



universität
wien

MASTERARBEIT

Titel der Masterarbeit

Ein Evaluierungsmodell zur Auswahl eines IT Systems
zur Unterstützung eines Internen Kontrollsystems und
dessen Test bei der Austrian Airlines AG

Verfasser

Christoph Brandner, BSc.

angestrebter akademischer Grad

Diplom-Ingenieur (Dipl.-Ing.)

Wien, 2011

Studienkennzahl lt. Studienblatt:

A 066 926

Studienrichtung lt. Studienblatt:

Masterstudium Wirtschaftsinformatik

Betreuer:

Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Schriftliche Versicherung

Hiermit versichere ich, dass die vorliegende Arbeit von mir selbstständig und ausschließlich mit den angegebenen Quellen und Hilfsmitteln verfasst wurde.

Diese Arbeit wurde weder in gleicher noch in ähnlicher Form bis dato einer Prüfungsbehörde vorgelegt.

Wien, August 2011

Danksagungen

An erster Stelle möchte ich mich besonders bei meiner Familie bedanken, die mir ermöglicht hat, dass ich dieses Studium absolvieren konnte und mich immer unterstützt hat. Außerdem möchte ich mich bei all jenen bedanken, die mich in meiner Studienzeit begleitet haben, sowie all jenen, die mich im Laufe der Erstellung der Diplomarbeit mit Verbesserungen und Denkanstößen inspiriert haben.

Weiters möchte ich mich bei meinem Betreuer Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr bedanken, der mir in zahlreichen Gesprächen mit Anregungen und Korrekturen weitergeholfen hat.

Ein spezieller Dank gilt Herrn Mag. Michael Koegler, der die Kooperation mit der Austrian Airlines AG im Zuge dieser Masterthesis ermöglicht hat und diese Arbeit tatkräftig unterstützt hat.

Abstract

It is important for enterprises to control the complexity of their commerce, therefore they have to understand and to document their internal processes. After the documentation of the processes an enterprise has the opportunity to optimize and control the process. Furthermore, within the last years the need of a proper internal control occurred to ensure to reach the legal regulations and to achieve the company's requirements. In addition a mature system for internal controls will step up the trust into the company and decrease the failures.

As a result of the need of a mature system of internal controls the main focus of this masterthesis is the development of an evaluation method for internal control systems, which will support the decision making process. At the beginning there has to be declared which perspectives will be examined and how the information will support the decision. The evaluation will consist of a product-specific evaluation and a strategic business view. Especially the product-specific evaluation is based on essential requirements for internal control systems, which can be easily enlarged by customer requirements. The strategic business view is based on Cobit and will deliver information about the IT-support in reaching the business goals. For that reason the Cobit maturity model for internal control and the Cobit maturity attribute table will be used which includes different perspectives. Both of these evaluations will give a recommendation for an internal control system based on the result. Furthermore the results will be examined and it will be analyzed if there is a way to speed up the evaluation process or if there is coherence between these two evaluations and if a suggestion for the sequence of the evaluations can be made to simplify the evaluation process. The Austrian Airlines AG supported the test of the evaluation process within an industrial environment. In cooperation the Austrian Airlines AG applied the developed method and assist throughout the development.

At the end of the thesis a general implementation process will be developed besides the evaluation process. This implementation process is described in a general way on purpose. This is caused by the fact that enterprises can use their common project management standard.

Inhaltsverzeichnis

1	Einleitung.....	13
1.1	Motivation und Zielsetzung	13
1.2	Aufbau der Arbeit	14
2	Risikomanagement	15
2.1	Risiko.....	16
2.2	Risikomanagementansätze	17
2.2.1	Risikobeurteilung	18
	Risikoidentifikation.....	18
	Risikoanalyse	19
	Interne Risikofelder.....	19
	Externe Risikofelder.....	21
2.2.2	Risikobehandlung.....	22
	Risikobewältigung.....	22
	Risiko- und Maßnahmenüberwachung.....	23
2.3	Standards für interne Kontrollsysteme und Risikomanagement	23
2.3.1	Australisch-neuseeländischer Standard AS/NZS 4360.....	24
	Communication and Consult	25
	Monitor and review	25
	Establish the context.....	25
	Identify Risk.....	26
	Analyse Risk	26
	Evaluate Risk	26
	Risk Treatment (Risikobehandlung)	27
2.3.2	COSO I und COSO II.....	27
	Internes Umfeld.....	28
	Zielfestlegung.....	28
	Ereignisidentifikation.....	29
	Risikobeurteilung	29
	Risikosteuerung.....	29
	Kontrollaktivitäten	29
	Information & Kommunikation.....	29

Überwachung	29
2.3.3 ONR 4900X.....	29
2.3.4 COBIT	31
3 Interne Kontrollsysteme.....	35
3.1 Bestandteile eines Internen Kontrollsystems	36
3.1.1 Prozessintegrierte Überwachungssysteme	36
Organisatorische Sicherungsmaßnahmen.....	36
Kontrollen	37
3.1.2 Prozessunabhängige Überwachungssysteme	37
Interne Revision	37
Sonstiges	37
3.2 Gesetzliche Grundlagen	38
3.2.1 Österreich	38
3.2.2 Deutschland	38
3.2.3 Schweiz	39
3.3 Branchenübliche Richtlinien.....	39
3.3.1 Basel II	39
3.3.2 Solvency II	40
4 Entwicklung eines Evaluierungsmodells zur Auswahl eines toolgestützten Internen Kontrollsystems.....	41
4.1 Produktspezifische Evaluierung.....	44
4.1.1 Kriterienkatalog definieren.....	44
Themengebiete und Themenblöcke.....	44
4.1.2 Prioritäten & Bewertungsskala definieren.....	45
Bewertungsmethode	46
KO Kriterien.....	47
4.1.3 Gewichtung der Themengebiete und Themenblöcke	47
Gewichtung der Themenblöcke.....	47
Gewichtung der Themengebiete.....	48
4.1.4 Evaluierungsschritte	48
Funktionale Evaluierung	48
Technische Evaluierung	49
Finanzielle Evaluierung.....	50

4.1.5	Auswertung	51
4.2	COBIT-Evaluierung.....	51
4.2.1	Bewertungsskala.....	52
4.2.2	Auswertung	54
5	Rahmenbedingungen bei der Austrian Airlines AG	55
5.1	Gesetzliche Rahmenbedingungen	56
5.2	Vorgaben des Konzerns und der Austrian Airlines.....	57
6	Evaluierung ausgewählter Interner Kontrollsysteme	58
6.1.1	Adonis Prozessportal.....	58
	Software	58
6.1.2	BWise	59
	Software	60
6.1.3	Oracle GRC	61
	Software	61
6.1.4	RSA Archer.....	62
	Software	62
6.1.5	SAP GRC	63
	Software	63
7	Vorgehensweise bei der Lösungserarbeitung für die Austrian Airlines AG...	64
7.1	Produktspezifische Evaluierung.....	64
7.1.1	Kriterienkatalog definieren.....	64
	Themengebiete und Themenblöcke.....	65
7.1.2	Prioritäten & Bewertungsskala definieren.....	65
	Funktionale Evaluierung	66
	Technische Evaluierung	74
	Finanzielle Evaluierung.....	79
	KO Kriterien.....	80
7.1.3	Gewichtung der Themengebiete und Themenblöcke	80
	Gewichtung der Themenblöcke.....	80
	Gewichtung der Themengebiete.....	81
7.1.4	Evaluierungsschritte	82
	Funktionale Evaluierung	82

Technische Evaluierung	83
Finanzielle Evaluierung.....	83
7.1.5 Auswertung	84
7.2 COBIT-Evaluierung.....	85
7.2.1 Auswertung	87
Adonis Prozessportal.....	87
BWise.....	88
Oracle	89
SAP	89
7.3 Evaluierungsergebnis	91
7.3.1 Gesamtauswertung	92
7.3.2 Resümee	95
Produktspezifische Evaluierung	95
Cobit-Evaluierung	96
Gesamteindruck.....	96
8 Einführungskonzept	97
8.1 Einführungsstrategie	97
8.1.1 Simultane Einführung.....	97
8.1.2 Sukzessive Einführung	98
8.1.3 Konzeption für die Systemeinführungsstrategie eines Internen Kontrollsystems bei der Austrian Airlines AG	99
8.2 Vorgehensmodell zur Einführung eines Internen Kontrollsystems	101
8.2.1 Vorbereitungsphase	102
Zielsetzung	102
8.2.2 Organisationsphase.....	103
Zielsetzung	103
8.2.3 Analysephase.....	104
Zielsetzung	105
8.2.4 Konzeptionsphase.....	105
Zielsetzung	105
8.2.5 Anpassungsphase.....	106
Zielsetzung	106
8.2.6 Umstellungsphase.....	107

	Umstellungsarten.....	107
	Aufgaben.....	107
	Projekterfolg ermitteln	108
	Zielsetzung	108
8.2.7	Betriebsphase.....	108
	Zielsetzung	109
8.2.8	Nachfolgeprojekt	109
9	Lessons learned.....	110
10	Grafikverzeichnis	112
11	Tabellenverzeichnis.....	113
12	Literaturverzeichnis.....	114
13	Anhang	118
13.1	Evaluierungen	118
13.1.1	Adonis Prozessportal.....	119
	Funktionale Evaluierung	120
	Technische Evaluierung	122
	Finanzielle Evaluierung.....	124
13.1.2	BWise.....	125
	Funktionale Evaluierung	127
	Technische Evaluierung	129
	Finanzielle Evaluierung.....	131
13.1.3	Oracle GRC.....	132
	Funktionale Evaluierung	134
	Technische Evaluierung	136
	Finanzielle Evaluierung.....	138
13.1.4	RSA Archer.....	139
	Funktionale Evaluierung	141
	Technische Evaluierung	143
	Finanzielle Evaluierung.....	145
13.1.5	SAP GRC	146
	Funktionale Evaluierung	148
	Technische Evaluierung	150

Ein Evaluierungsmodell zur Auswahl eines IT Systems zur Unterstützung eines Internen Kontrollsystems und dessen Test bei der Austrian Airlines AG	11
--	----

Finanzielle Evaluierung.....	152
13.2 Cobit 4.1 – Maturity Attribute Table	153
13.3 Cobit 4.1 – Maturity Model for Internal Control	154

1 Einleitung

1.1 Motivation und Zielsetzung

Um als Unternehmen die steigende Komplexität in der Geschäftswelt bewältigen zu können und die internen Abläufe effizient und effektiv zu gestalten, ist es essentiell, die Abläufe im Unternehmen zu analysieren und zu dokumentieren, sowie diese auch zu kontrollieren. Basierend auf dieser Überlegung wurde vor einigen Jahren die Notwendigkeit eines Internen Kontrollsystems erkannt. Dabei stehen die Kontrolle und rechtmäßige Einhaltung von rechnungslegenden Geschäftsprozessen, die zu den internen kontrollsystemrelevanten Prozessen zu zählen sind, und gesetzlichen Bestimmungen im Vordergrund. Durch die Einhaltung der genannten Vorgaben soll das Unternehmen einen detaillierten Überblick über die unternehmensinternen Tätigkeiten erhalten und so das Unternehmensvermögen schützen. Des Weiteren wird durch ein Internes Kontrollsystem und dessen IT Unterstützung die Erreichung von Zielen bzw. Vorgaben sowie die Verhinderung bzw. Vermeidung von Fehlern erleichtert, wie dies in [Hen06] angegeben ist.

Als einleitende und zentrale Frage stellt sich jedoch für ein Unternehmen die Auswahl einer geeigneten Methode für die Verwendung eines Internen Kontrollsystems und die Auswahl eines zweckmäßigen IT Systems zur Unterstützung. Im Zuge der Masterthesis wird ein Modell entwickelt, das den Auswahlprozess eines IT Tools für ein Internes Kontrollsystem unterstützt. Dabei werden unterschiedliche Anforderungen berücksichtigt, wobei bestimmte Anforderungen vorgegeben werden, die ein IT gestütztes Internes Kontrollsystem zur Verfügung stellen muss. Weiters ist es einem Anwender auch möglich die Anforderungen eines Unternehmens in den Prozess einzubinden. Bei der Anwendung des Modells werden zwei unterschiedliche Evaluierungen durchgeführt, die zur Entscheidungsfindung beitragen, wobei die Entscheidungsgrundlage auf toolrelevanten Funktionalitäten, wirtschaftlichen und strategischen Gesichtspunkten basiert. Austrian Airlines AG begleitet als Kooperationspartner die Anwendung des Evaluierungsmodells und testet die Eignung des Evaluierungsmodells.

Das Ziel der Masterthesis ist die Entwicklung einen Evaluierungsprozess für die Auswahl eines Tools, welches die Aufgaben eines Internen Kontrollsystems erfüllt und die unternehmensspezifischen Anforderungen, wie beispielsweise Monitoringaufgaben oder Auditierungen abdeckt. Dabei sollen zwei unterschiedliche Evaluierungszugänge betrachtet werden. Zum einen wird eine produktspezifische Evaluierung durchgeführt und zum anderen wird eine Evaluierung durchgeführt, die einen strategischen Blick auf das Tool wirft, dabei wird untersucht, ob ein Tool die Unternehmensziele unterstützen kann. In diesem Zusammenhang wird betrachtet, ob der Evaluierungsprozess mit Hilfe der strategischen Sichtweise effizienter durchlaufen werden kann.

In einem weiteren Schritt ist die Erarbeitung des Projektablaufs für die Systemeinführung eines Internen Kontrollsystems in einem Unternehmen angestrebt, welche in einem allgemein gültigen Kontext gehalten werden soll, damit die

Einführung für Unternehmen in jeder Branche, sowie für jeden Projektmanagementstandard anwendbar ist.

1.2 Aufbau der Arbeit

Zu Beginn wird sich die Arbeit in Kapitel 2 mit dem Risikomanagement beschäftigen. Dabei werden Definitionen erläutert und aufgezeigt welche Bereiche ein Risikomanagement umfasst. Weiters werden unterschiedliche Standards betrachtet und vorgestellt, die im laufenden Geschäftsbetrieb verwendet werden und auch bei der Implementierung von Risikomanagementsystemen oder Internen Kontrollsystemen zur Anwendung kommen können.

Die Bestandteile sowie die herrschenden Rahmenbedingungen eines Internen Kontrollsystems werden im 3. Kapitel aufgezeigt. In diesem Kapitel wird auf die gesetzlichen Vorschriften in Österreich, Deutschland und der Schweiz eingegangen. Außerdem werden einige branchenübliche Richtlinien betrachtet, die ein Internes Kontrollsystem auch abzudecken hat, damit ein Unternehmen am Markt bestehen kann.

Nachdem die einleitenden Erklärungen und Abgrenzungen durchgeführt wurden, beschäftigt sich das Kapitel 4 mit der Entwicklung des Evaluierungsmodells zur Auswahl eines IT Systems, welches die Aufgaben eines Internen Kontrollsystems unterstützt. Dieser Teil stellt einen Kern der Masterthesis dar, die sich mit der Erstellung des Modells und den relevanten Bereichen für die Toolauswahl beschäftigen. Darunter fallen einerseits die unterschiedlichen Evaluierungsschritte bei der produktspezifischen Evaluierung, andererseits aber auch die Betrachtung der strategischen Dimension um den Evaluierungsprozess zu unterstützen. In diesem Bereich stellt die Bewertungsmethode und die damit verbundene Priorisierung und Bewertung einen wichtigen Teilbereich dar, um die Evaluierung durchführen zu können.

Bevor das Evaluierungsmodell am Beispiel der Austrian Airlines AG Anwendung findet, werden die Rahmenbedingungen bei der Austrian Airlines AG im folgenden Kapitel dargestellt. Dabei werden die speziellen gesetzlichen Vorgaben betrachtet, sowie auch die Konzernvorgaben.

Im folgenden Kapitel werden auch jene Toolhersteller von Internen Kontrollsystemen vorgestellt, die der Evaluierung unterzogen werden.

Der Einsatz des entwickelten Evaluierungsmodells wird in Kapitel 7 in Kooperation mit der Austrian Airlines AG in einem Unternehmenskontext aufgezeigt. Dabei werden die Rahmenbedingungen der Austrian Airlines AG verwendet und die unternehmens- und konzernspezifischen Ansprüche im Zuge der produktspezifischen Evaluierung betrachtet. Die Betrachtung der Tools in einem strategischen Kontext wird mit Hilfe von Cobit durchgeführt und soll Aufschluss darüber geben, ob ein Tool die Unternehmensziele unterstützen kann. Aus den gewonnen Erkenntnissen kann eine Auswertung und eine Toolempfehlung für ein Internes Kontrollsystem für das Unternehmen abgegeben werden.

In Kapitel 8 wird ein Konzept beschrieben, das im Zuge der Systemeinführung eines Internen Kontrollsystems anzuwenden ist und in einem allgemeinen

Vorgehensmodell realisiert ist. Dabei wird in den einzelnen Phasen auf die anfallenden Aufgaben eingegangen und die Zielsetzung bezüglich zu erstellender Artefakte festgelegt.

Am Ende der Arbeit wird in Kapitel 9 ein Resümee über die verfasste Arbeit anfertigt, welches die Arbeit sowie auch den Arbeitsfortschritt revuepassieren lässt und auftretende Probleme bzw. Erkenntnisse widerspiegelt.

Abschließend möchte ich darauf hinweisen, dass aus Gründen der leichteren Lesbarkeit auf die explizite Nennung beider Geschlechter verzichtet wurde, wo eine geschlechtsneutrale Formulierung nicht möglich war. Ich möchte jedoch betonen, dass die verwendeten männlichen Begriffe als nicht geschlechtsspezifisch zu betrachten sind.

2 Risikomanagement

Seit jeher ist der Mensch von Risiken umgeben, dies war bereits vor mehreren tausenden Jahren der Fall, als unsere Vorfahren Tiere gejagt haben, um danach von der erlegten Beute zu leben. Damals gingen die Menschen verschiedene Risiken ein, je nachdem, welches Tier sie jagten. Wenn damals ein Mammut gejagt wurde, so gingen die Menschen ein sehr hohes Risiko ein, da dieses Tier schwer zu erlegen war, jedoch war der mögliche Gewinn deutlich höher als beispielsweise bei einem Wildpferd, das mit weniger Risiko erlegt worden wäre.

In der heutigen Geschäftswelt kann man ein ähnliches Phänomen betrachten, da auch jene Projekte bzw. Geschäfte mit einem höheren Risiko verbunden sind, die einen großen Ertrag erwarten lassen. Jedoch ist es nicht die primäre Anforderung eines Unternehmens den größten Ertrag zu erwirtschaften, sondern neben dem Kerngeschäft stellt die Existenzsicherung des Unternehmens eine zentrale Aufgabe dar. Dass dies jedoch nicht immer erzielt werden kann, zeigt die folgende Statistik des Kreditschutzverbandes bezüglich der Insolvenzfälle der Österreichischen Unternehmen im Jahr 2010.

Bundesland	Fälle 2010	Fälle 2009	Veränderung	Passiva 2010 in Mio. EUR
Vorarlberg	288	263	9,5%	137
Burgenland	189	193	-2,1%	81
Kärnten	443	460	-3,7%	477
Tirol	458	484	-5,4%	256
Steiermark	832	894	-6,9%	865
Wien	2.023	2.180	-7,2%	1.751
Salzburg	400	449	-10,9%	199
Niederösterreich	914	1.031	-11,3%	476
Oberösterreich	829	948	-12,6%	459
Gesamt	6.376	6.902	-7,6%	4.700

Table 1. Insolvenzstatistik Unternehmen 2010¹

Obwohl im Vergleich zum Vorjahr ein Rückgang der Unternehmensinsolvenzen verzeichnet werden konnte, waren im Jahr 2010 dadurch 24.000 Dienstnehmer betroffen. Anzumerken ist, dass dadurch Insolvenzverbindlichkeiten in Höhe von EUR 4,7 Milliarden entstanden.

Die Statistik zeigt somit deutlich, dass ein Unternehmen ständig von Risiken bedroht wird und eine Vielzahl die Existenz eines Betriebes gefährdet. Um klar aufzeigen zu können wie man den Risikobegriff definiert und welche Risiken es für ein Unternehmen gibt bzw. in welche Kategorien diese unterteilt werden können, wird in den nachstehenden Kapiteln darauf eingegangen.

2.1 Risiko

Wie bereits erwähnt, ist das Risiko ein ständiger Begleiter des Menschen und so kommt es auch, dass das Wort „Risiko“ vom italienischen Wort „ris(i)co“ stammt, welches ein Vorhaben bzw. eine Unternehmung beschreibt, welches mit einem Wagnis oder einer Gefahr verbunden ist. [Dud07]

Eine eindeutige Definition des Begriffs für die heutige Zeit bzw. den unternehmerischen Einsatz gibt es nicht, da sich dazu in der Literatur zahlreiche Definitionen finden. So werden in weiterer Folge einige wenige aufgezeigt.

Risiko ist ein Ereignis, von dem nicht sicher bekannt ist, ob es eintreten und/oder in welcher genauen Höhe es einen Schaden verursachen wird. [Sch97]

Risiko ist die aus der Unvorhersehbarkeit der Zukunft resultierende, durch „zufällige“ Störung verursachte Möglichkeit, geplante Ziele zu verfehlen. [Gle01]

¹ Vgl. [KSV11]

Bei Risiken handelt es sich um Informationsunsicherheit über den Eintritt eines Sachverhaltes und die dadurch induzierte Möglichkeit der Beeinträchtigung von Zielen. **[Ris11]**

Wie zu sehen ist, gibt es für den Begriff mehrere Definitionen, die alle eine ungewisse Eintrittswahrscheinlichkeit und eine Auswirkung beinhalten. Aus diesem Grund finde ich die rudimentäre ISO/IEC Guide 73:2002 Definition passend und auch in einer mathematischen Formel darstellbar. Die Definition in dem genannten Standard lautet wie folgt.

Ein Risiko ist die Kombination der Wahrscheinlichkeit eines Ereignisses und seiner Konsequenz.²

In einer mathematischen Formel verpackt, kann die Definition wie folgt dargestellt werden.

$$R = W \times A^3$$

R	...	Risiko
W	...	Eintrittswahrscheinlichkeit
A	...	Abweichung / Konsequenz

2.2 Risikomanagementansätze

Nachdem nun definiert wurde, worum es sich bei Risiken handelt, ist es von hoher Bedeutung, dass diese vom Unternehmen mit Hilfe von Maßnahmen bekämpft werden, da ein Unternehmen diese Risiken nicht tragen möchte bzw. nicht tragen kann.

Um einen Einblick über die Maßnahmen eines Risikomanagements zu erhalten, werden auf den folgenden Seiten verschiedene Bereiche des Risikomanagements, die von besonderer Wichtigkeit sind, in einem abstrakten Kontext erläutert, welche aus **[Wie10]**⁴ stammen.

Nachdem sich ein Unternehmen dazu entschließt ein Risikomanagement einzuführen, wird ein iterativer Prozess gestartet, der sich mit der Risikoidentifizierung, der Risikoanalyse, der Risikobewältigung, sowie auch der Risiko- und Maßnahmenüberwachung beschäftigt. Dieser zyklische Vorgang wird auch in der nachstehenden Grafik dargestellt, die aus **[Wie10]** entnommen wurde und in weiterer Folge detailliert betrachtet wird, wobei sich die Ausführungen ebenfalls auf die angegebene Quelle stützen.

² Vgl. ISO/IEC Guide 73:2009

³ Vgl. ISO/IEC Guide 73:2009

⁴ Vgl. **[Wie10]** Seite 17 ff.

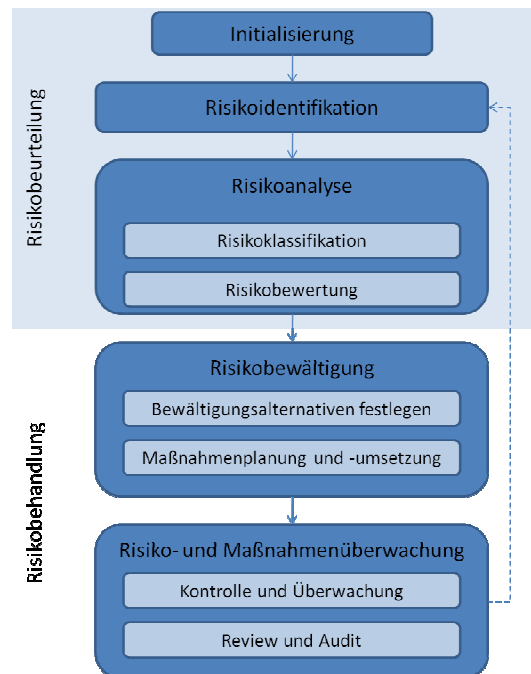


Fig. 1. Risikomanagementprozess⁵

2.2.1 Risikobeurteilung

Die erste Phase bei der Einführung eines Risikomanagements nennt sich Initialisierung. In diesem Abschnitt werden erste Schritte eingeleitet, sowie grundlegende Entscheidungen im Bezug auf Abgrenzungen und Aufgaben des Risikomanagements getroffen. Dabei stützen sich die Ausführungen in diesem Kapitel auf die Informationen aus [Wie10]⁶.

Risikoidentifikation

Um ein Risikomanagement effektiv zu betreiben ist es wichtig Risiken frühzeitig zu erkennen. Dafür ist ein detailliertes Branchenwissen nötig um die unterschiedlichen Einflussfaktoren zu entdecken und diese auch einschätzen zu können. Um jedoch die Risiken zu identifizieren, werden beispielsweise Szenario-Techniken, Post-Mortem Analysen oder auch die Delphi-Methode herangezogen.

⁵ Vgl. [Wie10] Seite 22

⁶ Vgl. [Wie10] Seite 22 ff.

Risikoanalyse

Nachdem die Risiken anhand einer gewählten Methode, die im Risikoidentifikationsprozess angewandt wird, aufgedeckt wurden, werden diese kategorisiert und bewertet.

Bei der Klassifikation unterscheidet man zwischen internen und externen Risikofeldern, wobei sich die internen Risikofelder auf jene Bereiche beziehen, die im Unternehmen ein Risiko darstellen können. Die externen Faktoren geben Auskunft über jene Risikofelder, die von außen auf ein Unternehmen einwirken können, wie dies auch in der nachstehenden Grafik, welche aus [Wie10] entnommen wurde, dargestellt ist.

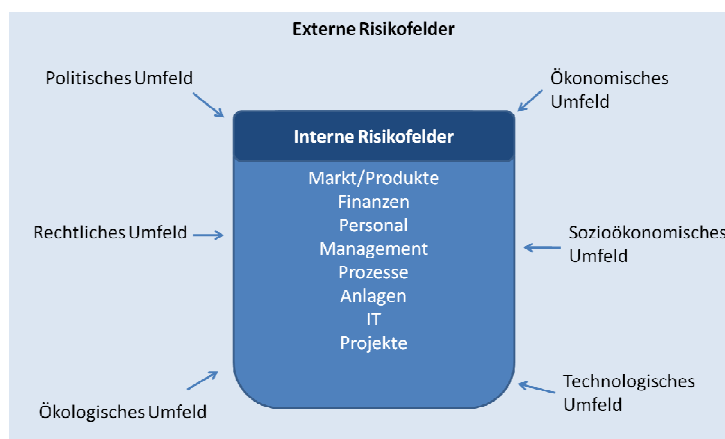


Fig. 2. Risikofelder⁷

Die Beschreibung der einzelnen Kategorien ist ebenfalls auf die Ausführungen in [Wie10]⁸ zurückzuführen und wird auf den nächsten Seiten in den einzelnen Punkten dargestellt.

Interne Risikofelder

- Markt/Produkte

Wenn man vom Markt und Produkt als internes Risikofeld spricht, so wird dieser Bereich einerseits von der Branchenkonstellation, der Wettbewerbssituation und der Kundenabhängigkeit geprägt. Andererseits sind auch die Marketingkampagnen und im Besonderen die Produkte- und Dienstleistungen ausschlaggebend für diesen Risikofaktor.

⁷ Vgl. [Wie10] Seite 11

⁸ Vgl. [Wie10] Seite 10 ff.

- **Finanzen**

Der finanzielle Aspekt ist ebenfalls ein sehr bedeutender, der stark von der Liquidität und Bonitätssituation abhängt. Das Kennzahlensystem, die Aktienkurssituation sowie auch Kreditausfälle können einen erheblichen Einfluss auf dieses Risikofeld ausüben.

- **Personal**

Das interne Risikofeld, das sich mit dem Personal beschäftigt, beinhaltet all jene Risikofaktoren, die sich um die Arbeitnehmer drehen. Dabei kann die Personalstruktur, die Personalbeschaffung oder auch die Personalfluktuations als Risikoquelle genannt werden. Außerdem fallen darunter auch Schlüsselpersonen, die Arbeitssicherheit oder auch die Qualifikationen bzw. das Know-how.

- **Management**

Auch das Management birgt Risikofaktoren, die in den internen Risikofeldern aufzuzeigen sind. So ist die Organisation, die Führungsstruktur oder auch das Managementinformationssystem für Risiken im Unternehmen verantwortlich. Außerdem können die Unternehmensstrategien und Unternehmensziele Risikofaktoren beinhalten.

- **Prozesse**

In einem Unternehmen lässt sich in allen Prozessen ein gewisses Risikopotential finden. Davon sind keine Prozesse ausgenommen, daher sind die Kunden- und Lieferantenprozesse, die Managementprozesse sowie auch die Unterstützungsprozesse detailliert zu betrachten.

- **Anlagen**

Von Risiken bleiben auch Anlagen nicht verschont, daher ist auch auf die Infrastruktur, sowie auf die Gebäudesicherheit zu achten. Risikofaktoren treten in diesem Bereich ebenfalls in der Instandhaltung auf.

- **IT**

Im Bereich der Informationstechnologie befinden sich auch zahlreiche Risikofaktoren, die sich auf das interne Umfeld auswirken. Darunter fallen beispielsweise die Daten- und Programmintegrität, der Datenschutz oder auch die Datensicherheit und die Notfallplanung. Ein weiterer Faktor, der zu beachten ist, ist die Systemabhängigkeit und die Systemverfügbarkeit.

- **Projekte**

Da in einem Unternehmen laufend Projekte durchgeführt werden und es sich bei Projekten um komplexe, neuartige und riskante Vorhaben handelt, ist es nicht verwunderlich, dass es auch in diesem Bereich zahlreiche Risikofaktoren gibt. Darunter fallen beispielsweise Risiken in der Planung oder hinsichtlich der Qualität, weiters ist auch auf das Entwicklungsverfahren und die Entwicklungswerkzeuge zu achten.

Externe Risikofelder

Die externen Risikofelder werden in den folgenden Punkten dargestellt und mit Risikofaktoren näher erläutert.

- Politisches Umfeld

Risiken können auch vom politischen Umfeld abhängen, da die globale Entwicklung und die politische Stabilität bedeutenden Einfluss auf ein Unternehmen nimmt. Weiters bestimmt die Wirtschaftspolitik der Legislative ein Unternehmen maßgeblich und kann auch Risikopotential mit sich bringen.

- Rechtliches Umfeld

Zusätzlich zum politischen Risikofeld besteht das rechtliche Risikofeld, welches unterschiedliche Rechte beinhaltet, wie das Steuerrecht, Vertragsrecht, Patentrecht oder auch das Gesellschaftsrecht an das sich Unternehmen zu halten haben.

- Ökologisches Umfeld

Ein Unternehmen wird auch stark von Umweltschutzfaktoren beeinflusst, so kann man auch Risikopotential bezüglich Recyclingverordnungen feststellen.

- Ökonomisches Umfeld

Das ökonomische Umfeld wird durch die Konjunktur- und Wechselkursentwicklung beeinflusst. Außerdem stellen die Inflation, die Zinssätze, das Investitions- und Konsumverhalten weitere Einflussfaktoren dar. Die Infrastruktur- und Rohstoffversorgung kann ebenfalls in diesem Risikofeld angesiedelt werden.

- Sozioökonomisches Umfeld

Ein weiterer Aspekt der externen Risikofelder betrifft demographische Daten über den Wirkungsraum eines Unternehmens, wie beispielsweise deren Entwicklung bezüglich Altersstruktur, Einkommens- und Vermögensverteilung oder auch Ausbildungsqualität. Weiters können der Wertewandel und die Arbeitsmentalität auch entscheidende Auswirkungen auf die Risikofaktoren haben.

- Technologisches Umfeld

In der heutigen hochtechnologischen Zeit sind Risiken aus diesem Bereich nicht außer acht zu lassen. So sind etwa Veränderungen im Informatik- und Telekommunikationsbereich oder auch Prozess- und Produktionsinnovationen detailliert zu betrachten, welche Risiken dahinter verborgen sein können.

Nachdem ein Risiko einer Kategorie zugeordnet wurde, ist in einem weiteren Schritt eine Bewertung des Risikos nötig, dazu wird das Risikopotential bestimmt. Ein Risikopotential oder auch Risiko wird anhand der Kombination aus Eintrittswahrscheinlichkeit des Risikos und der Schadenshöhe (Abweichung / Konsequenz) ermittelt. Dies wurde bereits bei der Definition des Risikos in Kapitel 2.1 aufgezeigt und lautet wie folgt.

$$R = W \times A^9$$

R	...	Risiko
W	...	Eintrittswahrscheinlichkeit
A	...	Abweichung / Konsequenz

Aus der Formel ergibt sich für ein Risiko ein Risikowert, der die Auswirkung angibt. Je höher der Wert des Risikos ist, desto gefährlicher sind die Auswirkungen für ein Unternehmen, wenn dieses Szenario eintritt. Dabei wird davon ausgegangen, dass die Abweichung / Konsequenz als Mehrkosten angegeben werden.

2.2.2 Risikobehandlung

Nachdem im ersten Teil des Risikomanagements die Risikobeurteilung mit der Identifikation und der Bewertung von Risiken im Mittelpunkt stand, werden in einem weiteren Prozessschritt die Maßnahmen und Strategien, wie Risiken abgewandt werden können, behandelt. Des Weiteren muss auch die Vorgehensweise und die Kontrolle für diese Strategien festgelegt werden, welche ebenfalls in diesem Kapitel dargestellt werden und laut den Ausführungen aus [Wie10]¹⁰ essentiell sind.

Risikobewältigung

Bei der Risikobewältigung gibt es zwei unterschiedliche Ansätze, die verfolgt werden können, wobei eine Kombination aus beiden in der Praxis laufend zur Anwendung kommt. Es handelt sich dabei um die aktive und die passive Risikobewältigung, wie dies in [Sch02]¹¹ erläutert wird und in diesem Abschnitt aufgezeigt wird. Bei der aktiven Risikobewältigung wird versucht die Eintrittswahrscheinlichkeit und/oder die Auswirkung eines Risikos zu minimieren. Dafür werden Strategien wie die Risikoverminderung, die Risikovermeidung und die Risikodiversifikation angewandt. Außerdem gibt es noch die Risikoakzeptanz, bei der das Risiko in Kauf genommen wird und somit nicht zu den klassischen Risikobewältigungsstrategien zählt.

Bei der Risikoverminderung werden Maßnahmen zur Minimierung der Eintrittswahrscheinlichkeit bzw. der Auswirkungen erstellt und angestrebt. Die Risikoverminderung verfolgt das Ziel kein Risiko einzugehen, damit keine Gefahr auftreten kann. Jedoch kann sich ein Unternehmen alleine durch diese Strategie um den Geschäftserfolg bringen, da ein Erfolg ohne Risiko nicht erzielt werden kann. Wenn man von Risikodiversifikation spricht bedeutet dies, dass das Risiko eines Unternehmens auf mehrere Vermögenswerte aufgeteilt wird, damit der Eintritt eines Risikos nicht das gesamte Unternehmen betrifft, sondern lediglich einen Teil. Des Weiteren gibt es noch die Risikoakzeptanz, die eingegangen wird, falls der Nutzen,

⁹ Vgl. ISO/IEC Guide 73:2009

¹⁰ Vgl. [Wie10] Seite 18

¹¹ Vgl. [Sch02] Seite 352 ff.

für den das Risiko eingegangen wird, deutlich höher ist als das Risikopotential und zugleich alternative Risikobewältigungsstrategien nicht möglich sind.

Im Gegensatz zu dem zuvor erläuterten Ansatz wird bei der passiven Risikobewältigung die Abwälzung der Konsequenzen verfolgt. Dabei stehen der Risikotransfer sowie auch die Risikovorsorge im Mittelpunkt. Von Risikotransfer spricht man, wenn ein Unternehmen Deckungsmaßnahmen für Verluste bereitstellt. Dies kann beispielsweise durch die Verwendung des Übergewinns, der als Gewinnbestandteil über dem Mindestgewinn definiert ist, oder durch Stille Reserven erfolgen. Diese beiden Varianten scheinen nach außen nicht auf und können somit vor Dritten verborgen werden. Weiters besteht die Möglichkeit, dass der Mindestgewinn verwendet oder weiteres Kapital herangezogen wird. Dies kann in Form von Ergänzungskapital von Banken zur Verfügung gestellt werden. Von einem Risikotransfer spricht man hingegen, wenn das Risiko auf Dritte abgewälzt wird, wie dies bei Versicherungen der Fall ist.

In diesem Arbeitsschritt ist für die identifizierten Risiken abzuwägen, welche oben genannte Risikobewältigungsstrategie man anwendet und welche Vorgehensweise man im Falle eines Risikoeintrittes wählt.

Risiko- und Maßnahmenüberwachung

Um zu gewährleisten, dass es sich bei den Risiken immer um aktuelle Risiken sowie auch aktuelle Risikoeinschätzungen handelt, sind eine laufende Kontrolle und Überwachung der Risiken bzw. der Risikopotentiale nötig. Dazu werden detaillierte Pläne erstellt, in welchen Perioden bzw. bei welchen Prozessvorkommnissen welche Risiken betrachtet werden, damit der Status bezüglich des Risikoeintritts kontrolliert und gegebenenfalls aktualisiert werden.

Dafür gibt es Prozessverantwortliche, die für die Überprüfung und die Dokumentation der Risiken verantwortlich sind. Aus [Wie10]¹² kann entnommen werden, dass aus den gewonnenen Daten Kontrolldokumente, Reviews oder auch Audits erstellt werden können. Des Weiteren kümmert sich die Interne Revision, die sich laufend um die Einhaltung der definierten Methode kümmert, um die Prüfung des Reifegrads der Methodik.

2.3 Standards für interne Kontrollsysteme und Risikomanagement

Die Betrachtung der Phasen des Risikomanagements in Kapitel 2.2 dient für das Verständnis und ist eine Kombination aus mehreren Standards. Einzelne Standards für die Vorgehensweise bezüglich einer Risikoabwehr bzw. Handhabung des Risikomanagements werden in den folgenden Kapiteln näher erläutert.

Bereits in den 90er Jahren wurden unterschiedliche Standards erarbeitet, die einen Best-Practice Ansatz darstellen. Diese Standards wurden in den Jahren laufend weiterentwickelt und dienen als Basis für Risikomanagement- und Internen Kontrollsystemen, da sich diese bewährt haben und international anerkannt sind.

¹² Vgl. [Wie10] Seite 41

2.3.1 Australisch-neuseeländischer Standard AS/NZS 4360

Der Australisch-neuseeländische Standard wurde bereits 1995 veröffentlicht und wurde damals durch das Mitwirken von Ministerien, akademischen Einrichtungen, Ingenieurverbänden und Versicherern erarbeitet. Da an der Ausarbeitung viele unterschiedliche Interessensvertreter mitgewirkt haben, handelt es sich bei dem AS/NZS 4360 um einen branchenneutralen Standard, der in den Jahren 1999 und 2004 in neuen Versionen erschienen ist. Weiters wurde zu jeder Version ein Handbuch verfasst, um Informationen für die Anwendung des Standards weiterzugeben.

Der Standard kann in drei grundlegende Elemente unterteilt werden, welche wie folgt definiert werden können.

- Definition von Fachbegriffen
- Beschreibung des Risikomanagement-Prozesses
- Beschreibung der Entwicklung und Implementierung eines Risikomanagement-Systems.

Die Grundlage für den Standard bildet der Prozess des Risikomanagements, der nachstehend dargestellt und beschrieben wird. Die Grafik sowie alle weiteren Informationen der einzelnen Bereiche wurden aus [Aus04] entnommen und wiedergegeben.

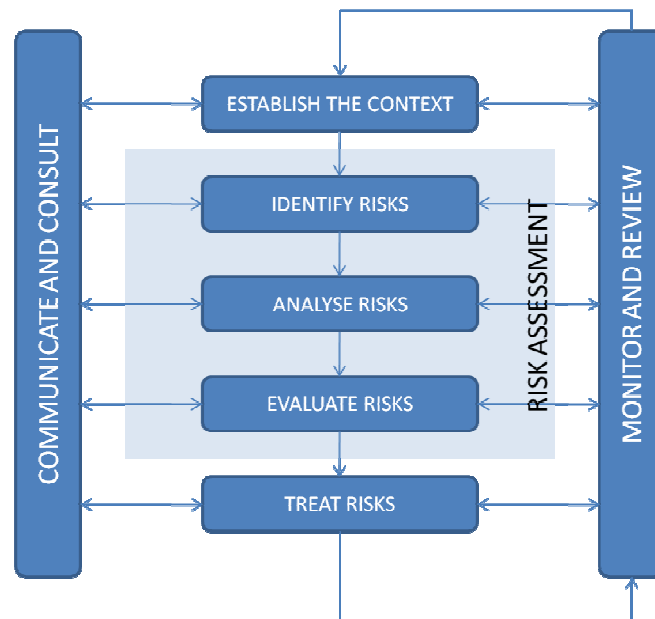


Fig. 3. Überblick Risikomanagement nach AS/NZS 4360:2004¹³

¹³ Vgl. [Aus04] Seite 9

Eingangs wird auf die beiden Komponenten eingegangen, die sich auf der linken und rechten Seite der Grafik befinden, da diese beiden Bereiche während des gesamten Prozesses in Verbindung mit den einzelnen Teilbereichen stehen und laufend Anwendung finden.

Communication and Consult

Dieses Element der Grafik stellt den laufenden Dialog dar, der in allen Phasen des Risikomanagements mit beteiligten Akteuren, wie Prozessverantwortlichen oder auch Stakeholdern zu erfolgen hat.

In [Aus04]¹⁴ wird darauf hingewiesen, dass durch die Kommunikation mit unterschiedlichen Akteuren auch unterschiedlichen Anforderungen erfüllt werden müssen. So ist es essentiell, dass jeder Benutzer jene Informationen erhält, die für ihn relevant sind. So ist ein Kommunikationsplan mit internen und externen Prozessbeteiligten und Informationslieferanten zu erstellen, bei denen beispielsweise Themen, wie die unterschiedlichen Risiken und deren Eintrittswahrscheinlichkeit, sowie deren Auswirkungen besprochen werden. Weiters ist es auch essentiell, die Interessen der Stakeholder laufend zu erheben und diese in das Risikomanagement zu integrieren, da diese Informationen dem Unternehmen als Entscheidungsgrundlage dienen.

Für die Erhebung von Informationen ist es sinnvoll, ein Befragungsteam im Unternehmen zu erstellen, das sich mit Befragungen aller Interessensgruppen beschäftigt und Ansprechpartner dient.

Monitor and review

Um den Managementplan zu erreichen und die zuvor beschriebenen Informationen einzuhalten bzw. umzusetzen, ist ein Review nötig. Des Weiteren kann ein Unternehmen aus älteren Reviews Erkenntnisse aus vergangenen Ereignissen ableiten und die Risiken, sowie deren Ausgang für die Zukunft besser einschätzen. Außerdem ist die Kontrolle der einzelnen Phasen ein nützliches Werkzeug, um die Vorgänge im Risikomanagement in den einzelnen Phasen zu optimieren, wie dies in [Aus04]¹⁵ vermerkt ist.

Establish the context

In diesem ersten Schritt des Risikomanagementablaufs, der in [Aus04]¹⁶ zu finden ist, werden Basisparameter definiert, die festlegen, welche Risikobereiche behandelt werden müssen. Somit wird der Anwendungsbereich des Risikomanagements in einem ersten Schritt geregelt. In dieser Phase wird zwischen der externen und internen Unternehmensumgebung unterschieden, um die Risiken in weiterer Folge in die korrekte Kategorie einzuteilen.

¹⁴ Vgl. [Aus04] Seite 11

¹⁵ Vgl. [Aus04] Seite 22

¹⁶ Vgl. [Aus04] Seite 12 ff.

Identify Risk

Um auf ein Risiko detailliert einzugehen und unterschiedliche Teilbereiche eines Risikos zu beleuchten, wird eine Risikoidentifizierung durchgeführt. Dabei stellen sich folgende Fragen, die für ein jedes Risiko beantwortet werden müssen, die in [Aus04]¹⁷ definiert sind.

- Was kann passieren?
- Wann kann etwas passieren?
- Wo kann etwas passieren?
- Wie kann etwas passieren?
- Warum kann etwas passieren?

Wenn man diese Fragen beantwortet hat, wird ein Risiko von unterschiedlichen Sichten beleuchtet und kann in einem weiteren Schritt analysiert werden.

Des Weiteren ist festzuhalten, dass nach Rücksprache mit Herrn Prof. Quirchmayr ein zusätzlicher Aspekt bei der Risikoidentifizierung von Bedeutung ist und nicht außer Acht gelassen werden sollte. Somit handelt es sich um eine Erweiterung, die sich mit folgender Fragestellung beschäftigt.

- Wer kann den Eintritt eines Risikos verursachen?

Analyse Risk

Bei der Risikoanalyse, die in [Aus04]¹⁸ betrachtet wird, wird versucht, die Entstehung von Risiken zu analysieren um das Risiko detailliert zu prüfen. Nachdem man das Risiko und die Zusammenhänge mit den Geschäftsprozessen verstanden hat, kann man die Risiken festhalten, indem man diese anhand von Qualitativer, Semi-quantitativer oder Quantitativer Analyse betrachtet.

Von Qualitativer Analyse spricht man, wenn in Wörtern die Konsequenzen und die Eintrittswahrscheinlichkeit einer Konsequenz beschrieben werden. Wenn man die textuelle Beschreibung der Konsequenzen und der Eintrittswahrscheinlichkeit zusätzlich mit Zahlenwerten versieht, so handelt es sich um eine Semi-quantitative Analyse. Bei der Quantitativen Analyse werden lediglich Werte für die Risiken und die Eintrittswahrscheinlichkeit verwendet, wodurch die Risiken besser verglichen werden können.

Evaluate Risk

Nachdem die Risikoanalyse durchgeführt wurde, wird diese als Ausgangsbasis für die Risikoevaluierung herangezogen um zu definieren, welche Strategie zur Risikobehandlungen angewandt wird. Dabei wird die Priorität des Risikos festgelegt, wie dies in [Aus04]¹⁹ beschrieben ist.

¹⁷ Vgl. [Aus04] Seite 16

¹⁸ Vgl. [Aus04] Seite 16 ff.

¹⁹ Vgl. [Aus04] Seite 19

Risk Treatment (Risikobehandlung)

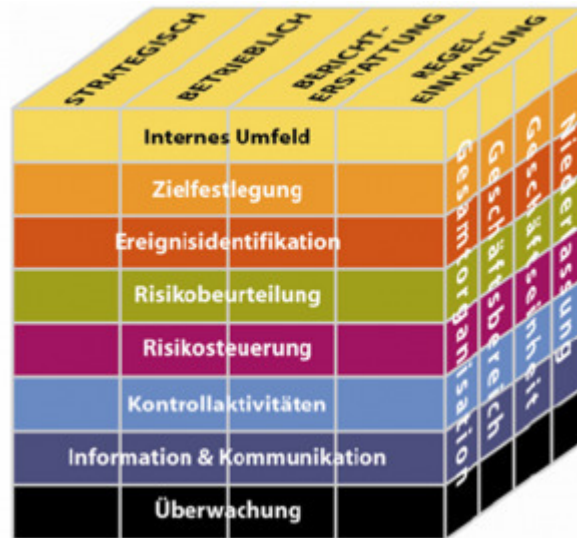
Dieser Schritt des Risikomanagements beschäftigt sich mit der Risikobehandlung und wie die Risikoabwehr bewerkstelligt werden kann bzw. wie man einem Risiko gegenübertritt. Diese Maßnahmen wurden bereits in Kapitel 2.2.2 behandelt und können nachgeschlagen werden. Weiters kann die Risikobehandlung auch in [Aus04]²⁰ eingesehen werden.

Des Weiteren kann in Bezug auf den Australisch-neuseeländischen Standard erwähnt werden, dass dieser nationale Standard, der sich etablieren konnte, für verschiedene weitere Standards wie beispielsweise dem ISO Standard für Risikomanagement Norm 30.100 als Grundlage dient, da viele wichtige Aspekte daraus übernommen wurden.

2.3.2 COSO I und COSO II

Das Committee of Sponsoring Organizations of the Treadway Commission ist jene Organisation, die für die Entwicklung des COSO Modells verantwortlich ist und dafür auch Namensgeber ist. Bereits 1992 hat die Organisation ein COSO Modell publiziert, das von der United States Securities and Exchange Commission standardisiert wurde. Da dieses Modell nicht sehr umfangreich war, wurde im Jahr 2004 das COSO II Modell veröffentlicht, welches mit einigen Erweiterungen erschienen ist. Diese Erweiterungen beziehen sich auf die horizontalen Ebenen des Internen Umfeldes, der Zielfestlegung, Ereignisidentifikation und der Risikosteuerung, die in der neuen Modellversion zusätzlich enthalten sind. Dieses COSO II Modell ist nachstehend mit sämtlichen Ebenen angegeben.

²⁰ Vgl. [Aus04] Seite 20 ff.

Fig. 4. COSO II Modell²¹

Grundsätzlich beschäftigt sich das dreidimensionale Modell mit den Komponenten des Internen Kontrollsystem (Internes Umfeld, Zielfestlegung, ...), den Unternehmenseinheiten (Niederlassung, Geschäftseinheit, ...) und den Zielkategorien (Strategisch, Betrieblich, ...). Um das unternehmensweite Risikomanagement ausreichend behandeln zu können, ist die ständige Verknüpfung der acht internen Kontrollsystemkomponenten, die im COSO II Modell dargestellt sind, laut **[Com04]** ein essentieller Bestandteil. Wenn man diese Punkte beachtet, kann gewährleistet werden, dass die Bewertung und die Verbesserung des Internen Kontrollsystems eines Unternehmens bewerkstelligt wird. Die Bedeutungen der Komponenten werden nun in weiterer Folge erläutert, um den Zusammenhang zu verdeutlichen, diese wurden aus **[Com04]** ²² entnommen.

Internes Umfeld

Das interne Umfeld beschreibt die Kultur eines Unternehmens und bildet die Grundlage dafür, wie Risiken durch die Mitarbeiter betrachtet und behandelt werden. Mit eingeschlossen sind dabei die Risikophilosophie und Risikobereitschaft, Integrität und ethische Werte. Zudem beschreibt das Interne Umfeld die Gegebenheiten, in dem das Unternehmen agiert.

Zielfestlegung

Ziele müssen festgelegt sein, bevor Führungskräfte mögliche Ereignisse, die deren Erreichen beeinflussen, bestimmen können. Das unternehmensweite

²¹ Vgl. **[Com04]** Seite 11

²² Vgl. **[Com04]** Seite 9 ff.

Risikomanagement ist Teil eines Prozesses, um Ziele zu setzen und um sicher zu stellen, dass die gewählten Ziele erreicht werden.

Ereignisidentifikation

Interne und externe Ereignisse, die das Erreichen der Ziele beeinflussen, müssen bestimmt und in Risiken und Chancen unterschieden werden. Chancen gehen in den Strategiebildungs- oder Zielsetzungsprozess der Führungskräfte ein.

Risikobeurteilung

Um eine Grundlage für die Steuerung von Risiken zu erhalten werden in diesem Bereich die Risiken unter Berücksichtigung von Auswirkung und Eintrittswahrscheinlichkeit betrachtet.

Risikosteuerung

Es werden Instrumente zur Risikosteuerung (Vermeiden, Vermindern, ...) erarbeitet und zu Risiken zugewiesen, damit die Risiken nicht die Risikotoleranz und Risikobereitschaft des Unternehmens übersteigt.

Kontrollaktivitäten

Vorschriften und Verfahren, die sicherstellen, dass Risikoreaktionen wirksam ausgeführt werden, werden festgelegt und umgesetzt.

Information & Kommunikation

Wesentliche Informationen sind in Form und Zeitrahmen erkannt, erfasst und verbreitet. Diese ermöglichen es Mitarbeitern, ihre Verantwortlichkeit wahrzunehmen. Wirksame Kommunikation findet auch in einem weiteren Sinne statt, abwärts, lateral und aufwärts in einem Unternehmen.

Überwachung

Die Gesamtheit des unternehmensweiten Risikomanagements und des damit in Verbindung stehenden Risikomanagementtools werden überwacht und erforderliche Anpassungen werden vorgenommen. Die Überwachung wird durch laufende Führungstätigkeiten und separate Beurteilungen erreicht.

Da in diesem Risikomanagementansatz im Modell auf den ersten Blick nicht ersichtlich ist, dass es sich um eine iterative Vorgehensweise handelt, ist anzumerken, dass es sich um einen multidirektionalen, iterativen Ablauf handelt, wobei jede Komponente eine jede andere Komponente beeinflussen kann.

2.3.3 ONR 4900X

Das Austrian Standard Institut hat mit der ONR-Serie „Risikomanagement für Organisationen und Systeme“ im Jahr 2010 eine neue Version des Risikomanagementstandards, welcher den Namen ONR 4900X trägt, definiert. Der

Standard besteht aus mehreren Dokumenten, die bestimmte Bereiche abdecken, wie dies auch in der folgenden Grafik dargestellt ist.

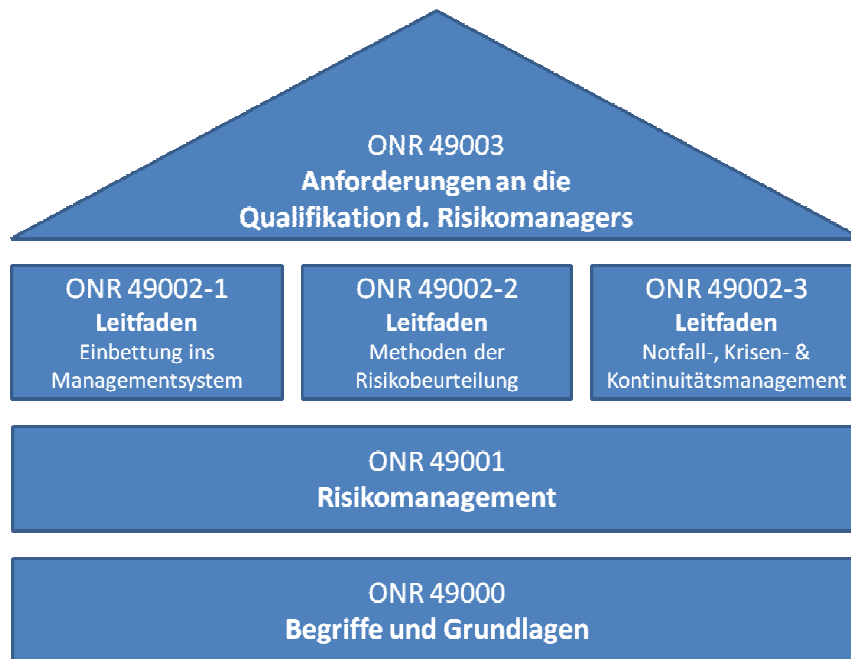


Fig. 5. Aufbau der ONR 4900X²³

Der Standard basiert aus mehreren Komponenten, die in Summe das Rahmenwerk darstellen, wie in [Öst10] angegeben. Die Basis bildet die Definition der Begriffe und Grundlagen worauf das Risikomanagement aufsetzt und spezifiziert wird. Zudem gibt es in dem Standard auch Leitfäden für die Einbettung ins Managementsystem, die Methoden der Risikobeurteilung und einen Leitfaden für das Notfall-, Krisen- & Kontinuitätsmanagement. In einem vierten Bereich werden die Anforderungen an die Qualifikationen des Risikomanagers erläutert.

Um die Umsetzung des Standards bestmöglich zu erreichen ist es wichtig, alle Bereiche genau zu betrachten und anzuwenden. Eine besondere Bedeutung kommt dem Risikomanagement zuteil, der anhand des folgenden Modells in der ONR 4900X umgesetzt wurde.

Das Risikomanagement ist als Managementkreislauf (Plan – Do – Check – Act) dargestellt, welcher in der folgenden Grafik abgebildet ist, wobei das Risikomanagement in den „Do“-Bereich des Kreislaufs fällt.

Im Bereich des „Plan“ werden Dokumentationsaufgaben, sowie Ressourcenplanung und Verantwortung der Leitung angesiedelt. Unter Verantwortung der Leitung versteht man die Managerpflichten, welche die Definition einer Risikopolitik und die Bewertung des Systems beinhaltet.

²³ Vgl. [Öst10] Seite 4

Im Risikomanagementprozess, der wie bereits erwähnt als „Do“-Bereich gilt, werden die Systemdefinition bzw. Systemabgrenzung, die Risikobeurteilung, die Risikobewältigung und die Risikosystemüberwachung betrachtet.

Die Systemüberwachung (Check) des Managementkreislaufs beinhaltet regelmäßige interne Audit und die Bewertung von möglichen Systemverbesserungen.

Die Verbesserung des Systems nimmt mit dem „Act“ Teil einen eigenen Platz ein und soll Korrektur- bzw. Verbesserungsmaßnahmen laufend ermöglichen.

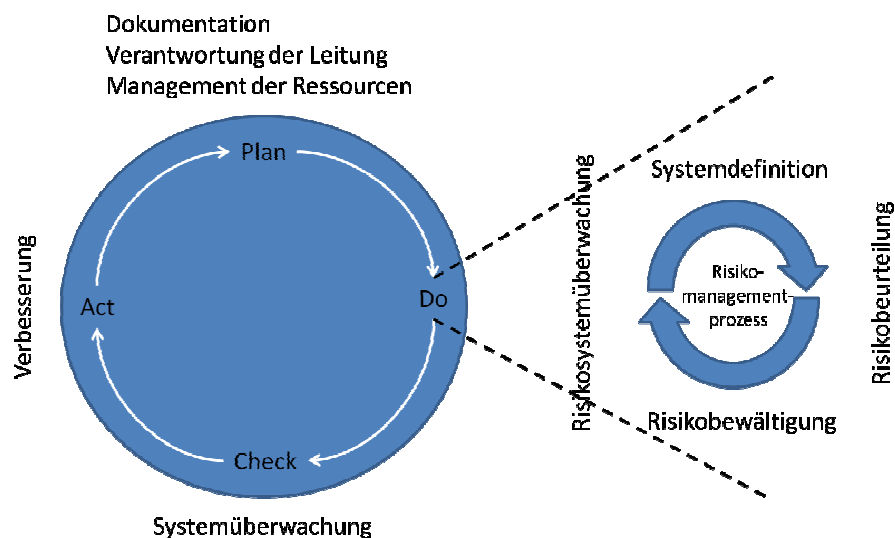


Fig. 6. Risikomanagement nach ONR 4900X²⁴

2.3.4 COBIT

Ein weiterer Standard, der im Zusammenhang mit IT Governance zu erwähnen ist, wurde 1996 erstmals veröffentlicht und trägt den Namen Cobit (Control Objectives for Information and related Technology). Der Standard wurde in den ersten Jahren vom Verband der IT-Prüfer mit dem Namen Information Systems Audit and Control Association (ISACA) entwickelt und untersteht seit der Jahrtausendwende der Schwesterorganisation IT Governance Institute.

Wie in [Gol06] erwähnt handelt es sich bei Cobit um eine Zusammenfassung einer Vielzahl von Standards aus unterschiedlichen Quellen, der als IT Governance Leitfaden dient und ein Best-Practice Framework anbietet. Cobit beschäftigt sich mit den Anforderungen, die beispielsweise durch gesetzliche Vorschriften an die IT gestellt werden und versucht diese optimiert bezüglich der Sicherheit, Qualität und Ordnungsmäßigkeit in der Informationstechnologie umzusetzen. Dabei wird nicht vorgegeben, wie die Anforderungen umgesetzt werden, sondern welche Anforderungen umzusetzen sind.

²⁴ Vgl. [BOC08] Seite 15

Cobit stellt für die Planung, Organisation, Implementierung, Überwachung und Optimierung 34 Prozesse zur Verfügung, die in Domänen unterteilt sind. Diese Prozesse bestehen in weiterer Folge aus Aktivitäten, wie dies in der folgenden Grafik anhand der IT Prozesse dargestellt ist. Außerdem ist die Grafik mit zwei weiteren Dimensionen versehen, welche die Geschäftsanforderungen und die IT Ressourcen aufzeigen und Einfluss auf die IT nehmen.

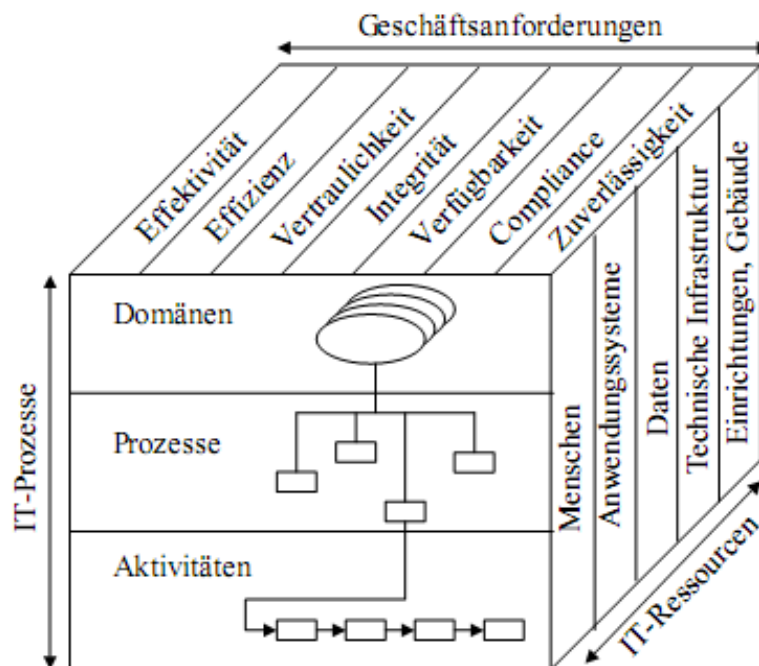


Fig. 7. Cobit Governance Würfel²⁵

Wenn man von den vier Cobit-Domänen spricht, so ist darauf zu achten, dass ein Regelkreis vorgegeben ist, der jedoch in dieser Arbeit nicht näher erläutert wird. Vielmehr werden im Folgenden die Prozesse aufgezeigt, die in einer Domäne enthalten sind. Dabei wurden die Ausführungen aus [Gol06] übernommen und in der Arbeit aufgezeigt.

- Planung & Organisation

Die Aufgabe in dieser Domäne liegt in der Erarbeitung der Strategie und der Taktik der IT. Dabei wird der beste Weg für die Erreichung der Geschäftsziele ermittelt, außerdem ist es unumgänglich, dass die Strategie geplant, kommuniziert und durchgeführt wird. Daraus ergeben sich folgende Prozesse.

²⁵ Vgl. [Gol06] Seite 26

Planung & Organisation	
PO1	Definieren eines strategischen IT-Plans
PO2	Definieren der Informationsarchitektur
PO3	Definieren der technischen Ausrichtung
PO4	Definition der IT-Organisation und ihrer Beziehungen
PO5	IT-Investitionsmanagement
PO6	Kommunizieren der Management Ziele und Strategien
PO7	IT-Personalführungsmanagement
PO8	Managen der Qualität
PO9	Risikomanagement
PO10	Projektmanagement

Table 2. Cobit-Prozesse – Planung & Organisation²⁶

In diesem Bereich stellen die ersten vier Prozesse PO1 – PO4 sogenannte Hauptprozesse dar, die interaktiv und iterativ auszuführen sind. Es ist auch anzumerken, dass diese Ergebnisse die folgenden Prozesse beeinflussen.

- Akquisition & Implementierung

Damit eine IT Lösung festgelegt werden kann, ist es notwendig, dass eine IT-Strategie umgesetzt wird. Dazu ist es unerlässlich, sich für eine IT-Lösung zu entscheiden und diese zu erwerben, sowie die dafür nötige Infrastruktur. Wie in [Gol06] erwähnt unterliegt die IT-Lösung einer ständigen Veränderung oder kann auch durch Störungen beeinflusst werden, darum wurde in dieser Domäne auch ein Change-Managementprozess integriert.

Akquisition & Implementierung	
AI1	Identifizierung automatisierter Lösungen
AI2	Erwerb und Pflege von Applikationssoftware
AI3	Erwerb und Pflege der technischen Infrastruktur
AI4	Befähigen des Betriebes
AI5	Zur Verfügungstellung von IT-Ressourcen
AI6	Change Management
AI7	Installieren und Abnehmen von Systemen und Änderungen

Table 3. Cobit-Prozesse – Akquisition & Implementierung²⁷

- Delivery & Support

Diese Domäne beschäftigt sich mit der Lieferung der IT-Services, damit sind das Operating, die Administration, die Schulungen und auch das Thema Sicherheit gemeint. Damit es möglich ist, dass diese Services bereitgestellt werden, sind Supportprozesse nötig. So kann als Beispiel genannt werden, dass DS1 laut den Ausführungen aus [Gol06] mit DS2, DS6 in Verbindung steht, um die Ausrichtung

²⁶ Vgl. [Gol06] Seite 28

²⁷ Vgl. [Gol06] Seite 28

der Services optimal zu gewährleisten. Weiters liefert der erste Prozessinput Informationen für die Prozesse DS11 bis DS 13.

Delivery & Support	
DS1	Service Level Management
DS2	Lieferanten Management
DS3	Performance und Kapazitätsmanagement
DS4	Continuity Management
DS5	System Security Management
DS6	Kostenmanagement
DS7	Anwenderschulung und Training
DS8	Anwenderunterstützung
DS9	Konfigurationsmanagement
DS10	Problem Management
DS11	Data Management
DS12	Facility Management
DS13	Operationsmanagement

Table 4. Cobit -Prozesse – Delivery & Support²⁸

- Monitoring und Evaluierung

Um laufend zu überprüfen, ob die festgelegten Standards und die Qualitätskriterien eingehalten werden, ist die letztgenannte Domäne unumgänglich. In diesem Bereich werden die Einhaltung der gesetzlichen Vorschriften und die Durchdringung der Governancestrukturen in die gesamte Organisation sichergestellt. Dabei liefert ME4 die Basis an der sich die anderen Prozesse orientieren, bei denen die operativen Durchführungen im Fokus stehen.

Monitoring und Evaluierung	
ME1	Überwachen und evaluieren IT Performance
ME2	Überwachen und evaluieren interner Kontrollen
ME3	Sicherstellung der Einhaltung gesetzlicher Vorschriften
ME4	Sorgen für IT-Governance

Table 5. Cobit -Prozesse – Monitoring und Evaluierung²⁹

All diese Prozesse können mit Hilfe von Cobit auch hinsichtlich des Reifegrads bewertet werden. Dies dient dazu, dass ein Unternehmen einen objektiveren Eindruck über die Abläufe erhält und so auch Verbesserungspotential aufdecken kann. Dabei kann zwischen unterschiedlichen Reifegraden unterschieden werden, die sich von nicht existent bis hin zu optimiert erstrecken und die in detaillierter Ausführung in [Gov07] nachgeschlagen werden können. Der Bereich der Reifegradanalyse wird im

²⁸ Vgl. [Gol06] Seite 28

²⁹ Vgl. [Gol06] Seite 28

Zuge der Evaluierung ebenfalls Anwendung finden und in den Kapitel 4.2 und 7.2 behandelt werden.

Nach diesen einleitenden Worten über das Risiko, sowie dessen Bedeutung, das Risikomanagement und die derzeit verwendeten Standards im Risikomanagementbereich wird in Kapitel 3 näher auf das Interne Kontrollsystem sowie dessen Positionierung im Risikomanagement eingehen.

3 Interne Kontrollsysteme

Ein organisatorisches Grundelement des Risikomanagements stellt das Interne Kontrollsystem dar. Darin enthalten sind die Grundsätze und Maßnahmen, welche von der Unternehmensleitung definiert wurden. Des Weiteren ist es für zahlreiche Unternehmen auf Grund von gesetzlichen Vorschriften von Nöten, dass ein Internes Kontrollsystem im Unternehmen integriert wird.

Wenn man ein Internes Kontrollsystem im Unternehmen einsetzt, so stellen sich laut **[Hen06]**³⁰ Vorteile für ein Unternehmen ein, da die nachstehenden Ziele verfolgt werden.

- Sicherstellung des Geschäftsvermögens, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen
- Zuverlässigkeit/Vollständigkeit der finanziellen und operativen Informationen (Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung)
- Untersuchung der Effektivität und Effizienz der Unternehmensprozesse (Aufdeckung möglicher Veränderungs- und Steigerungspotentiale)
- Erfüllung gesetzlicher Anforderungen und Vorschriften, sowie Einhaltung von Verträgen
- Vereinheitlichung von konzernweiten Standards und Richtlinien
- Insolvenzrisiken frühzeitig zu erkennen
- Berichterstattung
- Steigerung der Transparenz des Internen Kontrollsystems
- Erhöhung der Effizienz des Internen Kontrollsystems

Weiters sind sich Experten im Risikomanagementbereich, wie der BWiSe CEO Robert Pijselman, einig, dass die Verwendung eines Internen Kontrollsystems für ein Unternehmen nicht nur eine Pflicht sein muss, sondern dass es bei einer gewissenhaften Verwendung ein Unternehmen stärken kann und dieses mit Hilfe des Tools eine bessere Verbesserung der Unternehmenskontrolle erhält. **[BWi]**

³⁰ Vgl. **[Hen06]** Seite 31 ff.

3.1 Bestandteile eines Internen Kontrollsystems

Wie in der nachstehenden Grafik, die eine Kombination aus [Hen06] und [Lat10] zeigt, dargestellt ist, besteht ein Internes Kontrollsystem aus dem Internen Steuerungssystem, welches ein System aus Regelungen zur Steuerung der Unternehmensaktivitäten vorgibt. Der zweite Bereich eines Internen Kontrollsystems besteht aus dem Internen Überwachungssystem, das sich mit der Einhaltung der definierten Regelungen auseinandersetzt.

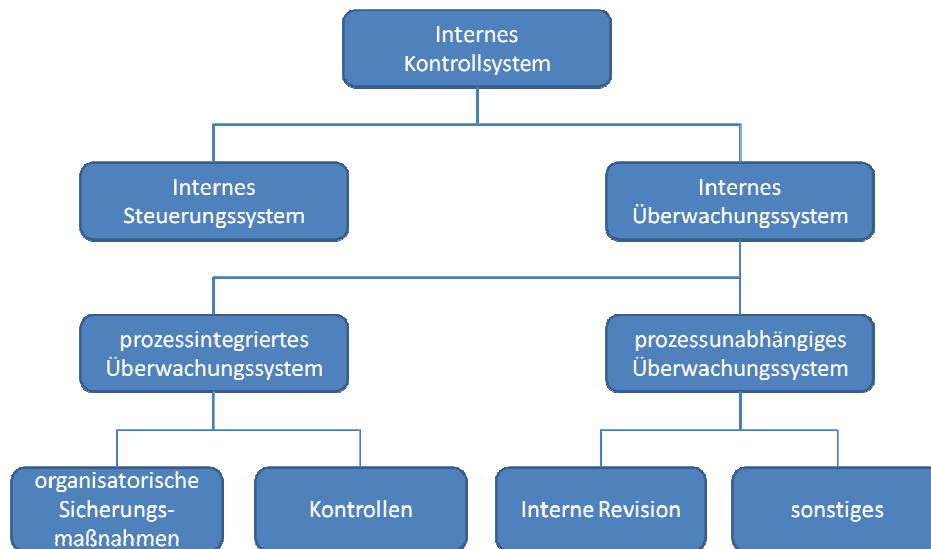


Fig. 8. Internes Kontrollsystem³¹

Da dieses Gebiet aus mehreren Unterkategorien besteht, werden diese in Anlehnung an [Hen06]³² nachfolgend näher beschrieben.

3.1.1 Prozessintegrierte Überwachungssysteme

Organisatorische Sicherungsmaßnahmen

Damit ein gewisses Sicherheitsniveau erreicht werden kann, werden in einem Unternehmen organisatorische Sicherungsmaßnahmen, die laufend durchgeführt werden, eingeführt.

Dabei gibt es *selbstständige Kontrollen*, die laufende, automatische, fehlervermindernde Maßnahmen beinhalten, die in der Ablauf- und Aufbauorganisation integriert sind. Außerdem sind *manuelle Kontrollen* für ein wirksames Internes Kontrollsystem nötig. Darunter fallen Überwachungsmaßnahmen und Leistungskontrollen durch die Geschäftsleitung (Budgetvergleiche, ...),

³¹ Vgl. [Hen06] Seite 34 und vgl. [Lat10] Seite 205

³² Vgl. [Hen06] Seite 38 ff.

Kontrollen im Informationsfluss (kompetenzgerechte Genehmigungen, abklären von Differenzmeldungen, ...) sowie physische Kontrollen (Inventur, ...). Weiters besteht die Möglichkeit von *programmierten Kontrollen*, wobei man hier zwischen applikationsunabhängigen und applikationsabhängigen Kontrollen sprechen kann. Mit applikationsunabhängigen Kontrollen sind beispielsweise Authentifizierungs- oder auch Kontrollsummenkontrollen gemeint. Dem gegenüber stehen die Überprüfung von Daten bei der Erfassung, Verarbeitung und Ausgabe durch Plausibilitätstests mit applikationsabhängigen Kontrollen. *Flankierende Maßnahmen* stellen einen weiteren Bereich dar. Darunter fällt beispielsweise, einen Posten im Unternehmen, der geschäftsschädigende Handlungen ausführen kann nicht einzig auf Grund der fachlichen Eignung zu besetzen, sondern auch die Vertrauenswürdigkeit und die Zuverlässigkeit mit in die Beurteilung einfließen zu lassen. Dabei gibt es unterschiedliche Vorgehensweisen je nachdem, ob es sich um eine interne oder eine externe Besetzung handelt. So kann man bei einer externen Besetzung ein polizeiliches Führungszeugnis oder Auskünfte von früheren Arbeitsgebern einholen. Bei internen Besetzungen kann man als Bewertung für die Vertrauenswürdigkeit und die Zuverlässigkeit den Eindruck der letzten Jahre heranziehen, indem es ein systematisches Mitarbeiterbeurteilungssystem gibt.

Kontrollen

Im Bereich der Kontrollen ist es möglich, dass man die Kontrolle zu unterschiedlichen Phasen durchführt, genauso kann man auch bei den Methoden der Kontrolle verschiedene anwenden. So kann der Kontrollzeitpunkt vor-, gleich- oder auch nachgeschaltet sein. Abhängig von der Methode, die man für einen Kontrollzeitpunkt auswählt, kann man diese manuell durch eine Person oder mit Hilfe eines IT System durchführen.

3.1.2 Prozessunabhängige Überwachungssysteme

Unter prozessunabhängige Überwachungssysteme fallen in diesem Zusammenhang lediglich Rollen, die ein Mitarbeiter einnimmt, um gewisse Aufgaben zu übernehmen. Diese Aufgaben werden vor allem von der Internen Revision übernommen.

Interne Revision

Die Interne Revision übernimmt in einem Internen Kontrollsystem die meisten Aufgaben der prozessunabhängigen Überwachung. Darunter fallen die Prüfung von Kontrollen und Sicherungen auf Vollständigkeit, Wirksamkeit und Zweckmäßigkeit im Rahmen der Prüfung aller Betriebs- und Geschäftsabläufe bzw. Geschäftseinheiten.

Sonstiges

Unter diesen Punkt fallen weitere Beauftragte, die für Überwachungsmaßnahmen verantwortlich sind, die keinem speziellen Prozess zugeordnet werden. Dies sind beispielsweise der Risikomanager, Compliance Officer oder Datenschutzbeauftragter, die mit der Überwachung bestimmter Bereiche beauftragt sind.

3.2 Gesetzliche Grundlagen

Da es um die Jahrtausendwende in den Vereinigten Staaten von Amerika zu einigen Bilanzskandalen von großen Firmen gekommen war, wurde ein amerikanisches Bundesgesetz verabschiedet, welches das Vertrauen der Anleger wieder zurückgewinnen sollte. Dies war der Sarbanes-Oxley Act, der 2002 eingeführt wurde, damit die Richtigkeit und die Verlässlichkeit von veröffentlichten Finanzdaten bewerkstelligt werden. Das Gesetz findet seither Anwendung bei allen Unternehmen, die an einer amerikanischen Börse notiert sind.

Da sich zu Beginn dieses Jahrtausends in Europa ebenfalls Finanzskandale ereignet haben, wurden die Richtlinien 2006/43/EG und 2006/46/EG des Europäischen Parlaments und des Rates ratifiziert. Diese sind auch als 8. EU-Richtlinie oder als EuroSOX bekannt, da die Richtlinien zahlreiche Ähnlichkeiten zur amerikanischen Umsetzung aufweisen. Diese Richtlinie hatte in weiterer Folge von den Mitgliedsstaaten in nationalen Gesetzen verankert werden müssen, wie dies auch unter [Bey08] zu finden ist. Dabei können folgende Punkte als wesentliche Inhalte genannt werden, die mit der Einführung verfolgt wurden und aus [Bey08] entnommen wurden.

- Unabhängigkeit des Abschlussprüfers
- Kompetenzen und Zusammensetzung des Prüfungsausschusses
- Befristetes Tätigkeitsverbot für Abschlussprüfer
- Unabhängigkeit des Honorars des Abschlussprüfers - keine Beratungstätigkeiten
- Umfang Management Letter und Prüfbericht

3.2.1 Österreich

Die Umsetzung der beiden Richtlinien wurde in Österreich durch das Unternehmensrechtsänderungsgesetz (URÄG) und dem Rechnungslegungsänderungsgesetz (RLÄG) erreicht. Das URÄG soll die Finanzberichterstattung transparenter machen und das Vertrauen in die Tätigkeit von Abschlussprüfern erhöhen. Das RLÄG verpflichtet Unternehmen in Österreich, alle relevanten Risiken innerhalb eines Konzernlageberichts anzuführen und zu beschreiben.

Des Weiteren sind im Aktiengesellschaftsgesetz (AktG) und in dem Gesellschaft mit beschränkter Haftung Gesetz (GmbH) die Verwendung eines Internen Kontrollsystems verankert.

3.2.2 Deutschland

In Deutschland trat bereits im Jahr 1998 das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) in Kraft. Dieses Gesetz wurde zur Stabilisierung des Finanzmarktes entwickelt, da dieser durch finanzielle Schwierigkeiten schwer gezeichnet war. Um die Berichterstattung eines Unternehmens zu verbessern, wurde daraufhin das Bilanzrechtsreformgesetz (BilReG) ratifiziert, welches ein Unternehmen auch zur Prognoseberichterstattung verpflichtet. Deshalb müssen

deutsche Unternehmen die zukünftige Geschäftsentwicklung beschreiben und die damit verbundenen Risiken und Chancen bewerten. Des Weiteren gibt es in Deutschland das Transparenz- und Publizitätsgesetz (TransPubG), das die Unternehmensführung und Unternehmensüberwachung transparenter gestalten soll.

Das neueste Gesetz wurde im Mai 2009 in Kraft gesetzt und lautet Bilanzrechtsmodernisierungsgesetz (BilMoG). Dieses Gesetz zielt auf eine bessere Aussagekraft des Jahresabschlusses, sowie die detaillierte Umsetzung der Richtlinien 2006/43/EG in Ergänzung durch die Richtlinie 2008/30/EG und der Richtlinie 2006/46/EG des Europäischen Parlaments und des Rates.

3.2.3 Schweiz

Schweizer Unternehmen mit der Rechtsform einer Aktiengesellschaft, Gesellschaft mit beschränkter Haftung, Genossenschaft und Stiftung unterliegen dem Gesetz mit dem Namen Revision des Obligationsrechts (OR), das ein Unternehmen verpflichtet sich mit den Unternehmensrisiken auseinanderzusetzen und diese zu beurteilen. Außerdem muss im Zuge der Revision eine Überprüfung des Internen Kontrollsystems vorgenommen werden.

3.3 Branchenübliche Richtlinien

Neben den gesetzlichen Vorschriften wurden in zahlreichen Branchen Richtlinien entwickelt, um das Vertrauen der Geschäftspartner und Kunden zu gewinnen und eine bessere Einsicht zu gewähren. Auf den folgenden Seiten werden die Richtlinien, die im Banken- und Versicherungsbereich eingeführt wurden, näher erklärt.

3.3.1 Basel II

Der Basler Bankenausschuss hat das Rahmenwerk Basel II entworfen und in [Ban06] festgehalten, welche in diesem Kapitel als Referenz verwendet wurde. Anzumerken ist, dass im europäischen Raum dieses Rahmenwerk seit der Novellierung der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates für alle Kreditinstitute, die in der Europäischen Union tätig sind, anzuwenden ist.

Im Rahmenwerk wurde definiert, dass die Stabilität des Finanzsystems auf drei Säulen aufbaut, die in [Ban06]³³ zu finden ist.

- Säule 1: Mindestkapitalvorschrift
- Säule 2: Das aufsichtliche Überprüfungsverfahren
- Säule 3: Marktdisziplin

Die erste Säule beschäftigt sich mit der Mindestkapitalausstattung, wobei das Eigenkapital in einem bestimmten Verhältnis zu dem Risikoprofil der Bank stehen muss. Diese Eigenkapitalausstattung wird durch einen laufenden Prozess, der Internal Capital Adequacy Assessment Process (ICAAP) genannt wird, geprüft. Dabei werden

³³ Vgl. [Ban06] Seite 7

die Risiken identifiziert und gemessen und darauf aufsetzend das interne Kapital gemäß dem Risikoprofil ausgestattet.

Bezüglich eines Internen Kontrollsystems ist die zweite Säule von besonderer Bedeutung, da sich diese mit Empfehlungen zum Risikomanagement und zur Transparenz und Rechenschaftspflicht bezüglich der Risiken im Bankgeschäft beschäftigt.

Der Bankenausschuss ist davon überzeugt, dass die Marktdisziplin bereits durch die ersten beiden Säulen bewerkstelligt wird, jedoch wird in der dritten Säule die Offenlegung von Unternehmensinformationen zusätzlich explizit gefordert.

Anzumerken ist, dass während der Ausarbeitung der vorliegenden Masterthesis eine neue Version durch den Basler Bankenausschuss ausgegeben wurde, der sich Basel III nennt. Somit gibt es eine neue Richtlinie, die in dieser Arbeit nicht näher betrachtet wird, welche eine Weiterentwicklung von Basel II darstellt.

3.3.2 Solvency II

Wie die österreichische Finanzmarktaufsicht in **[FMA11]** angibt, wurde bereits 1995 eine Arbeitsgruppe auf europäischer Ebene installiert, welche die Unterschiede von Solvabilitätsvorschriften für Versicherungen in Europa untersuchte. Danach wurden 1997 die nötigsten Änderungen bei bestehenden Richtlinien überarbeitet und Solvency I veröffentlicht. Eine Überarbeitung des gesamten Systems brachte eine Methode zur risikobasierten Steuerung der Solvabilität eines Versicherungsunternehmens, die Solvency II genannt wurde. Diese Methode wurde in den Richtlinien 2002/12/EG und 2002/13/EG des Europäischen Parlaments und des Rates verankert und in Österreich 2004 in nationales Recht übernommen.

In Solvency II können die folgenden Punkte als wesentlich bezeichnet werden, die in **[FMA11]** aufgezeigt sind.

- Risikobasierte Unternehmenssteuerung und risikobasierte Eigenmittelberechnung
- Harmonisierung/Konvergenz in Europa
- Basel II Kompatibilität (in Bereichen, wo es sinnvoll erscheint, gewisse Techniken auch für Versicherungen anzuwenden.)
- Wandel von einem regelbasierten System zu einem prinzipienbasierten System (z.B.: Wegfall von starren Regeln, dafür flexiblere Eingriffsmöglichkeiten und mehr qualitative Anforderungen)
- Kompatibilität mit International Financial Reporting Standard (IAS/IFRS)
- Drei Säulen Ansatz

Das Drei Säulen Prinzip wurde von Basel II übernommen und an die speziellen Anforderungen eines Versicherungsunternehmens angepasst.

Die erste Säule beschäftigt sich mit den Eigenkapitalanforderungen eines Versicherungsunternehmens, dabei werden Bestimmungen für die Berechnung der Rückstellungen festgelegt, sowie auch Überprüfungen für die Berechnungsansätze.

Die Säule mit dem Namen Supervisory Review Report ist die zweite Säule und in dieser werden einerseits die Grundsätze und Methoden der Aufsicht und andererseits

die qualitativen Anforderungen an die Ausübung der Tätigkeit der Versicherungsunternehmen festgelegt.

In Hinsicht auf die Umsetzung der Marktdisziplin und Markttransparenz ist die dritte Säule, die als Marktdisziplin und Veröffentlichungspflicht bezeichnet wird, besonders wichtig. Hier werden beispielsweise Überschneidungen mit den IAS/IFRS berücksichtigt.

4 Entwicklung eines Evaluierungsmodells zur Auswahl eines toolgestützten Internen Kontrollsystems

Um eine Evaluierung für ein IT System, welches die Aufgaben eines Internen Kontrollsystem unterstützt, in einem Unternehmen durchzuführen, ist es nötig eine Vorgehensweise, wie bei einem Projekt zu initiieren um dieses Unterfangen abzuwickeln. Auf eine detaillierte Beschreibung der Projektphasen wird in dieser Arbeit nicht eingegangen, jedoch soll klargestellt werden, dass es sich bei der Evaluierung um ein eigenständiges Projekt handelt.

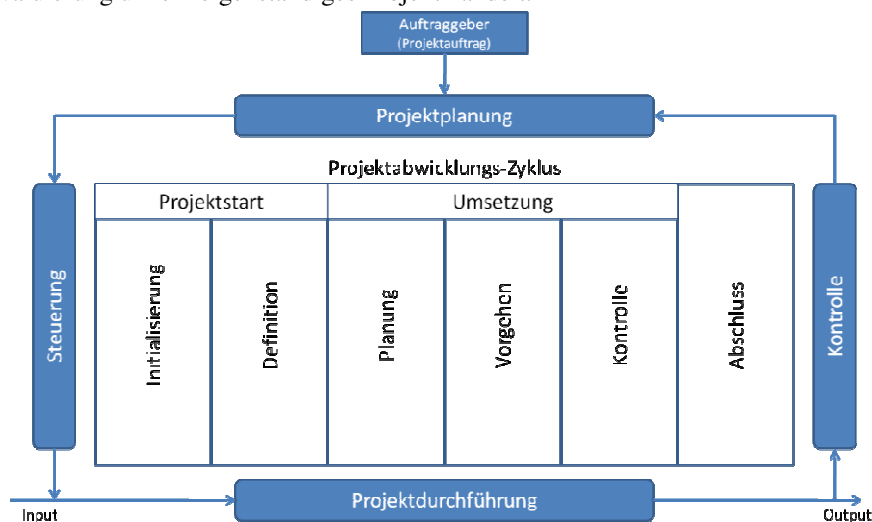


Fig. 9. Projektentwicklungs-Zyklus im Regelkreis³⁴

Wie in Abbildung 8 dargestellt finden sich in einem Projektentwicklungs-Zyklus nach [Jen01] die Phasen Initialisierung und Definition unter dem Oberbegriff Projektstart. In der Umsetzung werden die Planung, das Vorgehen und die Kontrolle genannt, worauf der Abschluss folgt, der ein Projekt beendet. Des Weiteren sind in der Grafik die Projektplanung, Steuerung, Durchführung und Kontrolle aufgezeigt, welche iterative Prozesse im Projekt darstellen, die den Projektentwicklungs-Zyklus begleiten. Die Evaluierung eines Internen Kontrollsystems, das in Kapitel 7

³⁴ Vgl. [Jen01] Seite 459

durchgeführt wird, basiert auf der oben dargestellten Vorgehensweise. Die Vorgehensweise für die Einführung des Systems ist auf einem anderen Modell, welches speziell für IT Einführungsprojekte entwickelt wurde, aufgesetzt und stellt ein eigenes Projekt dar. Dies wird zu einem späteren Zeitpunkt jedoch noch deutlicher aufgezeigt.

Nachdem nun definiert wurde, in welcher Phase eines Projekts die Evaluierung angesiedelt ist, kann auf das Konzept für die Evaluierung eingegangen werden. Dazu wird auf die zuvor genannten Aspekte, sowie unternehmensinterne Anforderungen bei der Toolauswahl für ein Internes Kontrollsystem eingegangen. Um ein Evaluierungsmodell zu erstellen muss fixiert werden, welche Bereiche betrachtet werden sollen. Dazu wird die Evaluierung an die Phasen Analyse und Entwurf eines Vorgehensmodells für Softwareentwicklung, wie dies aus [Sta02]³⁵ entnommen wurde, angelehnt. Damit wird die Evaluierung in Teilbereiche zerlegt und beschäftigt sich in jedem Bereich mit einer bestimmten Frage.

Frage 1: WAS soll das System leisten?

Frage 2: WIE soll das System realisiert werden?

Die erste Frage wird mit Hilfe eines Evaluierungsschritts beantwortet, der sich funktionale Evaluierung nennt. In einem weiteren Schritt, wird sich die technische Evaluierung beispielsweise mit der Umsetzung im Bereich Infrastruktur und Sicherheit beschäftigen, somit wird die zweite Frage beantwortet.

Zusätzlich ergibt sich aus wirtschaftlicher Sicht eine weitere Fragestellung, die aus Unternehmenssicht ebenfalls einen essentiellen Blickwinkel auf die Toolauswahl darstellt, damit ist die Frage nach den Kosten gemeint. Um die Kosten abschätzen zu können, sind unterschiedliche Kostenfaktoren zu beachten, die in diesem Evaluierungsschritt berücksichtigt werden, dadurch ergibt sich eine weitere Frage, die wie folgt formuliert werden kann.

Frage 3: WIEVIEL kostet das System?

Aus diesen drei Fragestellungen ergeben sich nun die Themengebiete, mit denen sich der produktspezifische Evaluierungsprozess beschäftigt und somit durch das Evaluierungsmodell abgedeckt werden sollen.

- Funktionale Evaluierung
- Technische Evaluierung
- Finanzielle Evaluierung

Bei der Betrachtung dieser Gebiete ist einfürend anzumerken, dass die Reihenfolge der Betrachtung nicht als Vorgabe für die Verwendung dient. Es werden lediglich die Themengebiete aufgezeigt, die bei einer Betrachtung untersucht werden müssen. Die Reihenfolge ist bei jedem Projekt selbstständig festzulegen.

³⁵ Vgl. [Sta02] Seite 214

Die Evaluierungsschritte stellen den Kern des Evaluierungsmodells dar, jedoch sind zuvor einige Definitionen und Abgrenzungen nötig, um die Evaluierung mit klaren Regeln zu versehen und eine einheitliche und nachvollziehbare Evaluierung gewährleisten zu können. So ist die Definition des Kriterienkatalogs der erste Schritt, der von der Festlegung der Prioritäten und der Bewertungsskala gefolgt wird. Die Gewichtung der Themengebiete und Themenblöcke stellt den letzten Punkt der Vorarbeiten dar.

Wenn nun alle Punkte geklärt sind, so steht die Evaluierungsphase bevor, die aus den drei oben genannten Teilbereichen besteht. Diese Teilbereiche sind in einer bestimmten Reihenfolge durchzuführen, wobei ein Teilbereich abgeschlossen sein muss, bevor der nächste begonnen wird. Die Auswertung stellt den letzten Punkt des produktspezifischen Evaluierungsmodells dar, welcher durch den vorgefertigten Microsoft Excel Sheet automatisch durchgeführt werden kann.

In grafischer Form werden die entwickelten Schritte der produktspezifischen Evaluierung nachstehend dargestellt und in den folgenden Kapiteln detailliert beschrieben.

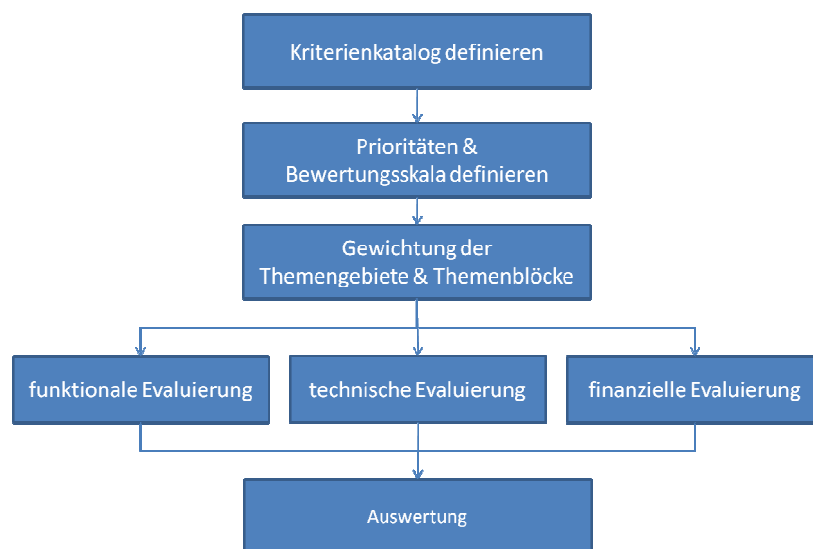


Fig. 10. Evaluierungsmodell für IKS Tools

Um den Evaluierungsprozess um einem Aspekt zu erweitern, wird neben der produktspezifischen Evaluierung eine Betrachtung der Tools in Verbindung mit dem Reifegradmodell aus Cobit durchgeführt. Dies trägt dazu bei, dass die Evaluierungsergebnisse neben den Teilbereichen, die in der produktspezifischen Evaluierung untersucht werden, auch die strategische Dimension geprüft wird. Dabei steht im Fokus der Evaluierung, ob ein Tool die Erreichung von Unternehmensziele unterstützen kann. Zu diesem Zweck werden unterschiedliche Attribute beleuchtet,

aus denen sich der Reifegrad zusammensetzen lässt, wie dies in [Gov07] ³⁶ angegeben ist.

4.1 Produktspezifische Evaluierung

Die Methodikbeschreibung der produktspezifischen Evaluierung, die in der Abbildung 10 dargestellt wurde, wird in diesem Kapitel detailliert beschrieben. Die Ausführung dient in weiterer Folge für die Toolevaluierung an einem Praxisbeispiel, wie auch für sämtliche folgende Evaluierungen.

4.1.1 Kriterienkatalog definieren

Durch die gesetzlichen, sowie auch durch die unternehmensinternen Anforderungen müssen zu Beginn Kriterien definiert werden, welche für die Toolevaluierung betrachtet werden und die Entscheidungsfindung beeinflussen sollen. Um diese Kriterien zu erarbeiten ist es nötig, dass die Gesetzeslage betrachtet wird und die Vorgaben des Gesetzgebers befolgt werden. Es ist jedoch anzumerken, dass meist die Gesetze bereits in den Tools, die ein Internes Kontrollsystem anbieten, integriert sind und somit diese Anforderungen berücksichtigt sind. Der Vollständigkeit halber ist dieser Punkte jedoch nie außer Acht zu lassen.

Besondere Bedeutung kommt den unternehmensinternen Anforderungen zu, welche man in zwei Bereiche unterteilen kann. Einerseits gibt es branchenspezifische Anforderungen für ein Unternehmen, wie dies beispielsweise bei Versicherungen oder Banken mit den in Kapitel 3.3 erwähnten branchenspezifischen Anforderungen ist. Andererseits ist die Berücksichtigung von firmeninternen Richtlinien, sowie auch Anwenderwünsche wichtig. Besonders die Berücksichtigung von Anwenderwünschen kann in weiterer Folge die Akzeptanz des Tools im Unternehmen positiv beeinflussen.

Um diese Kriterien herauszuarbeiten ist es wichtig Gespräche mit Spezialisten aus dem Unternehmen und Anwendern zu führen. Dabei können Anforderungen und Wünsche formuliert und diskutiert werden, was in weiterer Folge eine positive Auswirkung auf die Akzeptanz des Tools im Unternehmen bringen kann.

Themengebiete und Themenblöcke

Damit jedoch nicht eine Vielzahl an Kriterien in einem Pool als Ergebnis am Ende der Erarbeitung der Kriterien aufscheint, wurden die drei Themengebiete (funktionale, technische und finanzielle Evaluierung) definiert. Dadurch kann die Evaluierung unterteilt werden und wird aus diesem Grund übersichtlicher. Um in den einzelnen Evaluierungen eine weitere Kategorisierung zu erreichen, werden Themenblöcke gebildet, in denen sich die Kriterien befinden, die wie folgt definiert sind.

³⁶ Vgl. [Gov07] Seite 21

Funktionale Evaluierung

In der funktionalen Evaluierung scheinen fünf Themengebiete auf, die wie folgt lauten.

- generelle Anforderungen
- Kundenanforderungen
- Customizinganforderungen
- Nachvollziehbarkeits-/Workflowanforderungen
- Überwachung des Internen Kontrollsystems (Revision)

Technische Evaluierung

Bei der technischen Evaluierung werden die Themenblöcke

- Systemplattform
- Methodikhandbuch
- Software
- Sicherheit
- Sonstiges
- Systemanforderungen

mit Kriterien befüllt und betrachtet.

Finanzielle Evaluierung

Da bei der finanziellen Evaluierung lediglich wenige Kriterien evaluiert werden, gibt es keine Themenblöcke, in denen sich die Kriterien befinden.

Für die Evaluierungen wird ein Microsoft Excel Sheet im Zuge der Masterthesis zur Verfügung gestellt, der bereits Kriterien beinhaltet, die zur Evaluierung vorgeschlagen werden und welche von einem Tool für Interne Kontrollsysteme gefordert sein sollten. Ziel der Erarbeitung der Kriterien ist die Finalisierung der Evaluierungsbögen hinsichtlich der zu betrachtenden Kriterien, dabei sollen vorgeschlagene Kriterien um die unternehmensinternen Anforderungen erweitert werden.

4.1.2 Prioritäten & Bewertungsskala definieren

Nachdem die Kriterien definiert wurden, ist die Bestimmung der Priorität jedes einzelnen Kriteriums wichtig. Diesbezüglich ist bereits in den Vorgesprächen darauf zu achten, wie wichtig einzelne Kriterien eingestuft werden. In Abstimmung mit den verantwortlichen Rollen für das Interne Kontrollsystem ist die Bewertung der einzelnen Kriterien erforderlich. Diese Festlegung der Priorität ist vor der Evaluierung durchzuführen und darf danach nicht mehr verändert werden, damit das Ergebnis der Evaluierung nicht verfälscht wird. Die Skala der Priorität und der Bewertung wird auf den nächsten Seiten genauer erklärt.

Bewertungsmethode

Um die Bewertungsergebnisse zu erhalten, muss zuvor eine Bewertungsmethode gewählt werden, welche im Fall dieses Evaluierungsmodells die Multifaktorenmethode ist. Dabei wird eine Form der Multifaktorenmethode für sämtliche Evaluierungsschritte benützt, die nach folgendem Prinzip angewandt wird und an jene aus [Sta02]³⁷ angelehnt ist.

1. Die in Kapitel 4.1 definierten Kriterien scheinen in den Evaluierungsbögen auf, wie diese zuvor vom Unternehmen definiert wurden.
2. Die Bedeutung bzw. Priorität der Kriterien wird durch einfache Gewichte zum Ausdruck gebracht.

5 = sehr wichtig
 4 = wichtig
 3 = weniger wichtig
 2 = nicht wichtig
 1 = wird nicht benötigt

3. Das geplante Anwendungssystem wird danach mit Hilfe einer Punktbewertung beurteilt, in wie weit der Nutzen für das Unternehmen besteht. Dabei kann man sich an folgende Aufstellung als Evaluierer halten.

4 = sehr gute Umsetzung inkl. Dokumentation
 3 = Umsetzung laut Informationsmaterial von Dritten
 2 = Umsetzung durch Workaround / Anpassung möglich
 1 = lückenhafte Umsetzung bzw. Umsetzung ist durch
 Eigenimplementierung möglich
 0 = keine Umsetzung / keine Informationen erhalten

Es ist jedoch anzumerken, dass die Bewertungsskala für einzelne Kriterien nicht immer so umgelegt werden kann, da die Antworten für jede Fragestellung andere sind. Daher ist es ratsam, für alle Kriterien festzulegen, welche Bewertung für welche Antwort verwendet wird.

4. Die in (3) vergebenen Punkte werden Kriterium für Kriterium mit den zugehörigen Gewichten aus (2) multipliziert.
5. Der Nutzen der Anwendung kann in diesem Beispiel auf Grund der Produktsumme nach (4) ermittelt werden. Je höher die Gesamtsumme (5) des Bewertungsbogens ist, desto mehr Nutzen stellt die Anwendung für das Unternehmen dar.

Um die textuelle Beschreibung besser nachvollziehen zu können wird ein Beispiel für die Methode in der nachstehenden Tabelle gegeben.

³⁷ Vgl. [Sta02] Seite 255

Kriterium (1)	Priorität (2)	Bewertung (3)	Produkt (4)
Clientzugang per Webbrowser	5	4	20
Anfügen von Dateien/Links	3	4	12
Gesamtbewertung (5)			32

Table 6. Beispiel für Multifaktorenmethode

Bei der Multifaktorenmethode ist anzumerken, dass darauf zu achten ist, dass die Auswahl und die Gewichtung der Kriterien, sowie die Bewertung der Kriterien stark von der subjektiven Einschätzung des Bewertungsteams bzw. jener Person, welche die Bewertung durchführt, abhängig sind.

KO Kriterien

Neben der Priorisierung der Kriterien ist die Festlegung von KO Kriterien ein weiterer Punkt.

Unter KO Kriterien sind all jene Kriterien gemeint, die aus Sicht des Unternehmens unumgänglich umgesetzt sein müssen. Da die Wichtigkeit für das Unternehmen sehr hoch ist, wird es sich bei KO Kriterien meist um Kriterien mit einer Priorität von fünf handeln. Es können jedoch auch weitere Kriterien als KO Kriterien benannt werden, die eine geringere Priorität haben.

Im Rahmen des Evaluierungsprozesses kann somit für sämtliche Kriterien, die eine Priorität von fünf Punkten hat ein Bewertungsergebnis mindestens den Durchschnitt erreichen muss. Wenn die Bewertung jedoch nur 0 oder 1 ist, so konnte das KO Kriterium nicht zur Zufriedenheit erfüllt werden. Wenn KO Kriterien nicht erfüllt werden, so ist das Tool aus der Evaluierung zu nehmen und die restlichen Evaluierungen für dieses Tool werden nicht mehr vorgenommen.

4.1.3 Gewichtung der Themengebiete und Themenblöcke

Nachdem die Anzahl der Kriterien in den einzelnen Themenblöcken und in weiterer Folge auch in den Evaluierungsschritten unterschiedlich ist, wurde für diese beiden Bereiche eine Gewichtung eingeführt. Durch diese Gewichtung kann der Fokus auf einzelne Teilbereiche gelegt werden, wenn diese als wichtiger eingestuft werden.

Dieser Arbeitsschritt ist ebenfalls vor der Evaluierung der Tools durchzuführen und in Absprache mit den Verantwortlichen für das Interne Kontrollsystem zu klären.

Gewichtung der Themenblöcke

Die Themenblöcke in den Evaluierungen können für die Ermittlung des Ergebnisses für einen Evaluierungsschritt mit Gewichtung versehen werden, damit es nicht vorkommen kann, dass ein Themenbereich mit einer großen Anzahl an Kriterien das Gesamtergebnis in eine bestimmte Richtung verzerrt, obwohl dieser Bereich nicht als sehr wichtig betrachtet wird.

Gewichtung der Themengebiete

Auf oberster Ebene ist es möglich, dass die unterschiedlichen Evaluierungen mit unterschiedlicher Gewichtung belegt werden. Je nach Anforderungen des Unternehmens kann eine bestimmte Evaluierung als bedeutender eingestuft werden. Beispielsweise kann dies zur Anwendung kommen, wenn für ein Unternehmen der finanzielle Aspekt primär von Bedeutung ist. So kann dieses Unternehmen die finanzielle Evaluierung mit einer Gewichtung von 50% belegen und die beiden anderen Evaluierungen mit jeweils 25% gewichten. Dies ändert die Gesamtbewertung des Tools und stellt die Anforderungen des Unternehmens besser dar.

4.1.4 Evaluierungsschritte

Nach den genannten Definitionen beginnt die eigentliche Toolevaluierung der Internen Kontrollsysteme. Dabei sind die drei nachstehenden Evaluierungsschritte zu betrachten, wobei es sich hier um keine vorgegebene Reihenfolge handelt.

- Funktionale Evaluierung
- Technische Evaluierung
- Finanzielle Evaluierung

Vor dem ersten Evaluierungsschritt ist eine Einteilung der Evaluierungsschritte von Nöten. Diese Reihenfolge kann auf Grund der unternehmensspezifischen Präferenzen festgelegt werden. Die Reihenfolge ist für alle Tools bindend und jeder Evaluierungsschritt soll parallel ausgeführt werden. So ist sichergestellt, dass die Tools in gleicher Zeit evaluiert werden und die Ergebnisse zu einem gleichen Zeitpunkt geliefert werden.

Um einen Einblick in die Evaluierung zu bekommen, werden in den folgenden Kapiteln der Masterthesis nochmals die Themenblöcke mit den vordefinierten Kriterien aufgezeigt, die in weiterer Folge durch Benutzeranpassungen an das Unternehmen erweitert werden sollen.

Bei der Erarbeitung der Kriterien hat sich die Kooperation mit Herrn Prof. Quirchmayr und Herrn Mag. Michael Kogler als sehr lohnend entpuppt, da zahlreiche Punkte erarbeitet und diskutiert wurden. Durch die Kooperation mit der Austrian Airlines AG und deren Inputs sind einige Kriterien bzw. Themengebiete ein wenig luftfahrtsspezifisch, wobei anzumerken ist, dass diese Kriterien auch für andere Branchen anwendbar sind. Weiters möchte ich anmerken, dass einige Kriterien, die von Herrn Mag. Michael Kogler vorgebracht wurden, auf Grund von Vorgaben des Lufthansakonzerns in die Bewertung mit eingeflossen sind.

*Funktionale Evaluierung**generelle Anforderungen*

- Benutzer-Rollenkonzept
- Einhaltung von Compliance-Vorgaben (BilMoG, URÄG, RLÄG, ...)

- Benutzerfreundlichkeit (easy-to-use for Clients) auf Basis von Standards (z.B. ISO Norm 9241)

Kundenanforderungen

- Datenübernahme aus operativen System
- Verlinkung zum Risikomanagementtool
- Event-Management (Reminderfunktionen, E-Mailnotifikation, ...)

Customizinganforderungen

- Konfigurierbarkeit und Anpassungsmöglichkeit
- Individuell gestaltbare Auswertungen
- zusätzliche Kontrollen (benutzerdefinierte, konzerninterne Kontrollen)

Nachvollziehbarkeits-/Workflowanforderungen

- Protokollierung (Sicherstellung der Nachvollziehbarkeit)
- Historisierung der Kontrollergebnisse
- Workflow zur Erfassung/Bearbeitung/Bestätigung von Steuerungs-/Überwachungsinstrumenten
- Automatische Kontrollen von Grenzwertüberschreitungen anhand hinterlegter Regeln aus den importierten Daten

Überwachung des Internen Kontrollsystems (Revision)

- Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor
- Übersicht zum Stand der Aktualisierung des ISK
- Übersicht der Ergebnisse der Wirksamkeitsprüfung

Technische Evaluierung

Systemplattform

In diesem Bereich soll die IT Infrastruktur des Unternehmens aufscheinen, dabei sollen die aktuellen Server- und Clientumgebungen aufgezeigt werden. Darunter fallen die verwendeten Betriebssysteme auf Server und Clientseite, sowie weitere Applikationen, die den Geschäftsbetrieb unterstützen. Damit sind Datenbanksysteme oder auch Applikationsserver gemeint, wenn sich solche im Einsatz befinden. Weiters ist auch abzuklären, ob in näherer Zukunft Änderungen in diesem Bereich anstehen, damit diese ebenfalls berücksichtigt werden können.

Die angepassten Kriterien für die Austrian Airlines AG werden im Kapitel 7.1.2 dargestellt und mit deren Bewertung aufgezeigt.

Methodikhandbuch

- Quickinfo (Handbuch für die täglichen Aufgaben der Enduser)

Software

- Einführungsaufwand (in Tagen)
- Lizenzmodell (Concurrent)

Sicherheit

- Datensicherheit
- Datensicherung

Sonstiges

- Helpdesk
- Wartungsvertrag

Systemanforderungen

- minimale Systemanforderungen

Finanzielle Evaluierung

Bei der gemeinsamen Erarbeitung der Kriterien wurden folgende Punkte für wesentlich erachtet.

- Anschaffungskosten
- Wartungskosten (pro Jahr)
- Customizingkosten

Weiters können in diesem Bereich auch Wirtschaftlichkeitsvergleiche für sämtliche Tools angestellt werden, die in die Bewertung einfließen. Dabei kann zwischen unterschiedlichsten Wirtschaftlichkeitsbewertungen, wie in **[Sta02]** ³⁸ angeführt, unterschieden werden.

³⁸ Vgl. **[Sta02]** Seite 251 ff.

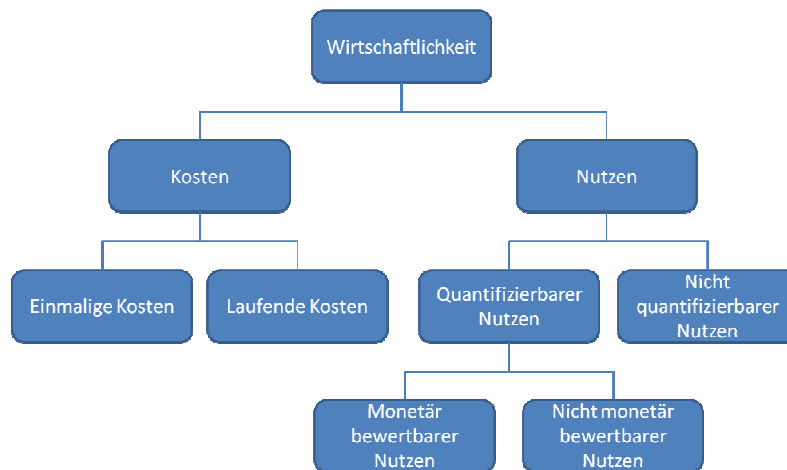


Fig. 11. Struktur von Wirtschaftlichkeitsvergleichen³⁹

Bei den Methoden der Wirtschaftlichkeitsvergleiche können reine Kostenvergleiche angestellt werden, oder Kosten/Nutzen-Vergleiche. Dabei sind die Kostenvergleichsrechnung oder die Kostenvergleichsrechnung mit Amortisationsrechnung bei den Kostenvergleichen zu nennen. Bei den Kosten/Nutzen-Vergleichen werden auch Bereiche bewertet, die nicht monetär zu bewerten sind, darunter fallen beispielsweise Qualitätsverbesserungen. Die Nutzwertanalyse ist in diesem Bereich beispielsweise zu nennen, da diese oftmals Anwendung findet.

4.1.5 Auswertung

Die Auswertung stellt den abschließenden Teil des Evaluierungsmodells dar, dazu werden die Ergebnisse der einzelnen Evaluierungen mit der in Kapitel 4.1.3 genannten Gewichtung berechnet und zusammen zu einem Gesamtergebnis kombiniert.

Dazu wurde im Zuge der Masterthesis ein Microsoft Excel Sheet erstellt, der diesen Vorgang realisiert. Die Verwendung eines solchen Microsoft Excel Sheets wurde gewählt, da die Verwendung in Unternehmen sehr stark verbreitet ist und sich durch eine einfache Handhabung auszeichnet.

4.2 COBIT-Evaluierung

Durch die Cobit-Evaluierung kann sich ein Unternehmen einen objektiven Blick auf die unterstützenden Technologien machen und feststellen welchen Nutzern die Informationstechnologie für das Unternehmen hat. Im Zuge einer solchen Analyse ist

³⁹ Vgl. [Sta02] Seite 254

es sinnvoll eine Situationsaufnahme zu erstellen und eine Zielvorgabe für die Zukunft. Mit Hilfe dieser Erkenntnis aus dem IST und SOLL Vergleich kann eine Verbesserung des Managements und der Steuerung von IT Prozessen bewerkstelligt werden, die mit Hilfe des Cobit-Reifegradmodells ermittelt werden kann.

Um die Bewertung aussagekräftig gestalten zu können, wurden in das Cobit-Reifegradmodell verschiedene Attribute mit eingearbeitet. Dazu zählen jene sechs Attribute, die in [Gov07]⁴⁰ zu finden sind und sich beispielsweise mit der Zielmessung, den Werkzeugen und der Automation oder auch den Fähigkeiten und Erfahrungen beschäftigt.

4.2.1 Bewertungsskala

Für die Bewertungsskala werden im Zuge der Cobit Dokumentation für die einzelnen Prozesse, die in Kapitel 2.3.4 aufgezeigt wurden, detaillierte Beschreibungen aufgelistet, welche die Bewertung für einen Prozess bestimmen. Um jedoch ein allgemeines Verständnis für die Bewertungsskala zu erhalten, gibt es eine generische Bewertungsskala, die in [Gov07] angegeben ist und wie folgt aufgebaut ist, wobei auch die deutsche Version von Cobit [Gov11] als Informationsquelle gedient hat.

0	Non-existent (nicht existent)	Es ist kein Prozess erkennbar. Das Unternehmen hat nicht einmal den Bedarf erkannt, dass das Thema in Angriff genommen werden soll.
1	Initial / Ad Hoc (initial)	Es bestehen Anzeichen, dass das Unternehmen den Bedarf erkannt hat, das Thema zu behandeln. Es existieren jedoch keine standardisierten Prozesse, es ist vielmehr ein ad-hoc-Ansatz in Verwendung, der individuell und situationsbezogen angewandt wird. Der gesamthafte Managementansatz ist nicht organisiert.
2	Repeatable but intuitive (wiederholbar)e	Prozesse wurden soweit entwickelt, dass gleichartige Verfahren von unterschiedlichen Personen angewandt werden, die dieselbe Aufgabe übernehmen. Es besteht kein formales Training oder eine Kommunikation der Standardverfahren und die Verantwortung ist Einzelpersonen überlassen. Es wird stark auf das Wissen von Einzelpersonen vertraut, demzufolge sind Fehler wahrscheinlich.
3	Defined Process (definiert)	Verfahren wurden standardisiert und dokumentiert und durch Trainings kommuniziert. Die Einhaltung der Prozesse ist jedoch der Einzelperson überlassen und die Erkennung von Abweichungen ist unwahrscheinlich. Die Verfahren sind nicht ausgereift und sind ein formalisiertes Abbild bestehender Praktiken.

⁴⁰ Vgl. [Gov07] Seite 21

4	Managed and Measureable (gemanagt)	Es ist möglich, die Einhaltung von Verfahren zu überwachen und zu messen, sowie Aktionen dort zu ergreifen, wo Prozesse nicht wirksam funktionieren. Prozesse werden laufend verbessert und folgend Good Practices. Automatisierung und Werkzeugunterstützung findet eingeschränkt und nicht integriert statt.
5	Optimised (optimiert)	Prozesse wurden, basierend auf laufender Verbesserung und Vergleichen mit anderen Unternehmen, auf ein Best-Practice-Niveau verbessert. IT wird integriert für die Workflow-Automatisierung verwendet, stellt Werkzeuge für die Verbesserung der Qualität und Wirksamkeit zur Verfügung und macht das Unternehmen flexibel, sich Änderungen anzupassen.

Table 7. Cobit 4.1 – generische Bewertungsskala⁴¹

Die unterschiedlichen Sichtweisen auf eine Problemstellung werden mit Hilfe von mehreren Attributen beschrieben, diese Attribute sind im Anhang im Kapitel 13.2 zu finden. Wobei angemerkt werden soll, dass dabei folgende Blickwinkel behandelt werden, die aus [Gov07]⁴² entnommen wurden.

- Bewusstsein und Kommunikation
- Policies, Standards und Verfahren
- Werkzeuge und Automatisierung
- Skills und Expertise
- Zuständigkeit und Verantwortlichkeit
- Zielsetzung und Messung

Mit diesen Sichtweisen werden auch die Tools, die zur Auswahl stehen, betrachtet und bewertet. Zur Anwendung kommt in diesem Bereich ebenfalls eine weitere Cobit Ausführung, die in [Gov07] auf Seite 175 zu finden ist, dabei handelt es sich um eine Bewertungsskala für Interne Kontrollen, die in Kapitel 13.3 wiedergegeben ist. Somit wurden jene Bereiche definiert, die im Zuge der Cobit-Evaluierung betrachtet und bewertet werden.

In Summe kann ein Tool somit maximal 35 Punkte erreichen, da die Bewertung für eine optimierte Lösung in einem Teilbereich bei fünf Punkten liegt und die Bewertung in sieben Bereiche unterteilt ist, in denen Punkte vergeben werden.

Bevor die Cobit-Evaluierung für die neuen Tools, die dem Evaluierungsprozess unterzogen werden, durchgeführt wird, stellt die Cobit-Evaluierung für die IST Situation einen wichtigen Bereich dar. Auf Grund dieser Evaluierung kann sich ein Unternehmen wie bereits erwähnt einen Einblick über die derzeitige Technologienutzung verschaffen. Weiters besteht die Möglichkeit, wie dies in Abbildung 12 dargestellt ist, zukünftige Ziele hinsichtlich der Technologienutzung festzulegen und im Unternehmen zu positionieren. Bei der Festlegung der Ziele wird

⁴¹ Vgl. [Gov07] Seite 19, vgl. [Gov11] Seite 22

⁴² Vgl. [Gov07] Seite 21

aus Kostengründen jedoch nicht immer eine optimierte Lösung angestrebt, welche mit fünf Punkten bewertet wird, sondern oft auch eine etwas niedriger eingestufte Lösung. Mit Hilfe der Ermittlung des Reifegrads kann eine Zielerreichung nachvollziehbar dargestellt und dokumentiert werden.

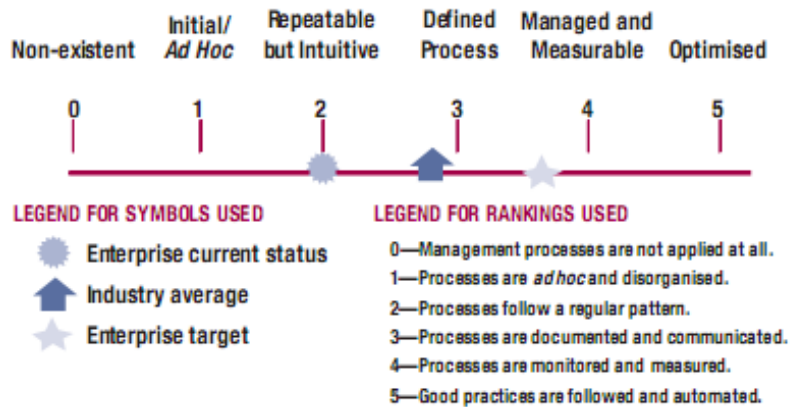


Fig. 12. Cobit 4.1 – Strategie für das Reifegradmodell⁴³

4.2.2 Auswertung

Um die Cobit-Evaluierung bewerten zu können wird abschließend eine Auswertung erstellt, die einerseits Aufschluss über die IST Situation gibt uns sich andererseits mit den Werten befasst, die von den Tools erreicht werden.

Im ersten Schritt werden die Punkte für den IST Stand ermittelt und dargestellt und auf Grund dieser Erkenntnis werden die SOLL Werte erarbeitet. Dazu werden die erreichten Punkte betrachtet, die auf Grund der Cobit-Bewertungsskala für die Sichten erreicht wurden. Die erreichten Punkte werden addiert und in daraus kann eine Reihenfolge der Tools abgeleitet werden. Außerdem kann dadurch gezeigt werden, ob ein Tool die strategische Zielerreichung unterstützen kann und für das Unternehmen als Systemlösung in Frage kommt.

In einem weiteren Schritt werden die Ergebnisse genauer geprüft und mit Hilfe der Varianz betrachtet, daraus kann in weiterer Folge abgelesen werden, ob es eine große Streuung hinsichtlich der einzelnen Werte gibt. Dabei basiert die Berechnung auf den Ausführungen aus [Koh05]⁴⁴, die wie folgt lautet.

$$\sigma^2 = \frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^2$$

Dabei ergibt sich das arithmetische Mittel ($\bar{x}$) durch die allgemein gültige Formel.

⁴³ Vgl. [Gov07] Seite 18

⁴⁴ Vgl. [Koh05] Seite 74

$$\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$$

Mit Hilfe der Bewertung kann der strategische Blickwinkel auf die Toolevaluierung gewährleistet werden und durch die Erkenntnisse der Varianz kann das Ergebnis der Cobit-Evaluierung genauer interpretiert werden.

5 Rahmenbedingungen bei der Austrian Airlines AG

Um die Einflussfaktoren sowie die Anforderungen der Austrian Airlines AG an ein toolgestütztes Internes Kontrollsystem zu erarbeiten, ist es von besonderer Bedeutung, einerseits die gesetzlichen Rahmenbedingungen zu analysieren und andererseits die gewünschten Anforderungen zu definieren. Bei einem Unternehmen wie der Austrian Airlines AG müssen dafür zahlreiche Interessen von Partnern berücksichtigt werden. Darauf wird in diesem Kapitel näher eingegangen und die unterschiedlichen Interessensgruppen werden kurz dargestellt.

Zunächst wird auf die Austrian Airlines AG eingegangen, um das Unternehmen und die Verflechtungen mit Partnern aufzuzeigen, dabei soll ein kurzer geschichtlicher Überblick als Information dienen.

Die Austrian Airlines AG kann bereits auf eine lange Unternehmensgeschichte zurückblicken, die 1957 mit der Gründung begonnen hat. Bereits im darauffolgenden Jahr fand der erste Flug von Wien nach London am 31.03. statt.

In den 70er und 80er Jahren entwickelte sich die Austrian Airlines AG zu einer Fluglinie mit zahlreichen Flugzeugen und laufenden Erweiterungen, wie beispielsweise die Einführung eines elektronischen Reservierungssystems. Am Ende der 80er Jahre wurde die Aktie der Austrian Airlines an der Wiener Börse eingeführt. Im März 1997 wurde eine Beteiligung bei der Lauda Air erworben und im Dezember desselben Jahres wurde dies auch bei der Tyrolean Airways gemacht. Auf eine 100% Beteiligung erhöhte die Austrian Airlines AG bei der Tyrolean Airways kurz darauf am 23.03.1998.

Nach der Jahrtausendwende trat die Austrian Airlines AG der weltumspannenden „Star Allianz“ bei, des Weiteren erwarb die Austrian Airlines AG in den folgenden Jahren die 100%ige Beteiligung an der Rheintalflug und an der Lauda Air.

Am 03.09.2009 wurde die Austrian Airlines AG ein Mitglied des Deutschen Lufthansa-Konzerns, wodurch die Lufthansa-Gruppe zur größten Fluggesellschaft in Europa wurde.

Heutzutage ist die Austrian Airlines AG als eine zuverlässige Fluglinie bekannt, die im Jahr 2010 ein Passagierplus von 9,7%, was eine Passagieranzahl von 10,9 Millionen bedeutet, verbuchen konnte.

5.1 Gesetzliche Rahmenbedingungen

Da die Fluglinie die Rechtsform einer Aktiengesellschaft besitzt, sind das Aktiengesetz (AktG), sowie das Unternehmensgesetzbuch (UGB) für das Interne Kontrollsystem von besonderer Bedeutung.

	<i>Bestehend</i>	<i>Zusätzlich durch das Unternehmensrechtsänderungsgesetz</i>
Vorstand	§82 AktG Der Vorstand hat dafür zu sorgen, dass ein Internes Kontrollsystem geführt wird, das den Anforderungen des Unternehmens entsprechen.	§243a UGB Zu den Aufgaben des Vorstands zählen die Beschreibung der wichtigsten Merkmale des Internen Kontrollsystems und des Risikomanagements im Hinblick auf die Rechnungslegung im Lagebericht.
Aufsichtsrat, Prüfungsausschuss	§96 AktG Der Aufsichtsrat hat den Jahresabschluss und den Lagebericht zu prüfen.	§92 Abs4a AktG Einrichtung eines Prüfungsausschusses bei Unternehmen im öffentlichen Interesse, unter anderem mit der Aufgabe, den Rechnungslegungsprozess, die Wirksamkeit des Internen Kontrollsystems, ggf. der Internen Revision und des Risikomanagements der Gesellschaft zu überwachen.
Abschlussprüfer	§274 Abs1 u §5 UGB Der Abschlussprüfer hat das Ergebnis seiner Prüfung in einem Bestätigungsvermerk zusammenzufassen.	§273 Abs2 UGB Der Abschlussprüfer hat dem Vorstand und dem Aufsichtsrat unverzüglich über wesentliche Schwächen bei der Internen Kontrolle des Rechnungslegungsprozesses zu berichten. §274 Abs5 UGB Der Abschlussprüfer macht im Bestätigungsvermerk eine Aussage, ob die wichtigsten Merkmale eines Internen Kontrollsystems und Risikomanagements im Hinblick auf die Rechnungslegung im

		Lagebericht zutreffend beschrieben sind.
--	--	--

Table 8. gesetzliche Bestimmungen für Aktiengesellschaften in Österreich⁴⁵

5.2 Vorgaben des Konzerns und der Austrian Airlines

Nicht außer Acht zu lassen ist, dass die Austrian Airlines AG durch die Fusion mit dem Deutschen Lufthansa-Konzern auch die Vorschriften anzuwenden hat, die von der Muttergesellschaft vorgegeben werden. Somit sind auch die gesetzlichen Vorschriften aus dem Kapitel 3.2.2 für das Unternehmen nicht zu vernachlässigen, auch wenn diese in einer etwas anderen bzw. abgeschwächten Form anzuwenden sind, wie dies in [Aus10]⁴⁶ aufgezeigt ist.

Darauf aufbauend wurde bereits ein Anforderungskatalog der Deutschen Lufthansa erstellt, der die gesetzlichen Rahmenbedingungen und die konzerninternen Vorstellungen beinhaltet. Die Erstellung des Bewertungsbogens für die Austrian Airlines wurde vom Anforderungen der Deutschen Lufthansa klar beeinflusst und konnten in Kooperation mit Herrn Mag. Michael Kogler erarbeitet und besprochen werden. Weiters wurden in zahlreichen Gesprächen die Wünsche der Austrian Airlines AG erarbeitet und in den Evaluierungsprozess mit eingearbeitet. So konnten nachstehende Anforderungen definiert werden, welche sich auch in der Evaluierung wiederfinden lassen.

- Kompatibel zu Adonis
- HTML basiert
- easy-to-use für Clients
- Kosten
 - Lizenzen
 - Operationale Kosten
 - Customizingkosten
- Customizing
- Integration von Microsoft Standardsoftware
 - MS Exchange Server
 - MS SharePoint Server
 - MS Office
- E-Mailnotifikation für Reminders und Befragungen
- Feedbackschleife bezogen auf Prozess, Risiko und Kontrolle
 - Plan – Do – Check – Act (PDCA Methode) für Prozess, Risiko, Kontrolle
- Prozessfehler vs. Datenfehler („Double Loop Learning“)
- Feedbackfragebogen
- Feedback an Prozessverantwortliche, Prozessexperte, ...
- Revisionierung (für Nachvollziehbarkeit, Dokumentation)

⁴⁵ Vgl. [Aus10] Seite 5

⁴⁶ Vgl. [Aus10] Seite 5

6 Evaluierung ausgewählter Interner Kontrollsysteme

Nachdem die Rahmenbedingungen für die Austrian Airlines AG geklärt wurden und die Anforderungen bereits in ersten Gesprächen erhoben werden konnten, ist eine erste Vorauswahl bei den Toolherstellern zu treffen. Dabei wurden Toolvorschläge von Seiten des Deutschen Lufthansakonzerne sowie auch von der Austrian Airlines AG berücksichtigt. Nachdem eine Einigung erzielt wurde, welche Tools für die Evaluierung herangezogen werden, konnten die Recherchetätigkeit begonnen werden. Um einen ersten Einblick in die Tools zu erhalten, werden diese in dem folgenden Kapitel kurz vorgestellt.

Vorweg möchte ich anmerken, dass sämtliche Toolanbieter von Internen Kontrollsystemen einer einheitlichen Auffassung bezüglich der Wichtigkeit eines durchdachten Internen Kontrollsystems sind, wie dies Luc Brandts [BW10], der Chief Technical Officer bei der Firma B Wise ist, bestätigt. Er meinte, dass es in zahlreichen Unternehmen bereits Risikomanagementmethoden gibt, die jedoch oft auf Basis von Listen wie beispielsweise Excel Spreadsheets realisiert sind. Dies sei jedoch ein falscher Ansatz, da die Organisation bzw. die Realisierung in solchen Listen maximal bei wenigen Listen nur kurze Zeit fehlerfrei funktionieren kann. Darum empfiehlt er den Einsatz eines durchdachten Tools, um die Komplexität einer solchen Methode im Unternehmen zu etablieren.

Die Folge der Tools ist auf Grund der alphabetischen Reihenfolge zustande gekommen und stellt keine Präferenz dar.

6.1.1 Adonis Prozessportal

Das Adonis Prozessportal ist ein Produkt der BOC Information Technologies Consulting GmbH, die 1995 von Univ. Prof. Dr. Dimitris Karagiannis gegründet wurde. Nachdem zu Beginn die Niederlassungen in Wien und Berlin zu finden waren, ist das Unternehmen zum heutigen Zeitpunkt in zahlreichen anderen europäischen Ländern vertreten, darunter fallen beispielsweise Griechenland, Italien, Spanien, Irland oder die Schweiz. Das Unternehmen ist auf Strategie- und Performancemanagement, auf Geschäftsprozess- und Supply Chainmanagement sowie auf IT Management spezialisiert und besteht aus mehr als 150 Mitarbeitern. Dabei umfasst der Kundenstock verschiedenste Unternehmensgrößen, angefangen von multinationalen Konzernen bis hin zu Klein- und Mittelunternehmen in unterschiedlichen Branchen.

Software

Da Adonis als Spin-off der BPMS (Business Process Management Systems) Gruppe der Abteilung Knowledge Engineering der Universität Wien entwickelt wurde, ist es verständlich, dass die Anwendung zahlreiche Funktionalitäten im Bereich der Geschäftsprozessmodellierung zur Verfügung stellt. So kann ein Adonis-Spezialist (z.B. Prozessmodellierer) folgende Anwendungsszenarien laut den Angaben aus [BOC11] abdecken.

- Organisationsentwicklung
- Prozessoptimierung
- Qualitätsmanagement
- Prozess-Performance-Management
- Risikomanagement
- Prozessbasiertes Anweisungswesen
- Prozessbasierte Anwendungsentwicklung
- Fachanalyse für Serviceorientierte Architektur (SOA)
- Prozesskostenrechnung
- Personalbedarfsplanung

Da für eine Vielzahl von Akteuren diese umfangreiche Funktionalität nicht nötig ist und diese auch nicht zur Verfügung stehen soll, wurde das Adonis Prozessportal entwickelt. Durch dieses Portal ist es möglich, dass jede Rolle spezielle Sichten auf die Prozesse hat und somit auch die prozessrelevanten Aufgaben bestmöglich erledigen kann, ohne eine Applikation auf den Rechnern zu installieren, da es sich um ein browserbasiertes System handelt. So ist es dem Adonis Prozessportal möglich, zielgruppengenaue Informationen sowie auch Funktionen zur Verfügung zu stellen. Wie in [BOC111] beschrieben sind typische Funktionen und Szenarien.

- Online-Publikation und Zugriff auf Arbeitsanweisungen, Formulare, etc.
- IKS-Dokumentation, Risikomanagement und Auditierung
- Verbesserungsmanagement / Online-Feedback
- Aufgaben- und Maßnahmenmanagement
- Qualitätssicherung und Freigabe von Prozessen über das Web
- Dezentrale Datenerhebung
- Kennzahlen- / Prozess-Performance-Management
- alle Szenarien, die Zusammenarbeit mehrerer Personen, aktuelle Daten und einen intuitiven, rollenspezifischen Web-Zugang erfordern.

6.1.2 B Wise

Im Jahr 1994 wurde B Wise von zwei Beratern gegründet, wobei Luc Brandts, welcher derzeit den Posten des Chief Technology Officer (CTO) inne hat, einer der beiden war. In den ersten Jahren bot das Unternehmen sämtliche Beratungsleistungen im Bereich Risikomanagement und internes Kontrollwesen an. 1997 wurde von B Wise ein Softwareprodukt entwickelt, das sich als stabiles Compliance-Werkzeug durchsetzte und ein neues Standbein der Firma wurde. Das Unternehmen konnte sich am Weltmarkt mit dieser Compliance- und Risikomanagementlösung derart gut positionieren, dass sich die derzeitigen Standorte in den Niederlanden, den Vereinigten Staaten von Amerika, in Großbritannien, in Indien und in Deutschland befinden. Diese Standorte sind nötig, um die mehr als 300.000 Anwender in über 80 Ländern bestmöglich zu betreuen.

Software

Da das Unternehmen eine Vergangenheit im Bereich der Geschäftsprozesse aufweist, ist es verständlich, dass sämtliche Module auf die Geschäftsprozesse aufsetzen, wie dies in der nachstehenden Abbildung dargestellt ist. Somit kann ein integrierter Ansatz für alle Bereiche des Governance-, Risk- und Compliancemanagements realisiert werden, der zentral verwaltet und gesteuert werden kann.

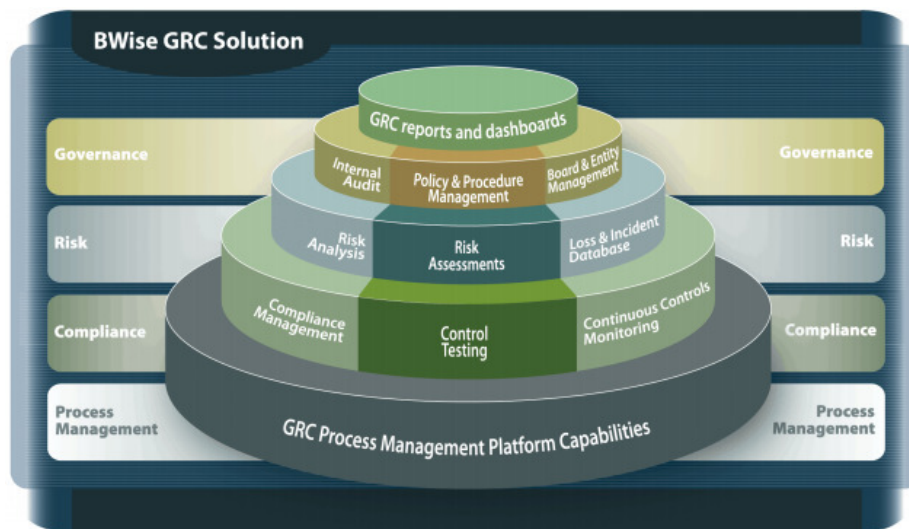


Fig. 13. B Wise Softwarelösung⁴⁷

Um jedoch eine Lösung anbieten zu können, die bei den Anwendern Akzeptanz findet, wurde das international anerkannte COSO Rahmenwerk herangezogen und Anforderungen wie in [BWi101]⁴⁸ erläutert umgesetzt, die wie folgt lauten.

- Finanzielle Berichterstattung (Interne Kontrolle und Revision)
- Compliance (Gesetzgebungen und Richtlinien)
- Operationelles Risikomanagement
- Strategisches Risikomanagement (Grundlage für strategische Entscheidungen)
- Board & Entity Management
- IT Governance (managen von IT Risiken & Vorschriften)
- Prozessmanagement und -monitoring

umgesetzt.

Bei der Entwicklung des Internen Kontrollsystems wurde versucht, den Ansprüchen eines Internen Kontrollsystems gerecht zu werden und darüber hinaus die Erstellung und die Pflege des Systems so einfach wie möglich zu gestalten. Weiters

⁴⁷ Vgl. [BWi101] Seite 4

⁴⁸ Vgl. [BWi101] Seite 4

sollte die Existenz bzw. die Wirksamkeit des Internen Kontrollsystems nachgewiesen werden können.

BWise behauptet von sich, dass es sich durch die einfache Handhabung, die Skalierbarkeit, die Effizienz und die Transparenz gegenüber Mitbewerbern abhebt und dadurch am Markt etabliert.

6.1.3 Oracle GRC

Als Larry Ellison, Bob Miner und Ed Oates im Jahr 1977 eine Firma gründeten, die sich mit der kommerziellen Entwicklung eines relationalen Datenbank Managementsystems (RDBMS) beschäftigte, dachte wohl niemand daran, dass dies der Anfang einer unglaublichen Erfolgsgeschichte sein sollte. Damals wurde Oracle gegründet und seither ist die Assoziation von Datenbanken und Oracle unumgänglich. Neben den Datenbanksystemen entwickelt Oracle, einer der größten Softwarehersteller, auch Unternehmenslösungen, wie die E-Business Suite und Collaboration Suite und versucht sich so im Enterprise Resource Planning- und Groupwarebereich einen Namen zu machen.

Diese weiteren Unternehmenslösungen hat Oracle durch interne Entwicklungen sowie auch durch Übernahmen bewerkstelligen können, darunter fallen beispielsweise die Übernahme von PeopleSoft, Siebel Systems oder auch Sun Microsystems. Durch diese unternehmensinternen Entwicklungen in den letzten Jahren bzw. Jahrzehnten hat sich Oracle zu einem Softwarehersteller mit mehr als 100.000 Mitarbeitern in 145 Ländern entwickelt.

Software

Das Governance, Risk and Compliance Management (GRC) von Oracle stellt eine Komponente der Oracle Fusion Application dar. Diese Applikation bietet wie in [Ora11] gezeigt, folgende Komponenten und kann beliebig zusammengestellt werden.

- Financials
- Human Capital Management
- Procurement
- Customer Relationship Management
- Supply Chain Management
- Project Portfolio Management
- Governance, Risk and Compliance

Mit der GRC Komponente möchte Oracle seinen Kunden eine einheitliche Informationsdarstellung aller GRC Aktivitäten im Unternehmen geben, sowie das Unternehmen bei GRC relevanten Prozessen unterstützen. Weiters kann man sich automatisierte Kontrollen erwarten, die für mehrere Unternehmensanwendungen anwendbar sind.

Durch die Fähigkeiten der Komponente verspricht sich Oracle für die Unternehmen einen Fokus auf Compliance, auf Effizienz und auf eine Wertsteigerung des Unternehmens, welche durch verbesserte Performance erreicht werden soll.

6.1.4 RSA Archer

Das Risikomanagementtool Archer wurde von RSA entwickelt, das seit 2006 eine Tochtergesellschaft von EMC ist. RSA ist ein Unternehmen, das auf IT Sicherheit spezialisiert ist und beispielsweise eine Kryptografie-Programmbibliothek oder ein Authentifizierungssystem entwickelte. Der Hauptsitz des Unternehmens befindet sich in Bedford (Amerika), von wo aus sämtliche Niederlassungen in der Welt, wie beispielsweise China, Deutschland oder auch Russland, geführt werden.

Software

Für die Lösung von RSA Archer wurde eine Plattform entwickelt, die auf vier Teilbereiche von der IT Landschaft bis hin zu gesetzlichen Vorgaben aufgebaut ist. Die Applikation setzt darauf auf und wendet die Governance, Risk und Compliance Lösungen darauf an, somit kann die Software über das ganze Unternehmen gespannt und angewandt werden.



Fig. 14. RSA Archer eGRC Platform⁴⁹

Das Unternehmen verspricht sich, wie in [RSA17] erwähnt, durch die übergreifende Lösung über die IT Landschaft, die Finanzen, die Operationen sowie

⁴⁹ Vgl. [RSA11]

die gesetzlichen Vorgaben eine effiziente Applikation, wobei die Applikation die folgenden Bereiche abdecken kann, wie in [RSA17] erwähnt.

- Policy Management
- Risk Management
- Compliance Management
- Enterprise Management
- Incident Management
- Vendor Management
- Thread Management
- Business Continuity
- Audit Management

Weiters ist das Unternehmen besonders von der Erweiterbarkeit sowie der Anpassbarkeit der Applikation überzeugt, da dafür eine codefreie Realisierung angewandt werden kann.

6.1.5 SAP GRC

SAP ist ein Softwarehersteller für Unternehmenssoftware, der 1972 in Walldorf (Deutschland) gegründet wurde. Heutzutage ist SAP in 120 Ländern vertreten und stellt Lösungen für klein- und mittelständische Unternehmen, sowie umfassende Lösungen für internationale Großunternehmen zu Verfügung.

Neben den Softwarelösungen für beispielsweise die Bereiche der Buchführung, des Einkaufs sowie des Verkaufs stellt SAP ein Modul für ein Risikomanagement bereit. SAP Österreich hat im Mai 2007 die Anwendung SAP GRC Risk Management bei der Kundenkonferenz SAPPHIRE '07 vorgestellt. Mit diesem neuen Modul werden einerseits die Unternehmenssteuerung (Governance), das Risikomanagement (Risk) sowie auch die gesetzlichen Auflagen (Compliance) in der Gesamtstrategie von SAP unterstützt. [SAP07]

Software

Im Zuge der Entwicklung der SAP BusinessObjects GRC-Lösung wurden einerseits branchenübergreifende Anforderungen erarbeitet und umgesetzt, damit eine Vielzahl von Unternehmen die neue Lösung nutzen können. Andererseits hat sich SAP detailliert mit den branchenspezifischen Anforderungen einiger Branchen, wie beispielsweise die Automobilindustrie oder die Bankenbranche, beschäftigt. In diesen Branchen sind spezielle Anforderungen unabdingbar um am Markt bestehen zu können bzw. ernst genommen zu werden, so ist beispielsweise im Bankenbereich die Einhaltung der Basel II Richtlinie, wie in Kapitel 3.3.1, unumgänglich. Die ISO/TS 16949 Norm ist in der Automobilindustrie von besonderer Bedeutung, da ohne nachweisliche Einhaltung dieser Norm ein Zulieferungsunternehmen nicht bei der Angebotslegung berücksichtigt wird.

Unter den branchenübergreifenden Funktionen werden in der SAP BusinessObjects GRC Lösung folgende Punkte geführt, die aus [SAP11] entnommen wurden.

- Risikomanagement
- Überwachung der Funktionstrennung
- Kontrolle der Geschäftsprozesse
- Global Trade
- Umwelt-, Gesundheits- und Arbeitsschutz

7 Vorgehensweise bei der Lösungserarbeitung für die Austrian Airlines AG

Um die praktische Verwendung des Evaluierungsmodells zu zeigen, konnte wie bereits erwähnt mit der Austrian Airlines AG ein Kooperationspartner gefunden werden, der bereit war jene Informationen zur Verfügung zu stellen, die für die Toolauswahl eines Internen Kontrollsystems benötigt werden. Damit sind Anforderungen von Seiten des Gesetzgebers, sowie auf Unternehmens- und Konzernbasis gemeint. Anzumerken ist an dieser Stelle jedoch, dass die Austrian Airlines AG bereits ein funktionierendes Internes Kontrollsystem im Einsatz hat und durch die Evaluierung mögliche Optimierungen aufgedeckt werden sollen.

Die Informationsquellen für die Evaluierungen sind durch die Unterstützung der Toolhersteller sowie zahlreicher Recherchen zustande gekommen. Da mir im Laufe der Evaluierungen nicht sämtliche Informationen zugänglich waren, ist es möglich, dass die Bewertung einiger Kriterien oder Attribute in der Cobit-Reifegradevaluierung das Tool nicht vollständig widerspiegelt. Ich möchte mich trotzdem bei allen Herstellern für die Weitergabe von Informationen bedanken.

Im ersten Schritt wird die allgemeine Evaluierung näher betrachtet, die von der Cobit-Evaluierung gefolgt ist, wobei nach jeder Evaluierung ein Ergebnis erstellt wird.

7.1 Produktspezifische Evaluierung

Im Zuge der produktspezifischen Evaluierung werden die Tools hinsichtlich der angebotenen Funktionalitäten, der technischen Umsetzung und der finanziellen Voraussetzungen beurteilt. Um eine einheitliche Vorgehensweise sicherstellen zu können, wird das erarbeitete Konzept aus Kapitel 4.1 angewandt.

7.1.1 Kriterienkatalog definieren

Da die Austrian Airlines AG, wie bereits erwähnt wurde, zum Deutschen Lufthansakonzern gehört, ist darauf zu achten, dass bei der Einführung eines solchen Systems zahlreiche Interessengruppen zu berücksichtigen sind. Aus diesem Grund gibt der Deutsche Lufthansakonzern für solche Situationen gewisse Richtlinien vor. Es gibt eine Vielzahl an Kriterien, die vom Mutterkonzern vorgegeben werden und bei der Auswahl berücksichtigt werden müssen. Neben den Konzernvorgaben war es natürlich unumgänglich, die gesetzlichen Rahmenbedingungen zu erarbeiten und diese ebenfalls mit in die Evaluierungsphase einzubinden. Ein sehr wichtiger Punkt

war der Kontakt mit Herrn Mag. Michael Kogler von der Austrian Airlines AG, der in zahlreichen Gesprächen die Anforderungen des Unternehmens und der Angestellten mit mir erarbeitet und diskutiert hat.

Die detaillierte Aufstellung der Kriterien und der dazugehörigen Gewichtungen folgt in Kapitel 7.1.2.

Themengebiete und Themenblöcke

Bei den Themengebieten und den Themenblöcken wurde das zuvor definierte Evaluierungsmodell angewandt, daher ergibt sich folgende Struktur, die bereits in Kapitel 4.1.3 dargestellt ist. Die erste Ebene stellt die Themengebiete dar und die zweite Ebene gibt die Themenblöcke wieder. In den genannten Themenblöcken befinden sich die erarbeiteten Kriterien der Evaluierung.

- Funktionaler Aspekt
 - generelle Anforderungen
 - Kundenanforderungen
 - Customizinganforderungen
 - Nachvollziehbarkeits-/Workflowanforderungen
 - Überwachung des Internen Kontrollsystems (Revision)
- Technischer Aspekt
 - Systemplattform
 - Methodikhandbuch
 - Software
 - Sicherheit
 - Sonstiges
 - Systemanforderungen
- Finanzieller Aspekt

7.1.2 Prioritäten & Bewertungsskala definieren

Bevor die Priorität und die Bewertungsskala für die Evaluierung festgelegt werden, wird auf die Bewertungsmethode eingegangen. Dabei wird, wie im Evaluierungsmodell vorgegeben, die Multifaktorenmethode angewandt. Die Bewertungen und Prioritäten für die einzelnen Kriterien werden nach dem Schema des Evaluierungsmodells gewählt, wobei eine genaue Aufschlüsselung der Bewertungskriterien nachstehend für alle Kriterien gegeben wird. Die Aufschlüsselung dient dazu, dass das Ergebnis nachvollzogen werden kann und damit sich der Evaluierer bei der Durchführung an eine Vorgabe halten kann.

Die Festlegung der Gewichtung der Kriterien, sowie bei der Bewertung wurde mit den Verantwortlichen der Austrian Airlines AG diskutiert und abgeklärt. Wie bei einigen Kriterien ersichtlich ist, kann auch die Eventualität auftreten, dass nicht alle fünf Antwortmöglichkeiten benötigt werden, da es eine Entscheidungsfrage mit den Antwortmöglichkeiten ja oder nein gibt, oder dass weniger Antwortmöglichkeiten von Nöten sind. In einem solchen Fall ist es wichtig, dass die Bewertungen klar definiert sind und eingehalten werden.

Funktionale Evaluierung

Für die funktionale Evaluierung wurden bei der Austrian Airlines AG sämtliche Kriterien, die vorgegeben sind wie vorgeschlagen, verwendet und mit einigen weiteren Kriterien ergänzt. Auf den folgenden Seiten sind die Kriterien mit deren Priorität und Bewertungsskala angegeben.

<i>Kriterium</i>	<i>Priorität</i>
generelle Anforderungen	

Benutzer-Rollenkonzept (Berechtigungen, ...)	4
--	---

0	Rollenkonzept wird nicht verwendet
1	
2	Verwendung des Rollenkonzeptes geht aus inoffizieller Quelle (Dokument, Gespräch, ... von Partner etc.) hervor
3	
4	Verwendung des Rollenkonzeptes geht aus offizieller Quelle (Dokument, Gespräch, ...) hervor

Einhaltung von Compliance-Vorgaben (BilMoG, URÄG, RLÄG, ...)	5
--	---

0	Keine Umsetzung der Vorgaben
1	Keine Informationen bezüglich der Umsetzung der Vorgaben
2	Umgesetzte Vorgaben wurden auf Grund von Recherchen erhoben
3	Inoffizielle Dokumentation (von Partnern des Herstellers) der Vorgaben
4	Offizielle Dokumentation der IKS Anforderungen

Integration von Microsoft Standardsoftware - MS Word	5
--	---

0	Keine Integration / Keine Informationen
1	Integration durch Recherchen möglich (unbestätigte Quelle)
2	Integration durch Anpassung / Workaround möglich
3	Integration von Partner des Toolherstellers bestätigt
4	Integration von Toolhersteller bestätigt

Integration von Microsoft Standardsoftware - MS Excel	5
---	---

0	Keine Integration / Keine Informationen
1	Integration durch Recherchen möglich (unbestätigte Quelle)
2	Integration durch Anpassung / Workaround möglich
3	Integration von Partner des Toolherstellers bestätigt
4	Integration von Toolhersteller bestätigt

Integration von Microsoft Standardsoftware - MS Outlook 5

0	Keine Integration / Keine Informationen
1	Integration durch Recherchen möglich (unbestätigte Quelle)
2	Integration durch Anpassung / Workaround möglich
3	Integration von Partner des Toolherstellers bestätigt
4	Integration von Toolhersteller bestätigt

Integration von Microsoft Standardsoftware - MS Exchange 5

0	Keine Integration / Keine Informationen
1	Integration durch Recherchen möglich (unbestätigte Quelle)
2	Integration durch Anpassung / Workaround möglich
3	Integration von Partner des Toolherstellers bestätigt
4	Integration von Toolhersteller bestätigt

Integration von Microsoft Standardsoftware - MS SharePoint 5

0	Keine Integration / Keine Informationen
1	Integration durch Recherchen möglich (unbestätigte Quelle)
2	Integration durch Anpassung / Workaround möglich
3	Integration von Partner des Toolherstellers bestätigt
4	Integration von Toolhersteller bestätigt

Benutzerfreundlichkeit (easy-to-use for Clients) auf Basis von Standards (z.B. ISO Norm 9241) 5

0	Nicht benutzerfreundlich (auf Grund von Foreneinträgen bzw. Bewertungen)
1	Keine Informationen, lediglich gute Eindrücke durch Screenshots
2	Benutzerfreundlichkeit durch gewohnte Umgebung
3	Benutzerfreundlichkeit durch gewohnte nicht überladene Umgebung
4	Benutzerfreundlichkeit auf Basis von einem Standard

Kriterium
Kundenanforderungen

Priorität

Webbrowserbasierter Clientzugang - Internet Explorer 7 5

0	Nicht möglich
1	Keine Informationen
2	-
3	Laut Angaben von Dritten möglich

4	Laut Angaben des Herstellers möglich
---	--------------------------------------

Webbrowserbasierter Clientzugang - Mozilla Firefox 3.5 5

0	Nicht möglich
1	Keine Informationen
2	-
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Kompatibel zu Adonis 5

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Datenübernahme aus operativen Systemen - SAP 3

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Vorhandener Katalog mit Standard-Kontrollen zu SAP 3

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Verlinkung zum Risikomanagement (IKS-Instrument Risiken zuweisen) - Risk to change (Schleupen AG) 3

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Anfügen von Dateien/Links 3

0	Nicht möglich
1	Keine Informationen

2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich ODER in Teilbereichen (Risiko, Kontrolle, ...) möglich
4	Laut Angaben des Herstellers möglich

Event-Management (Reminderfunktion, E-Mailnotifikation) 5

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich bzw. im Workflow integriert

Umfrage-Management 5

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Feedbackschleife im Bezug auf Prozess, Risiko und Kontrolle (Plan - Do - Check - Act) 5

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich. ODER Laut Angaben des Herstellers ist es durch kleine Anpassungen möglich
4	Laut Angaben des Herstellers automatisch möglich

Möglichkeit zur zentralen Benennung der Steuerungs- / Überwachungsinstrumente 3

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

*Kriterium**Priorität***Customizinganforderungen**

Konfigurierbarkeit und Anpassungsmöglichkeiten

5

0	Nicht möglich
1	Keine Informationen
2	Anpassungen werden ausschließlich vom Hersteller vorgenommen
3	Laut Dritten können alle Anpassungen vom Kunden erledigt werden ODER Laut Angaben des Herstellers können zahlreiche Anpassungen vom Kunden erledigt werden.
4	Laut Angaben des Herstellers können alle Anpassungen vom Kunden erledigt werden

Individuell gestaltbare Auswertungen

5

0	Nicht möglich
1	Keine Informationen
2	Auswertungsanpassungen werden ausschließlich vom Hersteller vorgenommen
3	Laut Dritten können alle Auswertungsanpassungen vom Kunden erledigt werden ODER Laut Angaben des Herstellers können zahlreiche Auswertungsanpassungen vom Kunden erledigt werden
4	Laut Angaben des Herstellers können alle Auswertungsanpassungen vom Kunden erledigt werden

Zusätzliche Kontrollen (benutzerdefinierte, konzerninterne Kontrollen)

5

0	Nicht möglich
1	Keine Informationen
2	Zusätzliche Kontrollen werden ausschließlich vom Hersteller erstellt
3	Laut Dritten können zusätzliche Kontrollen vom Kunden erstellt werden
4	Laut Angaben des Herstellers können zusätzliche Kontrollen vom Kunden erstellt werden

Einbindungsmöglichkeit weiterer Attribute (Anforderungsart, Instrumenttyp)

5

0	Nicht möglich
1	Keine Informationen
2	Weitere Attribute werden ausschließlich vom Hersteller

	miteingebunden
3	Laut Dritten können weitere Attribute vom Kunden eingebunden werden
4	Laut Angaben des Herstellers können weitere Attribute vom Kunden eingebunden werden

Kriterium

Priorität

Nachvollziehbarkeits-/Workflowanforderungen

Protokollierung (Sicherstellung der Nachvollziehbarkeit)

5

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround (eigene Protokollierung) möglich
3	Laut Angaben von Dritten wird mitprotokolliert
4	Laut Angaben des Herstellers wird mitprotokolliert

Historisierung der Kontrollergebnisse

5

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround (etwa durch eigene Historisierung in der Datenbank) möglich
3	Laut Angaben von Dritten realisiert
4	Laut Angaben des Herstellers realisiert

Durchführbarkeit von Self Assessment

3

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Möglichkeit zur Kommentierung/Nachverfolgung bei Grenzwertüberschreitungen

3

0	Kommentierung ist nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround ist die Kommentierung möglich
3	Laut Angaben von Dritten ist die Kommentierung möglich
4	Laut Angaben des Herstellers ist die Kommentierung möglich

Workflow zur Erfassung/Bearbeitung/Bestätigung von Steuerungs-/Überwachungsinstrumenten 5

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich ODER Laut Angaben des Herstellers teilweise enthalten (maximal ein Workflowschritt, beispielsweise Erfassung, darf fehlen)
4	Laut Angaben des Herstellers enthalten

Automatische Nachverfolgung von Prüfungsfeststellungen (Workflow) 4

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Automatisierte Kontrollen von Grenzwertüberschreitungen anhand hinterlegter Regeln aus den importierten Daten 3

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Kriterium

Priorität

Überwachung des Internen Kontrollsystems (Revision)

Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor 2

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Erfassen der Wirksamkeitsprüfung der Steuerungs- 2
/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch
Auditor offline (optional)

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Prüfungsplanung zur Wirksamkeit der Steuerungs- 2
/Überwachungsinstrumente

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Übersicht zu Stand der Aktualisierung des IKS 2

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Übersicht der Ergebnisse der Wirksamkeitsprüfung 2

0	Nicht möglich
1	Keine Informationen
2	Durch Anpassungen / Workaround möglich
3	Laut Angaben von Dritten möglich
4	Laut Angaben des Herstellers möglich

Technische Evaluierung

In diesem Abschnitt werden die Kriterien der technischen Evaluierung vorgestellt, wobei diese in den Themenblöcken wiedergegeben werden und mit deren Priorität versehen dargestellt werden.

*Kriterium**Priorität***Systemplattform**

IT Infrastruktur Server - Windows Server 2003

5

0	Nicht möglich
1	Keine Informationen
2	-
3	Laut Angaben von Dritten wird diese Version unterstützt
4	Laut Angaben des Herstellers wird diese Version unterstützt

IT Infrastruktur Server - Windows Server 2008

5

0	Nicht möglich
1	Keine Informationen
2	-
3	Laut Angaben von Dritten wird diese Version unterstützt
4	Laut Angaben des Herstellers wird diese Version unterstützt

IT Infrastruktur Server - Microsoft SQL Server 2005

5

0	Nicht möglich
1	Keine Informationen
2	-
3	Laut Angaben von Dritten wird diese Version unterstützt
4	Laut Angaben des Herstellers wird diese Version unterstützt

IT Infrastruktur Client - Windows XP

5

0	Nicht möglich
1	Keine Informationen
2	-
3	Laut Angaben von Dritten wird diese Version unterstützt
4	Laut Angaben des Herstellers wird diese Version unterstützt

IT Infrastruktur Client - Windows 7

5

0	Nicht möglich
1	Keine Informationen
2	-
3	Laut Angaben von Dritten wird diese Version unterstützt

4	Laut Angaben des Herstellers wird diese Version unterstützt
---	---

IT Infrastruktur Client - Microsoft Office 2003 5

0	Nicht möglich
1	Keine Informationen
2	-
3	Laut Angaben von Dritten wird diese Version unterstützt
4	Laut Angaben des Herstellers wird diese Version unterstützt

IT Infrastruktur Client - Microsoft Office 2010 5

0	Nicht möglich
1	Keine Informationen
2	-
3	Laut Angaben von Dritten wird diese Version unterstützt
4	Laut Angaben des Herstellers wird diese Version unterstützt

Kriterium

Priorität

Methodikhandbuch

Quickinfo 4

0	Es wird keine Dokumentation zur Verfügung gestellt
1	Keine Informationen
2	-
3	Es wird eine allgemeine Dokumentation zur Verfügung gestellt
4	Es wird neben weiteren Dokumentationen vom Hersteller eine Quickinfo für die Benutzer zur Verfügung gestellt

Benutzerfreundlichkeit des Methodikbuches 4

0	Kein Methodikbuch vorhanden
1	
2	Umfangreiche Dokumentation, welche nicht für den schnellen Einsatz genutzt werden kann
3	
4	Geringer Umfang mit allen essentiellen Informationen, welche leicht verständlich sind

**Kriterium
Software***Priorität*

Einführungsaufwand

3

0	Keine Informationen bzw. länger als 30 Arbeitstage
1	Zwischen 16 und 30 Arbeitstagen
2	Zwischen 11 und 15 Arbeitstagen
3	Zwischen 6 und 10 Arbeitstagen
4	Weniger als 5 Arbeitstage

Skalierbarkeit

4

0	Keine Informationen bzw. nicht möglich
1	
2	
3	
4	Skalierbarkeit ist gegeben

Concurrent-Lizenzmodell

5

0	Keine Informationen bzw. nicht möglich
1	
2	Lizenzkombination mit Named-User-Lizenzmodell
3	
4	Concurrent-Lizenzmodell möglich

Das eben genannte Kriterium (Concurrent-Lizenzmodell) wird nicht als KO Kriterium behandelt, obwohl es mit der Priorität von 5 eingestuft wurde. Der Rückstand durch 0 Punkte wird das Tool nach hinten fallen lassen und somit die Möglichkeit einer guten Bewertung verringern.

LDAP Schnittstelle bezüglich Autorisierung

3

0	Nicht möglich
1	Keine Informationen
2	Schnittstelle kann durch Anpassung / Workaround erstellt werden
3	Schnittstelle ist laut Dritter gegeben
4	Schnittstelle ist laut Hersteller gegeben

Kriterium
Sicherheit

Priorität

Datensicherheit (Verschlüsselung)

5

0	Nicht möglich
1	Keine Informationen
2	Kann durch Anpassung / Workaround (innerhalb der Datenbank oder des Filesystems) gewährleistet werden
3	Ist laut Dritter gegeben
4	Ist laut Hersteller gegeben

Datensicherung (Gesamtspiegelung)

5

0	Nicht möglich
1	Keine Informationen
2	
3	Ist laut Dritter gegeben
4	Ist laut Hersteller möglich und es werden die Sicherungskonzepte des Unternehmens unterstützt

Zugriffsbeschränkung

5

0	Nicht möglich
1	Keine Informationen
2	
3	Ist laut Dritter gegeben
4	Ist laut Hersteller gegeben

Kriterium
Sonstiges

Priorität

Support im geographischen Sinn

3

0	Keine Information
1	Niederlassung in Europa
2	Servicepartner in Österreich
3	Niederlassung in Österreich
4	Niederlassung in Wien

Helpdesk (Telefon, Webbasiert)

3

0	Keinen Supportkanal
1	Einen Supportkanal
2	Zwei Supportkanäle
3	Drei Supportkanäle

4	Vier Supportkanäle
---	--------------------

Hierbei wird untersucht, wie viele Supportwege der Hersteller zur Verfügung stellt. Da vier Kanäle untersucht werden, erhält jedes Tool so viele Bewertungspunkte wie es Kanäle anbietet, so kann eine Bewertung zwischen 0 und 4 Punkten liegen. Nachstehend ist die Auswertung für die Tools aufgezeigt, da dies im Evaluierungsbogen nicht nachvollziehbar ist.

<i>Tool</i>	<i>Call Center</i>	<i>Webbasierte Anfragen</i>	<i>Online Chat</i>	<i>Foren & Informationsaustausch</i>
Adonis	X	X		
BWise	X	X		X
Oracle GRC	X	X	X	X
RSA Archer	X	X		X
SAP GRC	X	X	X	X

Durchschnittliche Antwortzeit

3

0	Sehr langsam (länger als 7 Werkzeuge)
1	Keine Information
2	Langsam (innerhalb von 7 Werktagen)
3	Schnell (max. 3 Werkzeuge)
4	Sehr schnell (innerhalb eines Werktags)

Für die Bewertung dieses Kriteriums werden auch die Antwortzeiten auf die Anfragen bei der Informationsbeschaffung berücksichtigt.

Wartungsvertrag

4

0	Nicht möglich
1	Keine Informationen
2	Ist laut Dritter möglich
3	Ist laut Hersteller möglich
4	Ist laut Hersteller bei der Anschaffung integriert

Kriterium

Priorität

Systemanforderungen

Minimale Systemanforderungen

3

0	Übersteigen die Systemvoraussetzungen des Unternehmens erheblich
1	
2	Sind mit den gegebenen Systemvoraussetzungen im Unternehmen durch leichte Anpassungen abgedeckt
3	

4	Sind mit den gegebenen Systemvoraussetzungen im Unternehmen abgedeckt
---	---

Finanzielle Evaluierung

Da die finanziellen Evaluierung nur wenige Kriterien beinhaltet und durch die Anforderungen der Austrian Airlines AG nur ein zusätzliches Kriterium hinzugekommen ist, wird es auch in diesem Beispiel keine Unterteilung in Themengebiete geben.

Kriterium

Priorität

Anschaffungskosten

5

0	> € 100.000,-
1	€ 75.001,- – € 100.000,-
2	€ 50.001,- – € 75.000,-
3	€ 25.001,- – € 50.000,-
4	€ 0,- – € 25.000,-

Betriebskosten

3

0	> € 16.000,-
1	€ 12.001,- – € 16.000,-
2	€ 8.001,- – € 12.000,-
3	€ 4.001,- – € 8.000,-
4	€ 0,- – € 4.000,-

Wartungskosten

3

0	> € 20.000,-
1	€ 15.001 - € 20. 00,-
2	€ 9.001 - € 15.000,-
3	€ 4.001 - € 9.000,-
4	€ 0 - € 4.000,-

Customizingkosten pro Tag

4

0	> € 3.000 -
1	Keine Informationen bzw. projektbezogen
2	€ 2.001,- – € 3.000,-
3	€ 1.001,- – € 2.000,-
4	€ 0,- – € 1.000,-

KO Kriterien

Als KO Kriterium wurde von der Austrian Airlines AG vorgegeben, dass sämtliche Kriterien darunter fallen, welche die Höchstpriorität von fünf Punkten haben und eine Bewertung, die kleiner als 2 ist. Wenn dies eintritt, so ist das Tool für den weiteren Evaluierungsprozess nicht mehr relevant. Dies wird somit wie in Kapitel 4.1.2 gehandhabt.

7.1.3 Gewichtung der Themengebiete und Themenblöcke

Bei der Gewichtung der Themengebiete und der Themenblöcke wurde nach Rücksprache mit Herrn Mag. Michael Koegler von der Austrian Airlines AG die Wichtigkeit der einzelnen Bereiche ausgearbeitet. In den folgenden Kapiteln werden die detaillierten Gewichtungen aufgezeigt. Des Weiteren werden für die normierten Bewertungen der einzelnen Themenblöcke fiktive Bewertungsangaben angeführt, um die Bewertung inklusiver Gewichtung zu verdeutlichen.

Gewichtung der Themenblöcke

Bei der Gewichtung der Themenblöcke werden alle Themenblöcke eines Themengebiets betrachtet und auf Grund der Bedeutung für die Austrian Airlines AG gewichtet. Die Gewichtung wird auf Grund von prozentueller Aufteilung vorgenommen. In Summe müssen die Gewichtungswerte 100 Prozent ergeben, da ansonsten die Berechnung nicht gültig ist.

Bei der funktionalen Evaluierung werden die fünf Themenblöcke wie folgt gewertet.

funktionale Evaluierung			
Evaluierungsbeginn			
Evaluierungsende			
Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
generelle Anforderungen	70,00%	20%	14,00%
Kundenanforderungen	70,00%	20%	14,00%
Customizinganforderungen	70,00%	10%	7,00%
Nachvollziehbarkeits-/Workflowanforderungen	70,00%	20%	14,00%
Überwachung des Internen Kontrollsystems (Rev	70,00%	30%	21,00%
		100%	70,00%

Fig. 15. Gewichtung der funktionalen Themenblöcke

Die technische Evaluierung setzt sich wie bereits in Kapitel 7.1.1 erwähnt aus sechs Themenblöcken zusammen, die wie folgt gewichtet werden.

technisch Evaluierung			
Evaluierungsbeginn			
Evaluierungsende			
Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
Systemplattform	75,00%	20%	15,00%
Methodikhandbuch	75,00%	11%	8,25%
Software	75,00%	22%	16,50%
Sicherheit	75,00%	10%	7,50%
Sonstiges	75,00%	17%	12,75%
Systemanforderungen	75,00%	20%	15,00%
		100%	75,00%

Fig. 16. Gewichtung der technischen Themenblöcke

Da bei der finanziellen Evaluierung alle Kriterien in einem Themenblock gesammelt sind, wird dieser wie nachstehend dargestellt mit 100 Prozent gewichtet.

finanzielle Evaluierung			
Evaluierungsbeginn			
Evaluierungsende			
Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
Kosten	80,00%	100%	80,00%
		100%	80,00%

Fig. 17. Gewichtung der finanziellen Themenblöcke

Gewichtung der Themengebiete

Bei der Gewichtung der Themengebiete werden die einzelnen Evaluierungsschritte mit einer Wertigkeit, die mit der Austrian Airlines AG definiert wurde, belegt. Hier ist darauf zu achten, dass die Summe wieder 100 Prozent ergeben muss, da ansonsten kein Ergebnis im Microsoft Excel Sheet dargestellt wird und die Berechnung ungültig ist.

Bei der Austrian Airlines AG wurden sämtlich Themengebiete für gleich wichtig eingestuft, daher beträgt die Gewichtung für alle Evaluierungen 33,3° Prozent

Gesamtbewertung	Bewertung	Blockgewichtung in %	Bewertung nach der Eval.gewichtung
funktionale Evaluierung	70,00%	33,3%	23,33%
technische Evaluierung	75,00%	33,3%	25,00%
finanzielle Evaluierung	80,00%	33,3%	26,67%
		100%	75,00%

Fig. 18. Gewichtung der Themengebiete

7.1.4 Evaluierungsschritte

Bevor nun die Evaluierung der einzelnen Themengebiete beginnt ist noch die Reihenfolge für die Evaluierungsschritte festzulegen. Die Reihenfolge wurde wie folgt festgelegt und für alle Tools strikt eingehalten.

1. Funktionale Evaluierung
2. Technische Evaluierung
3. Finanzielle Evaluierung

Nachdem alle Rahmenbedingungen und Definitionen abgeklärt sind, kann die Evaluierung beginnen. Nachfolgend werden die einzelnen Ergebnisse der Evaluierungsschritte vorgestellt.

Die Bewertung der einzelnen Evaluierungen kann im Anhang in den beigelegten Evaluierungsbögen nachgeschlagen werden. Eine genauere Betrachtung der Evaluierungsbögen kann auf der beigelegten Compact Disc (CD) eingesehen werden. Darin sind auch detaillierte Verweise auf die Informationsherkunft enthalten. In den folgenden Kapiteln wird lediglich auf die Ergebnisse der einzelnen Schritte eingegangen.

Funktionale Evaluierung

Bei der funktionalen Evaluierung konnten durch die Bank alle Tools überzeugen, wobei bereits in diesem Schritt deutlich wurde, dass es bei manchen Tools schwer ist, zu brauchbaren Informationen zu kommen, um die Kriterien bewerten zu können. Für diesen Evaluierungsschritt wurden zahlreiche Dokumentationen durchgearbeitet sowie Informationen von den Toolherstellern eingeholt.

Die Ergebnisse dieses Evaluierungsschritts lauten für die Tools wie in der nachstehenden Tabelle aufgezeigt.

<i>Tool</i>	<i>Funktionale Evaluierung</i>
Adonis Prozessportal	85,52%
BWise	79,99%
Oracle GRC	74,59%
RSA Archer	61,82%
SAP GRC	85,39%

Table 9. Ergebnis der funktionalen Evaluierung

Technische Evaluierung

Bei der technischen Evaluierung konnten zahlreiche Antworten ebenfalls aus dem Informationsmaterial, das von den Toolherstellern zur Verfügung gestellt wurde, entnommen werden. Einige Bewertungen für die Kriterien konnten jedoch nur durch eine detaillierte Abklärung per E-Mail, in einem persönlichen Gespräch oder mit Hilfe eines Telefonats geklärt werden.

In der nachstehenden Tabelle ist das Ergebnis des Evaluierungsschritts dargestellt, wobei auffällt, dass RSA Archer nur eine Bewertung von 36,65% erreicht.

<i>Tool</i>	<i>Technische Evaluierung</i>
Adonis Prozessportal	87,50%
BWise	88,74%
Oracle GRC	82,38%
RSA Archer	36,56%
SAP GRC	76,51%

Table 10. Ergebnis der technischen Evaluierung

Da es trotz mehrmaliger Kontaktversucht mit RSA Archer leider nicht funktioniert hat, spezifischeres Informationsmaterial zu erhalten, konnten zahlreiche Punkte in diesem Evaluierungsschritt nicht beantwortet oder sehr schlecht bewertet werden. Daraufhin wurde RSA Archer aus der Evaluierung herausgenommen, da mit den vorhandenen Informationen keine aussagekräftige und dem Tool entsprechende Evaluierung bewerkstelligt werden kann. Außerdem konnten einige KO Kriterien die geforderte Bewertung nicht erreichen und so musste das Tool aus der Evaluierung ausscheiden.

Finanzielle Evaluierung

Da finanzielle Informationen von den Herstellern in offiziellen Aussendungen nicht angegeben werden, konnte dieser Teil der Evaluierung auf Grund der Informationen nach den Anfragen bei den vier übrig gebliebenen Herstellern, beantwortet werden.

<i>Tool</i>	<i>Finanzielle Evaluierung</i>
Adonis Prozessportal	80,00%
BWise	81,67%
Oracle GRC	48,33%
RSA Archer	-
SAP GRC	40,00%

Table 11. Ergebnis der finanziellen Evaluierung

Grundsätzlich ist bei dieser Evaluierung anzumerken, dass sich die großen Softwarehersteller preislich in einem anderen Segment befinden als das Adonis Prozessportal und die Lösung von BWise. Die beiden letztgenannten sind in diesem Bereich beinahe ident.

7.1.5 Auswertung

Bei der Betrachtung der Gesamtbewertung werden alle Evaluierungen zusammengefasst und wie bereits im Kapitel 4.1.5 aufgezeigt, speziell nach den Anforderungen der Austrian Airlines AG bewertet.

Bei der Bewertung ergibt sich folgendes Ergebnis, welches in der nachstehenden Tabelle gezeigt ist. Dabei ist ersichtlich, dass das Adonis Prozessportal und BWise Kopf an Kopf an der Spitze liegen.

<i>Tool</i>	<i>gesamte Evaluierung</i>
Adonis Prozessportal	84,34%
BWise	83,47%
Oracle GRC	71,01%
RSA Archer	-
SAP GRC	67,30%

Table 12. Ergebnis der produktspezifischen Evaluierung

Um die Erkenntnisse aus der produktspezifischen Evaluierung in grafischer Form aufzubereiten, werden die Ergebnisse in der nachstehenden Abbildung dargestellt, wobei die drei Evaluierungsbereiche des Tools aufeinander gesetzt werden und das Endergebnis der produktspezifischen Evaluierung aufgezeigt wird.

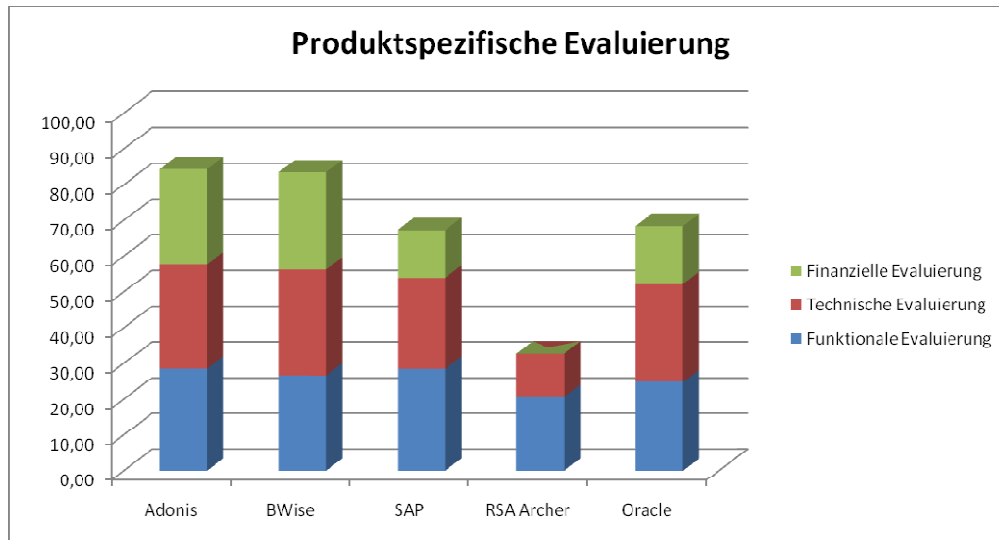


Fig. 19. Ergebnis der produktspezifischen Evaluierung

Auf Grund der produktspezifischen Evaluierung kann für die Entscheidungsfindung bei der Austrian Airlines AG eine Empfehlung für das Adonis Prozessportal abgegeben werden. Eine Begründung für diese Entscheidung wird im folgenden Kapitel 7.3.2 gegeben.

7.2 COBIT-Evaluierung

Neben der allgemeinen Toolevaluierung, die in Kapitel 7.1 in einer Auswertung endete wird ebenfalls die Möglichkeit angewandt, die Evaluierung um einen Aspekt zu erweitern. Dazu wird wie bereits in Kapitel 4.2 erwähnt Cobit angewandt. Einerseits soll dadurch der Nutzen durch die Technologieverwendung aufgezeigt werden und untersucht werden, ob die Tools die Zielerreichung unterstützen kann.

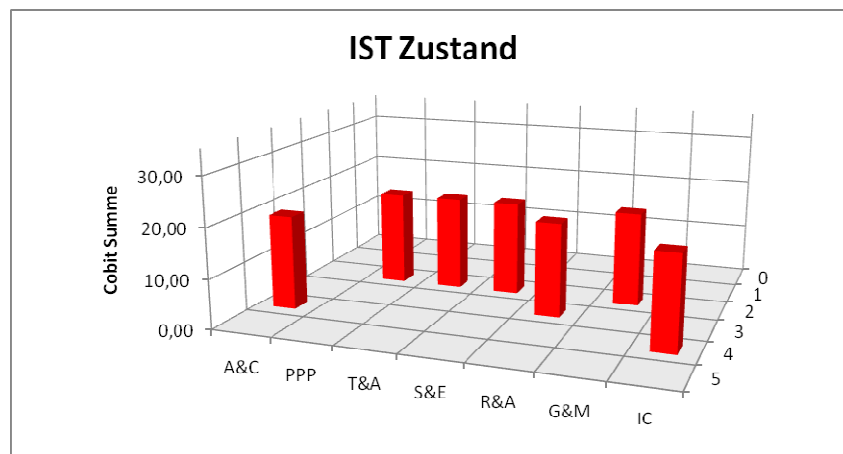
Eingangs wird die bestehende Umgebung beleuchtet und anhand der Cobitvorgaben bewertet. Danach wird eine SOLL Situation dargestellt, die in Kooperation mit der Austrian Airlines AG erarbeitet wurde. In einem weiteren Schritt werden die Tools betrachtet, ob diese die geforderten Reifegrade erreichen und somit das Unternehmen bei der Erreichung der Ziele unterstützen kann.

Bei der Betrachtung des IST Zustand hat sich ergeben, dass ein Wert von 19 von 35 möglichen Punkten erreicht wird. Dieser setzt sich wie folgt zusammen.

Maturity Attribute Table (Cobit 4.1)						Internal Control	
	Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement	Maturity Model for Internal Control
0							
1							
2		X	X	X		X	
3					X		
4	X						X
5							

Table 13. Cobit Auswertung – IST Zustand

Nachdem die tabellarische Darstellung angibt in welchem Reifegrad sich der IST Zustand für bestimmte Attribute der Reife befinden, wird in der folgenden Grafik auf der x- und y- Achse dieselbe Einheit aufgetragen. Zusätzlich wird auf der z-Achse die Summe der Cobit Evaluierung angegeben, die wie erwähnt beim IST Zustand bei 19 liegt.

**Fig. 20.** Cobit Auswertung – IST Zustand

Durch die oben angeführte Darstellung kann erkannt werden, dass die Attribute unterschiedliche Reifegrade aufweisen, es lässt sich auch erkennen, in welchen Bereichen Optimierungspotential besteht. Eine hohe Varianz von 0,78 unterstreicht den Eindruck einer großen Streuung der Werte für die einzelnen Bereiche.

Aus diesem Grund wird ein Sollwert für jeden Bereich definiert, der in Zukunft durch ein neues System, sowie auch durch Optimierungen innerhalb des Unternehmens erreicht werden soll und für die Tools einen Richtwert darstellt.

	Maturity Attribute Table (Cobit 4.1)						Internal Control
	Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement	Maturity Model for Internal Control
0							
1							
2							
3							
4	X	X	X	X	X	X	
5							X

Table 14. Cobit Auswertung – SOLL Zustand

Dieser angestrebte Wert liegt bei 29 Punkten, wobei die meisten Bereiche den Reifegrad 4 erreichen sollen. Dies bedeutet, dass in einigen Bereichen eine enorme Steigerung erreicht werden soll. Eine derartige Verbesserung bedarf wie bereits erwähnt einer durchdachten Systemlösung, welche die Erreichung der Ziele unterstützen kann.

7.2.1 Auswertung

Der Cobit Auswertung stellen sich nach der praktischen Softwareevaluierung jene vier Tools, welche die Evaluierungsschritte mit einem positiven Ergebnis abgeschlossen haben.

Eingangs dieser Evaluierung ist anzumerken, dass es Teilbereiche gibt, die nicht ausschließlich vom Tool abhängig sind, sondern von den Gegebenheiten im Unternehmen beeinflusst werden. Es wird untersucht, ob ein Tool in der Lage ist ein vorgegebenes strategisches Unternehmensziel zu erreichen und in welchem Ausmaß dies von dem Tool unterstützt wird.

Adonis Prozessportal

Das Adonis Prozessportal kann in allen belangen den SOLL Zustand erreichen und erreicht in Summe eine Cobit Bewertung von 32 Punkten, womit das beste Ergebnis in der Cobit-Evaluierung erreicht werden konnte. Außerdem ist anzumerken, dass lediglich eine Varianz von 0,24 bei dieser Bewertung auftritt.

Maturity Attribute Table (Cobit 4.1)						Internal Control	
	Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement	Maturity Model for Internal Control
0							
1							
2							
3							
4	X			X	X		
5		X	X			X	X

Table 15. Cobit Auswertung – Adonis

In Verbindung mit den erreichten Punkten hinsichtlich der Cobit-Evaluierung kann folgende grafische Aufbereitung für das Adonis Prozessportal erstellt werden. Diese Grafik kann mit jener des IST Zustands verglichen werden und zeigt die Verbesserungen deutlich auf. Für die folgenden Tools wird auf eine derartige grafische Aufbereitung verzichtet, da die Abbildung lediglich eine Erweiterung der angegebenen Auswertungstabelle ist.

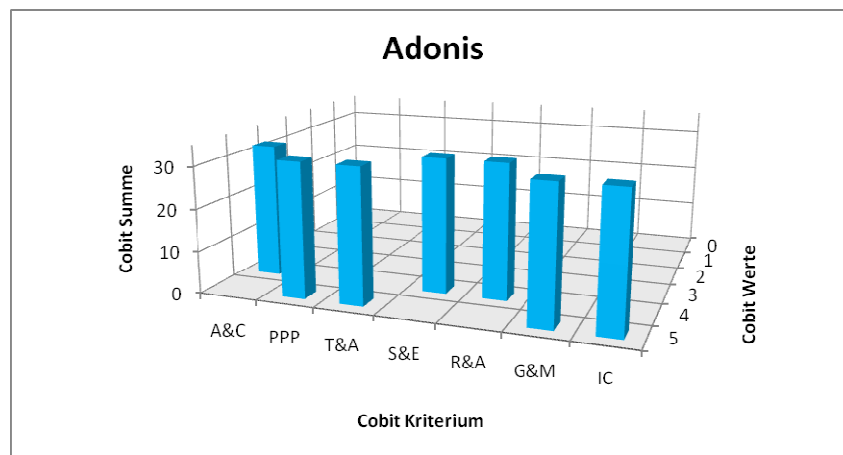


Fig. 21. Cobit Auswertung – Adonis

BWise

Die BWise Lösung kann in den meisten Bereichen die Anforderungen erreichen, die als SOLL Werte definiert wurden, lediglich in einem Bereich besteht Verbesserungspotential, wodurch sich ein Evaluierungsergebnis von 29 Punkten (Varianz: 0,41) ergibt. Jedoch deutet die hohe Varianz auf eine sehr große Schwankung der einzelnen Bewertungen hin.

	Maturity Attribute Table (Cobit 4.1)						Internal Control
	Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement	Maturity Model for Internal Control
0							
1							
2							
3		X					
4	X		X	X	X		
5						X	X

Table 16. Cobit Auswertung – B Wise

Oracle

Oracle zeigt in den Bereichen Tools and Automation und Skills and Expertise, dass die Bereiche definiert sind, jedoch kein umfangreiches Management und keine durchdachte Messbarkeit für die Bereiche besteht. Aus diesem Grund gibt es eine Bewertung von drei Punkten für die beiden Bereiche, was in Summe eine Bewertung von 29 Punkten (Varianz: 0,12) bringt.

	Maturity Attribute Table (Cobit 4.1)						Internal Control
	Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement	Maturity Model for Internal Control
0							
1							
2							
3							
4	X	X	X	X	X	X	
5							X

Table 17. Cobit Auswertung – Oracle

SAP

Die Evaluierung des SAP Systems hat gezeigt, dass alle Bereiche einen sehr hohen Reifegrad aufweisen und durchwegs mit vier Punkten bewertet werden können. Somit erreicht das System sämtliche SOLL Vorgaben und kann aus diesem Grund auch eine sehr gute Bewertung in diesem Bereich erreichen. Mit 30 Punkten (Varianz: 0,2) findet sich das SAP System im vordersten Bereich der Auswertung.

	Maturity Attribute Table (Cobit 4.1)						Internal Control
	Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement	Maturity Model for Internal Control
0							
1							
2							
3							
4	X	X		X	X	X	
5			X				X

Table 18. Cobit Auswertung – SAP

Bei der Betrachtung der Ergebnisse der Cobit-Evaluierung kann festgestellt werden, dass das Adonis Prozessportal die meisten Punkte erreicht. SAP liegt knapp dahinter und unmittelbar danach liegen B Wise und Oracle.

In Summe ist anzumerken, dass alle Tools die SOLL Vorgaben weitestgehend unterstützt und im Vergleich zum IST Stand eine optimierte Lösung darstellen.

Auch in diesem Bereich kann angegeben werden, dass Adonis eine sehr gute Lösung anbietet, jedoch liegen die Ergebnisse sehr knapp beisammen. Außerdem erfüllen alle Tools großteils die Vorgaben hinsichtlich des Reifegrades, sodass alle Tools mit einem sehr guten Ergebnis abschneiden.

<i>Tool</i>	<i>Cobit-Evaluierung</i>	<i>Varianz</i>
Adonis Prozessportal	32	0,24
B Wise	29	0,41
Oracle GRC	29	0,12
RSA Archer	0	0,00
SAP GRC	30	0,20

Table 19. Ergebnis der Cobit-Evaluierung

In grafischer Form können die erreichten Wertungen für die einzelnen Cobit Kriterien, die auch der x-Achse aufgetragen sind, für die Tools und den IST Zustand (z-Achse) wie folgt aufgezeigt werden.

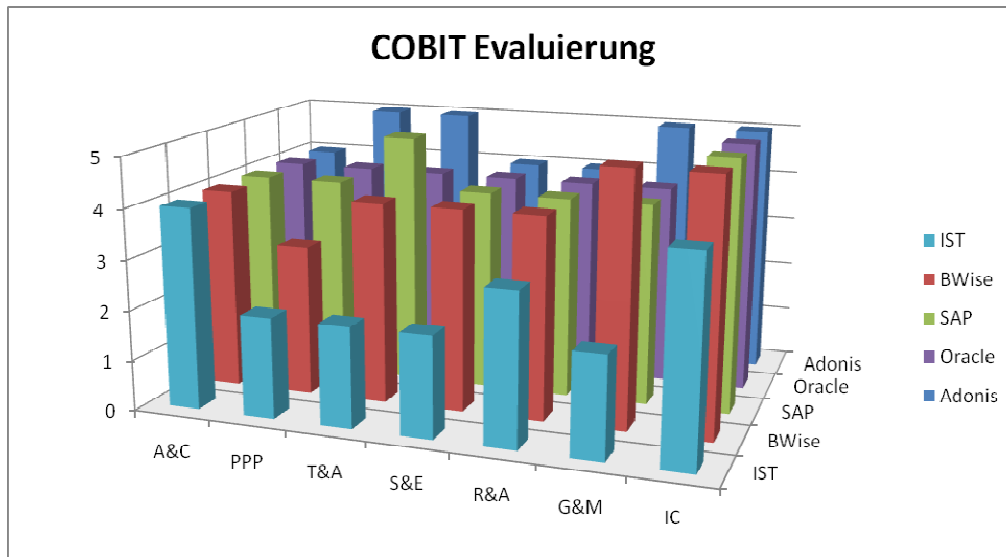


Fig. 22. Vergleich der Cobit-Evaluierungen

Die Abkürzungen in der obigen Darstellung beziehen sich auf die Cobit Sichten und haben folgende Bedeutung.

A&C	Awareness and Communication
PPP	Policies, Plans and Procedures
T&A	Tools and Automation
S&E	Skills and Expertise
R&A	Responsibility and Accountability
G&M	Goal Setting and Measurement
IC	Maturity Model for Internal Control

7.3 Evaluierungsergebnis

Nachdem beide Evaluierungen abgeschlossen sind, sollen in erster Instanz beide Ergebnisse getrennt voneinander betrachtet werden und auf Grund der Erkenntnisse eine Entscheidung getroffen werden.

In einem weiteren Schritt wird versucht die beiden Ergebnisse in diesem Kapitel zusammenzuführen und aufzubereiten um eine weiter Entscheidungshilfe zu geben.

Abschließend wird betrachtet ob die Vorgehensweise bei der Evaluierung optimiert werden kann bzw. welche Feststellungen sich im Laufe der Evaluierung entwickelt haben.

7.3.1 Gesamtauswertung

Wenn man beide Evaluierungsergebnisse unabhängig voneinander betrachtet, kann festgestellt werden, dass in beiden Fällen das Adonis Prozessportal sehr gut abschneidet. Einerseits kann dieses System in der produktspezifischen Evaluierung den besten Wert erreichen, andererseits überzeugt das Tool auch hinsichtlich der strategischen Dimension, die durch die Cobit-Evaluierung dargestellt wird. Dahinter reiht sich die B Wise Lösung ein, die mit einer guten produktspezifischen Evaluierung die beiden anderen Tools auf Distanz halten kann. Bei der Cobit Evaluierung hingegen landet es an dritter Stelle mit Oracle, wobei der Punkterückstand in diesem Bereich sehr gering ist.

<i>Tool</i>	<i>produktspezifische Evaluierung</i>	<i>Cobit-Evaluierung</i>
Adonis Prozessportal	84,34%	32
B Wise	83,47%	29
Oracle GRC	71,01%	29
RSA Archer	-	0
SAP GRC	67,30%	30

Table 20. Ergebnis der Gesamtevaluierung

Um die Ergebnisse anschaulich aufzubereiten wurde eine grafische Darstellung erarbeitet. Dabei wurde eine Kombination aus beiden Evaluierungen dadurch erreicht, dass die Bewertungen in einer Grafik zusammengeführt wurden, indem die Werte aus der produktspezifischen Evaluierung auf der y-Achse und die Cobit Werte auf der z-Achse aufgetragen wurden. Auf der x-Achse befinden sich die Cobit Kriterien, die wie folgt abgekürzt wurden.

A&C	Awareness and Communication
PPP	Policies, Plans and Procedures
T&A	Tools and Automation
S&E	Skills and Expertise
R&A	Responsibility and Accountability
G&M	Goal Setting and Measurement
IC	Maturity Model for Internal Control

Für alle Tools wurde eine solche Grafik erstellt, die nachstehend aufgezeigt werden.

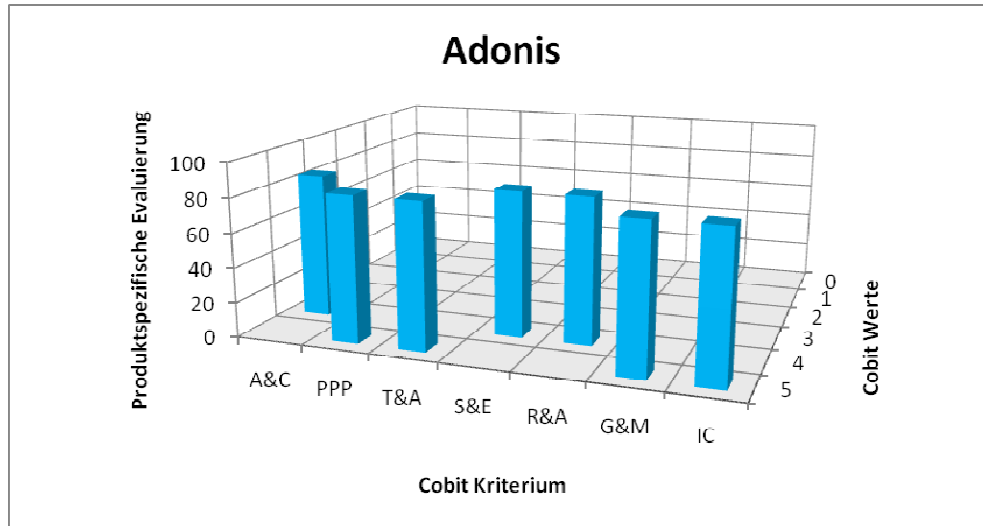


Fig. 23. Gesamtauswertung Adonis

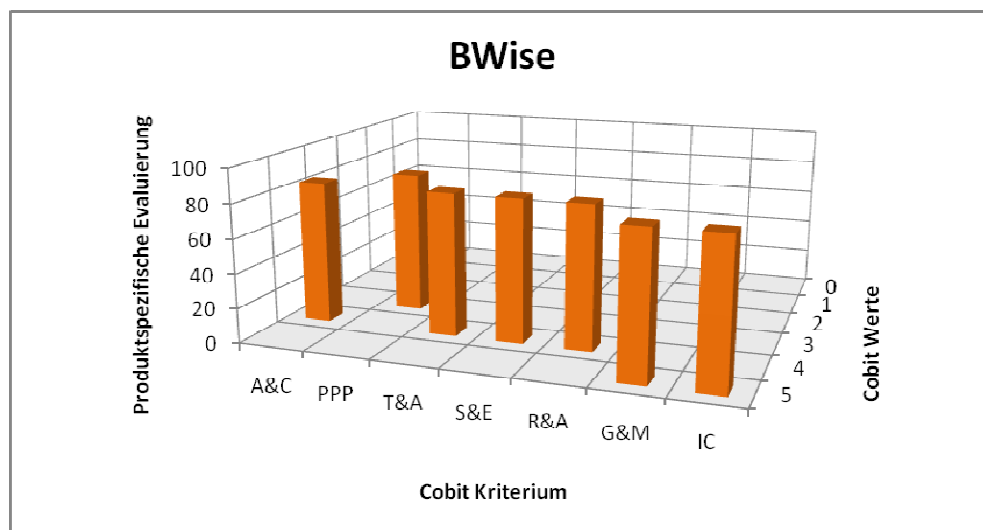


Fig. 24. Gesamtauswertung BWiSe

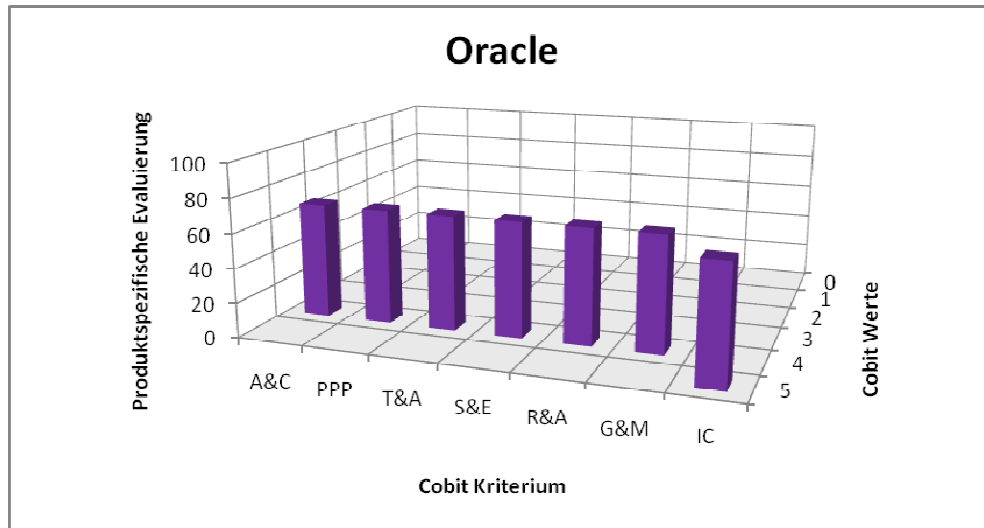


Fig. 25. Gesamtauswertung Oracle

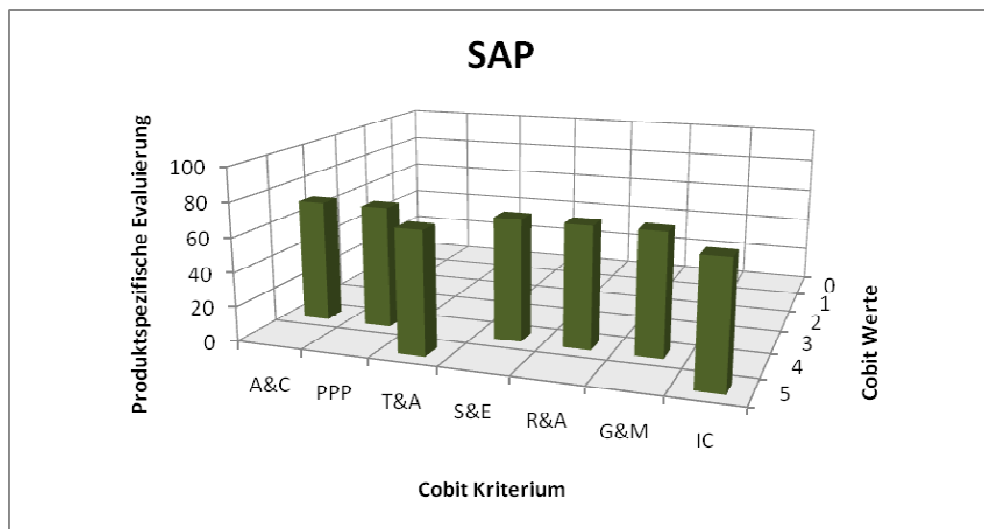


Fig. 26. Gesamtauswertung SAP

7.3.2 Resümee

In diesem Kapitel wird auf die einzelnen Ergebnisse der Evaluierung eingegangen, sowie eine Empfehlung abgegeben, die sich auf die zuvor durchgeführten Ausarbeitungen stützt. Weiters wird der Gesamteindruck und eine Stellungnahme zu den Evaluierungen abgegeben.

Produktspezifische Evaluierung

Wie bereits erwähnt, wird in diesem Kapitel näher auf die Empfehlung für die Toolauswahl eingegangen, wobei auch jene Funktionalitäten bzw. Implementierungen aufgezeigt werden, die von einzelnen Tools realisiert wurden und einen zusätzlichen Nutzen für das ausgewählte Interne Kontrollsystem darstellen. Dadurch werden jene Features aufgedeckt, die nicht von allen Tools realisiert wurden und einen Benefit darstellen. Diese Implementierungen hinsichtlich der produktspezifischen Eigenschaften sind für andere Tools erstrebenswert und sollten angedacht werden.

Eingangs ist zu erwähnen, dass das Adonis Prozessportal und B Wise nach der produktspezifischen Evaluierung, wie in Kapitel 7.1.5 aufgezeigt, an der Spitze abgeschlossen haben und nur durch wenige Punkte getrennt sind. Aus diesem Grund wurden die beiden Tools nochmals betrachtet und die Unterschiede herausgearbeitet. Die Entscheidung für das Adonis Prozessportal ist aus folgenden Gründen geschehen und unterstreicht die Auswahl nach der produktspezifischen Evaluierung.

Adonis wird bereits bei der Austrian Airlines AG für die Geschäftsprozessmodellierung verwendet und dadurch sind Benutzer bereits mit der Umgebung von Adonis vertraut. Dies spart in weiterer Folge Kosten und Aufwand im Schulungs- und Einarbeitungsbereich. Des Weiteren ist aus den Gesprächen bei der Kriterienerhebung klar hervorgegangen, dass es eine Schnittstelle des neuen IKS Tools zu Adonis geben soll, damit die bestehenden Geschäftsprozessmodelle übernommen werden können. B Wise kann diese Schnittstelle standardmäßig nicht zur Verfügung stellen und somit würde eine Schnittstellenentwicklung unumgänglich sein. Diese Entwicklung würde wiederum Kosten und Zeit in Anspruch nehmen, außerdem würden bei dieser Lösung redundante Modelle entstehen, da die Modelle in zwei Systemen betreut werden müssen. Dies stellt einen doppelten Wartungsaufwand dar und außerdem kann nicht sichergestellt werden, ob die Schnittstelle auch bei neuen Versionen eines Tools weiterhin voll funktionsfähig ist. Ein weiterer Aspekt, der für das Adonis Prozessportal spricht, ist die Tatsache, dass die BOC eine Niederlassung in Wien hat und bereits auf eine positive Zusammenarbeit zurückgeblickt werden kann. Dies bildet bereits einen vertrauenswürdigen Grundstock für die Aufgaben, die auf das Unternehmen zukommen.

Um jedoch auch Verbesserungspotential für die untersuchte Version des Adonis Prozessportals aufzuzeigen, soll die hervorragende Implementierung des Reifegradberichtwesens der B Wise-Implementierung nicht unerwähnt bleiben. Dabei wird nicht nur die Existenz des Internen Kontrollsystems nachgewiesen, sondern auch speziell auf den Reifegrad des Systems eingegangen. Hierzu werden Prozess- und Kontrollverantwortliche über die Wirksamkeit und Effizienz, sowie auch Nachvollziehbarkeit von Kontrollmechanismen anhand von Webfragebögen um ihre Meinung gebeten. Diese Art der Reifegradberichte für jeden einzelnen Prozess bzw.

jede einzelne Kontrolle wurde in B Wise besonders übersichtlich und trotzdem detailliert umgesetzt. Diese Implementierung ist auch im Sinne des Systems, da das System in weiterer Folge effizienter verwendet werden kann und der Umgang mit dem System verbessert wird.

Cobit-Evaluierung

Im Zuge der Cobit-Evaluierung wurden die Tools hinsichtlich einer Kombination aus dem Reifegradmodell für Interne Kontrollen und den Attributen des Reifegrads nach [Gov07] evaluiert. Dabei lag der Fokus auf der Betrachtung der Tools hinsichtlich der Unterstützung zur Zielerreichung.

Daraus ging ebenfalls das Adonis Prozessportal mit der besten Bewertung hervor, das durch den hohen Reifegrad in sämtlichen Bereichen überzeugen konnte und alle SOLL Anforderungen erfüllt. Bezüglich der Erreichung des SOLL Zustands konnten durchwegs alle Tools überzeugen. Weiters möchte ich anmerken, dass alle Tools ähnliche Ergebnisse erzielen konnten und im Hinblick auf die strategische Zielerreichung das Unternehmen sehr gut unterstützen können. Der gravierend geringere zeitliche Aufwand bei der Evaluierung im Vergleich zu der produktspezifischen Evaluierung sollte an dieser Stelle auch angemerkt werden.

Gesamteindruck

Zusammenfassend kann festgestellt werden, dass die vier übrigen Tools die Anforderungen gut erfüllen. Das Adonis Prozessportal konnte bei allen Evaluierungen überzeugen und kann somit als Empfehlung für die Austrian Airlines AG angegeben werden.

Während der Evaluierungsprozesse hat sich herausgestellt, dass die produktspezifische Evaluierung im Gegensatz zur Cobit-Evaluierung sehr zeitaufwendig ist. Aus diesem Grund hat sich ergeben, dass ein Evaluierungsprozess in zwei Etappen unterteilt werden soll. Zu Beginn sollte das Tool aus einer strategischen Sicht betrachtet werden. Dabei stellt sich die Frage, ob das Tool sinnvoll eingesetzt werden kann und etwas zur Erreichung der Unternehmensziele beitragen kann. Wenn diese Frage positiv beantwortet wird, kann mit einer produktspezifischen Evaluierung fortgefahren werden. Da somit nicht für alle Tools eine produktspezifische Evaluierung gemacht werden muss, spart dies bei einem Evaluierungsprozess, bei dem etwa 30 unterschiedliche Tools betrachtet werden, viel Zeit und Geld. Dies kann damit belegt werden, da der Zeitaufwand für eine Cobit-Evaluierung im Gegensatz zum Zeitaufwand einer produktspezifischen Evaluierung sehr gering ist, da diese innerhalb einiger Stunden abgeschlossen werden kann. Im Gegensatz dazu wurde für die produktspezifische Evaluierung ein Zeitraum von mehreren Wochen benötigt.

Somit sollte ein solcher Ansatz für die Vorauswahl von Tools in jeden Fall in Betracht gezogen werden. Ferner ist die Betrachtung des IST Systems eine objektive Standortbestimmung hinsichtlich der strategischen Dimension. Aus diesen Erkenntnissen kann in weiterer Folge ein SOLL Zustand erarbeitet werden, den man

als Unternehmen erreichen möchte und der von den betrachteten Tools erreicht werden soll.

Ein weiterer Vorteil der Cobit-Evaluierung ist die Tatsache, dass Cobit weitverbreitet ist und durch den Einsatz in der Wirtschaft laufend an die Anforderungen angepasst und verbessert wird.

Somit stellt einerseits die weitverbreitete und standardisierte Anwendung von Cobit und andererseits die zeitliche Einsparung ein Optimierungspotential hinsichtlich der Toolevaluierung dar. Besonders die zeitliche Komponente, die im beruflichen Umfeld auf die Kosten und Ressourcen umgelegt werden kann, enthält ein deutliches Einsparungspotential, welches durch die detaillierte Beschreibung in [Gov07] erreicht wird.

8 Einführungskonzept

Bei der Erarbeitung eines Konzepts zur Einführung eines IT Systems ist es erforderlich darauf zu achten, dass es sich dabei um ein Projekt handelt, das eine Vielzahl an Ressourcen verbraucht. Der Einführungsprozess ist als eigenständiges Projekt zu betrachten, welches in diesem Kapitel näher beleuchtet wird. Die Einführungsstrategie ist stark von den Gegebenheiten im Unternehmen abhängig, sowie auch von den Zielen der Einführung. Wie dies in [Hes07] erwähnt wird kann man bei der Einführungsstrategie zwischen der sukzessiven und der simultanen Einführungsstrategie sprechen, die in der Masterthesis in Kapitel 8.1 näher erläutert werden. Des Weiteren stellen die Projektziele, die vom Unternehmen vorgegeben werden, eine wesentliche Entscheidungsgrundlage für die Einführungsstrategie dar.

In diesem Teil der Arbeit wird ein Konzept für die Einführung vorgestellt, das an die Anforderungen eines Unternehmens angepasst werden kann. In dieser Ausarbeitung wird auf die Anforderungen der Austrian Airlines AG bezüglich des Einführungsprozesses eingegangen.

8.1 Einführungsstrategie

Um die beiden Einführungsstrategien, die in der Geschäftswelt verwendet werden besser zu verstehen, werden diese in den folgenden Kapitel näher erklärt. Dabei werden die Vorteile und Nachteile der Methoden aufgezeigt, um im weiteren Verlauf eine Entscheidung für die Austrian Airlines AG treffen zu können.

8.1.1 Simultane Einführung

Wenn alle Module eines Systems zum gleichen Zeitpunkt produktiv gesetzt werden, so spricht man von einer simultanen Einführung, jedoch kann dies bei großen Unternehmen und Projekten zu einem enormen Anstieg des administrativen

Projektaufwandes führen. Dies bringt mich zu den Vor- und Nachteilen, wie diese auf Grundlage von [Hes07]⁵⁰ erarbeitet wurden.

Durch die Einführung zu einem bestimmten Zeitpunkt ergeben sich mehrere Vorteile. So kann vermieden werden, dass zahlreiche Schnittstellen zu Altsystemen während der Umstellung benötigt werden. Weiters kann durch diese Einführungsmethode die Laufzeit des Projekts verkürzt werden und somit das System früher in einem vollen Funktionsumfang verwendet werden.

Dem gegenüber stehen die erhöhten Anforderungen, die an das Projektmanagement gestellt werden. Darunter fallen beispielsweise längere Vorlaufzeiten oder auch höhere Zusatzbelastungen. Außerdem werden besondere Anforderungen an die Umstellungsaktivitäten gestellt, da das System nicht mehr oder nur sehr kurz außer Betrieb genommen werden kann. Deshalb können Planungsfehler enorme Auswirkungen haben und unter anderem die Akzeptanz des Systems sehr schwächen.

8.1.2 Sukzessive Einführung

Wenn man von der sukzessiven Einführung spricht, so ist gemeint, dass einzelne Module eines Systems zu unterschiedlichen Zeitpunkten in Betrieb genommen werden. Dies ist jedoch nur möglich, wenn es sich bei dem System um ein modular aufgebautes System handelt, wie dies auch in [Hes07]⁵¹ beschrieben ist.

Für diese Methode der Systemeinführung können die Nachteile der simultanen Einführung großteils als Vorteile der sukzessiven Einführung umgelegt werden. So handelt es sich durchwegs um eine überschaubare Projektgröße, da jede Moduleinführung als einzelnes Projekt betrachtet wird und somit die Komplexität der einzelnen Projekte verringert wird. Durch diese Einführungsstrategie werden die Kosten über einen größeren Zeitraum verteilt, was wiederum aus finanziellen Gesichtspunkten für ein Unternehmen von Vorteil ist. Ein Vorteil, der nicht außer acht gelassen werden soll ist, dass schneller Erfolgserlebnisse verbucht werden können, da sich eine positive Einführung eines Teilbereichs positiv auf die Motivation der Projektteilnehmer und auch der Anwender auswirken kann.

Ferner ist anzumerken, dass es bei der sukzessiven Einführungsstrategie zwei unterschiedliche Ansätze gibt, wie sich die stufenweise Einführung untergliedert. Eine Möglichkeit besteht darin, dass man die Einführung funktionsorientiert durchführt, dabei handelt es sich um Softwaremodule, die eine Funktion zur Verfügung stellen, die innerhalb begrenzter Strukturen, wie einer Abteilung, genutzt werden. In der näheren Vergangenheit hat sich jedoch der prozessorientierte Ansatz vermehrt durchgesetzt, da bei dieser Einführungsstrategie all jene Module eingeführt werden, die an einem Geschäftsprozess beteiligt sind. Dadurch wird bewerkstelligt, dass ein Modul mit zusätzlichen Komponenten von anderen Modulen integriert wird, um die Abwicklung eines Geschäftsprozesses über Abteilungen hinweg realisieren zu können.

⁵⁰ Vgl. [Hes07] Seite 99

⁵¹ Vgl. [Hes07] Seite 100

Bei der Anwendung dieser Einführungsmethode gibt es einen gravierenden Nachteil. Da meistens Altsysteme abgelöst werden besteht eine Schnittstellenproblematik, welche das alte System, welches Schritt für Schritt abgelöst wird, mit dem neuen System kommunizieren lässt. Die lange Laufzeit des Projekts, welche aus finanzieller Sicht noch einen positiven Eindruck hinterlassen hat, kann auch als Nachteil gesehen werden, da die komplette Nutzung des neuen Systems erst nach der vollständigen Einführung gegeben ist. Diese lange Laufzeit kann den Anwendern auch den Charakter einer Zwischenlösung vermitteln und schädigt somit die Akzeptanz des Systems im Unternehmen.

8.1.3 Konzeption für die Systemeinführungsstrategie eines Internen Kontrollsystems bei der Austrian Airlines AG

Um die Auswahl der Einführungsstrategie für die Austrian Airlines AG bezüglich eines toolgestützten Internen Kontrollsystems zu definieren, ist wie bei jedem Projekt zu Beginn festzustellen, mit welchen Rahmenbedingungen sich die Einführung auseinandersetzen muss. Dazu ist das zu verwendende Einführungsszenario in einem ersten Schritt abzuklären. Dabei besteht die Möglichkeit zwischen einer Ablösung eines oder mehrerer Altsysteme und einer Einführung ohne Ablösung, die auch grüne Wiese Szenario genannt wird, zu unterscheiden.

Für die Auswahl der Einführungsstrategie wurde die nachstehende Tabelle anhand der Anforderungen der Austrian Airlines AG betrachtet.

In Absprache mit Herrn Mag. Michael Koegler wurden die Unternehmensziele der Austrian Airlines AG erarbeitet, die für die IT-Systemeinführung von Seiten des Unternehmens wichtig sind. Diese wurden in der nachstehenden Tabelle durch ein X gekennzeichnet und stellen die Grundlage für die Einführungsstrategie dar.

Unternehmensziele	Simultane Einführung	Sukzessive Einführung	AUA Priorität
Geringes unternehmerisches Risiko	-	+	X
Geringer Aufwand für Schnittstellen	+	-	X
Kurze Gesamtprojektlaufzeit	+	-	X
Geringe Personalkapazität	-	+	X
Schnelle Ablösung bestehender Systeme	+	-	
Frühe Nutzung der Integrationsvorteile	+	-	X
Geringe Belastung durch heterogene Systeme	+	-	
Schnelle Einführungssteilerfolge	-	+	
Geringe Einführungskosten	?	?	

Table 21. Bewertung der Einführungsstrategien in Bezug auf Unternehmensziele⁵²

Da mit der simultanen Einführung mehr positive Aspekte der Unternehmensziele abgedeckt werden, ist die simultane Einführungsstrategie für dieses Projekt besser geeignet, als die sukzessive Einführung.

⁵² Vgl. [Hes07] Seite 103

Damit die Ziele des Projekts erreicht werden, ist unumgänglich, dass bestimmte Faktoren berücksichtigt werden, die auch in [Hes07] beschrieben sind. Es werden die vier Erfolgsfaktoren aus [Hes07]⁵³ im Weiteren aufgezeigt und erklärt, damit diese im Projekt nicht außer Acht gelassen werden.

Der Auftraggeber eines Projekts stellt den ersten Erfolgsfaktor dar, damit ist jene Person, die das Projekt in Auftrag gibt und dieses auch am Ende abnimmt. Während des Projektes ist der Auftraggeber für die Bereitstellung der Ressourcen verantwortlich und er wird über den Projektverlauf stets informiert. Je höher die hierarchische Stellung, desto besser ist dies für den Projektverlauf, da der Auftraggeber einen größeren Einfluss im Unternehmen hat. Dies kann ausschlaggebend für Entscheidungen während der Projektphase sein, da manche Entscheidungen die Kompetenzen des Projektleiters übersteigen können. Bei der Austrian Airlines AG ist der Auftraggeber der Vorstand des Unternehmens, damit ist der Einfluss im Unternehmen auf höchster Ebene sichergestellt.

Ein weiterer Punkt sind die Projektziele, die vor dem Projekt möglichst konkret zu formuliert und dokumentiert sind. Dadurch besteht am Ende des Projekts die Möglichkeit, dass ein erfolgreicher Projektabschluss anhand der Zielumsetzung abgeleitet werden kann. Dies ist jedoch bei langen Projekten oft schwierig, da sich Ziele auf Grund von geänderten Rahmenbedingungen oder Technologien ändern können. Die Zielerreichung ist oftmals jedoch durch sogenannte Zielkonflikte schwer zu erreichen, da die Ziele untereinander in Abhängigkeit stehen, wie dies in der nachstehenden Abbildung aufgezeigt ist. Bei der Systemeinführung eines Internen Kontrollsystems steht die Einhaltung der gesetzlichen Bestimmungen als Ziel an oberster Stelle, so ist es auch bei der Austrian Airlines AG. Des Weiteren kann festgehalten werden, dass eine einfache Handhabung des Systems und die Einhaltung der Kriterien der Evaluierung als Ziele vorgegeben sind.

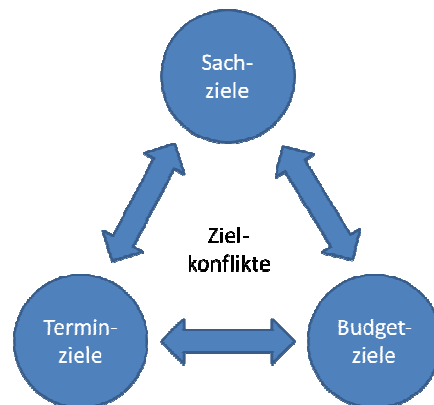


Fig. 27. Zielkonflikte⁵⁴

⁵³ Vgl. [Hes07] Seite 103

⁵⁴ Vgl. [Hen06] Seite 105

Die Projektgruppe stellt einen wesentlichen Erfolgsfaktor dar, da es sich dabei um jene personelle Ressourcen handelt, die mit der Zielerreichung beauftragt sind. Dabei setzt sich eine Projektgruppe aus Spezialisten unterschiedlicher Fachrichtungen zusammen. Es ist ebenfalls wichtig, dass die Anwender rechtzeitig in die Projektgruppe eingebunden werden und dem Team Feedback geben können, dies fördert wiederum die Akzeptanz des neuen Systems.

Der letzte Erfolgsfaktor, der in [Hes07] erwähnt wird, ist die Projektleitung. Die Projektleitung ist für das Ergebnis des Projekts verantwortlich und benötigt dafür entsprechende Rechte und Pflichten. So sollte es für die Projektleitung ein Mitspracherecht bei der Zusammensetzung des Projektteams geben. Hauptaufgabe der Projektleitung, die aus einer Person bestehen soll, sind unter anderem die Planung, Organisation, Koordinierung, Steuerung, Kontrolle sowie auch der Informationsfluss an den Auftraggeber und die Projektgruppe.

8.2 Vorgehensmodell zur Einführung eines Internen Kontrollsystems

Dieser Abschnitt der Masterthesis beschäftigt sich mit dem Vorgehensmodell für die Einführung des toolgestützten Internen Kontrollsystems und basiert auf den Ausführungen aus [Hes07]. Das Modell stellt eine methodische Vorlage dar, die in acht Phasen unterteilt ist, die sich klar voneinander abgrenzen.

Bei den Recherchen für die Einführung von IT Systemen hat sich gezeigt, dass einige Unternehmen ein eigenes Vorgehensmodell für die Einführung entwickelt haben. Da jedoch eine allgemein gültige Darstellung angestrebt wird, welche in weiterer Folge auf das ausgewählte Tool angewandt wird, wird keines der herstelllerspezifischen Vorgehensmodelle vorgestellt.

In der folgenden Grafik ist das allgemein gültige Vorgehensmodell für die Einführung eines IT Systems dargestellt, welches auf einem Wasserfallmodell basiert. Die Beschreibung der einzelnen Phasen wird in den Kapiteln 8.2.1 bis 8.2.8 detailliert vorgenommen, welche sich auf die Ausführungen in [Hes07] beziehen.

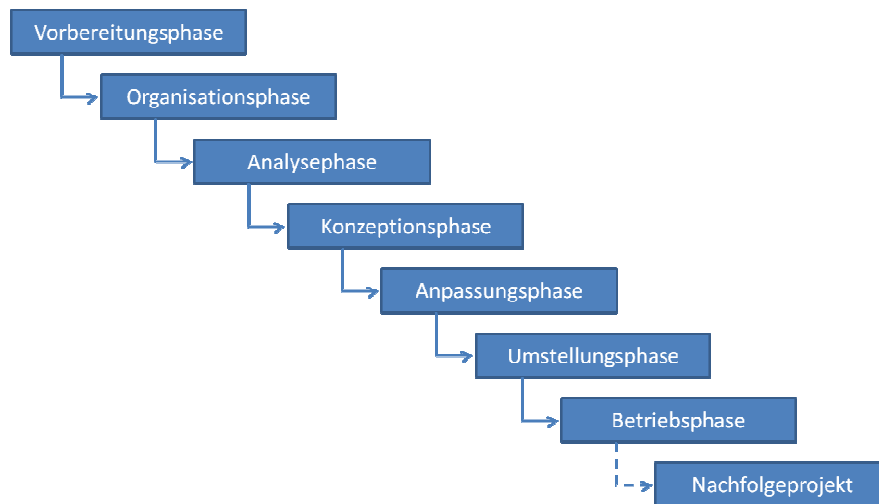


Fig. 28. Allgemeines Vorgehensmodell zur Einführung eines IT Systems⁵⁵

Zum einen wird in den folgenden Kapiteln aufgezeigt, welche Aufgaben in den Phasen abzuarbeiten sind. Zum anderen wird auch die Zielsetzung definiert, welche Artefakte und deren Inhalt darstellt. Es wird dabei nicht detailliert darauf eingegangen, wie diese Artefakte benannt sind, noch wird eine Dokumentationsvorschrift ausgegeben. Diese Vorgaben können aus einem beliebigen Projektmanagementstandard entnommen werden. Aus diesem Grund kann der unternehmensinterne bzw. vom Unternehmen definierte Projektmanagementstandard verwendet werden.

8.2.1 Vorbereitungsphase

Die erste Phase des Einführungsmodells ist die Vorbereitungsphase, die aus [Hes07] ⁵⁶ entnommen wurde, in der die Initiierung einer Systemveränderung vorgenommen wird. Darunter fallen weiters alle Vorstudien, sowie die Toolauswahl, die in den Kapiteln 5 und 7 ausführlich beschrieben wurden. Aus diesem Grund wird auf diese Phase nicht weiters eingegangen.

Zielsetzung

In dieser Phase ist die klare Vorgabe, dass die Toolauswahl abgeschlossen ist und klar definiert wurde, welches Tool im Unternehmen eingeführt wird. Weiters ist der Projektantrag zu entwickeln, der die Priorität, Komplexität und Bedeutung des Projekts beinhaltet.

⁵⁵ Vgl. [Hes07] Seite 116

⁵⁶ Vgl. [Hes07] Seite 116

8.2.2 Organisationsphase

Die zweite Phase ist angelehnt an die Ausführungen aus [Hes07]⁵⁷ und sind für eine effiziente Projektabwicklung von großer Wichtigkeit, da die vier Erfolgsfaktoren, die in Kapitel 8.1.3 erläutert wurden bereits in der Organisationsphase berücksichtigt werden. Im Speziellen ist damit gemeint, dass der Auftraggeber seine Ziele schriftlich dokumentiert und die Projektleitung bestimmt. Ein weiterer wichtiger Aspekt ist, dass das Projektteam gebildet wird.

Um die Rahmenbedingungen für ein Projekt festzulegen, sind in dieser Phase die Standards für die Projektabwicklung zu definieren. Dazu zählt die Festlegung von Standards für die Dokumentation und Kommunikation. Außerdem sind die Entscheidungsbefugnisse und die Vorgehensweise bei Änderungswünschen zu definieren.

Um eine Basis für den weiteren Projektablauf zu schaffen, ist die Erstellung eines Projektplans unumgänglich. Darin sollen Meilensteine definiert werden sowie eine Bedarfsplanung enthalten sein. Dazu zählt beispielsweise die Bereitstellung von technischen sowie auch räumlichen Ressourcen zu bestimmten Zeitpunkten bzw. über bestimmte Zeiträume hinweg zur Verfügung zu stellen. Die Planung des organisatorischen Bereichs ist ein weiterer Aspekt der abgedeckt werden muss. Dabei ist die Projektorganisation detailliert anzugeben um die beteiligten Instanzen abzustecken. Dazu zählen einerseits die Projektleitung, das Projektteam und der Auftraggeber sowie auch Kontrollorgane, wie die Revision, Berater oder Personen aus der Qualitätssicherung oder dem Controlling. Da die Kontrollorgane des Projekts zum Fortschritt bzw. dem Stand des Projekts laufend informiert werden sollen, ist auch das Berichtswesen in dieser Phase zu definieren.

Nachdem diese Aspekte in der Organisationsphase betrachtet wurden, kann die kommende Phase begonnen werden, welche meist durch ein Kick-off-Meeting eingeleitet und als offizieller Start angesehen wird.

Zielsetzung

Die klare Zielsetzung ist es in dieser Phase den Grundstein für das kommende Projekt zu legen, in dem alle grundlegenden Vorgaben und Rahmenbedingungen bestimmt werden, um in einen reibungslosen Projektablauf gewährleisten zu können.

Darunter fallen die Bestellung der Projektorganisation und der externen Kontrollorgane. Die Bereitstellung von Ressourcen im Bereich der Räumlichkeiten und Hardware ist ebenfalls in dieser Projektphase abzuklären und zu dokumentieren.

Weiters ist die Vorgabe bezüglich des Berichtwesens, der Dokumentationsvorschriften und der Kommunikationswege, sowie die Definition der Kommunikationsmedien von Bedeutung.

Da in einem Unternehmen laufend Projekte abgewickelt werden, wird meist ein Standard für das Projektmanagement verwendet wie beispielsweise der Projektmanagementansatz nach Gareis, an dem sich sämtliche Punkte dieses Kapitels orientieren, um ein übersichtliches und nachvollziehbares Projektmanagement im

⁵⁷ Vgl. [Hes07] Seite 117 ff.

Unternehmen zu etablieren. Dieser Projektmanagementansatz wurde erwähnt, da dieser auch bei der Austrian Airlines AG für Projekte verwendet wird.

Außerdem ist abzuklären, ob Schulungsmaßnahmen für die Projektmitarbeiter nötig sind. Diese können beispielsweise im Bereich des Projektmanagements oder im themenspezifischen Bereich liegen.

Die Gesamtheit der Ausführungen, die in dieser Phase zu betrachten sind, ist in einem Projektauftrag niederzuschreiben.

8.2.3 Analysephase

In der Analysephase wird eine Bestandsaufnahme durchgeführt, bei der untersucht wird, welche Geschäftsbereiche und Geschäftsprozesse von der Systemeinführung betroffen sind. Des Weiteren sollen auch die bestehenden Anwendungssysteme beleuchtet werden und nötige Schnittstellen aufgezeigt, sowie auch untersucht werden. Einige dieser Aufgaben decken sich mit Aufgaben des Evaluierungsprozesses aus Kapitel 4. Dass Aufgaben in einer vorangegangenen Phase bereits durchgeführt wurden ist auch in [Hes07] erläutert, da manche grundlegende Bereiche bereits in der Auswahlphase abgeklärt sein müssen.

Die Informationsquelle für diese Phase wurden aus [Hes07]⁵⁸ entnommen und durch Gespräche mit Toolherstellern erarbeitet. Eine detaillierte Bestandsaufnahme im Unternehmen ist möglich, wenn mit dem Systemhersteller Workshops abgehalten werden, die sich mit vier zentralen Fragen beschäftigen.

- Datenmodell
- Workflow
- Autorisierung
- Reporting

Die einzelnen Workshops befassen sich mit den oben genannten Themenbereiche, die mit den Verantwortlichen für das System, mit Prozessinhabern und dem Systemhersteller besprochen und diskutiert werden.

Bei dem Datenmodell-Workshop wird darauf eingegangen, welche Datenstruktur hinter dem System stehen soll. Dabei wird definiert welche Anforderungen von Anwenderseite nötig sind und wie diese persistent gehalten werden können.

Die vordefinierten Workflows des Systems müssen von Herstellern aufgezeigt werden und anhand von Beispielen erklärt werden. Dies dient dazu, dass zusätzliche Workflows besprochen werden können, die man sich als Kunde vom System erwartet.

Um gewährleisten zu können, dass jeder Benutzer die Daten vom System erhält, die ihn betreffen und für die er eine Berechtigung besitzt, ist die Autorisierung nötig. Dazu sind die Benutzergruppen zu definieren und auch die dazugehörigen Berechtigungen zu diskutieren.

Der letzte Themenpunkt beschäftigt sich mit dem Reporting. Dabei soll festgelegt werden, wie sich ein Report zusammenstellt und nach welchen Vorgaben dieser gestaltet sein soll. Außerdem ist abzuklären, welche Benutzergruppen Reports

⁵⁸ Vgl. [Hes07] Seite 121 ff.

erstellen müssen und an wen diese Reports weiterzuleiten sind. Die Reporterstellung ist in diesem Punkt auch zu klären, dabei kann man unterscheiden, ob Reports automatisch erstellt und an eine bestimmte Benutzergruppe weitergeleitet werden, oder ob Reports semiautomatisch erstellt werden. Bei einer semiautomatischen Verarbeitung bzw. Weiterleitung sind klare Regeln zu definieren, damit abgeklärt ist, was mit den Reports in weiterer Folge geschieht und wer dafür verantwortlich ist.

Nachdem die Themenbereiche erledigt sind, ist auch die Konzeption der Systemlandschaft möglich und ist mit dem Systemhersteller abzuklären. In diesem Punkt ist auch darauf zu achten, dass etwaige Systemneuerungen nicht außer acht gelassen werden.

Zielsetzung

Die Dokumentation der ausgearbeiteten Punkte ist die primäre Aufgabe in der Analysephase. Dabei sind die erarbeiteten Bereiche detailliert zu dokumentieren, da dies die Basis für die gewünschte Funktionalität und auch für folgende Anpassungen ist.

In einem weiteren Schritt kann bereits mit einer groben Konzeption der Systemlandschaft begonnen werden, nachdem der Umfang und die Anforderungen in der Analysephase bereits erarbeitet wurden. Dieses erste Konzept wird in weiterer Folge noch überarbeitet und detailliert betrachtet.

8.2.4 Konzeptionsphase

Die Systemanforderungen werden in der Konzeptionsphase genau betrachtet, damit das System den Soll-Zustand erreicht, der zu Beginn des Projekts definiert wurde. Ein Großteil der Funktionalitäten des Systems wurde bereits in der Evaluierungsphase geprüft und daher stellt das System, das eingeführt wird bereits eine umfangreiche Funktionalität zur Verfügung.

In der Konzeptionsphase wird das System von unterschiedlichen Seiten betrachtet, so ist darauf einzugehen, wie man das System bzw. die Geschäftsprozesse optimieren kann. Dabei kann man bei der Anpassung der Geschäftsprozesse auf langjährige Erfahrungen der Hersteller vertrauen und so in Kooperation die Prozesse effizienter gestalten. Andererseits ist es auch möglich, dass anstelle der Prozesse die Systeme angepasst werden, da es sich um spezielle Prozesse handelt, die seit Jahren praktiziert werden und so weitergeführt werden sollen.

Die genannten Ausführungen sind an die Erarbeitungen aus [Hes07]⁵⁹ angelehnt.

Zielsetzung

Wie bereits erwähnt gilt die genaue Dokumentation der Anpassungen als zentrale Zielsetzung. Dabei werden die erarbeiteten Anforderungen der Workshops der Analysephase detailliert aufgezeigt, sowie auch das Optimierungspotential der Geschäftsprozesse. Des Weiteren werden alle Anpassungen im Bereich der Funktionalität des Systems, der Schnittstellen und auch der Verarbeitungsverfahren

⁵⁹ Vgl. [Hes07] Seite 123 ff.

dokumentiert. Die gesamte Dokumentation und Anforderungserhebung wird in einem Pflichtenheft vereint und dient für die weitere Vorgehensweise als Fundament.

8.2.5 Anpassungsphase

In der Anpassungsphase werden die Änderungswünsche umgesetzt sowie auch getestet. Dabei stellt die Dokumentation der Anpassungen einen sehr wichtigen Punkt dar, der für die weitere Verwendung des Systems wichtig ist. Dabei kann sich die Dokumentation wie in [Hes07]⁶⁰ erwähnt unter anderem auf folgende Bereiche erstrecken, die angepasst wurden.

- Abbilden der Aufbau- und Ablauforganisation
- Kundenindividuelle Anpassungen
- Erweiterungen der Funktionalität
- Anpassung von Berichts- und Formularwesen
- Einrichten und dokumentieren von Schnittstellen
- Berechtigungskonzept

Neben der Dokumentation der Änderungen sind weitere Dokumentationen der Anpassungsphase zu erstellen.

- Benutzerdokumentation und Schulungsunterlagen
- Schulung der Endanwender
- Einrichten von Benutzern für die Endanwender
- Altdatenübernahme
- Integrationstest

Wie die zuvor gezeigte Auflistung bereits erahnen lässt, werden in der Anpassungsphase auch Testfälle durchgespielt, um die korrekte Funktionalität des Systems gewährleisten zu können und daraus eine unternehmensspezifische Dokumentation sowie auch Schulungsunterlagen erstellen zu können. Die Testfälle werden dazu in einem Entwicklungssystem durchgeführt, in dem auch das Berechtigungskonzept getestet wird. Das Entwicklungssystem wird auch für automatische Integrationstests angewandt, welche in der kommenden Phase für das Produktivsystem von enormer Bedeutung ist.

Zielsetzung

In der Anpassungsphase stehen nicht mehr die Ermittlung von Anforderungen im Mittelpunkt, sondern die Umsetzung der zuvor definierten Forderungen und deren Dokumentation. Darunter fallen beispielsweise die Erweiterung der Funktionalität, die kundenspezifischen Anpassungen, die Einrichtung von Schnittstellen oder auch die Integrationstests.

Neben den Aufgaben, um die Kundenwünsche zu erfüllen, ist es auch essentiell weitere Aufgaben durchzuführen. Dazu zählen die Datenübernahme und die Einrichtung von Benutzerkonten für die Endanwender. Einen wichtigen Bereich

⁶⁰ Vgl. [Hes07] Seite 127 ff.

nimmt die Erstellung von Schulungsunterlagen ein. Als eine weitere Aufgabe ist die Schulung von Benutzern und Anwendern zu sehen, die bereits begonnen werden kann.

8.2.6 Umstellungsphase

Nachdem die Anforderungen an das System erfüllt sind und die Endabnahme vorgenommen wurde, kann das System in den Produktivbetrieb übergehen. Dabei können unterschiedliche Strategien verfolgt werden, wie dies nachstehenden dargestellt ist. Außerdem sind einige Aufgaben erforderlich bevor das System umgestellt wird, damit ein reibungsloser Betrieb sichergestellt werden kann.

Umstellungsarten

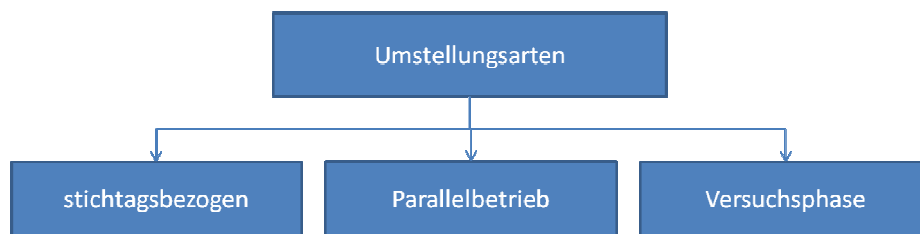


Fig. 29. Umstellungsarten von Systemen⁶¹

Bei der stichtagsbezogenen Umstellung wird ein bestimmter Tag definiert, an dem die Umstellung von einem Alt- zu einem Neusystem vorgenommen wird. Da die Migration je nach Unternehmensgröße einige Zeit in Anspruch nimmt, wird diese Umstellungsvariante an arbeitsfreien Tagen durchgeführt.

Wenn man von einem Parallelbetrieb spricht, so wird das Altsystem eine gewisse Übergangszeit neben dem neuen System betrieben. Diese Form wird von den Anwendern jedoch nicht gerne angewandt, da die Erfassung und die Bearbeitung von Daten doppelt vorgenommen werden muss, was einen gewaltigen Mehraufwand darstellt.

Die dritte Variante ist die Versuchsphase, bei der lediglich einzelne Arbeitsplätze mit dem neuen System arbeiten, welche zur letzten Überprüfung der Korrektheit betrieben werden. Somit kann das Risiko einer fehlschlagenden Produktivsetzung minimiert werden.

Aufgaben

Die Umstellungsart muss festgelegt werden, wobei anzumerken ist, dass dies bereits in der Organisationsphase betrachtet werden sollte. Im Zuge der Umstellung ist nicht außer acht zu lassen, dass es noch Aufgaben gibt, die erledigt werden müssen, um den Betrieb des neuen Systems zu bewerkstelligen und die

⁶¹ Vgl. [Hes07] Seite 131

Umstellungsphase abzuschließen. Zu den erforderlichen Aufgaben gehören unter anderem, wie in [Hes07]⁶² erwähnt.

- Übernahme der Altdaten
- Aktivieren der Schnittstellen
- Freischalten der Benutzer
- Offizieller Projektabschluss

Um jedoch zum offiziellen Projektabschluss durch den Auftraggeber zu kommen ist es von Vorteil, dass das System zuerst eine kurze Phase im laufenden Betrieb verwendet wird, um etwaige Probleme aufzuzeigen. Außerdem sollte in dem Abschlussbericht enthalten sein, ob es noch offene Punkte, vorhandene Restarbeiten, sowie anstehende Änderungs- oder Erweiterungswünsche gibt, die jedoch in einem neuen Projekt abgewickelt werden sollten.

Projekterfolg ermitteln

Nachdem das Projekt abgeschlossen wurde besteht die Möglichkeit, dass die zuvor definierten Projektziele, wie in Kapitel 8.1.3 erwähnt, analysiert werden. Dadurch besteht die Möglichkeit den Projekterfolg aus den Zielsetzungen für das Projekt abzuleiten.

Zielsetzung

Primäres Ziel in der Umstellungsphase ist die Einführung des neuen Systems mit der möglicherweise damit verbunden Ablösung eines oder mehrere Altsysteme. Damit einher geht die Übernahme der Altdaten, die Aktivierung der Schnittstellen sowie das Freischalten der Benutzer.

Der Abschluss dieser Phase ist auch gleichzeitig der Abschluss des Einführungsprojektes, das durch einen Abschlussbericht gekennzeichnet ist. Um das Projekt auch offiziell abzuschließen ist die Unterzeichnung des Abnahmedokuments des Projekts erforderlich. Darin enthalten sein soll der Stand des Projektes zum Übergabezeitpunkt.

8.2.7 Betriebsphase

Der laufende Betrieb nach der eigentlichen Einführung des Systems ist als Betriebsphase gekennzeichnet, welche in [Hes07]⁶³ beschrieben ist. In dieser Phase können Wartungs- und Administrationsarbeiten anfallen. Darunter fällt die Datensicherung, die auf Grund von gesetzlichen Vorschriften sehr wichtig ist. Weiters ist die Überwachung und Optimierung ein Aspekt, der im laufenden Betrieb beachtet werden muss. So ist die Überwachung des Systems ein wichtiges Hilfsmittel, um kritische Situation frühzeitig zu erkennen und um Maßnahmen einleiten zu können, um solchen Situationen entgegenzuwirken. Neben den Technologieänderungen, auf die der Systemhersteller reagieren muss, ist es auch wichtig durch den Administrator

⁶² Vgl. [Hes07] Seite 132

⁶³ Vgl. [Hes07] Seite 133

neue Releases einzuspielen, da ansonsten der Hersteller-Support enden kann. Außerdem werden mit neuen Releases neue und erweiterte Funktionalitäten bereitgestellt und die Zuverlässigkeit sowie auch die Leistungsfähigkeit des Systems werden dadurch gesteigert. Die Wartung des Systems kann weiters durch einen Wartungsvertrag mit dem Hersteller vertraglich beschlossen werden.

Zielsetzung

Im laufenden Betrieb ist darauf zu achten, dass die laufenden Releases und Updates eingespielt werden, damit ein reibungsloser Betrieb gewährleistet werden kann. In dieser Phase sind die Administratoren des Systems für den laufenden Betrieb verantwortlich, die Herstellerunterstützung beantragen können.

8.2.8 Nachfolgeprojekt

Eine weitere Phase, die jedoch nicht unmittelbar zum Vorgehensmodelle für die Einführung eines IT Systems gehört, ist die Nachfolgeprojekt-Phase. Dabei handelt es sich um eigenständige Projekte, die sich mit der Verbesserung, Erweiterung oder Änderung des Systems beschäftigen. Dafür werden neue Projekte initiiert, wofür wieder alle genannten Phasen aus den Kapiteln 8.2.1 bis 8.2.7 durchlaufen werden.

Diese Projekte werden in der Regel von jenen Partnern abgewickelt, die auch bei der Einführung des Systems mitgearbeitet haben, da diese bereits einen Einblick in das unternehmensspezifische Umfeld haben und ein Vertrauensverhältnis zwischen den beiden Parteien besteht.

9 Lessons learned

Das Ziel der Masterthesis war die Entwicklung eines Evaluierungsmodells für die Auswahl eines IT Systems zur Unterstützung eines Internen Kontrollsystems für Unternehmen. Dabei lag das Hauptaugenmerk darauf, dass eine universell einsetzbare Methode als Lösung angefertigt wird. Die Entwicklung des Evaluierungsmodells konnte durch kompetente Inputs von Seiten meines Betreuers Prof. Quirchmayr und der wirtschaftlichen Einflüsse von Herrn Mag. Michael Kogler in einem sehr guten Umfeld geschehen. Deshalb konnte eine Methode erarbeitet werden, die den Ansprüchen der Wirtschaft gerecht wird und durch die Anwendung bei der Austrian Airlines AG erstmals in einem unternehmerischen Kontext angewandt werden konnte. Besonders die unterschiedlichen Blickwinkel auf die Toolumsetzung eines Internen Kontrollsystems, sowie die Anpassbarkeit an verschiedene Anforderungen zeichnen das Evaluierungsmodell aus. Dabei wurde einerseits die Evaluierung in einem produktspezifischen und andererseits in einem strategischen Kontext durchgeführt.

Bezüglich der Anwendung des Modells ist jedoch festzuhalten, dass es im Zuge der Masterthesis mit Schwierigkeiten verbunden war, zu aufschlussreichen Informationen bezüglich jener Tools zu kommen, die zur Evaluierung ausgewählt wurden. Bei ersten Versuchen produktspezifische Informationen einzuholen, war die Rücklaufquote sehr gering, da einzig angegeben wurde, dass das Informationsmaterial für die Erstellung einer Masterthesis im Rahmen eines Wirtschaftsinformatikstudiums benötigt wird. Nachdem erneute Anfragen an die Toolhersteller gestellt wurden, welche mit dem Vermerk versehen wurden, dass die Masterthesis in Kooperation mit der Austrian Airlines AG erstellt wird, wurden von beinahe allen Hersteller Antwortschreiben verfasst. Es ist jedoch auch anzumerken, dass die Informationen unterschiedlich umfangreich und detailliert waren und auf weitere Rückfragen mit unterschiedlicher Kooperationsbereitschaft eingegangen wurde. Einerseits möchte ich mich bei der Austrian Airlines AG und im speziellen bei Herrn Mag. Michael Kogler bedanken, dass ich durch seine Mithilfe einen Einblick erhalten konnte, der ohne ihn nicht möglich gewesen wäre. Weiters möchte ich mich auch bei all jenen Personen bedanken, die meine Fragen beantwortet haben und mir ein persönliches Gespräch bezüglich eines Tools gestattet haben. Die Durchführung der Evaluierung konnte besonders durch jene Personen vereinfacht bzw. konkretisiert werden. Nichts desto trotz haben die Recherchen zahlreiche Stunden in Anspruch genommen, damit die Evaluierung nach besten Wissen und Gewissen durchgeführt werden konnte. Eine besondere Herausforderung nahm die produktspezifische Evaluierung mancher Kriterien in Anspruch, die von Anwenderseite vorgegeben wurden, da es in diesem Bereich sehr wichtig ist, dass die Anforderungen sehr detailliert beschrieben sind. Diese Erkenntnis wurde erst nach den ersten Evaluierungsversuchen gemacht, sodass bei manchen Kriterien ein weiteres Gespräch bzw. eine genauer Definition von Nöten war. Es ist somit darauf zu achten, dass eine genaue Beschreibung der Kriterien den zeitlichen Aufwand der Evaluierung enorm verkürzen kann. Neben einer genauen Beschreibung ist eine eindeutige und aussagekräftige Benennung der Kriterien sehr hilfreich. Der genannte Punkt kann mit Sicherheit als einer der wichtigsten Kriterien

bei der produktspezifischen Evaluierung genannt werden, der zu einer raschen, fehlerfreien und zufriedenstellenden Durchführung führt.

Die Cobit-Evaluierung liefert hingegen schneller ein Evaluierungsergebnis, da man die Evaluierungen auf Basis eines vordefinierten Schemas durchführt. Die unterschiedlichen Bereiche sind definiert und die Kategorisierung, sowie die damit verbundene Bewertung sind klar vorgegeben. Somit ist lediglich die Einstufung aller Tools vorzunehmen, um ein Ergebnis zu erhalten. Dadurch kann gewährleistet werden, dass ein Resultat rasch erarbeitet werden kann und Aufschluss darüber gibt, ob ein Tool die Ziele des Unternehmens unterstützen kann oder nicht. Diese Evaluierung, welche in 7.3.2 beschrieben wurde, kann somit als ein erstes Auswahlverfahren dienen, um einen umfangreichen Evaluierungsprozess zu beschleunigen. Außerdem gibt die Cobit-Evaluierung eine weitere Sichtweise auf die ausgewählten Tools, sodass ein breiteres Spektrum in der Evaluierung abgedeckt werden kann.

Ferner stellt die Arbeit ein Konzept zur Verfügung, wie ein Unternehmen die Einführung des Systems bewerkstelligen kann und welche Aspekte in diesem Bereich bzw. in jeder einzelnen Phase zu beachten ist. Die offene Gestaltung des Einführungskonzeptes kann für Unternehmen als sehr hilfreich eingestuft werden, da nicht ein neuer Standard bzw. eine genaue Vorgehensweise vorgeschrieben wird, sondern die Möglichkeit besteht, bekannte bzw. eigene unternehmensinterne Standards zu verwenden.

Diese Bereiche stellen somit die Umsetzung der geplanten Ziele dar, welche zu Beginn der Masterthesis ausgegeben wurden. Die Verwendung von Teilbereichen der Arbeit bei der Austrian Airlines AG zeigte bereits, dass die Ausarbeitung in einem unternehmerischen Umfeld erfolgreich zur Anwendung gebracht werden kann.

10 Grafikverzeichnis

Fig. 1. Risikomanagementprozess	18
Fig. 2. Risikofelder	19
Fig. 3. Überblick Risikomanagement nach AS/NZS 4360:2004	24
Fig. 4. COSO II Modell	28
Fig. 5. Aufbau der ONR 4900X	30
Fig. 6. Risikomanagement nach ONR 4900X	31
Fig. 7. Cobit Governance Würfel	32
Fig. 8. Internes Kontrollsystem	36
Fig. 9. Projektabwicklungs-Zyklus im Regelkreis	41
Fig. 10. Evaluierungsmodell für IKS Tools	43
Fig. 11. Struktur von Wirtschaftlichkeitsvergleichen	51
Fig. 12. Cobit 4.1 – Strategie für das Reifegradmodell	54
Fig. 13. B Wise Softwarelösung	60
Fig. 14. RSA Archer eGRC Plattform	62
Fig. 15. Gewichtung der funktionalen Themenblöcke	80
Fig. 16. Gewichtung der technischen Themenblöcke	81
Fig. 17. Gewichtung der finanziellen Themenblöcke	81
Fig. 18. Gewichtung der Themengebiete	82
Fig. 19. Ergebnis der produktspezifischen Evaluierung	85
Fig. 20. Cobit Auswertung – IST Zustand	86
Fig. 21. Cobit Auswertung – Adonis	88
Fig. 22. Vergleich der Cobit-Evaluierungen	91
Fig. 23. Gesamtauswertung Adonis	93
Fig. 24. Gesamtauswertung B Wise	93
Fig. 25. Gesamtauswertung Oracle	94
Fig. 26. Gesamtauswertung SAP	94
Fig. 27. Zielkonflikte	100
Fig. 28. Allgemeines Vorgehensmodell zur Einführung eines IT Systems	102
Fig. 29. Umstellungsarten von Systemen	107
Fig. 30. C 4.1 – Maturity Attribute Table	153
Fig. 31. Cobit 4.1 – Maturity Model for Internal Control	154

11 Tabellenverzeichnis

Table 1. Insolvenzstatistik Unternehmen 2010.....	16
Table 2. Cobit-Prozesse – Planung & Organisation	33
Table 3. Cobit-Prozesse – Akquisition & Implementierung.....	33
Table 4. Cobit -Prozesse – Delivery & Support	34
Table 5. Cobit -Prozesse – Monitoring und Evaluierung	34
Table 6. Beispiel für Multifaktorenmethode	47
Table 7. Cobit 4.1 – generische Bewertungsskala	53
Table 8. gesetzliche Bestimmungen für Aktiengesellschaften in Österreich.....	57
Table 9. Ergebnis der funktionalen Evaluierung	83
Table 10. Ergebnis der technischen Evaluierung.....	83
Table 11. Ergebnis der finanziellen Evaluierung.....	84
Table 12. Ergebnis der produktspezifischen Evaluierung	84
Table 13. Cobit Auswertung – IST Zustand	86
Table 14. Cobit Auswertung – SOLL Zustand	87
Table 15. Cobit Auswertung – Adonis	88
Table 16. Cobit Auswertung – B Wise	89
Table 17. Cobit Auswertung – Oracle	89
Table 18. Cobit Auswertung – SAP	90
Table 19. Ergebnis der Cobit-Evaluierung	90
Table 20. Ergebnis der Gesamtevaluierung.....	92
Table 21. Bewertung der Einführungsstrategien in Bezug auf Unternehmensziele	99

12 Literaturverzeichnis

[Aus04] Australien/NewZealand Standard: Risk Management AS/NZS 4360:2004 (, 2004).

[Aus10] Austrian Airlines AG: Handbuch des Internen Kontrollsystems (Wien, 2010).

[Ban06] Bank für internationalen Zahlungsausgleich: Internationale Konvergenz der Eigenkapitalmessung und Eigenkapitalanforderung (Basel, 2006).

[BOC08] BOC Österreich: Risikomanagement und Interne Kontrollsysteme mit dem BOC Management Office (Wien, 2008).

[BW101] BWise: Internes Kontrollsystem IKS (, 2009).

[Dud07] Dudenredaktion: Duden Das große Fremdwörterbuch - Herkunft und Bedeutung der Fremdwörter (Mannheim, Leipzig, Wien, Zürich, 2007).

[Gle01] Werner Gleißner, Günter Meier: Wertorientiertes Risiko-Management für Industrie und Handel (Wiesbaden, 2001).

[Gol06] Wolfgang Goltsche: COBIT kompakt und verständlich (Wiesbaden, 2006).

[Gov07] Governance Institute: COBIT 4.1 (USA, 2007).

[Hen06] Bernd Hentschel, Theodor Böhm: IKS-Starthilfe (Frechen, 2006).

[Hes07] Martin Hesseler, Marcus Görtz: Basiswissen ERP-Systeme (Birkach, 2007).

[Jen01] Bruno Jenny: Projektmanagement in der Wirtschaftsinformatik (Zürich, 2001).

[Koh05] Wolfgang Kohn: Statistik - Datenanalysis und Wahrscheinlichkeitsrechnung (Heidelberg, 2005).

[Lat10] Christoph Lattemann: Corporate Governance im globalisierten Informationszeitalter (München, 2010).

[Sch02] Henner Schierenbeck, Michael Lister: Value Controlling - Grundlagen Wertorientierter Unternehmensführung (München, 2002).

[Sch97] Uwe Schnorrenberg, Gabriele Goebels: Risikomanagement in Projekten (Hamburg, 1997).

[Sta02] Peter Stahlknecht, Ulrich Hasenkamp: Einführung in die Wirtschaftsinformatik (Berlin Heidelberg, 2002).

[Wie10] Bruno Wiederkehr, Rita-Maria Züger: Risikomanagementsystem im Unternehmen (Zürich, 2010).

Onlinequellen

[Bey08] Beyond Consulting GmbH: EUROSIX, EU-SOX, URAEG Unternehmensrecht 2008 (2008)
[http://www.eurosix.at/index_new.php?menuid=10] (Zugriff: 27. 01 2011).

[BOC11] BOC Group: BOC Group: ADONIS - Anwendungsszenarien ()
[<http://www.boc-group.com/de/produkte/adonis/anwendungsszenarien/>] (Zugriff: 21. 05 2011).

[BOC111] BOC Group: ADONIS - Anwendungsszenarien: BOC Group: ADONIS Prozessportal ()
[<http://www.boc-group.com/at/produkte/adonis/adonis-prozessportal/>] (Zugriff: 21. 05 2011).

[BW1] BWise: BWise at a glance ()
[<http://www.bwise.com/web-tv/about-bwise/bwise-at-a-glance>] (Zugriff: 27. 01 2011).

[BW10] BWise: BWise Product demonstration ()
[<http://www.bwise.com/web-tv/about-bwise/ad-hoc-or-structured-approach>] (Zugriff: 22. 12 2010).

[Com04] Committee of Sponsoring Organizations: Unternehmensweites Risikomanagement - Übergreifendes Rahmenwerk (2004)
[http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_German.pdf] (Zugriff: 24. 01 2011).

[FMA11] FMA - Österreichische Finanzmarktaufsicht: Solvency II ()
[<http://www.fma.gv.at/de/sonderthemen/solvency-ii/grundlagen-solvency-ii/historische-entwicklung.html>] (Zugriff: 08. 02 2011).

[Gov11] Governance Institute: Cobit 4.0 Deutsch ()
[<http://www.scribd.com/doc/38118896/CobIT-4-0-Deutsch>] (Zugriff: 17. 07 2011).

[KSV11] KSV - Kreditschutzverband von 1870: Insolvenzstatistik Unternehmen 2010 (2011)

[<http://www.ksv.at/KSV/1870/de/pdf/statistik/InsolvenzstatistikUnternehmen2010.pdf>] (Zugriff: 13. 01 2011).

[**Ora11**] Oracle: Fusion Applications | Oracle Applications | Oracle (2011)
[<http://www.oracle.com/us/products/applications/fusion/index.html>] (Zugriff: 28. 04 2011).

[**Öst10**] Österreichisches Normungsinstitut: Risikomanagement für Unternehmen und Systeme - Begriffe und Grundlagen (2010)
[<https://www.astandis.at/shopV5/Preview.action;jsessionid=862D2D771C994C2CC8D81F7A12AC32F6?preview=&dokkey=347213&selectedLocale=de>] (Zugriff: 24. 01 2011).

[**Ris11**] Wikipedia: Risiko – Wikipedia ()
[http://de.wikipedia.org/wiki/Risiko#Risiko_in_der_Wirtschaftswissenschaft] (Zugriff: 08. 02 2011).

[**RSA11**] RSA Archer: RSA Archer eGRC Solutions ()
[<http://www.archer.com/platform/index.html>] (Zugriff: 17. 04 2011).

[**RSA17**] RSA Archer: Enterprise GRC Solutions | Governance | Risk Management | Compliance Management ()
[<http://www.archer.com/solutions/index.html>] (Zugriff: 17. 04 2011).

[**SAP07**] SAP Österreich: SAP Österreich - SAP kündigt GRC Risk Management an (2007)
[<http://www.sap.com/austria/about/press/press.epx?pressid=7724>] (Zugriff: 20. 12 2010).

[**SAP11**] SAP Deutschland: SAP Deutschland - SAP BusinessObjects GRC- Lösungen | Schützen Sie Ihre Marke und Ihren guten Ruf. ()
[<http://www.sap.com/germany/solutions/sapbusinessobjects/large/governance-risk-compliance/index.epx>] (Zugriff: 31. 01 2011).

Ich habe mich bemüht, sämtliche Inhaber der Bildrechte ausfindig zu machen und ihre Zustimmung zur Verwendung der Bilder in dieser Arbeit eingeholt. Sollte dennoch eine Urheberrechtsverletzung bekannt werden, ersuche ich um Meldung bei mir.

13 Anhang

13.1 Evaluierungen

Evaluierungsbogen für IKS Tools

Gesamtevaluierung

Evaluierung zur Auswahl eines Internen Kontrollsystems

Unternehmen	Austrian Airlines AG
Evaluierer	Christoph Brandner
Applikation	Adonis Prozessportal

Gesamtbewertung

	Bewertung	Blockgewichtung in %	Bewertung nach der Eval.gewichtung
funktionale Evaluierung	85,52%	33,3%	28,51%
technische Evaluierung	87,50%	33,3%	29,17%
finanzielle Evaluierung	80,00%	33,3%	26,67%
		100%	84,34%

Hinweis bezüglich der Bewertung und der Auswertung

Legend für die Bewertung

Multifaktorenmethode	Bewertung	
	min. Punkte	0
	max. Punkte	4
	Priorität	
	min. Punkte	1
	max. Punkte	5

Die detaillierte Beschreibung der Punktevergabe ist in der Diplomarbeit ("Ein Evaluierungsmodell zur Auswahl eines Internen Kontrollsystems und dessen Test bei der Austrian Airlines AG") nachzulesen.

funktionale Evaluierung

Evaluierungsbeginn	01.02.2011
Evaluierungsende	29.04.2011

Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
generelle Anforderungen	83,97%	20%	16,79%
Kundenanforderungen	84,66%	20%	16,93%
Customizinganforderungen	86,84%	10%	8,68%
Nachvollziehbarkeits-/Workflowanforderungen	95,54%	20%	19,11%
Überwachung des Internen Kontrollsystems (Revision)	80,00%	30%	24,00%
		100%	85,52%

Anmerkung:

13.1.1 Adonis Prozessportal

Evaluierungsbogen für IKS Tools

Gesamtevaluierung

technisch Evaluierung			
Evaluierungsbeginn	01.02.2011		
Evaluierungsende	29.04.2011		
Block	normierte Bewertung	Blockgewich- tung in %	Bewertung nach der Blockgewichtung
Systemplattform	100,00%	20%	20,00%
Methodikhandbuch	100,00%	11%	11,00%
Software	80,00%	22%	17,60%
Sicherheit	61,54%	10%	6,15%
Sonstiges	75,00%	17%	12,75%
Systemanforderungen	100,00%	20%	20,00%
		100%	87,50%
Anmerkung:			

finanzielle Evaluierung			
Evaluierungsbeginn	01.02.2011		
Evaluierungsende	29.04.2011		
Block	normierte Bewertung	Blockgewich- tung in %	Bewertung nach der Blockgewichtung
Kosten	80,00%	100%	80,00%
		100%	80,00%
Anmerkung:			

Funktionale Evaluierung

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

Evaluierungsbogen
funktionale Anforderungen eines IKS für die Austrian Airlines AG

<i>Applikation</i>		Adonis Prozessportal	
<i>Prüfung abgeschlossen am</i>		29.04.2011	
Kriterium	Priorität	Bewertung	Produkt
generelle Anforderungen			131 (von 156)
Benutzer-Rollenkonzept (Berechtigungen, ...)	4	4	16
Einhaltung von Compliance-Vorgaben (BilMoG, URÄG, RLÄG, ...)	5	4	20
Integration von Microsoft Standardsoftware			
MS Word	5	4	20
MS Excel	5	4	20
MS Outlook	5	2	10
MS Exchange	5	2	10
MS SharePoint	5	4	20
Benutzerfreundlichkeit (easy-to-use for Clients) auf Basis von Standards (z.B. ISO Norm 9241)	5	3	15
Kundenanforderungen			149 (von 176)
Webbrowserbasierter Clientzugang (ab Version)			
Internet Explorer 7	5	4	20
Mozilla Firefox 3.5	5	4	20
Kompatibel zu Adonis	5	4	20
Datenübernahme aus operativen Systemen			
SAP	3	4	12
Vorhandener Katalog mit Standard-Kontrollen zu SAP	3	2	6
Verlinkung zum Risikomanagement (IKS-Instrument Risiken zuordnen)			
R2C - Risk to change (Schleupen AG)	3	2	6
Anfügen von Dateien/Links	3	3	9
Event-Management (Reminderfunktionen, E-Mailnotifikation...)	5	4	20
Umfrage-Management	4	3	12
Feedbackschleife im Bezug auf Prozess, Risiko und Kontrolle (Plan - Do - Check - Act)	5	3	15
Möglichkeit zur zentralen Vorgabe der Benennung der Steuerungs-/Überwachungsinstrumente	3	3	9
Customizinganforderungen			66 (von 76)
Konfigurierbarkeit und Anpassungsmöglichkeiten	5	3	15
Individuell gestaltbare Auswertungen	5	3	15
zusätzliche Kontrollen (benutzerdefinierte, konzerninterne Kontrollen)	5	4	20

Ein Evaluierungsmodell zur Auswahl eines IT Systems zur Unterstützung eines Internen
Kontrollsystems und dessen Test bei der Austrian Airlines AG 121

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

Einbindungsmöglichkeit weiterer Attribute (Anforderungsart, Instrumententyp)	4	4	16
Nachvollziehbarkeits-/Workflowanforderungen			107 (von 112)
Protokollierung (Sicherstellung der Nachvollziehbarkeit)	5	4	20
Historisierung der Kontrollergebnisse	5	4	20
Durchführbarkeit von Self Assessment	3	4	12
Möglichkeit zur Kommentierung/Nachverfolgung bei Grenzwertüberschreitung	3	4	12
Workflow zur Erfassung/Bearbeitung/Bestätigung von Steuerungs-/Überwachungsinstrumenten	5	3	15
Automatische Nachverfolgung von Prüfungsfeststellungen (Workflow)	4	4	16
Automatisierte Kontrollen von Grenzwertüberschreitungen anhand hinterlegter Regeln aus den importierten Daten	3	4	12
Überwachung des Internen Kontrollsystems (Revision)			32 (von 40)
Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor	2	4	8
Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor offline (optional)	2	0	0
Prüfungsplanung zur Wirksamkeit der Steuerungs-/Überwachungsinstrumente	2	4	8
Übersicht zu Stand der Aktualisierung des IKS	2	4	8
Übersicht der Ergebnisse der Wirksamkeitsprüfung	2	4	8

Gesamtpunkteanzahl

485

mögliche Gesamtpunkte

560

Technische Evaluierung

Evaluierungsbogen für IKS Tools

technische Evaluierung

Evaluierungsbogen technische Anforderungen eines IKS für die Austrian Airlines AG

<i>Applikation</i>		Adonis Prozessportal	
<i>Prüfung abgeschlossen am</i>		29.04.2011	
Kriterium	Priorität	Bewertung	Produkt
Systemplattform			140 von (140)
IT Infrastruktur Server			
Windows Server 2003	5	4	20
Windows Server 2008	5	4	20
Microsoft SQL Server 2005	5	4	20
IT Infrastruktur Client			
Windows XP	5	4	20
Windows 7	5	4	20
Microsoft Office 2003	5	4	20
Microsoft Office 2010	5	4	20
Methodikhandbuch			32 von (32)
Quickinfo	4	4	16
Benutzerfreundlichkeit des Methodikbuches	4	4	16
Software			48 von (60)
Einführungsaufwand	3		0
Skalierbarkeit	4	4	16
Concurrent-Lizenzmodell	5	4	20
LDAP Schnittstelle bezüglich Autorisierung	3	4	12
Sicherheit			32 von (52)
Datensicherheit (Verschlüsselung)	4	0	0
Datensicherung (Gesamtspiegelung)	4	3	12
Zugriffsbeschränkungen	5	4	20
Sonstiges			39 von (52)
Support im geographischen Umfeld	3	4	12
Helpdesk (Telefon, Webbasiert)	3	2	6
Durchschnittliche Antwortzeiten auf Anfragen	3	3	9
Wartungsvertrag	4	3	12
Systemanforderungen			12 von (12)
<i>derzeitige Systemvoraussetzungen im Unternehmen</i>			
Intel Core 2 Duo, Intel Core i3/i5			
3 GB Arbeitsspeicher			
250 GB HDD			

Ein Evaluierungsmodell zur Auswahl eines IT Systems zur Unterstützung eines Internen
Kontrollsystems und dessen Test bei der Austrian Airlines AG 123

Evaluierungsbogen für IKS Tools		technische Evaluierung	
<i>minimale Systemanforderungen</i>	3	4	12
2 CPU Kerne			
1.016 MB Arbeitsspeicher			
5.700 MB HDD (ausschließlich für das Adonis Prozessportal)			

Gesamtpunkteanzahl	303
mögliche Gesamtpunkte	348

Finanzielle Evaluierung

Evaluierungsbogen für IKS Tools

finanzielle Evaluierung

**Evaluierungsbogen
finanzielle Anforderungen eines IKS für die Austrian Airlines AG**

<i>Applikation</i>	Adonis Prozessportal
<i>Prüfung abgeschlossen am</i>	29.04.2011

Kriterium	Priorität	Bewertung	Produkt
Kosten			48 (von 60)
Anschaffungskosten	5	3	15
Betriebskosten	3	4	12
Wartungskosten	3	3	9
Customizingkosten	4	3	12

Gesamtpunkteanzahl	48
	mögliche Gesamtpunkte 60

13.1.2 B Wise

Evaluierungsbogen für IKS Tools

Gesamtevaluierung

Evaluierung zur Auswahl eines Internen Kontrollsystems

Unternehmen	Austrian Airlines AG
Evaluierer	Christoph Brandner
Applikation	BWise

Gesamtbewertung

	Bewertung	Blockgewichtung in %	Bewertung nach der Eval.gewichtung
funktionale Evaluierung	79,99%	33,3%	26,66%
technische Evaluierung	88,74%	33,3%	29,58%
finanzielle Evaluierung	81,67%	33,3%	27,22%
		100%	83,47%

Hinweis bezüglich der Bewertung und der Auswertung

Legend für die Bewertung

Multifaktorenmethode	Bewertung	
	min. Punkte	0
	max. Punkte	4
	Priorität	
	min. Punkte	1
	max. Punkte	5

Die detaillierte Beschreibung der Punktevergabe ist in der Diplomarbeit ("Ein Evaluierungsmodell zur Auswahl eines Internen Kontrollsystems und dessen Test bei der Austrian Airlines AG") nachzulesen.

funktionale Evaluierung

Evaluierungsbeginn	01.02.2011
Evaluierungsende	29.04.2011

Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
generelle Anforderungen	64,74%	20%	12,95%
Kundenanforderungen	81,25%	20%	16,25%
Customizinganforderungen	94,74%	10%	9,47%
Nachvollziehbarkeits-/Workflowanforderungen	86,61%	20%	17,32%
Überwachung des Internen Kontrollsystems (Revision)	80,00%	30%	24,00%
		100%	79,99%

Anmerkung:

Evaluierungsbogen für IKS Tools

Gesamtevaluierung

technisch Evaluierung			
Evaluierungsbeginn	01.02.2011		
Evaluierungsende	29.04.2011		
Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
Systemplattform	100,00%	20%	20,00%
Methodikhandbuch	100,00%	11%	11,00%
Software	66,67%	22%	14,67%
Sicherheit	100,00%	10%	10,00%
Sonstiges	76,92%	17%	13,08%
Systemanforderungen	100,00%	20%	20,00%
		100%	88,74%
Anmerkung:			

finanzielle Evaluierung			
Evaluierungsbeginn	01.02.2011		
Evaluierungsende	29.04.2011		
Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
Kosten	81,67%	100%	81,67%
		100%	81,67%
Anmerkung:			

Funktionale Evaluierung

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

Evaluierungsbogen funktionale Anforderungen eines IKS für die Austrian Airlines AG

Applikation		BWiSe	
Prüfung abgeschlossen am		29.04.2011	
Kriterium	Priorität	Bewertung	Produkt
generelle Anforderungen			101 (von 156)
Benutzer-Rollenkonzept (Berechtigungen, ...)	4	4	16
Einhaltung von Compliance-Vorgaben (BilMoG, URÄG, RLÄG, ...)	5	4	20
Integration von Microsoft Standardsoftware			
MS Word	5	4	20
MS Excel	5	4	20
MS Outlook	5	0	0
MS Exchange	5	3	15
MS SharePoint	5	0	0
Benutzerfreundlichkeit (easy-to-use for Clients) auf Basis von Standards (z.B. ISO Norm 9241)	5	2	10
Kundenanforderungen			143 (von 176)
Webbrowserbasierter Clientzugang (ab Version)			
Internet Explorer 7	5	4	20
Mozilla Firefox 3.5	5	4	20
Kompatibel zu Adonis	5	2	10
Datenübernahme aus operativen Systemen			
SAP	3	4	12
Vorhandener Katalog mit Standard-Kontrollen zu SAP	3	3	9
Verlinkung zum Risikomanagement (IKS-Instrument Risiken zuordnen)			
R2C - Risk to change (Schleupen AG)	3	2	6
Anfügen von Dateien/Links	3	4	12
Event-Management (Reminderfunktionen, E-Mailnotifikation...)	5	4	20
Umfrage-Management	4	4	16
Feedbackschleife im Bezug auf Prozess, Risiko und Kontrolle (Plan - Do - Check - Act)	5	3	15
Möglichkeit zur zentralen Vorgabe der Benennung der Steuerungs-/Überwachungsinstrumente	3	1	3
Customizinganforderungen			72 (von 76)
Konfigurierbarkeit und Anpassungsmöglichkeiten	5	4	20
Individuell gestaltbare Auswertungen	5	4	20
zusätzliche Kontrollen (benutzerdefinierte, konzerninterne Kontrollen)	5	4	20

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

Einbindungsmöglichkeit weiterer Attribute (Anforderungsart, Instrumententyp)	4	3	12
Nachvollziehbarkeits-/Workflowanforderungen			97 (von 112)
Protokollierung (Sicherstellung der Nachvollziehbarkeit)	5	4	20
Historisierung der Kontrollergebnisse	5	4	20
Durchführbarkeit von Self Assessment	3	3	9
Möglichkeit zur Kommentierung/Nachverfolgung bei Grenzüberschreitung	3	3	9
Workflow zur Erfassung/Bearbeitung/Bestätigung von Steuerungs-/Überwachungsinstrumenten	5	3	15
Automatische Nachverfolgung von Prüfungsfeststellungen (Workflow)	4	3	12
Automatisierte Kontrollen von Grenzüberschreitungen anhand hinterlegter Regeln aus den importierten Daten	3	4	12
Überwachung des Internen Kontrollsystems (Revision)			32 (von 40)
Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor	2	4	8
Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor offline (optional)	2	0	0
Prüfungsplanung zur Wirksamkeit der Steuerungs-/Überwachungsinstrumente	2	4	8
Übersicht zu Stand der Aktualisierung des IKS	2	4	8
Übersicht der Ergebnisse der Wirksamkeitsprüfung	2	4	8
Gesamtpunkteanzahl			445

mögliche Gesamtpunkte

560

Technische Evaluierung

Evaluierungsbogen für IKS Tools

technische Evaluierung

Evaluierungsbogen technische Anforderungen eines IKS für die Austrian Airlines AG

Applikation		BWiSe	
Prüfung abgeschlossen am		29.04.2011	
Kriterium	Priorität	Bewertung	Produkt
Systemplattform			140 von (140)
IT Infrastruktur Server			
Windows Server 2003	5	4	20
Windows Server 2008	5	4	20
Microsoft SQL Server 2005	5	4	20
IT Infrastruktur Client			
Windows XP	5	4	20
Windows 7	5	4	20
Microsoft Office 2003	5	4	20
Microsoft Office 2010	5	4	20
Methodikhandbuch			32 von (32)
Quickinfo	4	4	16
Benutzerfreundlichkeit des Methodikbuches	4	4	16
Software			40 von (60)
Einführungsaufwand	3	4	12
Skalierbarkeit	4	4	16
Concurrent-Lizenzmodell	5	0	0
LDAP Schnittstelle bezüglich Autorisierung	3	4	12
Sicherheit			52 von (52)
Datensicherheit (Verschlüsselung)	4	4	16
Datensicherung (Gesamtspiegelung)	4	4	16
Zugriffsbeschränkungen	5	4	20
Sonstiges			40 von (52)
Support im geographischen Umfeld	3	2	6
Helpdesk (Telefon, Webbasiert)	3	3	9
Durchschnittliche Antwortzeiten auf Anfragen	3	3	9
Wartungsvertrag	4	4	16
Systemanforderungen			12 von (12)
derzeitige Systemvoraussetzungen im Unternehmen			
Intel Core 2 Duo, Intel Core i3/i5			
3 GB Arbeitsspeicher			
250 GB HDD			

Evaluierungsbogen für IKS Tools

technische Evaluierung

<i>minimale Systemanforderungen</i>	3	4	12
Dual Prozessor			
3 GB RAM			
1,5 GB HDD am Applikations- und Reportingserver			
10 GB HDD am Datenbankserver			

Gesamtpunkteanzahl	316
---------------------------	------------

mögliche Gesamtpunkte

162996

Finanzielle Evaluierung

Evaluierungsbogen für IKS Tools

finanzielle Evaluierung

Evaluierungsbogen finanzielle Anforderungen eines IKS für die Austrian Airlines AG

Applikation	BWise
Prüfung abgeschlossen am	29.04.2011

Kriterium	Priorität	Bewertung	Produkt
Kosten			49 (von 60)
Anschaffungskosten	5	3	15
Betriebskosten	3	4	12
Wartungskosten	3	2	6
Customizingkosten	4	4	16

Gesamtpunkteanzahl	49
	mögliche Gesamtpunkte
	60

13.1.3 Oracle GRC

Evaluierungsbogen für IKS Tools

Gesamtevaluierung

Evaluierung zur Auswahl eines Internen Kontrollsystems

Unternehmen **Austrian Airlines AG**
 Evaluierer **Christoph Brandner**

Applikation **Oracle GRC**

Gesamtbewertung

	Bewertung	Blockgewichtung in %	Bewertung nach der Eval.gewichtung
funktionale Evaluierung	74,59%	33,3%	24,86%
technische Evaluierung	90,10%	33,3%	30,03%
finanzielle Evaluierung	48,33%	33,3%	16,11%
		100%	71,01%

Hinweis bezüglich der Bewertung und der Auswertung

Legend für die Bewertung

Multifaktorenmethode	Bewertung	
	min. Punkte	0
	max. Punkte	4
	Priorität	
	min. Punkte	1
	max. Punkte	5

Die detaillierte Beschreibung der Punktevergabe ist in der Diplomarbeit ("Ein Evaluierungsmodell zur Auswahl eines Internen Kontrollsystems und dessen Test bei der Austrian Airlines AG") nachzulesen.

funktionale Evaluierung

Evaluierungsbeginn **01.02.2011**
 Evaluierungsende **29.04.2011**

Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
generelle Anforderungen	71,15%	20%	14,23%
Kundenanforderungen	66,48%	20%	13,30%
Customizinganforderungen	84,21%	10%	8,42%
Nachvollziehbarkeits-/Workflowanforderungen	73,21%	20%	14,64%
Überwachung des Internen Kontrollsystems (Revision)	80,00%	30%	24,00%
		100%	74,59%

Anmerkung:

Ein Evaluierungsmodell zur Auswahl eines IT Systems zur Unterstützung eines Internen
Kontrollsystems und dessen Test bei der Austrian Airlines AG 133

Evaluierungsbogen für IKS Tools

Gesamtevaluierung

technisch Evaluierung			
Evaluierungsbeginn	01.02.2011		
Evaluierungsende	29.04.2011		
Block	normierte Bewertung	Blockgewich- tung in %	Bewertung nach der Blockgewichtung
Systemplattform	78,57%	20%	15,71%
Methodikhandbuch	62,50%	11%	6,88%
Software	80,00%	22%	17,60%
Sicherheit	84,62%	10%	8,46%
Sonstiges	80,77%	17%	13,73%
Systemanforderungen	100,00%	20%	20,00%
		100%	82,38%
Anmerkung:			

finanzielle Evaluierung			
Evaluierungsbeginn	01.02.2011		
Evaluierungsende	29.04.2011		
Block	normierte Bewertung	Blockgewich- tung in %	Bewertung nach der Blockgewichtung
Kosten	48,33%	100%	48,33%
		100%	48,33%
Anmerkung:			

Funktionale Evaluierung

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

Evaluierungsbogen
funktionale Anforderungen eines IKS für die Austrian Airlines AG

<i>Applikation</i>		Oracle GRC	
<i>Prüfung abgeschlossen am</i>		29.04.2011	
Kriterium	Priorität	Bewertung	Produkt
generelle Anforderungen			111 (von 156)
Benutzer-Rollenkonzept (Berechtigungen, ...)	4	4	16
Einhaltung von Compliance-Vorgaben (BilMoG, URÄG, RLÄG, ...)	5	4	20
Integration von Microsoft Standardsoftware			
MS Word	5	3	15
MS Excel	5	3	15
MS Outlook	5	3	15
MS Exchange	5	0	0
MS SharePoint	5	4	20
Benutzerfreundlichkeit (easy-to-use for Clients) auf Basis von Standards (z.B. ISO Norm 9241)	5	2	10
Kundenanforderungen			117 (von 176)
Webbrowserbasierter Clientzugang (ab Version)			
Internet Explorer 7	5	4	20
Mozilla Firefox 3.5	5	3	15
Kompatibel zu Adonis	5	1	5
Datenübernahme aus operativen Systemen			
SAP	3	1	3
Vorhandener Katalog mit Standard-Kontrollen zu SAP	3	1	3
Verlinkung zum Risikomanagement (IKS-Instrument Risiken zuordnen)			
R2C - Risk to change (Schleupen AG)	3	1	3
Anfügen von Dateien/Links	3	4	12
Event-Management (Reminderfunktionen, E-Mailnotifikation...)	5	4	20
Umfrage-Management	4	4	16
Feedbackschleife im Bezug auf Prozess, Risiko und Kontrolle (Plan - Do - Check - Act)	5	4	20
Möglichkeit zur zentralen Vorgabe der Benennung der Steuerungs-/Überwachungsinstrumente	3	0	0
Customizinganforderungen			64 (von 76)
Konfigurierbarkeit und Anpassungsmöglichkeiten	5	4	20
Individuell gestaltbare Auswertungen	5	4	20
zusätzliche Kontrollen (benutzerdefinierte, konzerninterne Kontrollen)	5	4	20

Ein Evaluierungsmodell zur Auswahl eines IT Systems zur Unterstützung eines Internen
Kontrollsystems und dessen Test bei der Austrian Airlines AG 135

Evaluierungsbogen für IKS Tools		funktionale Evaluierung	
Einbindungsmöglichkeit weiterer Attribute (Anforderungsart, Instrumententyp)	4	1	4
Nachvollziehbarkeits-/Workflowanforderungen			82 (von 112)
Protokollierung (Sicherstellung der Nachvollziehbarkeit)	5	4	20
Historisierung der Kontrollergebnisse	5	4	20
Durchführbarkeit von Self Assessment	3	3	9
Möglichkeit zur Kommentierung/Nachverfolgung bei Grenzüberschreitung	3	4	12
Workflow zur Erfassung/Bearbeitung/Bestätigung von Steuerungs-/Überwachungsinstrumenten	5	2	10
Automatische Nachverfolgung von Prüfungsfeststellungen (Workflow)	4	2	8
Automatisierte Kontrollen von Grenzüberschreitungen anhand hinterlegter Regeln aus den importierten Daten	3	1	3
Überwachung des Internen Kontrollsystems (Revision)			32 (von 40)
Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor	2	4	8
Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor offline (optional)	2	0	0
Prüfungsplanung zur Wirksamkeit der Steuerungs-/Überwachungsinstrumente	2	4	8
Übersicht zu Stand der Aktualisierung des IKS	2	4	8
Übersicht der Ergebnisse der Wirksamkeitsprüfung	2	4	8
Gesamtpunkteanzahl			406
	mögliche Gesamtpunkte		560

Technische Evaluierung

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

Evaluierungsbogen technische Anforderungen eines IKS für die Austrian Airlines AG

<i>Applikation</i>		Oracle GRC	
<i>Prüfung abgeschlossen am</i>		29.04.2011	
Kriterium	Priorität	Bewertung	Produkt
Systemplattform			110 von (140)
IT Infrastruktur Server			
Windows Server 2003	5	4	20
Windows Server 2008	5	1	5
Microsoft SQL Server 2005	5	4	20
IT Infrastruktur Client			
Windows XP	5	4	20
Windows 7	5	4	20
Microsoft Office 2003	5	4	20
Microsoft Office 2010	5	1	5
Methodikhandbuch			20 von (32)
Quickinfo	4	3	12
Benutzerfreundlichkeit	4	2	8
Software			48 von (60)
Einführungsaufwand	3	0	0
Skalierbarkeit	4	4	16
Concurrent-Lizenzmodell	5	4	20
LDAP Schnittstelle bezüglich Autorisierung	3	4	12
Sicherheit			44 von (52)
Datensicherheit (Verschlüsselung)	4	2	8
Datensicherung (Gesamtspiegelung)	4	4	16
Zugriffsbeschränkungen	5	4	20
Sonstiges			42 von (52)
Support im geographischen Umfeld	3	4	12
Helpdesk (Telefon, Webbasiert)	3	4	12
Durchschnittliche Antwortzeiten auf Anfragen	3	2	6
Wartungsvertrag	4	3	12
Systemanforderungen			12 von (12)
<i>derzeitige Systemvoraussetzungen im Unternehmen</i>			
Intel Core 2 Duo, Intel Core i3/i5			
3 GB Arbeitsspeicher			
250 GB HDD			

Ein Evaluierungsmodell zur Auswahl eines IT Systems zur Unterstützung eines Internen
Kontrollsystems und dessen Test bei der Austrian Airlines AG 137

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

<i>minimale Systemanforderungen</i>	3	4	12
3 GB RAM			
40 GB HDD			
Database min. 1,5GB			
2 GB HDD Space für Temporäre Dateien			
Oracle E-Business Suite (12, 11.5.9, 11.5.10, 11.5.7)			
Oracle Client Version (9.2.0.1 oder höher)			
Oracle Database 9i (oder höher)			
Apache Tomcat 5.0			

Gesamtpunkteanzahl	276
mögliche Gesamtpunkte	162996

Finanzielle Evaluierung

Evaluierungsbogen für IKS Tools

finanzielle Evaluierung

**Evaluierungsbogen
finanzielle Anforderungen eines IKS für die Austrian Airlines AG**

<i>Applikation</i>	Oracle GRC
<i>Prüfung abgeschlossen am</i>	29.04.2011

Kriterium	Priorität	Bewertung	Produkt
Kosten			29 (von 60)
Anschaffungskosten	5	2	10
Betriebskosten	3	3	9
Wartungskosten	3	2	6
Customizingkosten	4	1	4

Gesamtpunkteanzahl	29
	mögliche Gesamtpunkte

60

13.1.4 RSA Archer

Evaluierungsbogen für IKS Tools

Gesamtevaluierung

Evaluierung zur Auswahl eines Internen Kontrollsystems

Unternehmen **Austrian Airlines AG**
Evaluierer **Christoph Brandner**

Applikation **RSA Archer**

Gesamtbewertung

	Bewertung	Blockgewich- tung in %	Bewertung nach der Eval.gewichtung
funktionale Evaluierung	61,82%	33,3%	20,61%
technische Evaluierung	36,56%	33,3%	12,19%
finanzielle Evaluierung	0,00%	33,3%	0,00%
		100%	32,79%

Hinweis bezüglich der Bewertung und der Auswertung

Legend für die Bewertung

Multifaktorenmethode	Bewertung	
	min. Punkte	0
	max. Punkte	4
	Priorität	
	min. Punkte	1
	max. Punkte	5

Die detaillierte Beschreibung der Punktevergabe ist in der Diplomarbeit ("Ein Evaluierungsmodell zur Auswahl eines Internen Kontrollsystems und dessen Test bei der Austrian Airlines AG") nachzulesen.

funktionale Evaluierung

Evaluierungsbeginn **01.02.2011**
Evaluierungsende **29.04.2011**

Block	normierte Bewertung	Blockgewich- tung in %	Bewertung nach der Blockgewichtung
generelle Anforderungen	83,97%	20%	16,79%
Kundenanforderungen	74,43%	20%	14,89%
Customizinganforderungen	63,16%	10%	6,32%
Nachvollziehbarkeits-/Workflowanforderungen	74,11%	20%	14,82%
Überwachung des Internen Kontrollsystems (Revision)	30,00%	30%	9,00%
		100%	61,82%

Anmerkung:

Mir wurde zu Beginn mitgeteilt, dass ich keine Logindaten und keine Online-Demo erhalte, da ich kein Kunde bin.
Leider sind sämtliche Foren nur für Member zugänglich.
Zahlreiche Informationen stammen von Youtube.com

Evaluierungsbogen für IKS Tools

Gesamtevaluierung

technisch Evaluierung			
Evaluierungsbeginn	01.02.2011		
Evaluierungsende	29.04.2011		
Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
Systemplattform	82,14%	20%	16,43%
Methodikhandbuch	0,00%	11%	0,00%
Software	25,00%	22%	5,50%
Sicherheit	38,46%	10%	3,85%
Sonstiges	63,46%	17%	10,79%
Systemanforderungen	0,00%	20%	0,00%
		100%	36,56%
Anmerkung: Nach weiteren Anfragen bekam ich keine Antwort, daher ist die technische Evalierung bereits sehr lückenhaft. Ab diesem Punkt in der Evaluierung gab es kein Weiterkommen mehr. Daher scheidet das Tool aus.			

finanzielle Evaluierung			
Evaluierungsbeginn			
Evaluierungsende			
Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
Kosten	0,00%	100%	0,00%
		100%	0,00%
Anmerkung: 			

Funktionale Evaluierung

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

Evaluierungsbogen funktionale Anforderungen eines IKS für die Austrian Airlines AG

Applikation		RSA Archer	
Prüfung abgeschlossen am		29.04.2011	
Kriterium	Priorität	Bewertung	Produkt
generelle Anforderungen			131 (von 156)
Benutzer-Rollenkonzept (Berechtigungen, ...)	4	4	16
Einhaltung von Compliance-Vorgaben (BilMoG, URÄG, RLÄG, ...)	5	4	20
Integration von Microsoft Standardsoftware			
MS Word	5	4	20
MS Excel	5	4	20
MS Outlook	5	3	15
MS Exchange	5	4	20
MS SharePoint	5	4	20
Benutzerfreundlichkeit (easy-to-use for Clients) auf Basis von Standards (z.B. ISO Norm 9241)	5	0	0
Kundenanforderungen			131 (von 176)
Webbrowserbasierter Clientzugang (ab Version)			
Internet Explorer 7	5	4	20
Mozilla Firefox 3.5	5	4	20
Kompatibel zu Adonis	5	2	10
Datenübernahme aus operativen Systemen			
SAP	3	3	9
Vorhandener Katalog mit Standard-Kontrollen zu SAP	3	3	9
Verlinkung zum Risikomanagement (IKS-Instrument Risiken zuordnen)			
R2C - Risk to change (Schleupen AG)	3	2	6
Anfügen von Dateien/Links	3	1	3
Event-Management (Reminderfunktionen, E-Mailnotifikation...)	5	3	15
Umfrage-Management	4	4	16
Feedbackschleife im Bezug auf Prozess, Risiko und Kontrolle (Plan - Do - Check - Act)	5	4	20
Möglichkeit zur zentralen Vorgabe der Benennung der Steuerungs-/Überwachungsinstrumente	3	1	3
Customizinganforderungen			48 (von 76)
Konfigurierbarkeit und Anpassungsmöglichkeiten	5	2	10
Individuell gestaltbare Auswertungen	5	3	15
zusätzliche Kontrollen (benutzerdefinierte, konzerninterne Kontrollen)	5	3	15

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

Einbindungsmöglichkeit weiterer Attribute (Anforderungsart, Instrumententyp)	4	2	8
Nachvollziehbarkeits-/Workflowanforderungen			83 (von 112)
Protokollierung (Sicherstellung der Nachvollziehbarkeit)	5	3	15
Historisierung der Kontrollergebnisse	5	4	20
Durchführbarkeit von Self Assessment	3	4	12
Möglichkeit zur Kommentierung/Nachverfolgung bei Grenzüberschreitung	3	1	3
Workflow zur Erfassung/Bearbeitung/Bestätigung von Steuerungs-/Überwachungsinstrumenten	5	4	20
Automatische Nachverfolgung von Prüfungsfeststellungen (Workflow)	4	1	4
Automatisierte Kontrollen von Grenzüberschreitungen anhand hinterlegter Regeln aus den importierten Daten	3	3	9
Überwachung des Internen Kontrollsystems (Revision)			12 (von 40)
Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor	2	1	2
Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor offline (optional)	2	0	0
Prüfungsplanung zur Wirksamkeit der Steuerungs-/Überwachungsinstrumente	2	1	2
Übersicht zu Stand der Aktualisierung des IKS	2	1	2
Übersicht der Ergebnisse der Wirksamkeitsprüfung	2	3	6
Gesamtpunkteanzahl			405
	mögliche Gesamtpunkte		560

Technische Evaluierung

Evaluierungsbogen für IKS Tools

technische Evaluierung

Evaluierungsbogen technische Anforderungen eines IKS für die Austrian Airlines AG

Applikation		RSA Archer	
Prüfung abgeschlossen am		29.04.2011	
Kriterium	Priorität	Bewertung	Produkt
Systemplattform			115 von (140)
IT Infrastruktur Server			
Windows Server 2003	5	3	15
Windows Server 2008	5	3	15
Microsoft SQL Server 2005	5	3	15
IT Infrastruktur Client			
Windows XP	5	4	20
Windows 7	5	4	20
Microsoft Office 2003	5	3	15
Microsoft Office 2010	5	3	15
Methodikhandbuch			0 von (32)
Quickinfo	4	-	0
Benutzerfreundlichkeit des Methodikbuches	4	-	0
Software			15 von (60)
Einführungsaufwand	3	-	0
Skalierbarkeit	4	-	0
Concurrent-Lizenzmodell	5	-	0
LDAP Schnittstelle bezüglich Autorisierung	3	5	15
Sicherheit			20 von (52)
Datensicherheit (Verschlüsselung)	4	-	0
Datensicherung (Gesamtspiegelung)	4	-	0
Zugriffsbeschränkungen	5	4	20
Sonstiges			33 von (52)
Support im geographischen Umfeld	3	3	9
Helpdesk (Telefon, Webbasiert)	3	4	12
Durchschnittliche Antwortzeiten auf Anfragen	3	0	0
Wartungsvertrag	4	3	12
Systemanforderungen			0 von (12)
derzeitige Systemvoraussetzungen im Unternehmen			
Intel Core 2 Duo, Intel Core i3/i5			
3 GB Arbeitsspeicher			
250 GB HDD			

Evaluierungsbogen für IKS Tools

technische Evaluierung

minimale Systemanforderungen

3

-

0

Gesamtpunkteanzahl**183**

mögliche Gesamtpunkte

348

Finanzielle Evaluierung

Dieser Evaluierungsschritt wurde nicht mehr durchgeführt, da bereits in einem vorgelagerten Evaluierungsschritt die KO Kriterien nicht ausreichend erfüllt werden konnten.

Evaluierungsbogen für IKS Tools

finanzielle Evaluierung

Evaluierungsbogen finanzielle Anforderungen eines IKS für die Austrian Airlines AG

Applikation	RSA Archer
Prüfung abgeschlossen am	

Kriterium	Priorität	Bewertung	Produkt
Kosten			0 (von 60)
Anschaffungskosten	3	-	0
Betriebskosten	5	-	0
Wartungskosten	3	-	0
Customizingkosten	4	-	0

Gesamtpunkteanzahl	0
---------------------------	----------

mögliche Gesamtpunkte

60

13.1.5 SAP GRC

Evaluierungsbogen für IKS Tools

Gesamtevaluierung

Evaluierung zur Auswahl eines Internen Kontrollsystems

Unternehmen	Austrian Airlines AG
Evaluierer	Christoph Brandner
Applikation	SAP GRC

Gesamtbewertung

	Bewertung	Blockgewichtung in %	Bewertung nach der Eval.gewichtung
funktionale Evaluierung	85,39%	33,3%	28,46%
technische Evaluierung	76,51%	33,3%	25,50%
finanzielle Evaluierung	40,00%	33,3%	13,33%
		100%	67,30%

Hinweis bezüglich der Bewertung und der Auswertung

Legend für die Bewertung

Multifaktorenmethode	Bewertung	
	min. Punkte	0
	max. Punkte	4
	Priorität	
	min. Punkte	1
	max. Punkte	5

Die detaillierte Beschreibung der Punktevergabe ist in der Diplomarbeit ("Ein Evaluierungsmodell zur Auswahl eines Internen Kontrollsystems und dessen Test bei der Austrian Airlines AG") nachzulesen.

funktionale Evaluierung

Evaluierungsbeginn	01.02.2011
Evaluierungsende	29.04.2011

Block	normierte Bewertung	Blockgewichtung in %	Bewertung nach der Blockgewichtung
generelle Anforderungen	90,38%	20%	18,08%
Kundenanforderungen	84,09%	20%	16,82%
Customizinganforderungen	88,16%	10%	8,82%
Nachvollziehbarkeits-/Workflowanforderungen	88,39%	20%	17,68%
Überwachung des Internen Kontrollsystems (Revision)	80,00%	30%	24,00%
		100%	85,39%

Anmerkung:

Ein Evaluierungsmodell zur Auswahl eines IT Systems zur Unterstützung eines Internen
Kontrollsystems und dessen Test bei der Austrian Airlines AG 147

Evaluierungsbogen für IKS Tools

Gesamtevaluierung

technisch Evaluierung			
Evaluierungsbeginn	01.02.2011		
Evaluierungsende	29.04.2011		
Block	normierte Bewertung	Blockgewich- tung in %	Bewertung nach der Blockgewichtung
Systemplattform	85,71%	20%	17,14%
Methodikhandbuch	62,50%	11%	6,88%
Software	63,33%	22%	13,93%
Sicherheit	38,46%	10%	3,85%
Sonstiges	86,54%	17%	14,71%
Systemanforderungen	100,00%	20%	20,00%
		100%	76,51%
Anmerkung:			
Unter http://help.sap.com/ konnte man beinahe keine Dokumente öffnen, wenn man dafür keine Berechtigung (Benutzererkennung, Passwort) hat. Auf Anfrage bei SAP wurde mir ein Zugang verwehrt (Mail vom 11.03.2011).			

finanzielle Evaluierung			
Evaluierungsbeginn	01.02.2011		
Evaluierungsende	29.04.2011		
Block	normierte Bewertung	Blockgewich- tung in %	Bewertung nach der Blockgewichtung
Kosten	40,00%	100%	40,00%
		100%	40,00%
Anmerkung:			

Funktionale Evaluierung

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

Evaluierungsbogen
funktionale Anforderungen eines IKS für die Austrian Airlines AG

<i>Applikation</i>		SAP GRC	
<i>Prüfung abgeschlossen am</i>		29.04.2011	
Kriterium	Priorität	Bewertung	Produkt
generelle Anforderungen			141 (von 156)
Benutzer-Rollenkonzept (Berechtigungen, ...)	4	4	16
Einhaltung von Compliance-Vorgaben (BilMoG, URÄG, RLÄG, ...)	5	3	15
Integration von Microsoft Standardsoftware			
MS Word	5	4	20
MS Excel	5	4	20
MS Outlook	5	4	20
MS Exchange	5	4	20
MS SharePoint	5	4	20
Benutzerfreundlichkeit (easy-to-use for Clients) auf Basis von Standards (z.B. ISO Norm 9241)	5	2	10
Kundenanforderungen			148 (von 176)
Webbrowserbasierter Clientzugang (ab Version)			
Internet Explorer 7	5	4	20
Mozilla Firefox 3.5	5	4	20
Kompatibel zu Adonis	5	2	10
Datenübernahme aus operativen Systemen			
SAP	3	4	12
Vorhandener Katalog mit Standard-Kontrollen zu SAP	3	4	12
Verlinkung zum Risikomanagement (IKS-Instrument Risiken zuordnen)			
R2C - Risk to change (Schleupen AG)	3	2	6
Anfügen von Dateien/Links	3	3	9
Event-Management (Reminderfunktionen, E-Mailnotifikation...)	5	4	20
Umfrage-Management	4	4	16
Feedbackschleife im Bezug auf Prozess, Risiko und Kontrolle (Plan - Do - Check - Act)	5	4	20
Möglichkeit zur zentralen Vorgabe der Benennung der Steuerungs-/Überwachungsinstrumente	3	1	3
Customizinganforderungen			67 (von 76)
Konfigurierbarkeit und Anpassungsmöglichkeiten	5	4	20
Individuell gestaltbare Auswertungen	5	4	20
zusätzliche Kontrollen (benutzerdefinierte, konzerninterne Kontrollen)	5	3	15

Ein Evaluierungsmodell zur Auswahl eines IT Systems zur Unterstützung eines Internen
Kontrollsystems und dessen Test bei der Austrian Airlines AG 149

Evaluierungsbogen für IKS Tools

funktionale Evaluierung

Einbindungsmöglichkeit weiterer Attribute (Anforderungsart, Instrumententyp)	4	3	12
Nachvollziehbarkeits-/Workflowanforderungen			99 (von 112)
Protokollierung (Sicherstellung der Nachvollziehbarkeit)	5	4	20
Historisierung der Kontrollergebnisse	5	4	20
Durchführbarkeit von Self Assessment	3	4	12
Möglichkeit zur Kommentierung/Nachverfolgung bei Grenzüberschreitung	3	3	9
Workflow zur Erfassung/Bearbeitung/Bestätigung von Steuerungs-/Überwachungsinstrumenten	5	2	10
Automatische Nachverfolgung von Prüfungsfeststellungen (Workflow)	4	4	16
Automatisierte Kontrollen von Grenzüberschreitungen anhand hinterlegter Regeln aus den importierten Daten	3	4	12
Überwachung des Internen Kontrollsystems (Revision)			32 (von 40)
Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor	2	4	8
Erfassen der Wirksamkeitsprüfung der Steuerungs-/Überwachungsinstrumente (Aufbau-/Funktionsprüfung) durch Auditor offline (optional)	2	0	0
Prüfungsplanung zur Wirksamkeit der Steuerungs-/Überwachungsinstrumente	2	4	8
Übersicht zu Stand der Aktualisierung des IKS	2	4	8
Übersicht der Ergebnisse der Wirksamkeitsprüfung	2	4	8
Gesamtpunkteanzahl			487
	mögliche Gesamtpunkte		560

Technische Evaluierung

Evaluierungsbogen für IKS Tools

technische Evaluierung

Evaluierungsbogen
technische Anforderungen eines IKS für die Austrian Airlines AG

<i>Applikation</i> SAP GRC <i>Prüfung abgeschlossen am</i> 29.04.2011			
Kriterium	Priorität	Bewertung	Produkt
Systemplattform			120 von (140)
IT Infrastruktur Server			
Windows Server 2003	5	4	20
Windows Server 2008	5	4	20
Microsoft SQL Server 2005	5	4	20
IT Infrastruktur Client			
Windows XP	5	4	20
Windows 7	5	3	15
Microsoft Office 2003	5	4	20
Microsoft Office 2010	5	1	5
Methodikhandbuch			20 von (32)
Quickinfo	4	4	16
Benutzerfreundlichkeit des Methodikbuches	4	1	4
Software			38 von (60)
Einführungsaufwand	3	0	0
Skalierbarkeit	4	4	16
Concurrent-Lizenzmodell	5	2	10
LDAP Schnittstelle bezüglich Autorisierung	3	4	12
Sicherheit			20 von (52)
Datensicherheit (Verschlüsselung)	4	-	0
Datensicherung (Gesamtspiegelung)	4	-	0
Zugriffsbeschränkungen	5	4	20
Sonstiges			45 von (52)
Support im geographischen Umfeld	3	4	12
Helpdesk (Telefon, Webbasiert)	3	4	12
Durchschnittliche Antwortzeiten auf Anfragen	3	3	9
Wartungsvertrag	4	3	12
Systemanforderungen			12 von (12)
derzeitige Systemvoraussetzungen im Unternehmen			
Intel Core 2 Duo, Intel Core i3/i5			
3 GB Arbeitsspeicher			
250 GB HDD			

Ein Evaluierungsmodell zur Auswahl eines IT Systems zur Unterstützung eines Internen
Kontrollsystems und dessen Test bei der Austrian Airlines AG 151

Evaluierungsbogen für IKS Tools		technische Evaluierung	
<i>minimale Systemanforderungen</i>		3	4
2 GHz Pentium 4 prozessor 2 GB RAM			12
10,4 GB HDD (ohne Languagepack)			
15,5 GB HDD (mit Languagepack)			
min. Bildschirmauflösung 1024 x 768			
Gesamtpunkteanzahl		255	
		mögliche Gesamtpunkte	162996

Finanzielle Evaluierung

Evaluierungsbogen für IKS Tools

finanzielle Evaluierung

**Evaluierungsbogen
finanzielle Anforderungen eines IKS für die Austrian Airlines AG**

<i>Applikation</i>	SAP GRC
<i>Prüfung abgeschlossen am</i>	29.04.2011

Kriterium	Priorität	Bewertung	Produkt
Kosten			24 (von 60)
Anschaffungskosten	5	1	5
Betriebskosten	3	4	12
Wartungskosten	3	1	3
Customizingkosten	4	1	4

Gesamtpunkteanzahl	24
	mögliche Gesamtpunkte

60

13.2 Cobit 4.1 – Maturity Attribute Table

Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement
1 Recognition of the need for the process is emerging. There is sporadic communication of the issues.	There are ad hoc approaches to processes and practices. The processes and policies are undefined.	Some tools may exist; e.g. spreadsheets, desktop tools. There is no planned approach to the tool usage.	Skills required for the process are not identified. A training plan does not exist and no formal training occurs.	There is no definition of responsibility. People take ownership of issues based on their own initiative on a reactive basis.	Goals are not clear and no measurement takes place.
2 There is awareness of the need to act. Management communicates the overall issues.	Similar and common processes emerge, but are largely intuitive because of individual expertise. Some aspects of the process are repeatable because of individual expertise, and some documentation and informal understanding of policy and procedures may exist.	Common approaches to use of tools exist but are developed by key individuals. Vendor tools may have been acquired, but are probably not applied correctly, and may even be shelfware.	Minimum skill requirements are identified for critical areas. Training is provided in response to needs, either on the basis of an agreed plan, and informal training on the job occurs.	An individual assumes his/her responsibility and is usually held accountable, even if this is not formally defined. There is no discussion about responsibility when problems occur, and a culture of blame tends to exist.	Some goal setting occurs; some financial measures are established but are known only by senior management. There is no consistent monitoring in isolated areas.
3 There is understanding of the need to act. Management's more formal and structured in its communication.	Usage of good practices emerges. The process, policies and procedures are defined and documented for all key activities.	A plan has been defined for use and standardisation of tools to automate the process. Tools are being used for their basic purposes, but may not all be in accordance with the agreed plan, and may not be integrated with one another.	Skill requirements are defined and documented for all areas. A formal training plan has been developed but formal training is still based on individual initiatives.	Process responsibility and accountability are defined and documented for all areas. The process owner is unlikely to have the full authority to override the responsibilities.	Some effectiveness goals and measures are set, but are not consistently achieved. A clear link to business goals. Measurement processes emerge, but are not consistently applied. IT balanced scorecard is being adopted, as is occasional intuitive application of root cause analysis.
4 There is understanding of the full requirements. Mature communication techniques are applied and standard communication tools are in use.	The process is sound and complete; intended best practices are applied. All aspects of the process are documented and repeatable. Policies have been developed and applied. Standards for developing and maintaining the processes and procedures are adopted and followed.	Tools are implemented according to a standardised plan, and some have been integrated with other related tools. Tools are being used in accordance with the agreed plan, and are being used to manage the process and monitor critical activities and controls.	Skill requirements are routinely updated for all areas, proficiency is assured for all critical areas, and certification is encouraged. Mature training techniques are applied to the training plan, and knowledge sharing is encouraged. All internal domain experts are involved, and the effectiveness of the training plan is assessed.	Process responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	Effectivity and effectiveness are measured and communicated and linked to business goals and the IT strategic plan. The IT balanced scorecard is implemented in some areas with exceptions. Root cause analysis and root cause analysis is being standardised. Continuous improvement is emerging.
5 There is advanced forward-looking understanding of requirements. Proactive communication of issues based on trends exists, mature communication techniques are applied and integrated communication tools are in use.	External best practices and standards are applied. Process documentation is evolved to automate workflows. Processes, policies and procedures are standardised and integrated to enable end to end management and improvement.	Standardised toolsets are used across the enterprise. Tools are fully integrated with other related tools to enable end-to-end support of the processes. Tools are being used to support improvement of the process and automatically detect control exceptions.	The organisation formally encourages continuous improvement of skills, based on clearly defined personal and organisational goals. Training and education support external best practices and use of coding code concepts and techniques. Knowledge sharing is an enterprise wide requirement. Systems are being deployed. External experts and industry leaders are used for guidance.	Process owners are empowered to make decisions and take action. The process owner has cascaded down throughout the organisation in a consistent fashion.	There is an integrated performance measurement system linking IT performance to business goals. The IT balanced scorecard, exceptions are globally and consistently noted by management; are root cause analysis is applied. Continuous improvement is a way of life.

Fig. 30. C 4.1 – Maturity Attribute Table⁶⁴

⁶⁴ Vgl. [Gov07] Seite 21

13.3 Cobit 4.1 – Maturity Model for Internal Control

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Non-existent	There is no recognition of the need for internal control. Control is not part of the organisation's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/ <i>ad hoc</i>	There is some recognition of the need for internal control. The approach to risk and control requirements is <i>ad hoc</i> and disorganised, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an <i>ad hoc</i> basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritised or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and are adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. Whilst management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organised occasionally.
5 Optimised	An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes, and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organisation benchmarks to external good practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

Fig. 31. Cobit 4.1 – Maturity Model for Internal Control⁶⁵

⁶⁵ Vgl. [Gov07] Seite 175

LEBENS LAUF



Persönliche Daten

Christoph BRANDNER, BSc.

Geburtsdaten: 16. Dezember 1983, in Waidhofen/Ybbs
Familienstand: ledig
Nationalität: Österreich
Adresse: 1120 Wien, Aichhorngasse 16/7
Telefon: +43 (0) 650 / 85 14 670
E-Mail: brandner_chris@gmx.net

Schulbildung

1990 – 1994 Volksschule Weyer (Oberösterreich)
1994 – 1998 Hauptschule Weyer (Oberösterreich)
1998 – 2003 Bundeshandelsakademie Waidhofen/Ybbs (Niederösterreich)

Akademische Ausbildung

10/2005 – 02/2009 Bakkalaureatsstudium Wirtschaftsinformatik an der Technischen Universität Wien
abgeschlossen am 11.02.2009
03/2009 – heute Masterstudium Wirtschaftsinformatik an der Universität Wien
voraussichtlicher Abschluss: Sommer 2011

Berufliche Tätigkeiten

05/2004 – 08/2004 BMW Motoren Werke Steyr
03/2005 – 08/2005 Fa. Gasser GmbH im Motorenwerk BMW in Steyr
2006 – 2010 jeweils mehrmonatiges Praktikum im Sommer im Versicherungsbüro Brandner Weyer

Wehrdienst

09/2003 – 04/2004 Stabskompanie Pionierbataillon 3, Kaserne Melk

Auslandsaufenthalt

09/2004 – 03/2005 Auslandsaufenthalt in Australien