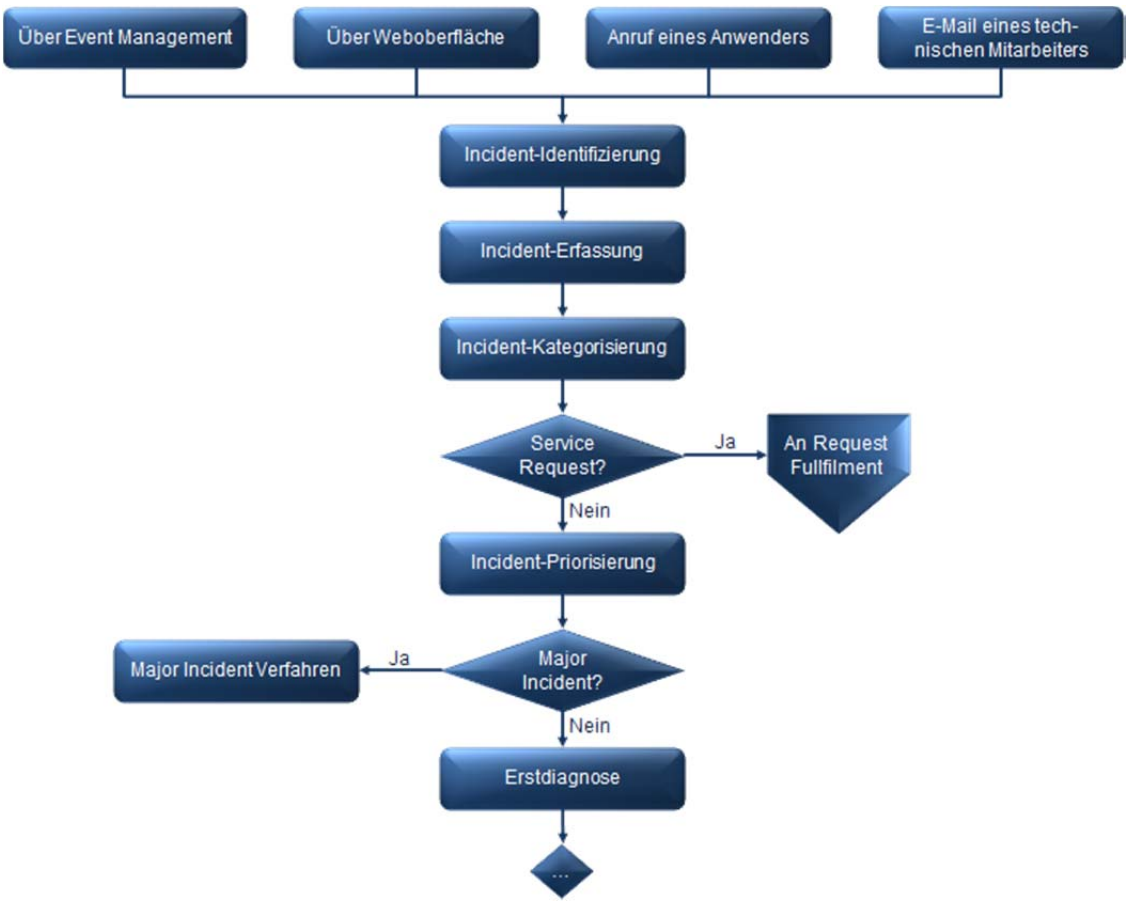


Abb. 92: Originaler ITIL®-Prozessfluss

Der vereinfachte Prozessablauf in Abbildung 15 zeigt, welche Prozessaktivitäten im Prozess "Incident Management" ablaufen. In ITIL® wird dieser Prozessablauf wie in Abbildung 16 abgebildet. Hierbei handelt es sich jedoch nur um einen Auszug aus dem originalen ITIL®-Prozessfluss des Incident-Management-Prozesses.

Die einzelnen Prozessaktivitäten müssen nun auf die Cronus AG abgestimmt werden. Wie das funktioniert, werden wir uns auf der nächsten Seite anhand eines Beispiels anschauen.

7.3.4 Prozessdefinition: Ausgestaltung des Prozesses II

Ein Originalauszug aus dem ITIL®-Prozessfluss zeigt, in welcher Reihenfolge die verschiedenen Prozessaktivitäten des Incident Managements ablaufen sollen. Zum Teil müssen wir die Reihenfolge und die einzelnen Aktivitäten noch auf unser Unternehmen abstimmen. Für die Incident-Priorisierung haben wir dies bereits getan.

In der Aktivität "Incident-Priorisierung" erfasst der Service-Desk-Mitarbeiter, wie weiter mit einem gemeldeten Incident verfahren wird. Diese Priorisierung erfolgt unter Berücksichtigung, wie schnell eine Lösung für den Incident gefunden werden muss und, welche wesentlichen Auswirkungen der Incident auf das Geschäft hat. ITIL® empfiehlt zu diesem Zweck ein einfaches System (Abb. 17). In der Cronus AG wird ein Incident schließlich nach diesem System beurteilt und gelöst.

		Auswirkung		
		Hoch	Mittel	Niedrig
Dringlichkeit	Hoch	1	2	3
	Mittel	2	3	4
	Niedrig	3	4	5

Prioritätscode	Beschreibung	Angestrebte Lösungszeit
1	Kritisch	1 Stunde
2	Hoch	8 Stunden
3	Mittel	24 Stunden
4	Niedrig	48 Stunden
5	Planung	Geplant

Abb. 93: Incident-Priorisierung nach ITIL®

Beispiel: Beim Service Desk der Cronus AG treffen mehrere Meldungen ein: Weder Mitarbeiter der Cronus AG noch Kunden sind in der Lage "Cronus myERP" zu verwenden. Die Betroffenen können ihre Aufgaben nur noch eingeschränkt erfüllen und der finanzielle Schaden liegt bei über 10.000€. Der vom Incident verursachte Schaden nimmt im Zeitverlauf zu und es sind Benutzer mit VIP-Status betroffen.

Zudem besteht eine große Gefahr, dass die Cronus AG durch den Vorfall in den Bankrott abrutscht und der Ruf des Unternehmens nachhaltig geschädigt wird. Daher wird der Incident in die Stufe 1 eingeordnet, mit einer angestrebten Lösungszeit von einer Stunde. Bei dem Incident handelt es sich um einen sogenannten Major Incident.

Bei einem Major Incident handelt es sich um einen schwerwiegenden Incident, der gravierende Unterbrechungen im Geschäftsablauf verursacht und daher mit höherer Dringlichkeit gelöst werden muss.

7.3.5 Prozessdefinition: Definition der Rollen

Damit der Incident-Management-Prozess reibungslos ablaufen kann, ist es nötig, dass wir einige Rollen fest besetzen. ITIL® gibt uns dabei vor, dass wir im Rahmen des Incident Ma-

nagements mindestens vier Rollen besetzen müssen: Incident Manager, 1st Level Support, 2nd Level Support und 3rd Level Support.

Diese Rollen können je nachdem, wer für den Support-Service eines Unternehmens zuständig ist, intern oder extern besetzt werden. Zudem ist es auch möglich, dass eine Person alleine alle Rollen abdeckt.

- **Incident Manager**: Der Incident Manager ist vor allem dafür zuständig Effizienz und Effektivität des Incident-Management-Prozesses voranzutreiben. Er ist sowohl für die Konzeption und Verwaltung des Incident-Management-Prozesses selbst, als auch für das Incident-Management-Verfahren und das Ticketsystem verantwortlich. Zudem fällt das Management von Major Incidents in seinen Aufgabenbereich. In der Cronus AG wird diese Rolle zukünftig von unserem Service-Desk-Leiter besetzt.
- **1st Level Support**: Der 1st Level Support ist die erste Anlaufstelle für eingehende Serviceanfragen. Die Mitarbeiter des 1st Level Supports erfassen die eingehenden Störungen und bearbeiten sie, wenn möglich, selbstständig. Wenn der 1st Level Support eine Störung nicht beheben kann, gibt er das Problem an den 2nd Level Support weiter. In der Cronus AG übernimmt unser eingerichteter Service Desk die Aufgabe des 1st Level Supports.
- **2nd Level Support**: Der 2nd Level Support dient dem 1st Level Support als Unterstützung. Wenn dieser einen Incident technisch oder zeitlich nicht lösen kann, gibt er die Aufgabe an den 2nd Level Support weiter. Dieser verfügt über fachspezifisches Wissen im gefragten Bereich. In der Cronus AG wird die Rolle des 2nd Level Support, je nach Problematik, von Mitarbeitern der IT-Abteilung übernommen.
- **3rd Level Support**: Der 3rd Level Support dient dem 1st und dem 2nd Level Support als Unterstützung. Er wird durch eine Reihe von internen oder externen Teams bereitgestellt und kümmert sich vor allem um Incidents mit tiefgründigen Ursachen oder neue Entwicklungen. Der Netzwerk-, Server- und Datenbank-Support wird für die Cronus AG extern von zwei verschiedenen Unternehmen übernommen.

7.3.6 Prozessdefinition: Definition der Prozesskennzahlen

Mit Hilfe unseres definierten Prozessnutzens, haben wir konkrete Kennzahlen (Abb. 18) abgeleitet, um später zu wissen, ob die Einführung des Prozesses erfolgreich war. Diese Kennzahlen sollen uns dazu dienen, später den Erfolg des Projekts (z. B. im ersten Jahr nach der Einführung unseres Prozesses) zu prüfen. Mit Hilfe der Kennzahlen vergleichen wir unsere Situation vor der Einführung des Incident Managements mit der Situation nach der Einführung.

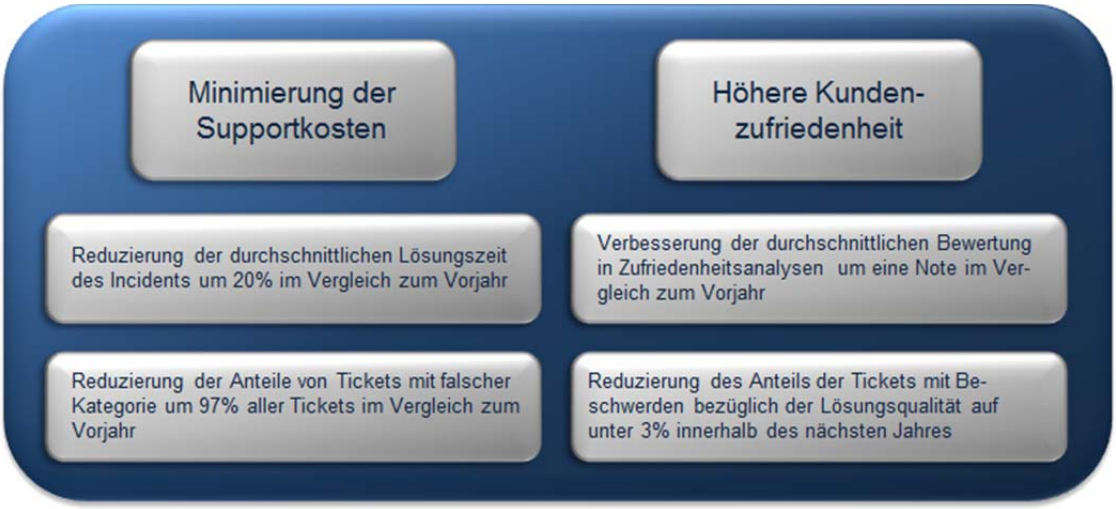


Abb. 94: Prozesskennzahlen

7.3.7 Prozessdefinition: Kriterien des Ticketsystems

Nachdem wir nun den Prozessablauf für den Incident-Management-Prozess auf die Cronus AG abgestimmt haben, müssen wir uns Gedanken über unsere Software machen. Mit Hilfe einer passenden Software müssen unsere IT-Mitarbeiter direkt alle Informationen zu einer gemeldeten Service-Anfrage erfassen.

ITIL® empfiehlt eine Reihe von Eigenschaften, die ein integriertes IT-Service-Management-Programm erfüllen sollte. Die Cronus AG hat Glück, denn wir verwenden bereits eine solche ITIL®- konforme Software: "OTRS IT-Service-Management-Software".

Die Software bietet der Cronus AG alles, was sie zu einem ordnungsgemäßen Betriebsablauf benötigt:

- Alle notwendigen Funktionen werden von der Software abgedeckt.
- Die Software ist intuitiv zu bedienen.
- Der Hersteller liefert die nötige Unterstützung.
- Erweiterungen können einfach eingebunden werden.

Unsere Ergebnisse der Prozessdefinition werden für unsere Mitarbeiter in Form eines Prozesshandbuchs dokumentiert. Dort wird später, wenn ITIL® komplett in der Cronus AG implementiert wurde, jeder Prozess dokumentiert sein.

7.3.8 Prozesse etablieren

Nachdem nun alle Einzelheiten zum Prozess geklärt wurden, starten wir eine Pilotphase für das Incident Management. Im Rahmen einer Pilotphase können wir aufkommende Fragen und Schwierigkeiten klären, bevor die gesamte Cronus AG davon betroffen ist.

Im Anschluss an unsere Pilotphase wird der Incident-Management-Prozess im Gesamtunternehmen eingeführt.

- **Pilotphase**: Unser Prozess wird zu Beginn der Pilotphase zunächst nur für interne Serviceanfragen in der Cronus AG verwendet. So ist es unseren Führungskräften möglich, Fragen unserer Mitarbeiter zu klären und zu schauen, wo unser Prozess noch Defizite aufweist. Im Rahmen der Pilotphase haben wir die Möglichkeiten diese Defizite zu beheben und so den Incident-Management-Prozess zu optimieren.
- **Einführung im Gesamtunternehmen**: Nach Abschluss der Pilotphase werden schließlich nicht nur interne sondern auch externe Service-Anfragen von unserem Support-Team, mit Hilfe des Incident-Management-Prozesses, betreut.

Die Einführung im Gesamtunternehmen ist sehr zeitaufwendig, da Kunden und Mitarbeiter über den neuen Serviceablauf informiert werden müssen. Im Rahmen des Incident Managements müssen Kunden nun z. B. ein Ticket verfassen, falls sie eine Funktionsstörung bei "Cronus myERP" feststellen.

7.3.9 Erfolg prüfen

Seit Einführung des Incident-Management-Prozesses ist viel Zeit vergangen. Nun möchten wir in der letzten Phase von EvI1 prüfen, ob wir unsere Ziele erreichen konnten. Dabei helfen uns die Prozesskennzahlen (Abb. 19), die wir in der Phase "Prozessdefinition" festgelegt haben. Vor Einführung des Incident-Management-Prozesses haben wir diese Kennzahlen bereits einmal gemessen, um jetzt die alte und die neue Situation vergleichen zu können.

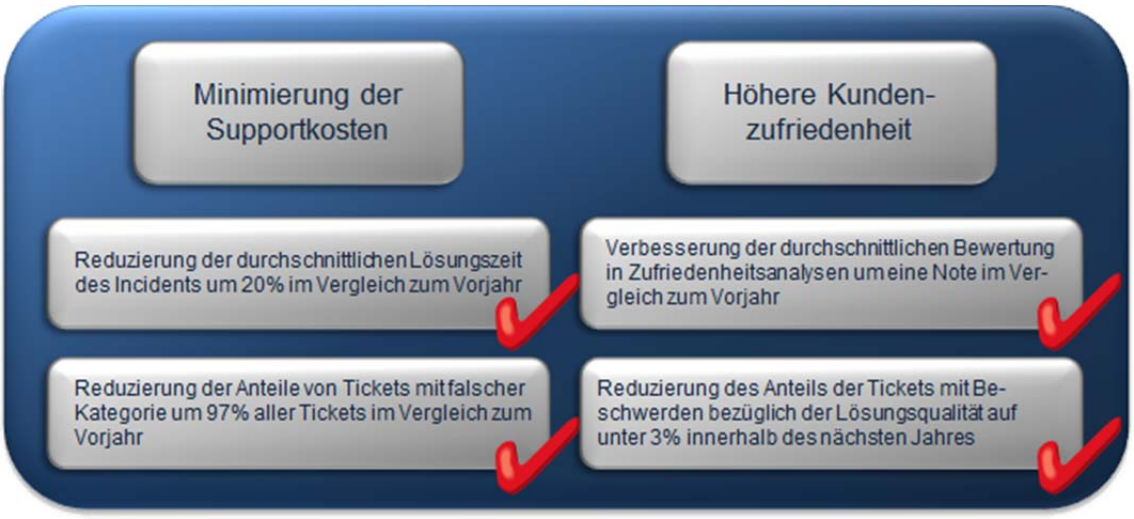


Abb. 95: Bestätigte Prozesskennzahlen

7.3.10 Zusammenfassung und Ausblick

Nachdem wir einen ersten ITIL®-Prozess erfolgreich in der Cronus AG implementiert haben, werden wir uns nun daran setzen, die anderen ITIL®-Prozesse einzuführen.

Damit der Incident-Management-Prozess sich nicht zu einer bürokratischen Last für die Cronus AG entwickelt, muss er kontinuierlich verbessert werden. Um dies zu gewährleisten, werden wir einen weiteren ITIL®-Prozess in der Cronus AG implementieren, den 7-Step-Improvement-Prozess. Im Rahmen dieses Prozesses werden Möglichkeiten zur Verbesserung von Services und Prozessen gesucht und schließlich im Unternehmen etabliert.

Das Incident Management war nur ein winziges Bruchstück unseres Gesamtprojekts und auch die anderen 25 Prozesse werden, ähnlich wie das Incident Management, in unserer AG eingeführt. Bis die Cronus AG ITIL®-konform ist, wird es also noch ein langer Weg!

Wenn unsere ITIL®-Implementierung gut verläuft, werden wir versuchen, in einem letzten Schritt die Zertifizierung über ISO/IEC 20000 zu erreichen. Wie genau das abläuft, werden wir uns gemeinsam im nächsten WBT anschauen.

7.4 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	ITIL® wurde von der britischen Regierungsbehörde CCTA entwickelt, um…		
	…die schlechte Qualität der IT-Dienstleistungen nachhaltig zu verbessern.		
	…Kosten zu senken.		
	…Staatseinnahmen zu generieren.		
2	IT-Innovationen, entwickelt von staatlichen Institutionen, stellen eine Seltenheit dar.		
	Richtig		
	Falsch		
3	Die ITIL®-Handbücher umfassen Best Practice, die nur in Dienstleistungsunternehmen eingesetzt werden können.		
	Richtig		
	Falsch		
4	Einige ITIL®-Prozesse werden in einen Service Lifecycle eingebettet, um Services stetig zu überarbeiten und weiterzuentwickeln.		
	Richtig		
	Falsch		
5	Ein Incident ist unter anderem ein Ereignis, das einen Service unterbrechen kann.		
	Richtig		
	Falsch		
6	Welche Aussage ist richtig? Das Incident Management…		
	…soll möglichst schnell den normalen Servicebetrieb wiederherstellen.		
	…kümmert sich um Incidents und Service Requests.		
	…ist einer der 26 standardisierten ITIL®-Prozesse.		
	…findet sich im Handbuch „Service Operation“ wieder.		

7	Der Prozessfluss zeigt, in welcher Reihenfolge Prozessaktivitäten ablaufen sollen.		
	Richtig		
	Falsch		
8	Welche ITIL®-Funktionen gibt es?		
	Service Desk		
	IT-Operations Management		
	Application Management		
	Request Fulfilment		
9	Welche Aussage ist richtig?		
	Der Service Desk führt in erster Linie die ITIL®-Prozesse „Incident Management“ und „Availability Management“ aus.		
	Die vier Funktionen, die in ITIL® benannt werden, dienen dazu einen stabilen Zustand der Betriebs-IT aufrechtzuerhalten.		
10	Bei einem Major Incident handelt es sich um einen schwerwiegenden Incident, der gravierende Unterbrechungen im Geschäftsablauf verursacht.		
	Richtig		
	Falsch		
11	Welche Aussagen sind richtig?		
	Der Service Desk ist einen von fünf Funktionen, die in ITIL® benannt werden.		
	Je nach Größe, Struktur, Sprache etc. kann der Service Desk unterschiedlich organisiert werden.		
	Durch das Incident Management können negative Auswirkungen auf das Geschäft möglichst klein gehalten werden.		
12	Die ITIL®-Einführung dient unter anderem als Basis für eine Zertifizierung nach ISO/IEC 20000.		
	Richtig		
	Falsch		

13	Welche Rollen müssen im Incident-Management-Prozess besetzt werden?		
	2nd Level Support		
	3rd Level Support		
	Service Desk		
	Incident Manager		

Tab. 8: Lösung zu den Übungsfragen WBT 07 – Fallstudie ITIL®

8 ISO/IEC 20000

8.1 Grundlagen

8.1.1 Einleitung

Im Rahmen der Business-Unit "IT" vertreibt die Cronus AG die ERP-Software "Cronus myERP". Damit wir uns beim Vertrieb dieser Software von unseren Konkurrenten abheben, möchte sich die Cronus AG nach ISO/IEC 20000 zertifizieren. Das ITIL®-Framework bietet an dieser Stelle eine gute Basis zur Zertifizierung nach ISO/IEC 20000.

Im Rahmen des letzten WBT "WBT 07 - Fallstudie ITIL®" wurde bereits ein erster ITIL®-Prozess in der Cronus AG eingeführt. Mittlerweile haben wir alle ITIL®-Prozesse erfolgreich in der Cronus AG implementiert und können nun die konkrete Zertifizierung nach ISO/IEC 20000 angehen.

Los gehts...!

8.1.2 Was ist ISO/IEC 20000?

ISO/IEC 20000 ist eine international anerkannte Norm, die 2005 aus dem nationalen britischen Standard BS 15000 hervorgegangen ist. Der britische Standard BS 15000 wurde von der ISO (International Organization of Standardization) in eine internationale Norm überführt, da das internationale Interesse an BS 15000 wuchs.

ISO/IEC 20000 ist eine Norm zum IT-Service-Management (ITSM), welches in "WBT 07 - Fallstudie ITIL®" thematisiert wurde. In ISO/IEC 20000 werden die Anforderungen für ein professionelles ITSM dokumentiert. ISO/IEC 20000 formuliert diese Anforderungen an das ITSM dabei nur grob. Über Empfehlungen hinaus werden keine konkreten Arbeitsanweisungen zur Umsetzung gegeben.

ISO/IEC 20000 bietet Unternehmen die Möglichkeit, sich zertifizieren zu lassen, um sich dadurch z. B. von Konkurrenzen zu unterscheiden, die nicht nach ISO/IEC 20000 zertifiziert sind.

- Die ISO (Abb. 20) ist der weltweit größte Entwickler von freiwilligen internationalen Normungen und hat mehr als 19.500 internationale Normungen herausgegeben. Finanziert wird die ISO über Beiträge ihrer Mitgliedsorganisationen und Verkaufseinkünfte ihrer Standards.

Einige Normungen werden zusammen mit anderen internationalen Normungsorganisationen, wie der Internationalen elektrotechnischen Kommission (IEC), entwickelt. Aus einer solchen Zusammenarbeit ist auch ISO/IEC 20000 entstanden.

Abb. 96: Logo der ISO

- Es bestehen hohe Übereinstimmung zwischen ITIL® und ISO/IEC 20000, da beide Standards unter dem Einfluss derselben Personen entstanden sind. Aufgrund dieser Übereinstimmungen können konkrete Arbeitsanweisungen zu den Anforderungen aus dem ITIL®-Standard (siehe "WBT 07 - Fallstudie ITIL®") entnommen werden.

Es ist jedoch auch möglich, die geforderten Prozesse in Eigenregie oder mit Hilfe eines anderen Standards zu erstellen, ohne ITIL® zu implementieren.

8.1.3 ISO/IEC 20000 und ITIL®

Damit wir uns beim Vertrieb unserer ERP-Software "Cronus myERP" von unseren Konkurrenten abheben, haben wir uns entschieden, uns nach ISO/IEC 20000 zertifizieren zu lassen. Zu diesem Zweck haben wir ITIL® (Abb. 21) in der Cronus AG implementiert.

Abb. 97: Logo der „Information Technology Infrastructure Library®“

ITIL® unterstützt die IT-Mitarbeiter dabei, unser ITSM konform zu den Anforderungen aus ISO/IEC 20000 zu gestalten. Die Gestaltung der ITSM-Prozesse mit Hilfe von ITIL® ist folg-

lich eine gute Basis für die Vorbereitung auf eine Unternehmenszertifizierung nach ISO/IEC 20000.

Ein Unternehmen muss mehrere Prozesse einführen, um annähernd zertifizierungsfähig zu sein. Diese können mit Hilfe von ITIL® umsetzt werden.

Die markierten ITIL®-Prozesse (Abb. 22) sind deckungsgleich zu den Anforderungen aus ISO/IEC 20000. Somit können sie direkt aus ITIL® übernommen werden. Diese ITIL®-Prozesse (oder äquivalente Prozesse anderer Standards) müssen in einem Unternehmen etabliert werden, um zertifizierungsfähig nach ISO/IEC 20000 zu sein.

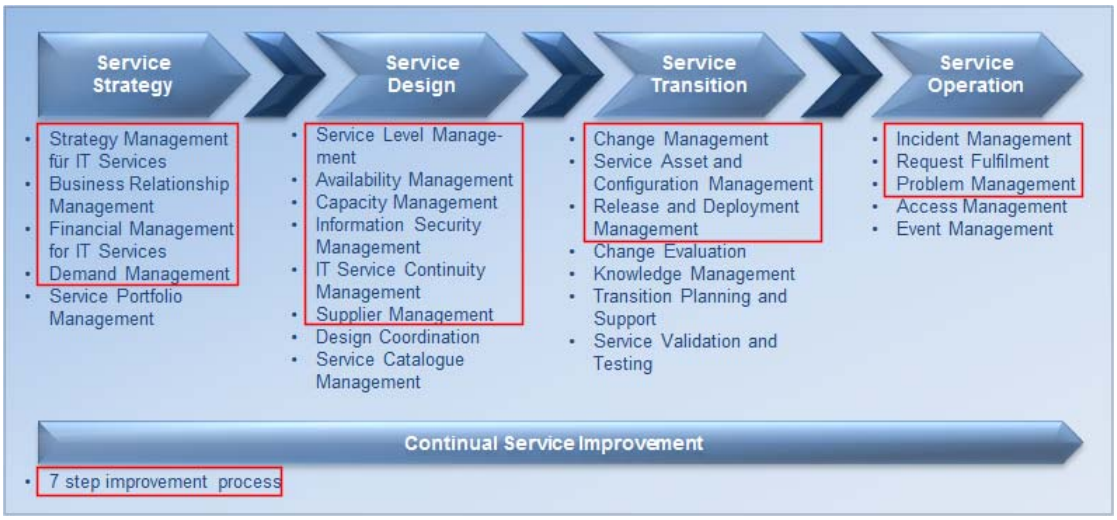


Abb. 98: ITIL®-Prozesse

8.1.4 Ziele der Standardisierung und Zertifizierung

Durch die Implementierung der ISO/IEC 20000-Anforderungen kann die Cronus AG eine hohe Servicequalität und deren kontinuierliche Verbesserung gewährleisten. Standardisierte Begrifflichkeiten erleichtern außerdem die Kommunikation zwischen der Cronus AG und ihren Partnern.

- Damit sich die Zertifizierung für die Cronus AG lohnt, ist es wichtig, dass auch alle Partner der Cronus AG nach ISO/IEC 20000 zertifiziert sind.

  Die Zertifizierung aller Hersteller ist z. B. notwendig, um eine einwandfreie Betreuung für das ERP-System sicherzustellen. Zur Betreuung gehört z. B. auch die Sicherstellung, dass der Server, auf dem die Software läuft, zu 99% der Geschäftszeiten verfügbar ist. Fällt ein Server aus, muss dieser innerhalb von 24h ersetzt werden. Ist der Hersteller des Servers nach ISO/IEC 20000 zertifiziert, kann er diese Problembehebung innerhalb von 24h gewährleisten.

Zudem kann die Cronus AG mit Hilfe der ISO/IEC 20000 den Nachweis für einen erfolgreichen Betrieb ihres ITSM erbringen, um sich so unter anderem von ihren Konkurrenten abzu-

heben. Eine Zertifizierung auf Basis der ISO/IEC 20000 verschafft der Cronus AG die Möglichkeit, ihre Bemühungen um das ITSM und die erfolgreiche Umsetzung einer internationalen Norm offiziell nachzuweisen. Dadurch können Kunden die Leistungsfähigkeit der Cronus AG besser einschätzen.

- Die Erbringung dieses Nachweises erfolgt im Rahmen einer Zertifizierung. Bei einer Zertifizierung wird ein bestimmter Qualitätsstandard gemessen und eine Bescheinigung darüber ausgestellt, dass man das "Richtige" tut. Die Qualität von IT-Services kann mit Hilfe der ISO/IEC 20000-Zertifizierung sichtbarer dokumentiert werden. Eine Zertifizierung wird im Auftrag der ISO durch nationale Zertifizierungsorganisationen, wie z. B. dem TÜV Süd, durchgeführt.

Im Rahmen der Zertifizierung kann ein ganzes Unternehmen, oder nur einzelne Teilbereiche eines Unternehmens, wie z. B. einzelne Standorte oder Services, zertifiziert werden.

8.1.5 Vor- und Nachteile der Standardisierung und Zertifizierung

Durch die Anpassung der Prozesse im Rahmen der ISO-Norm kann die Cronus AG mehrere Vorteile für sich nutzen. Diesen stehen jedoch auch einige Nachteile gegenüber.

Vorteile der Standardisierung und Zertifizierung sind:

- **Transparenz**: Die IT-Infrastruktur und -Prozesse werden durch die Überprüfung und Neuorganisation sowohl für interne (z. B. IT-Leiter), als auch für externe Stakeholder (z. B. Kunden) transparenter.
- **Leistungsfähigkeit**: Durch die Zertifizierungsmaßnahmen werden Defizite in der Qualitäts- und Leistungsfähigkeit aufgedeckt und behoben. Dies führt zu einer Verbesserung der Leistungsfähigkeit der IT-Services.
- **Kompetenz**: Durch die Zertifizierung kann die Kompetenz des ITSM eines Unternehmens objektiv nachgewiesen werden. Dies ist z. B. wichtig, um sich von Konkurrenten abzuheben.

Nachteile der Standardisierung und Zertifizierung sind:

- **Interne Barrieren**: Interne Barrieren, wie z. B. die Abneigung der Mitarbeiter gegen Veränderungen, können den Implementierungs- und Zertifizierungsaufwand zusätzlich erhöhen.
- **Wiederkehrende Kosten**: Es fallen auch langfristig Kosten in einem zertifizierten Unternehmen an, da das Zertifikat nur drei Jahre gültig ist. Um die Zertifizierung beizubehalten, müssen z. B. jährliche Evaluationen durchgeführt werden.

- **Aufwendige Erstzertifizierung**: Durch die erstmalige Zertifizierung entstehen hohe Initialkosten für das Unternehmen, z. B. durch den Einsatz externer Berater oder die Zertifizierungsgebühren.

8.1.6 Das Zertifizierungsverfahren

Das Zertifizierungsverfahren läuft bei allen ISO-Zertifizierungs-Produkten identisch ab. Wenn die Cronus AG ein Zertifikat erhält, ist dieses drei Jahre gültig. Danach muss eine Re-Zertifizierung veranlasst werden, um die kontinuierliche Umsetzung der Anforderungen weiterhin nachweisen zu können. Das Zertifizierungsverfahren läuft in vier Schritten ab (Abb. 23):

- **Vorgespräch**: Vor dem eigentlichen Zertifizierungsprozess findet ein Vorgespräch mit dem Zertifizierer statt. Die Cronus AG erhält im Vorgespräch wichtige Informationen über den Ablauf, die Kosten, die Audit-Themen und die Zeitplanung.
- **Vor-Audit**: Im ersten Schritt der Zertifizierung werden zunächst formale Voraussetzungen geprüft. Die Cronus AG muss Dokumente vorlegen, die anhand von Prüfkriterien gesichtet und bewertet werden. Ein Prüfkriterium ist z. B., ob alle notwendigen Dokumente vorhanden sind.

  Wenn Defizite festgestellt werden, muss die Cronus AG Nachbesserungen durchführen oder die Zertifizierung abbrechen. Die Ergebnisse werden schließlich in einem umfassenden Audit-Report dokumentiert.
- **Nachweis-Audit**: Im zweiten Schritt der Zertifizierung wird die Cronus AG vor Ort begutachtet. Dabei wird stichprobenartig die Umsetzung der Vorgaben, die ISO/IEC 20000 fordert, überprüft. Mängel werden im Audit-Report dokumentiert. Die Cronus AG hat die Möglichkeit, diese Mängel innerhalb einer festgelegten Frist zu beheben.

  Nach positivem Abschluss des Prüfungsprozesses wird ein Zertifikat mit einer Gültigkeit von drei Jahren ausgestellt.
- **Überwachungs-Audit**: Damit die Gültigkeit des Zertifikats gewahrt bleibt, muss die Cronus AG jährlich ein Überwachungs-Audit durchführen lassen. Dieses ist nicht so umfangreich, wie ein Nachweis-Audit.

Nach Ablauf von drei Jahren muss das gesamte Zertifizierungsverfahren noch einmal durchlaufen werden, um die Gültigkeit des Zertifikats zu erhalten.

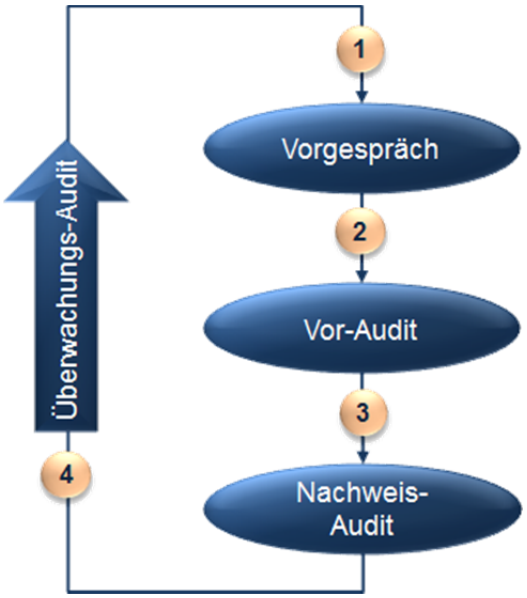


Abb. 99: Zertifizierungsverfahren

8.2 Aufbau der ISO-Norm 20000

8.2.1 Einleitung

Im ersten Kapitel haben wir einige Grundlagen zum Thema ISO/IEC 20000 kennengelernt. Nun wissen wir, wie eine Zertifizierung nach ISO/IEC 20000 abläuft und welche Vor- und Nachteile mit einer Standardisierung und einer Zertifizierung verbunden sind.

In diesem Kapitel werden wir uns mit dem Aufbau von ISO/IEC 20000 beschäftigen. Diese ISO-Norm gibt uns eine Reihe von Pflichtanforderungen vor, die wir für eine Zertifizierung erfüllen müssen. Neben diesen Anforderungen gibt ISO/IEC 20000 uns jedoch auch noch weitere Umsetzungsempfehlungen, die uns helfen sollen, diese Anforderungen zu erfüllen.

Doch was genau sind diese verpflichtenden Anforderungen? Schauen wir es uns gemeinsam an!

8.2.2 Struktur der ISO-Norm

Die ISO/IEC 20000 besteht aus den zwei Hauptteilen ISO/IEC 20000-1 und ISO/IEC 20000-2. Die gesamte ISO-Norm baut auf einer Reihe von Frameworks auf, die eine gute Grundlage zur Zertifizierung eines Unternehmens sind (Abb. 24).

- **Die Pflichtanforderungen** (ISO/IEC 20000-1): Im ersten Teil der ISO/IEC 20000 werden alle Pflichtanforderungen beschrieben, die die Cronus AG erfüllen muss, um eine Zertifizierung zu erreichen.

Diese Vorgaben müssen zwingend erfüllt sein, da eine Zertifizierung sonst nicht erlangt werden kann.

- **Die Umsetzungshilfe** (ISO/IEC 20000-2): Der zweite Teil der ISO/IEC 20000 enthält Empfehlungen zur Umsetzung der Pflichtanforderungen aus Teil 1 und beschreibt, was im Unternehmen zusätzlich getan werden sollte.

  Dieser Teil der ISO-Norm muss für die Zertifizierung nicht zwingend umgesetzt werden, sondern bietet Leitlinien und Erläuterungen zur Umsetzung von ISO/IEC 20000-1.

- **Die Basis zur Zertifizierung** (andere Frameworks und Standards): Die gesamte ISO-Norm baut auf unterschiedlichen Frameworks und Standards auf, wie z. B. dem ITIL®- und dem COBIT®-Framework.

Die Pflichtanforderungen können mit Hilfe einer Kombination dieser Frameworks im Unternehmen umgesetzt werden. Auch andere ISO-Standards sind eine gute Basis zur Zertifizierung nach ISO/IEC 20000. So orientiert sich ISO/IEC 20000 z. B. an den Grundlagen des Qualitätsmanagements, wie sie in ISO 9000 beschrieben sind. ISO/IEC 20000 bietet zudem noch drei Erläuterungen zur Umsetzung von ISO/IEC 20000-1 an, die am Ende des WBT thematisiert werden.

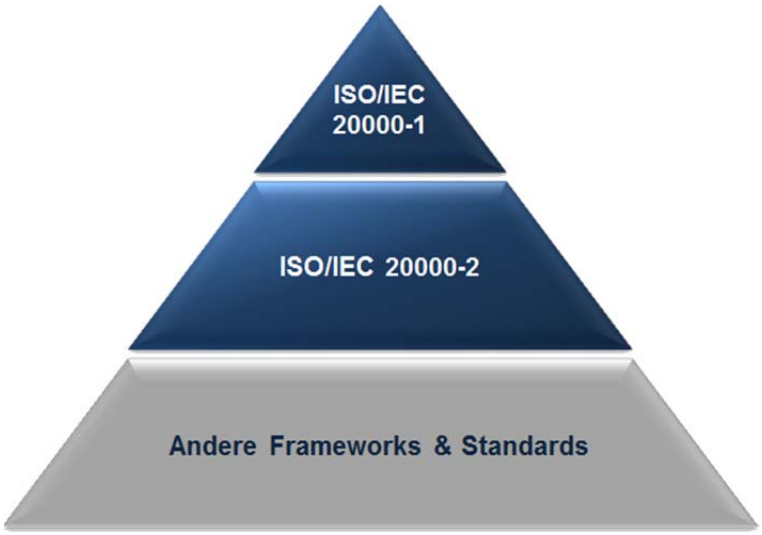


Abb. 100: Struktur der ISO-Norm

8.2.3 Bestandteile der ISO-Norm

Die ISO/IEC 20000-1 ist in neun Abschnitte gegliedert (Abb. 25). Die ersten fünf Abschnitte dienen zur Festlegung der Rahmenbedingungen und Maßgaben. Die verbleibenden vier Abschnitte beschreiben die notwendigen IT-Service-Management-Prozesse.

- Im ersten Abschnitt der ISO/IEC 20000-1 werden Anforderungen und Rahmenbedingungen zur Zertifizierung definiert.
- Der zweite Abschnitt der ISO/IEC 20000-1 dient der Erläuterung von anderen zugrundeliegenden Standards. In ISO/IEC 20000-2 wird z. B. ISO/IEC 20000-1 an dieser Stelle genannt.
- Im dritten Abschnitt der ISO/IEC 20000-1 werden grundlegende Begriffe und Definitionen geklärt, die im weiteren Verlauf der Norm wieder aufgegriffen werden.
- Der vierte Abschnitt der ISO/IEC 20000-1 befasst sich unter anderem mit dem Aufbau und der kontinuierlichen Verbesserung des IT-Service-Management-Systems. Was ein IT-Service-Management-System ist und wie Abschnitt [4] aufgebaut ist, wird auf der nächsten Seite erläutert.
- Der fünfte Abschnitt der ISO/IEC 20000-1 befasst sich mit der Bereitstellung neuer oder geänderter Services. Bei der Bereitstellung sollen sowohl die vereinbarte Qualität, als auch die vereinbarten Kosten eingehalten werden.
- In den Abschnitten sechs bis neun der ISO/IEC 20000-1 werden die notwendigen IT-Service-Management-Prozesse beschrieben. Zu diesem Zweck werden die Prozesse in fünf Prozessbereiche gegliedert. Die einzelnen Prozessgruppen werden im WBT noch genauer betrachtet.

Abb. 101: Bestandteile der ISO-Norm

8.2.4 ISO/IEC 20000-1: [4]: Das IT-Service-Management-System

Der vierte Abschnitt der ISO/IEC 20000-1 befasst sich unter anderem mit dem Aufbau und der kontinuierlichen Verbesserung des IT-Service-Management-Systems.

- Ein IT-Service-Management-System beschreibt alle Prozesse und Ressourcen, die koordiniert eingesetzt werden, um die vereinbarten Ziele der IT-Services zu erreichen. Ein funktionierendes IT-Service-Management-System ermöglicht eine effektive und effiziente Bereitstellung von IT-Services.

Anhand des PDCA-Zyklus nach Deming (Abb. 26) zeigt dieser Abschnitt auf, wie die notwendigen Maßnahmen für den Aufbau und die kontinuierliche Verbesserung des IT-Service-Management-Systems implementiert werden sollen. Dem IT-Mitarbeiter wird eine Handlungsrichtlinie vorgegeben, um die notwendigen ITSM-Prozesse umzusetzen.

Das PDCA-Modell (Plan-Do-Check-Act) geht davon aus, dass es vier Schritte gibt, die zyklisch ausgeführt werden:

- **Plan (Planen)**: Ausarbeitung der Prozesse und Ziele, die zum Erreichen der Ergebnisse erforderlich sind.

  Ziel: Planung der Einführung und Bereitstellung des IT-Service-Managements.

  ISO/IEC 20000-1 schreibt die Erstellung eines IT-Service-Management-Plans vor. In diesem Plan müssen unter anderem Ziele, Anforderungen und Verantwortlichkeiten festgelegt werden.

- **Do (Durchführen)**: Umsetzen der erforderlichen Prozesse.

  Ziel: Einführung der IT-Service-Management-Ziele und des IT-Service-Management-Plans.

Im Rahmen dieser Phase müssen Maßnahmen, wie z. B. ein Risikomanagement oder die Freigabe und Zuweisung der benötigten Finanzmittel, durchgeführt werden.

- **Check (Überprüfen)**: Überprüfen der Prozessabläufe und Services bezüglich der Zielerreichung und der Anforderungen.

  Ziel: Überwachung der Wirksamkeit der eingeführten Maßnahmen.

  ISO/IEC 20000-1 verpflichtet das Management der Cronus AG zu überprüfen, ob das IT- Service-Management konform mit der Norm durchgeführt wird und, ob die Maßnahmen effektiv umgesetzt werden.

- **Act (Handeln)**: Erkennen von Maßnahmen, die zur kontinuierlichen Verbesserung der Prozesse beitragen.

  Ziel: Verbesserung von Effektivität und Effizienz der IT-Service-Erbringung.

  ISO/IEC 20000-1 fordert die Existenz einer Richtlinie für die kontinuierliche Service-Verbesserung. Die Maßnahmen zur Verbesserung müssen dabei durch einen Prozess kontinuierlich gesteuert werden.

Abb. 102: PDCA-Zyklus

8.2.5 Prozessgruppen

In den Abschnitten [6] bis [9] der ISO/IEC 20000-1 werden die notwendigen IT-Service-Management-Prozesse (Abb. 27) beschrieben. Diese Prozesse müssen nicht zwangsläufig von der Cronus AG selbst betrieben werden. Es ist ebenfalls möglich, dass diese Prozesse vollständig oder teilweise durch andere Unternehmen übernommen werden.

In ISO/IEC 20000-1 werden vier Prozessgruppen beschrieben:

- **Service Delivery Processes**: ISO/IEC 20000-1 fordert sechs Servicebereitstellungs- und Lieferungsprozesse:

  Service Level Management, Capacity Management, Service Continuity and Availability Management, Information Security Management, Service Reporting und Budgeting and Accounting for Services.

- **Relationship Processes**: Im Rahmen der Relationship-Prozesse werden alle Aspekte der Beziehungen zwischen dem Service-Anbieter zu seinen Lieferanten, und zu seinen Kunden beschrieben.

- **Resolution Processes**: ISO/IEC 20000-1 fordert die Implementierung von Lösungsprozessen, wie dem Incident Management. Der Fokus dieser Prozesse liegt auf dem Umgang mit Störungen und Problemen.

- **Control Processes**: Im Rahmen der Steuerungsprozesse werden IT-Infrastruktur und IT-Services gesteuert und überwacht. Dadurch kann ein effektiver Umgang mit IT-Infrastruktur und IT-Services gewährleistet werden.

Abb. 103: Prozessgruppen

8.2.6 Ergänzungen von ISO/IEC 20000

Neben ISO/IEC 20000-1 und ISO/IEC 20000-2 bietet ISO/IEC 20000 drei Ergänzungen. Die drei Ergänzungen ISO/IEC 20000-3, ISO/IEC 20000-4 und ISO/IEC 20000-5 geben Empfehlungen und Hilfestellungen zur Umsetzung von ISO/IEC 20000-1 und ISO/IEC 20000-2 weiter.

Es gibt drei Ergänzungen von ISO/IEC 20000:

- **ISO/IEC 20000-3**: ISO/IEC 20000-3 dient als Hilfestellung zur Umsetzung von ISO/IEC 20000-1 und ISO/IEC 20000-2. Im Fokus steht dabei die Implementierung eines Management-Systems für alle IT-Services.

- **ISO/IEC 20000-4**: ISO/IEC 20000-4 beschreibt ein Prozessreferenzmodell zur Umsetzung der Service-Management-Prozesse, die in ISO/IEC 20000-1 gefordert werden. Die verschiedenen Prozesse werden in dieser Ergänzung detailliert beschrieben.
- **ISO/IEC 20000-5**: ISO/IEC 20000-5 gibt ein exemplarisches Beispiel zur Implementierung eines Service Managements, mit dem die Pflichtanforderungen aus ISO/IEC 20000-1 erfüllt werden können.

8.2.7 Zusammenfassung und Ausblick

In diesem WBT haben wir die ISO-Norm ISO/IEC 20000 kennengelernt. Eine Zertifizierung nach ISO/IEC 20000 ist keineswegs einfach!

Neben hohen Kosten und einem großen Implementierungsaufwand der Pflichtanforderungen müssen wir uns alle drei Jahre neu zertifizieren lassen. Um den Pflichtanforderungen von ISO/IEC 20000 auch weiterhin zu genügen, müssen alle betroffenen Prozesse stetig überprüft und verbessert werden.

Wie wir gesehen haben, bringt diese Zertifizierung allerdings auch viele Vorteile mit sich. So kann sich die Cronus AG nun endlich beim Vertrieb der "Cronus myERP" von ihren Konkurrenten abheben. Dies ist insbesondere im Hinblick auf öffentliche Ausschreibungen z. B. bei der EU ein großer Vorteil im Vergleich zu anderen Mitbewerbern.

Im Rahmen der WBT-Serie "IT-Governance" haben Sie einen umfassenden Überblick zum Thema IT-Governance bekommen. Weiterführende Informationen zu diesem Thema können Sie dem Reader der Veranstaltung und der Literatur entnehmen.

8.3 Abschlusstest

Nr.	Frage	Richtig	Falsch
1	Eine Zertifizierung nach ISO/IEC 20000 ist sinnvoll, um…		
	…den Nachweis für einen erfolgreichen Betrieb eines ITSM zu erbringen.		
	…sich von Konkurrenten abzuheben.		
	…Kosten im IT-Bereich zu vermeiden.		
2	Ein ISO/IEC 20000-Zertifikat ist zwei Jahre gültig. Danach muss sich die Cronus AG einer erneuten Zertifizierung unterziehen.		
	Richtig		
	Falsch		
3	ISO/IEC 20000 ist eine international anerkannte Norm, die aus dem britischen Standard BSI 15000 hervorgegangen ist.		
	Richtig		
	Falsch		
4	ISO/IEC 20000-2 ist genau wie ISO/IEC 20000-1 in neun Abschnitte gegliedert.		
	Richtig		
	Falsch		
5	Ein IT-Service-Mangement-System beschreibt alle Prozesse und Ressourcen, die koordiniert eingesetzt werden, um die vereinbarten Ziele der IT-Services zu erreichen.		
	Richtig		
	Falsch		

6	Welche Aussage ist richtig? ISO/IEC 20000…		
	…ist eine Norm zum IT-Service-Management.		
	…bietet konkrete Arbeitsanweisungen zur Umsetzung eines IT-Service-Managements.		
	…bietet Unternehmen die Möglichkeit, sich zertifizieren zu lassen.		
	…ist 2005 aus dem nationalen Standard BS 15000 hervorgegangen.		
7	Die geforderten Prozesse aus ISO/IEC 20000-1 können auch ohne die Hilfe von ITIL® eingeführt werden.		
	Richtig		
	Falsch		
8	Welche Prozessgruppen werden in ISO/IEC 20000-1 beschrieben?		
	Servicebereitstellungs- und Lieferungsprozesse		
	Lösungsprozesse		
	Steuerungsprozesse		
	Freigabeprozesse		
9	Welche Aussage ist richtig?		
	In der Phase „Act“ des PDCA-Zyklus werden die erforderlichen Prozesse umgesetzt.		
	Der PDCA-Zyklus umfasst die vier Phasen „Plan“, „Do“, „Check“ und „Act“.		
10	ISO/IEC 20000-1 und ISO/IEC 20000-2 sind Gegenstand einer Zertifizierung und müssen eingehalten werden.		
	Richtig		
	Falsch		

11	Welche Aussagen sind richtig?		
	ISO/IEC 20000-1 ist in neun Abschnitte gegliedert.		
	In ISO/IEC 20000-1 werden alle Pflichtanforderungen beschrieben, die ein Unternehmen erfüllen muss, um eine Zertifizierung zu erreichen.		
	Durch eine Zertifizierung werden die IT-Infrastruktur und –Prozesse transparenter. Dies ist ein Nachteil der Zertifizierung.		
12	Neben den beiden Hauptteilen ISO/IEC 20000-1 und ISO/IEC 20000-2 bietet ISO/IEC 20000 noch drei Ergänzungen zur eigentlichen ISO-Norm.		
	Richtig		
	Falsch		
13	Welche Schritte laufen bei einem Zertifizierungsverfahren ab?		
	Vor-Audit		
	Überwachungs-Audit		
	Nach-Audit		
	Nachweis-Audit		

Tab. 9: Übungsfragen WBT 08 – ISO/IEC 20000

Anhang

Lösungen zu den Übungsfragen in WBT 01

Nr.	Frage	Richtig	Falsch
1	Die Informationstechnologie hat in den letzten Jahrzehnten einen starken Bedeutungswandel erlebt. Dabei hat sich die Bedeutung der Informationstechnologie von der Nutzung als Rationalisierungs- und Automatisierungsinstrument hin zur heutigen strategischen Unterstützungs- und Servicefunktion hin entwickelt.		
	Richtig		X
	Falsch	X	
2	Heute ist die gesamte Wertschöpfungskette eines Unternehmens von IT durchzogen.		
	Richtig	X	
	Falsch		X
3	Da die gesamte unternehmensübergreifende Wertschöpfungskette komplett von IT-systemen durchzogen ist, werden Schnittstellen vermieden und somit sinkt das Risiko von IT-Fehlern, wie sie am Beispiel der Deutschen Bahn, Deutschen Telekom und Swiss Life beschrieben sind.		
	Richtig		X
	Falsch	X	
4	Heute lässt sich die IT aus welchen vier Perspektiven beschreiben?		
	IT als Servicefaktor		X
	IT als Wettbewerbsfaktor	X	
	IT als Produktionsfaktor	X	
	IT als Nutzenfaktor		X
	IT als Risikofaktor	X	
	IT als Kostenfaktor	X	

5	Bezogen auf den privatwirtschaftlichen Unternehmenssektor kann Corporate Governance allgemein als rechtlicher und faktischer Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens interpretiert werden.		
	Richtig	X	
	Falsch		X
6	Corporate Governance, als Teilbereich der IT-Governance, beschreibt den Prozess der verantwortungsvollen Steuerung von IT im Unternehmen.		
	Richtig		X
	Falsch	X	
7	IT-Governance lässt sich in zwei Teilbereiche aufteilen: IT-Performance und IT-Compliance.		
	Richtig	X	
	Falsch		X
8	Die IT-Performance, als innengerichtete Sichtweise der IT-Governance, beschreibt das regelkonforme Verhalten in der IT. Das meint den Zustand, in dem alle für die Unternehmens-IT relevanten Rechtsnormen (Gesetze und die damit zusammenhängenden Bestimmungen und Verordnungen) sowie Regelwerke nachweislich eingehalten werden.		
	Richtig		X
	Falsch	X	
9	Zur Messung von Performance gibt es allgemein zwei Verfahren: qualitative und quantitative Verfahren der Messung.		
	Richtig	X	
	Falsch		X
10	Eine interne Vorgabe an die man sich der IT-Compliance nach halten soll kann z. B. ein Service-Level-Agreement mit anderen Fachabteilungen sein.		
	Richtig		X
	Falsch	X	

Tab. 10: Lösung zu den Übungsfragen WBT 01

Lösungen zu den Übungsfragen in WBT 02

Nr.	Frage	Richtig	Falsch
1	IT-Performance befasst sich mit dem Vergleich von Kosten und Nutzen. Ist der Nutzen höher als die Kosten für z. B. die gesamte IT-Abteilung oder ein einzelnes IT-Projekt wird ein negativer Wertbeitrag zur Unternehmenssituation geleistet.		
	Richtig		X
	Falsch	X	
2	Das "Produktivitätsparadoxon der IT" besagt jedoch, dass kein empirischer positiver Zusammenhang zwischen Investitionen in die IT und der Produktivität eines Unternehmens besteht.		
	Richtig	X	
	Falsch		X
3	Im Zusammenhang mit der Diskussion um das Produktivitätsparadoxon der IT, wurde ein kontrovers diskutierter Beitrag namens "IT doesn’t matter" veröffentlicht. Die daraufhin erneut entbrannte Diskussion hat herausgestellt, dass die IT tatsächlich keinen Wertbeitrag zur Unternehmenssituation liefern kann.		
	Richtig		X
	Falsch	X	
4	In der Cronus AG wird die Umsetzung von Business-IT-Alignment in drei Phasen unterteilt. Die drei Phasen sind:		
	Soll- und Ist-Analyse		X
	Bestandsaufnahme	X	
	Messung und IT-Compliance	X	
	Anpassung	X	
	Messung der IT-Compliance		X
5	Diese Ausrichtung der Unternehmensziele und -strategie an die IT wird Business-IT-Alignment genannt.		
	Richtig		X
	Falsch	X	

6	Mit Hilfe des Strategic Alignment Models (SAM) lässt sich der Zusammenhang zwischen IT und Business theoretisch darstellen. Die einzelnen Pfeile zeigen, wie man das strategische Alignment im Unternehmen umsetzt.		
	Richtig		X
	Falsch	X	
7	Die zweite Phase beinhaltet die Anpassung der IT-Strategie an die Unternehmensstrategie. Damit ist die Anpassung von z. B. Systemen, Aktivitäten und Entscheidungsmustern im IT-Bereich an die Unternehmensziele und -Strategien gemeint.		
	Richtig	X	
	Falsch		X
8	Die erste Phase des Umsetzungsplans von Business-IT-Alignment der Cronus AG ist die Bestandsaufnahme. Im Zuge der Bestandsaufnahme wird eine Situationsanalyse durchgeführt. Die Situationsanalyse soll die vorhandene strategische Rolle der IT im Unternehmen betrachten. Dazu wird das Modell der kritischen Erfolgsfaktoren angewendet.		
	Richtig		X
	Falsch	X	
9	Ein typischer kritischer Erfolgsfaktor (KEF) für die Abteilung „Vertrieb“ ist der gewinnmaximale Umsatz.		
	Richtig	X	
	Falsch		X
10	Die zweite Phase des Umsetzungsplans von Business-IT-Alignment der Cronus AG ist die Anpassung. Im Zuge der Anpassung wird eine Strategie entwickelt. Dazu werden die IT-Ziele mit Kontrollgrößen versehen. Zur Zielplanung wird das Modell der kritischen Erfolgsfaktoren (KEF) angewendet.		
	Richtig	X	
	Falsch		X

11	Kosten von IT-Leistungen lassen sich unterteilen in einmalige und laufende Kosten. Es handelt sich bei Kosten immer um qualitative Werte.		
	Richtig		X
	Falsch	X	
12	Der Nutzen von IT-Leistungen setzt sich in der Regel sowohl aus quantitativen und qualitativen Werten zusammen.		
	Richtig	X	
	Falsch		X
13	Ein typisches Verfahren zur Ermittlung des quantitativen Nutzens ist die Nutzwertanalyse. Dabei werden Kriterien mit Hilfe des Scoring-Ansatzes bewertet und gewichtet.		
	Richtig		X
	Falsch	X	

Tab. 11: Lösung zu den Übungsfragen WBT 02

Lösungen zu den Übungsfragen in WBT 03

Nr.	Frage	Richtig	Falsch
1	Aus welchen Bestandteilen besteht die Business-Impact-Management-Pyramide?		
	Systems-Management	X	
	Geschäftsprozess-Management	X	
	IT-Performance-Management		X
	Service-Level-Management	X	
2	Das Business-Impact-Management verbindet die IT-Ressourcen mit den Geschäftsprozessen eines Unternehmens. So kann mit Hilfe des BIM eine Aussage über den Wertbeitrag der IT zum Unternehmenserfolg getätigt werden.		
	Richtig	X	
	Falsch		X
3	Das Systems-Management hat zum Ziel, die vorhandenen IT-Ressourcen technisch zu überwachen.		
	Richtig	X	
	Falsch		X
4	Ein Service-Level-Agreement beschreibt einen Vertrag zwischen der IT-Abteilung und der jeweiligen Fachabteilung. Ein Beispiel für ein SLA ist ein Vertrag über die Verfügbarkeit von dem CRM-System. Über eine kleine IT-Komponente wie z. B. Drucker werden kein SLA abgeschlossen.		
	Richtig		X
	Falsch	X	
5	Ziel vom Business-Impact-Management ist es, IT-Services mit den Geschäftsprozessen in Verbindung zu bringen.		
	Richtig		X
	Falsch	X	
6	Auf Grund der zahlreichen Vorteile, die eine BIM-Lösung hat, lohnt es sich auch für kleine Unternehmen eine BIM zu implementieren.		
	Richtig		X
	Falsch	X	

7	Das Geschäftsprozess-Management ist der erste Schritt der Implementierung von Business-Impact-Management in der Cronus AG. Dabei werden alle Geschäftsprozesse der Cronus AG durch die Unternehmensleitung identifiziert und modelliert.		
	Richtig	X	
	Falsch		X
8	Das Systems-Management ist der dritte Schritt zur Implementierung von BIM in der Cronus AG. Das Systems-Management meint dabei die Überwachung der Service-Level-Agreements.		
	Richtig		X
	Falsch	X	
9	SLA ist die Abkürzung für …		
	Systems-Level-Management		X
	Service-Level-Management	X	
	Software-Level-Management		X

Tab. 12: Lösung zu den Übungsfragen WBT 03

Lösungen zu den Übungsfragen in WBT 04

Nr.	Frage	Richtig	Falsch
1	Die Unternehmenspleite von ENRON ist zurückzuführen auf…		
	Unzureichende interne Kontrollsysteme.	X	
	Große Freiheitsgrade der Manager.	X	
	Eine schlechte Konjunkturlage.		X
2	Die Skandale zu Beginn des 21ten Jahrhunderts hatten keinen Einfluss auf das Vertrauen der Anleger.		
	Richtig		X
	Falsch	X	
3	Die Erfüllung von regulatorischen Anforderungen wird als Governance bezeichnet. Die entwickelten Gesetze und Regelwerke sollen Unternehmen zu einem transparenten Verhalten zwingen.		
	Richtig		X
	Falsch	X	
4	Die Business Unit „IT“ setzt sich aus den Mitarbeitern der sekundären IT-Abteilungen aller Business Units zusammen.		
	Richtig		X
	Falsch	X	
5	Die zentrale IT-Unit versteht sich als Dienstleister für die sekundären IT-Abteilungen der anderen Units.		
	Richtig	X	
	Falsch		X
6	In welche Unterbereiche lässt sich IT-Governance unterteilen?		
	IT-Management		X
	IT-Performance	X	
	IT-Compliance	X	
	IT-Controlling		X
7	In der Betrachtung - IT als Instrument – werden konkrete Anforderungen an die Daten und Informationsverarbeitung gestellt. Die IT ist der Träger von Compliance Anforderungen.		
	Richtig		X
	Falsch	X	

8	In welche Komponenten lässt sich IT-Compliance unterteilen?		
	Vorsorge gegen Gesetzesverstöße	X	
	Einrichtung eines Risikomanagement	X	
	Implementierung eines internen Kontrollsystems		X
	Persönliche Haftung des Managements	X	
9	Welche Aussage ist richtig?		
	Manager können von der persönlichen Haftung nicht entbunden werden.		X
	IT-Risikomanagement beschreibt die Schnittmenge aus IT-Risiken und Risiken aus Regelverstößen. Diese Schnittmenge wird als IT-Compliance-Risiken bezeichnet.	X	
10	Eine isolierte Betrachtung von IT-Compliance stellt sicher, dass alle Einflussfaktoren der IT auf ein Unternehmen berücksichtigt werden.		
	Richtig		X
	Falsch	X	
11	Welche Aussagen sind richtig?		
	Das Hauptinteresse der Eigenkapitalgeber liegt in der Erwirtschaftung einer möglichst hohen Rendite.	X	
	Der Hauptfokus des IT-Managements liegt zukünftig auf dem Managen von typischen IT-Risiken (z. B. Firewalls).		X
	Die Unternehmensleitung wird durch interne Kontrollsysteme verpflichtet, sich an die Rahmenbedingungen der Cronus AG zu halten.	X	
	Mitarbeiter sind keine relevante Anspruchsgruppe im Bereich der IT-Compliance		X
12	Zur Umsetzung der Gesetze, die sich an die IT-Compliance im Unternehmen richten, sind eine Reihe von Rahmenwerken und Best-Practices entwickelt worden.		
	Richtig	X	
	Falsch		X

13	Welche Synonyme für den Begriff Standards kennen Sie?		
	Framework	X	
	Rahmenwerk	X	
	Referenzmodell	X	
	Regelwerk		X

Tab. 13: Lösung zu den Übungsfragen WBT 04

Lösungen zu den Übungsfragen in WBT 05

Nr.	Frage	Richtig	Falsch
1	Wie werden die Phasen der Situationsanalyse in der Cronus AG genannt?		
	Soll-Analyse	X	
	Vorgaben identifizieren		X
	Ist-Situation	X	
	Konzeption & Implementierung		X
	Soll-Ist-Vergleich	X	
2	Eine regelmäßige Wiederholung aller Prozessschritte ist nötig, um eine kontinuierliche Verbesserung zu erreichen.		
	Richtig		X
	Falsch	X	
3	In der Phase „Soll-Analyse“ wird geprüft, welche Vorgaben bereits umgesetzt wurden.		
	Richtig		X
	Falsch	X	
4	„Umsetzung der IT-Compliance“ lässt sich nur durchführen, wenn das Projekt in der obersten Führungsebene angesiedelt ist und alle Betroffenen zusammenarbeiten.		
	Richtig	X	
	Falsch		X
5	IT-Compliance ist ein einmaliger, langfristiger Prozess.		
	Richtig		X
	Falsch	X	
6	Der IT-Compliance-Officer ist die Schnittstelle zwischen Compliance und IT. So berät er z. B. die Mitarbeiter der IT-Abteilung bei der Systementwicklung und –überarbeitung hinsichtlich der Compliance-Fragestellungen.		
	Richtig	X	
	Falsch		X

7	Das Ergebnis eines Soll-Ist-Vergleichs kann drei verschiedene Ausprägungen haben:		
	Die Ist-Analyse hat ergeben, dass bis dato einige Maßnahmen zur Erreichung von IT-Compliance eingeleitet worden sind, diese sind aber nicht effizient/ effektiv.	X	
	Die Ist-Analyse hat ergeben, dass wir alle Maßnahmen für eine vollständige IT-Compliance etabliert haben. Diese sind effizient und effektiv. Es besteht zunächst kein weiterer Handlungsbedarf.	X	
	Die Soll-Analyse hat ergeben, dass bis dato keine Maßnahmen zur Erreichung von IT-Compliance eingeleitet worden sind.		X
	Die Ist-Analyse hat ergeben, dass bis dato keine Maßnahmen zur Erreichung von IT-Compliance eingeleitet worden sind.	X	
8	Mit Hilfe der entwickelten To-Do-Liste werden in der Konzeptionsphase Maßnahmen entwickelt, mit denen IT-Compliance erreicht werden soll.		
	Richtig	X	
	Falsch		X
9	Die Ausrichtung der IT-Compliance an etablierten gesetzlichen Vorgaben ist aus zwei Gründen empfehlenswert: Einerseits kann die Anwendung den Enthaftungsbeweis für die Unternehmensleitung liefern, andererseits liefern Best-Practices auch einfache Hinweise zur konkreten Umsetzung von Compliance-Vorgaben.		
	Richtig		X
	Falsch	X	

10	Welche Aussagen sind richtig?		
	Eigene selbstentwickelte Maßnahmen haben unter anderem den Vorteil, dass der Nachweis eines ordentlichen Geschäftsbetriebs wenig aufwendig ist.		X
	Ein Nachteil eigener Maßnahmen ist, dass die Entwicklung dieser Maßnahmen extrem aufwendig ist.	X	
	Ein Vorteil von Maßnahmen aus Frameworks ist, dass die Maßnahmen anerkannt sind und Erläuterungen zur Umsetzung enthalten.	X	
	Ein Nachteil von Maßnahmen aus Frameworks ist, dass die Maßnahmen allgemein formuliert sind und noch auf die speziellen Anforderungen der Cronus AG angepasst werden müssen.		X
11	ITIL® ist ein typisches Referenzmodell, welches ausschließlich der Performancesichtweise zuzuordnen ist.		
	Richtig		X
	Falsch	X	
12	Hält man sich an COSO®-ERM-Referenzmodell, so ist man gesetzeskonform mit SOX.		
	Richtig	X	
	Falsch		X
13	Das COBIT®-Framework hilft bei der Umsetzung von Corporate Governance in die IT-Governance.		
	Richtig		X
	Falsch	X	
14	ITIL® kann als Best Practice bei der Erfüllung der Anforderungen von ISO/IEC 20000 helfen.		
	Richtig	X	
	Falsch		X
15	Im Rahmen des Monitoring der entwickelten Maßnahmen werden regelmäßige Prüfungen durchgeführt. Prüfungen können durch welche Prüfer durchgeführt werden?		
	Den Betriebsrat	X	
	Externe Wirtschaftsprüfer	X	
	Interne Wirtschaftsprüfer		X
	Interne Audits	X	

Tab. 14: Lösung zu den Übungsfragen WBT 05

Lösungen zu den Übungsfragen in WBT 06

Nr.	Frage	Richtig	Falsch
1	COBIT® ist ein Referenzmodell, welches sich konkret an die IT eines Unternehmens richtet. Weiterhin unterstützt COBIT® bei der Implementierung von IT-Governance in die Corporate Governance eines Unternehmens.		
	Richtig	X	
	Falsch		X
2	Ein Problem von COBIT® besteht im methodischen Ansatz des Referenzmodells. Damit ist gemeint, dass hauptsächlich beschrieben wird was zu tun ist, die Handlungsempfehlungen jedoch beschränkt sind.		
	Richtig	X	
	Falsch		X
3	Die 37 COBIT®-Prozesse sind standardisiert und können theoretisch von jedem Unternehmen als Referenzmodell genutzt werden, lediglich bedarf es unternehmensindividueller Anpassungen.		
	Richtig	X	
	Falsch		X
4	Aus welchen Hauptbestandteilen besteht der COBIT®-Würfel?		
	IT-Prozesse (Domänen, Prozesse, Reifegrad)		X
	IT-Ressourcen	X	
	Geschäftsanforderungen	X	
	Anforderungen der einzelnen Fachbereiche		X
	IT-Prozesse (Domänen, Prozesse, Aktivitäten)	X	
5	Die Geschäftsanforderungen sind als Ausgangspunkt zu sehen. Aus ihnen werden die IT-Ressourcen abgeleitet, die benötigt werden, um die IT-Prozesse umzusetzen.		
	Richtig	X	
	Falsch		X

6	Die gleichzeitige Umsetzung aller COBIT®-Prozesse ist sinnvoll, da dies für die Unternehmen am ökonomischsten ist.		
	Richtig		X
	Falsch	X	
7	Die IT-Ziele sind prozessspezifisch und werden durch die Aktivitäten eines Prozesses erreicht. Jedem IT-Ziel werden Metriken zugeordnet.		
	Richtig		X
	Falsch	X	
8	Der Prozess „BAI06 – Manage Changes“ lässt sich in vier Prozessanforderungen unterteilen. Den einzelnen Prozessanforderungen werden mit Hilfe des RACI-Charts die verantwortlichen Abteilungen und Führungspositionen zugeordnet.		
	Richtig	X	
	Falsch		X

Tab. 15: Lösung zu den Übungsfragen WBT 06

Lösungen zu den Übungsfragen in WBT 07

Nr.	Frage	Richtig	Falsch
1	ITIL® wurde von der britischen Regierungsbehörde CCTA entwickelt, um…		
	…die schlechte Qualität der IT-Dienstleistungen nachhaltig zu verbessern.	X	
	…Kosten zu senken.	X	
	…Staatseinnahmen zu generieren.		X
2	IT-Innovationen, entwickelt von staatlichen Institutionen, stellen eine Seltenheit dar.		
	Richtig	X	
	Falsch		X
3	Die ITIL®-Handbücher umfassen Best Practice, die nur in Dienstleistungsunternehmen eingesetzt werden können.		
	Richtig		X
	Falsch	X	
4	Einige ITIL®-Prozesse werden in einen Service Lifecycle eingebettet, um Services stetig zu überarbeiten und weiterzuentwickeln.		
	Richtig		X
	Falsch	X	
5	Ein Incident ist unter anderem ein Ereignis, das einen Service unterbrechen kann.		
	Richtig	X	
	Falsch		X
6	Welche Aussage ist richtig? Das Incident Management…		
	…soll möglichst schnell den normalen Servicebetrieb wiederherstellen.	X	
	…kümmert sich um Incidents und Service Requests.		X
	…ist einer der 26 standardisierten ITIL®-Prozesse.	X	
	…findet sich im Handbuch „Service Operation“ wieder.	X	

7	Der Prozessfluss zeigt, in welcher Reihenfolge Prozessaktivitäten ablaufen sollen.		
	Richtig	X	
	Falsch		X
8	Welche ITIL®-Funktionen gibt es?		
	Service Desk	X	
	IT-Operations Management	X	
	Application Management	X	
	Request Fulfilment		X
9	Welche Aussage ist richtig?		
	Der Service Desk führt in erster Linie die ITIL®-Prozesse „Incident Management“ und „Availability Management“ aus.		X
	Die vier Funktionen, die in ITIL® benannt werden, dienen dazu einen stabilen Zustand der Betriebs-IT aufrechtzuerhalten.	X	
10	Bei einem Major Incident handelt es sich um einen schwerwiegenden Incident, der gravierende Unterbrechungen im Geschäftsablauf verursacht.		
	Richtig	X	
	Falsch		X
11	Welche Aussagen sind richtig?		
	Der Service Desk ist einen von fünf Funktionen, die in ITIL® benannt werden.		X
	Je nach Größe, Struktur, Sprache etc. kann der Service Desk unterschiedlich organisiert werden.	X	
	Durch das Incident Management können negative Auswirkungen auf das Geschäft möglichst klein gehalten werden.	X	
12	Die ITIL®-Einführung dient unter anderem als Basis für eine Zertifizierung nach ISO/IEC 20000.		
	Richtig	X	
	Falsch		X

13	Welche Rollen müssen im Incident-Management-Prozess besetzt werden?		
	2nd Level Support	X	
	3rd Level Support	X	
	Service Desk		X
	Incident Manager	X	

Tab. 16: Lösung zu den Übungsfragen WBT 07

Lösungen zu den Übungsfragen in WBT 07

Nr.	Frage	Richtig	Falsch
1	Eine Zertifizierung nach ISO/IEC 20000 ist sinnvoll, um…		
	…den Nachweis für einen erfolgreichen Betrieb eines ITSM zu erbringen.	X	
	…sich von Konkurrenten abzuheben.	X	
	…Kosten im IT-Bereich zu vermeiden.		X
2	Ein ISO/IEC 20000-Zertifikat ist zwei Jahre gültig. Danach muss sich die Cronus AG einer erneuten Zertifizierung unterziehen.		
	Richtig		X
	Falsch	X	
3	ISO/IEC 20000 ist eine international anerkannte Norm, die aus dem britischen Standard BSI 15000 hervorgegangen ist.		
	Richtig		X
	Falsch	X	
4	ISO/IEC 20000-2 ist genau wie ISO/IEC 20000-1 in neun Abschnitte gegliedert.		
	Richtig	X	
	Falsch		X
5	Ein IT-Service-Mangement-System beschreibt alle Prozesse und Ressourcen, die koordiniert eingesetzt werden, um die vereinbarten Ziele der IT-Services zu erreichen.		
	Richtig	X	
	Falsch		X

6	Welche Aussage ist richtig? ISO/IEC 20000…		
	…ist eine Norm zum IT-Service-Management.	X	
	…bietet konkrete Arbeitsanweisungen zur Umsetzung eines IT-Service-Managements.		X
	…bietet Unternehmen die Möglichkeit, sich zertifizieren zu lassen.	X	
	…ist 2005 aus dem nationalen Standard BS 15000 hervorgegangen.	X	
7	Die geforderten Prozesse aus ISO/IEC 20000-1 können auch ohne die Hilfe von ITIL® eingeführt werden.		
	Richtig	X	
	Falsch		X
8	Welche Prozessgruppen werden in ISO/IEC 20000-1 beschrieben?		
	Servicebereitstellungs- und Lieferungsprozesse	X	
	Lösungsprozesse	X	
	Steuerungsprozesse	X	
	Freigabeprozesse		X
9	Welche Aussage ist richtig?		
	In der Phase „Act“ des PDCA-Zyklus werden die erforderlichen Prozesse umgesetzt.		X
	Der PDCA-Zyklus umfasst die vier Phasen „Plan“, „Do“, „Check“ und „Act“.	X	
10	ISO/IEC 20000-1 und ISO/IEC 20000-2 sind Gegenstand einer Zertifizierung und müssen eingehalten werden.		
	Richtig		X
	Falsch	X	

11	Welche Aussagen sind richtig?		
	ISO/IEC 20000-1 ist in neun Abschnitte gegliedert.	X	
	In ISO/IEC 20000-1 werden alle Pflichtanforderungen beschrieben, die ein Unternehmen erfüllen muss, um eine Zertifizierung zu erreichen.	X	
	Durch eine Zertifizierung werden die IT-Infrastruktur und –Prozesse transparenter. Dies ist ein Nachteil der Zertifizierung.		X
12	Neben den beiden Hauptteilen ISO/IEC 20000-1 und ISO/IEC 20000-2 bietet ISO/IEC 20000 noch drei Ergänzungen zur eigentlichen ISO-Norm.		
	Richtig	X	
	Falsch		X
13	Welche Schritte laufen bei einem Zertifizierungsverfahren ab?		
	Vor-Audit	X	
	Überwachungs-Audit	X	
	Nach-Audit		X
	Nachweis-Audit	X	

Tab. 17: Lösung zu den Übungsfragen WBT 08

Literaturverzeichnis

1. **Bauer, Silvia; Wesselmann, Carsten**: EuroSOX und die Compliance Organisation im Unternehmen, in: Wisu - das Wirtschaftsstudium – Zeitschrift zur Ausbildung, Prüfung, Berufseinstieg und Fortbildung, 37. Jahrgang, Heft 8-9, August/September 2008; S. 1128–1131.
2. **Beims, Martin:** IT-Service Management in der Praxis mit ITIL®, 3., aktualisierte Aufl., München: Carl Hanser Verlag 2012.
3. **Bergmann, Robert; Tiemeyer Ernst:** IT-Governance, in: Handbuch IT-Management– Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, Hrsg.: Tiemeyer, Ernst, 4. Aufl., München: Carl Hanser Verlag 2011.
4. **Böttcher, Roland:** IT-Service-Management mit ITIL® – 2011 Edition – Einführung, Zusammenfassung und Übersicht der elementaren Empfehlungen, 3., aktualisierte Auflage, Hannover: Heise Zeitschriften Verlag GmbH & Co KG 2013.
5. **Bucksteeg, Martin; Ebel, Nadin; Eggert, Frank; Meier, Justus; Zurhausen, Bodo:** ITIL® 2011 – der Überblick – Alles Wichtige für Einstieg und Anwendung, München: Addison-Wesley Verlag 2012.
6. **Buchta, Dirk; Eul, Marcus; Schulte-Croonenberg, Helmut:** Strategisches IT-Management – Wert steigern, Leistung steuern, Kosten senken, 3., überarb. und erweiterte Aufl., Wiesbaden: Gabler GWV Fachverlag GmbH 2009.
7. **Bungartz, Oliver:** Handbuch Interne Kontrollsysteme (IKS) - Steuerung und Überwachung von Unternehmen, Berlin: Erich Schmidt Verlag 2011.
8. **Dohle, Helge; Schmidt, Rainer; Schürmann, Thomas; Zielke, Frank:** ISO 20000 – Eine Einführung für Manager und Projektleiter, Heidelberg: dpunkt.verlag GmbH 2009.
9. **Falk, Michael:** IT-Compliance in der Corporate Governance – Anforderungen und Umsetzung, Wiesbaden: Gabler Verlag 2012.
10. **Gaulke, Markus:** Praxiswissen COBIT – Val IT – Risk IT – Grundlagen und praktische Anwendung für die IT-Governance, Heidelberg: dpunkt.verlag GmbH 2010.
11. **Gründler, Ansgar:** Computer und Produktivität – Das Produktivitätsparadoxon der Informationstechnologie, Wiesbaden: Gabler Verlag 1997.
12. **Häusler, Oliver:** Business-Impact-Management von Informationstechnologie im Unternehmen – Geschäftsprozessorientierte Planung, Steuerung und Kontrolle der IT, Wiesbaden: Gabler Verlag 2012.

13. **Henderson, John Charles; Venkatraman, Nirmala:** Strategic Alignment: Leveraging information technology for transforming organizations, in: IBM Systems Journal, Vol. 38, 1999; S. 472-484.

14. **Hesseler, Martin; Görtz, Marcus:** Basiswissen ERP-Systeme- Auswahl, Einführung und Einsatz betriebswirtschaftlicher Standardsoftware, Herdecke, Witten: W3l GmbH 2007.

15. **Hofmann, Jürgen; Schmidt, Werner:** Masterkurs IT-Management, Wiesbaden: Vieweg & Sohn Verlag 2007.

16. **International Organization of Standardization (Hrsg.):** Stichwort: Logo, Online im Internet: http://www.iso.org/iso/2012_iso-logo_print.png, 12.05.2014.

17. **ISACA (Hrsg.):** COBIT 5 - Enabling Processes, Rolling Meadows 2012.

18. **Johannsen, Wolfgang; Goeken, Matthias:** Referenzmodelle für IT-Governance-Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co, 2., aktualisierte und erweiterte Auflage, Heidelberg: dpunkt.verlag GmbH 2011.

19. **Jonen, Andreas; Lingau, Volker:** Bewertung von IT-Investitionen – Einbezug von Werttreibern und Risiken, in: ZfCM – Controlling und Management, 51. Jahrgang, Heft 4/2007, S. 246-250.

20. **Kamleiter, Jürgen; Langer, Michael**: Business IT Alignment mit ITIL, COBIT, RUP – Gegenüberstellung und Integration der Referenzmodelle von IT-Service-Management, IT-Governance und Anwendungsentwicklung, Bad Homburg: Serview GmbH 2006.

21. **Kargl, Herbert:** DV-Controlling, 4., unwesentlich veränderte Aufl., München, Wien, Oldenbourg: R. Oldenbourg Verlag 1999.

22. **Keller, Wolfgang:** IT-Unternehmensarchitektur – von der Geschäftsstrategie zur optimalen IT-Unterstützung, 2., überarb. und erweiterte Auflage, Heidelberg: dpunkt.verlag 2012.

23. **Kesten, Ralf; Schröder, Hinrich; Wozniak, Anja:** Konzept zur Nutzenbewertung von IT-Investitionen, Ausgabe 2006-03 von Arbeitspapiere der Nordakademie, Online im Internet: http://d-nb.info/1049774884/34, Oktober 2006.

24. **Klotz, Michael:** IT-Compliance, in: Handbuch IT-Management– Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, Hrsg.: Tiemeyer, Ernst, 4. Aufl., München: Carl Hanser Verlag 2011.

25. **Köhler, Peter Thomas:** ITIL – Das IT-Servicemanagement Framework, 2., überarbeitete Auflage, Berlin Heidelberg: Springer-Verlag 2007.

26. **Office of Government Commerce (Hrsg.):** Service Operation, ITIL®, Norwich NR3 1GN, 2007.

27. **Patas, Janusch; Mayer, Jörg H.; Goecken, Matthias; Wippel, Jürgen**: Der Wertbeitrag der IT, in: Wisu - das Wirtschaftsstudium – Zeitschrift zur Ausbildung, Prüfung, Berufseinstieg und Fortbildung, 41. Jahrgang, Heft 12, Februar 2012; S. 183–186.

28. **Quaas, Ralf:** Messung der qualitativ-strategischen Nutzeneffekte von II-Investitionen, Online im Internet: http://isento.biz/downloads/whitepapers/wirtschaftlichkeitsanalyse/wirtschaftlichkeitsanalyse_it-investitionen_2005.pdf, 2005.

    Qualified Advice Partners (Hrsg.): Stichwort: Logo, Online im Internet: http://www.qualified-audit-partners.be/user_images/Logos/ITIL-logo.jpg, 13.04.2014.

29. **Rüter, Andreas; Schröder, Jürgen; Göldner, Alex; Niebuhr, Jens:** IT-Governance in der Praxis, 2., Aufl., Berlin, Heidelberg: Springer Verlag 2010.

30. **Scholderer, Robert:** Management von Service-Level-Agreements – Methodische Grundlagen und Praxislösungen mit COBIT, ISO 20000 und ITIL, Heidelberg: dpunkt.verlag GmbH 2011.

31. **Schulze, Ulrich:** Informationstechnologieeinsatz im Supply Chain Management – Eine konzeptionelle und empirische Untersuchung zu Nutzenwirkung und Nutzenmessung, Wiesbaden: Gabler GWV Fachverlag GmbH 2009.

32. **Teubner, Alexander:** IT/Business Alignment, in: Wirtschaftsinformatik, 5/2006, S. 368-371.

33. **Wecker, Gregor; van Laak, Hendrik:** Compliance in der Unternehmenspraxis – Grundlagen, Organisation und Umsetzung, Wiesbaden: Gabler Verlag 2008.

34. **Werder, Axel:** Führungsorganisation. Grundlagen der Corporate Governance, Spitzen- und Leitungsorganisation, 2., aktual. und erw. Aufl., Wiesbaden: Gabler Verlag 2008.

35. **Wildenstein, Oliver; Pozinat, Anne:** Prozessverbesserung durch Process Mining – Überblick und Praxisfall, in: IT-Governance – Zeitschrift des ISACA Germany Chapter e.V., 17/ 2014, , S.9 ff.

36. **Zimmermann, Steffen:** Governance im IT-Portfoliomanagement – Ein Ansatz zur Berücksichtigung von Strategic Alignment bei der Bewertung von IT, in: Wirtschaftsinformatik, 5/2008, S.357-365.

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: https://wi.uni-giessen.de

Herausgeber: Prof. Dr. Axel Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
https://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungs-, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr-, Vortrags- und Kolloquiumsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Prof. Dr. Axel Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Prof. Dr. Bernhard Ostheimer, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit einem der Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Web-Adresse https://wi.uni-giessen.de/