Information Systems Audit and Control Association

News Letter

Nr. 68, April 2004

Thema IT-Governance

Switzerland Chapter
Germany Chapter
Austria Chapter

© 13.4.2004

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o Monika Josi
Novartis Animal Health
Global Information Technology
WRO-1032.1.90
4002 Basel

Redaktion:
Max F. Bretscher
KPMG Fides Peat
Badenerstrasse 172
8026 Zürich

Satz und Gestaltung:
WissensTransfer
Francesca Lüscher Baglioni,
8235 Lohn, SH

Jeder Nachdruck, auch auszugsweise, sowie Vervielfältigungen oder sonstige Verwertung von Texten oder Abbildungen aus dem *NewsLetter* nur mit schriftlicher Genehmigung des Herausgebers unter voller Quellenangabe.

Abo-Preis:
Mitglieder gratis
Abonnemente und Einzelnummern auf Anfrage

Inserate:
1 Seite CHF 400.–
1/2 Seite CHF 240.–
1/4 Seite CHF 160.–

Erscheint 5 Mal jährlich
Auflage: 1100 Exemplare

Nächste Ausgabe
(Thema: euroCACS2004): Juni 2004,
Redaktionsschluss: 14. Mai 2004

Inhaltsverzeichnis

Editorial 4

IT-Governance – Mit IT Werte generieren 5

IT-Governance – IT-Governance bei der Swiss Re 8

IT-Governance – Le débat « Maîtrise d'ouvrage / Maîtrise d'œuvre » du système d'information est-il toujours d'actualité ? 10

IT-Governance – Rosinen aus dem euroCACS2004-Kuchen 12

IT-Governance – Outsourcing der IT: Chancen und Risiken aus Sicht der Revision 14

The ISACA Crossword Puzzle 20

Express Line 22

Forum 23

DACH-News 28

Veranstaltungen 32

Germany Chapter 34

Austria Chapter 35

Switzerland Chapter 36

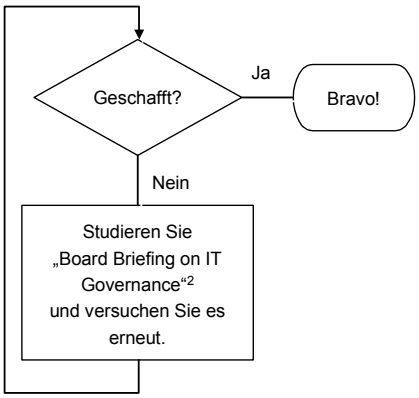
Editorial

„How do I use COBIT to implement IT governance?" steht als Blickfang auf dem Deckblatt der Broschüre IT Governance Implementation Guide[1]. COBIT als Implementierungshilfe? Ist es nicht eher ein Prüfhilfsmittel?

Eigentlich folgerichtig, wie sich die Informatikprüfung in den letzten Jahren entwickelt hat. Weg vom binären und checklistengestützten richtig/ falsch hin zu einem risikoorientierten und konstruktiven Ansatz. Dazu hat COBIT ganz wesentlich beigetragen. Die „Objectives" sind nicht diejenigen des Prüfers, sondern der Verantwortlichen. Plötzlich stellen Geprüfter und Prüfer fest, dass sie im Grunde genommen identische Ziele haben. Zugegeben, oft haben die Ziele nicht die gleiche Priorität. Eine lohnende Herausforderung, gemeinsam herauszufinden, welches nun die richtige objektive Priorität ist. Schon manchem haben diese Auseinandersetzungen die Augen geöffnet.

Wer kennt nicht die variantenreichen und gut begründeten Bedenken gegen die Anforderung, die IT zu „governancen"?

Nach dieser schweren Kost haben Sie eine kleine Pause verdient. Gehen Sie einen Kaffee trinken. Setzen Sie sich zu jemandem an einen Tisch. Und jetzt erläutern Sie ihm oder ihr, was „IT-Governance" ist.



Manchmal – oft Jahre später – trägt die Saat Früchte. Wie in der Natur braucht es dazu gelegentlich äussere Einwirkungen, beispielsweise Frost oder grosse Hitze. Die Umsätze frieren ein, der EBITA fällt unter Null und die Börse kocht. Plötzlich reift die Erkenntnis heran, dass auch Unternehmen etwas zu beherrschen und zu kontrollieren haben. Und nicht nur die IT, sondern das gesamte Unternehmen: „Corporate Governance". IT-Governance bekommt neben den anderen Governance-Elementen eine neue und tragende Bedeutung.

Im vorliegenden *NewsLetter* greifen wir das Thema „IT-Governance" auf und vertiefen es mit interessanten und lesenswerten Beiträgen. Wenn Sie das Thema weiter interessiert, sind Sie herzlich eingeladen, in der IG IT-Governance mitzuarbeiten. Die IG erarbeitet für die COBIT Kontrollziele Messgrössen für ein aussagekräftiges und „governance"-gesteuertes Management Reporting.

Rolf Merz
Koordinator Interessengruppen

1 IT Governance Institute, ISBN 1-893209-60-1, zu beziehen im ISACA-Bookstore
2 IT Governance Institute, ISBN 1-893209-64-4, zu beziehen im ISACA-Bookstore

IT-Governance

Mit IT Werte generieren

Was ist IT-Governance?

IT-Governance ist schlicht und einfach die Erkenntnis, dass nach vierzig Jahren kommerzieller Informatik endlich die Zeit gekommen ist, den Produktionsfaktor Informatik so zu steuern, dass er diejenigen Resultate liefert, die Stakeholder und Führungsebene erwarten.

IT-Governance hat nach heutiger Auffassung und Lehre[1] zwei Hauptrichtungen:

1. Mit IT Werte schaffen
2. IT-Risiken managen

Man sieht auf den ersten Blick, dass sich diese beiden Ziele grundlegend unterscheiden. Während die Thematik „Werte schaffen" eine starke betriebswirtschaftliche Komponente aufweist, ist das Risikothema eher dem Umfeld IT-Sicherheit & Kontrolle zuzuordnen. Während z.B. der Economist von „Cold Killer Application" spricht[2], wenn es um die Transparenz von Kosten/Nutzen-Verhältnissen von IT-Sourcern[3] geht, ist die Risikosicht stark durch Corporate Governance Ideen geprägt.

Inhaltlich ist eine Trennung dieser Aktivitäten nicht immer einfach, manchmal auch nicht sinnvoll. Viel wesentlicher ist die Abgrenzung der Themen aus Sicht des jeweiligen Umsetzers. Es ist ein wichtiger Unterschied, ob man eine fachliche Problemstellung aus Sicht des Revisors oder aus Sicht der Unternehmensführung betrachtet. Hier liegt denn auch der wesentliche Unterschied bei der Aufarbeitung und Umsetzung. Während die Wertediskussionen auf der aktiven Führungsebene stattfinden werden, sind risikofokussierte Problemstellungen eher eine Domäne der Risk-Manager, Revisoren und Juristen. Dieser Artikel konzentriert sich auf den Aspekt der Wertegenerierung.

In einer weltweiten Umfrage des Magazins CIO[4] wurde 2002 festgehalten, dass Nummer-1-Thema der CIOs die „Abstimmung der Geschäftsziele mit der IT, bzw. der IT-Strategie mit dem Geschäft" sei. Die gleichen Resultate wurden in einer Studie der Meta Group im Jahr 2003[5] erarbeitet; vergleichbare Untersuchungen gibt es auch von anderen Analysten.

Der Nutzen von IT-Governance liegt in der nachhaltigen Verbesserung der IT und damit auch einer Verbesserung des Cash-Flow. Im Grunde also einer Verknüpfung des Gedankens des Shareholder/Stakeholder-Value auf der Ebene Informatik.

Herausforderungen

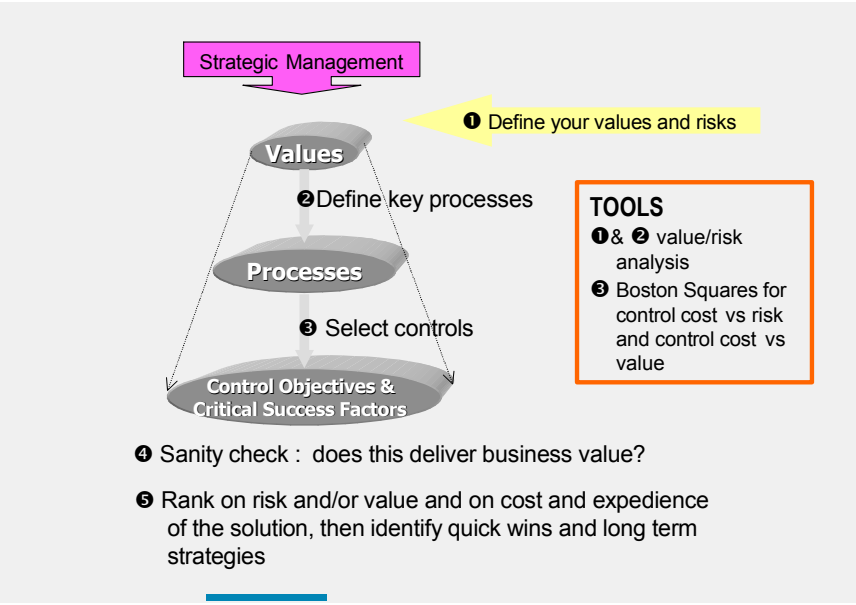
Man kann eine völlig optimierte IT-Abteilung betreiben und trotzdem beklagen sich die Geschäftseinheiten über hohe Kosten, weil ihnen der notwendige Gegenwert nicht geliefert wird. Eine IT-Abteilung kann nach Qualitätsstandards optimiert sein und perfekt funktionieren, trotzdem erhalten die Geschäftseinheiten nicht, was sie verlangen. Es ist demnach ein wesentlicher Unterschied, ob man eine kostenoptimierte IT-Abteilung betreibt, oder ob man einen Wertzuwachs (Cash-Flow) für das Unternehmen erwirtschaftet.

Die meisten Unternehmer und Manager kennen die Probleme aus eigener Erfahrung. 65 % der Informatikprojekte werden nie fertig und die Resultate beinhalten einen Bruchteil dessen, was ursprünglich geplant war. Zeitpläne dienen vor allem dem Verkauf. IT-Sourcer tendieren dazu, Leistungen zu erbringen, die an den wesentlichen Bedürfnissen der Kunden vorbeigehen. Dem gegenüber stehen endlose Diskussionen zwischen Informatikern und Geschäftseinheiten um die Finanzierung immer neuer IT-Vorhaben. Wesentlich für die unbefriedigenden Resultate der Informatik waren auch die Wildwüchse Ende der neunziger Jahre, die dazu geführt hatten, dass jede grössere Geschäftseinheit plötzlich begann, eigene IT-Ressourcen aufzubauen. Im Zuge der Restrukturierungen wird diese Entwicklung nun wieder zurückgefahren. Ob dies in jedem Fall sinnvoll ist, kann man nur beantworten, wenn man IT-Governance betreibt!

Umsetzung von IT-Governance

Wie schafft man es nun, die IT so zu gestalten, dass sie das geforderte Wertpotential freisetzt? Es ist zwingend, dass die IT der Unternehmensentwicklung folgt. IT-Governance-

Massnahmen müssen in den Strategieprozess eingebettet werden. Die Bedeutung der Informationsverarbeitung im Unternehmen ist Schlüsselfaktor für die richtige Umsetzung von IT-Governance-Aktivitäten. Es macht keinen Sinn, dass für Unternehmen, in denen die Informationsverarbeitung keine Schlüsselrolle spielt, die gleichen Aufwendungen getätigt werden, wie in einem Unternehmen, welches von der Informationsverarbeitung als Kernkompetenz lebt. Es ist für ein Unternehmen deshalb bedeutend, dass es einen moderierten Strategieentwicklungsprozess betreibt und die Vision, die Kernkompetenzen und die Strategien kennt. Ein Unternehmen, welches diesen Prozess nicht durchlaufen hat, kann schwerlich ableiten, welche Bedeutung IT in der Organisation besitzt (siehe Abbildung).



© The IT Governance Network 2003

IT-Governance ist demnach Teil der Unternehmensstrategie. Aus den Kernkompetenzen, Werten und dem Unternehmensumfeld leiten sich Strategien und Schlüsselprozesse ab. Diese wiederum werden nach bestimmten Standards abgewickelt, wobei geprüft wird, ob dadurch tatsächlich ein Mehrwert geschaffen wird:

Es ist einleuchtend, dass der „Best-Practice"-Ansatz nicht funktioniert, um Angleichung von Geschäfts- mit der IT-Strategie zu erreichen! Der Best-Practice-Ansatz funktioniert lediglich beim risikoorientierten Ansatz, der sich von unter her entwickelt. Insofern können z.B. Benchmarks zwischen Unternehmen nur dann gemacht werden, wenn sie ähnliche und vergleichbare Strategien verfolgen!

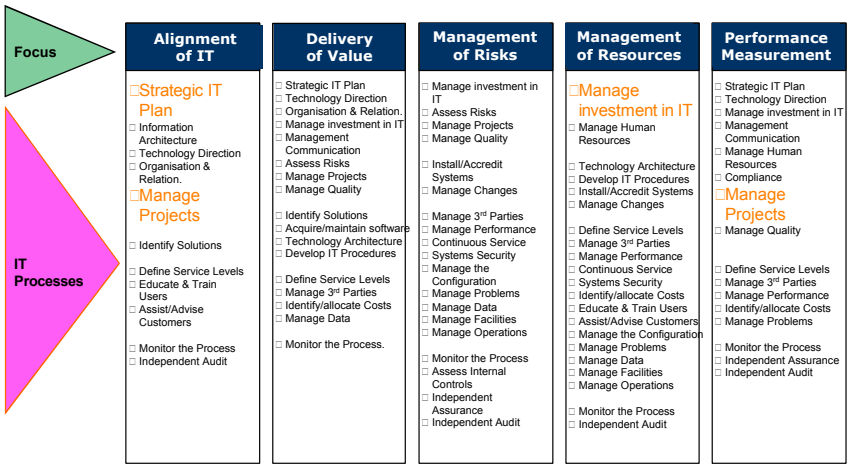
Was bedeutet dies nun für die IT-Führung?

Die folgenden Themen müssen angepackt werden:

- Einbringen von Wert, Kosten und Risiko Management in die IT-Kultur. Portfolio Management, d.h. das Kategorisieren als Kommunikations- und Investitionsoptimierungswerkzeug.
- Ausrollen von Personal-Management-Prozessen zum Erhöhen der Personal-Produktivität. Verbessern der Ausbildung und fördern von Breitenwissen.
- Sicherstellen, dass Schlüsselprozesse qualitativ hochstehend und wiederholbar sind; gut verständlich, konsistent, messbar, skalierbar und permanent verbessernd.
- Überzeugungsarbeit: Die CIOs müssen die Wahrnehmung des Managements verändern, sie müssen dazu sorgen, dass sie als tragendes Element des Geschäfts wahrgenommen werden.

Um die notwendige Vergleichbarkeit und Messbarkeit zu erzielen, bedarf es einer einheitlichen Grundlage. Man kann die erwähnten Ziele nur erreichen, wenn die zu Grunde liegenden IT-Prozesse standardisiert werden. Als Standardwerk dient der COBIT-Katalog[6], welcher auch bezüglich Erfahrung und Anwendung weltweit am meisten Verwendung findet. COBIT kann zur Überprüfung sehr gut eingesetzt werden und definiert einen Mindeststandard und ein Balanced-Scorecard-Modell. Je nach Spezialgebiet sind aber zusätzliche Quellen notwendig, so z.B. die CMM[7], ITIL[8] oder spezifische ISO Standards, wie z.B. ISO 17799 für die IT-Sicherheit.

Die Tabelle in der Abbildung auf der nächsten Seite zeigt die COBIT-Prozesse in Abhängigkeit des angestrebten Ziels/Focus:



"You cannot manage what you cannot measure"

Eine Tatsache, die gerade für die IT zentrale Bedeutung hat. In einer Welt, in welcher sich meist Geschäftsleute und Technokraten gegenübersitzen, haben technische Verwirrspiele System. Zahlen sind hier hilfreich; Messgrössen helfen, abstrakte IT-Verfahren transparent zu machen. Als Methode hat sich das Balanced-Scorecard-Verfahren etabliert, welches sich für solche Anwendungen sehr gut eignet. Das Festlegen der messbaren Grössen ist nicht einfach. Glücklicherweise gibt es hier bereits Vorarbeiten. So enthält COBIT z.B. eine sehr gute Liste mit Kritischen Erfolgsfaktoren, „Key Goal Indicators" und „Key Performance Indicators".

Die Zielbeschreibungen enthalten konkrete Beschreibungen von zu erreichenden Eigenschaften. „Key Performance Indicators" sind Kenngrössen, die über den Weg zum Ziel Auskunft geben, bzw. erlauben, die Fortschritte zu messen. Hinzu kommen kritische Erfolgsfaktoren, die für einen bestimmten Prozess darüber Auskunft geben, welche Faktoren besonders wichtig sind.

Balanced Scorcards (BSC) werden dabei sowohl für die geschäftsorientierten als auch die IT-Ziele beschrieben und kombiniert:

Für die einheitliche Dokumentation und Kommunikation ist ein spezialisiertes Werkzeug von grossem Nutzen.

Ein Unternehmen kann durchaus eigenen Benchmarks setzen, um die Implementierung der IT-Governance zu kontrollieren. Folgende Grafik zeigt eine Auswertung verschiedener IT-Prozesse, basierend auf dem COBIT-Balanced-Scorecard-Modell, mit dem aktuellen Stand und der Abweichung zu den gesetzten Zielen (siehe Abbildung).

Etliche Firmen haben die Zeichen der Zeit erkannt, und IT-Governance nicht nur auf ihre Fahne geschrieben, sondern auch konkret angepackt. Ein Beispiel ist die Swiss Re, wie von Daniela Gschwend in dieser Nummer des *NewsLetters* dargelegt.

Bruno Wildhaber, Schwerzenbach

Endnoten

1 IT Governance Institute; www.itgi.org

2 The Economist, Ausgabe vom 8. Mai 2003

3 Der Einfachheit halber sprechen wir hier von „Sourcern", d.h. internen oder externen IT-Anbietern.

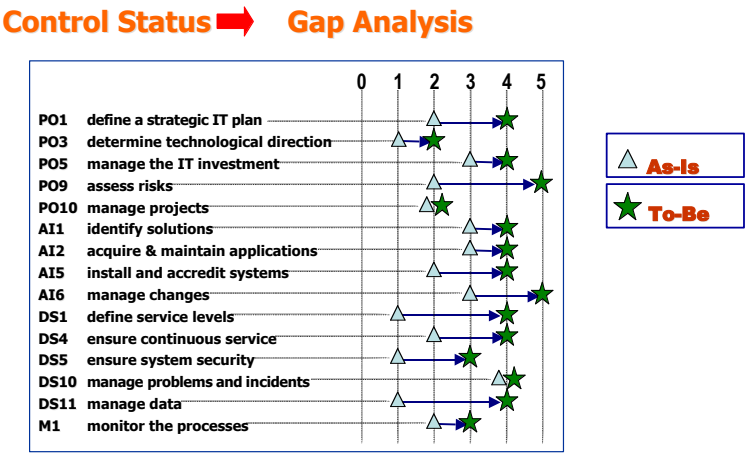
4 Auf www.cio.com findet man eine Vielzahl von Artikeln zum Thema. Da die Seiten sehr dynamisch sind, wird empfohlen, die „CIO Research Reports" zu besuchen, dort „The State of the CIO 2003".

5 www.metagroup.com, Studie vom 13. März 2003: CIO Priorities 2003: "Shifting from Efficiency to value"

6 Control Objectives for Information and related Technologies; www.isaca.org/cobit

7 Capability Maturity Model

8 ITIL = Information Technology Infrastructure Library



IT-Governance

IT-Governance bei der Swiss Re

Sind die Elemente der IT-Governance einfach „alte Bekannte in neuen Gewändern“? Ich glaube, es ist genug darüber geschrieben worden, um zu sehen, dass diese Sichtweise etwas zu einfach wäre.

Dass der IT-Governance eine zentrale Bedeutung zukommt, wurde bei der Swiss Re früh erkannt. Eine dedizierte Stelle wurde dazu anfangs 2002 geschaffen, u.a. um die Entwicklungen in diesem Bereich zu koordinieren. IT-Governance wird klar als Teil der Corporate Governance gesehen und trägt somit einen Teil zur Reputation am Markt, zum Operational Risk Management und zur allgemeinen Verbesserung der Prozesse in der IT im Unternehmen bei. Dies beinhaltet unter anderem Effizienz, Effektivität, Qualität, Stabilität und Langfristigkeit.

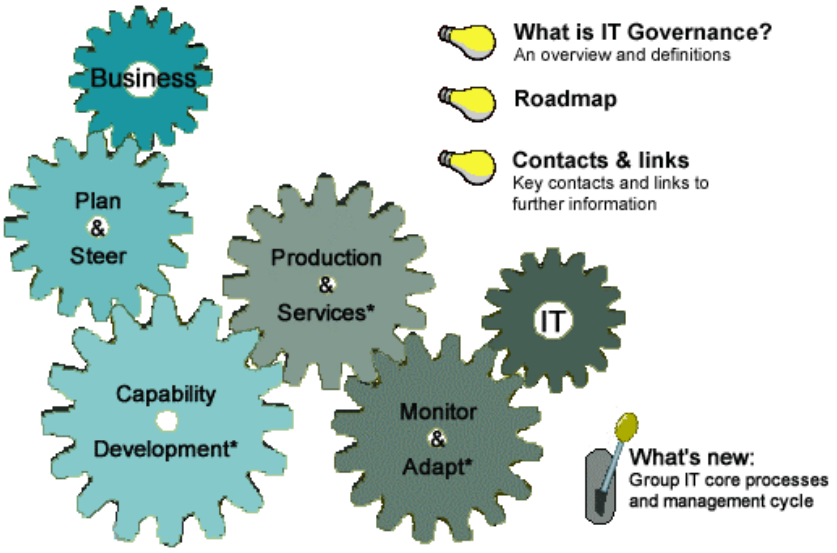
Es vergeht heute kaum ein Tag oder ein Meeting, an dem nicht von IT-Governance gesprochen wird. Aufgrund der verschiedenen Auffassungen, was darunter zu verstehen ist und was das für den Einzelnen bedeutet, haben wir den Begriff für uns neu definiert. Ziel war, dass jeder Mitarbeiter die Definition versteht: “IT Governance provides you with best practice guidance and principles to propose, make and enforce the right IT decisions to ensure that IT is aligned with and enables the business.”

Ziele und Vorgehen

Unser Ziel mit IT-Governance ist, die IT-Prozesse auf ein bestimmtes „akzeptables“ Niveau zu bringen, ähnlich wie es im vorherigen Artikel bereits vorgestellt wurde.

Um dies zu erreichen, haben wir zwei parallel verlaufende Vorgehensweisen gewählt:

- Top down: Zusammenstellung der Sicht „Steuerungsfunktion“ mit den verschiedenen Gremien und Kommittees, die sich mit IT befassen. Hierzu gehört die Definition der Verantwortlichkeiten und die „Verankerung“ von IT-Governance in den verschiedenen Charters. Als Beispiel sei hier ein Auszug des Charters des höchsten IT-Steuerungsgremiums erwähnt, dem Group Business Information Committee: „Mission: *The GBIC provides management oversight on Swiss Re Group Information and Technology and enables effective and efficient information, decision and governance processes.* Tasks: *…define and implement required IT Governance Group-wide.*“ Damit wurde das Bewusstsein für IT-Governance auf Geschäftsleitungsebene gesteigert, Verantwortlichkeiten festgelegt und eine Signalwirkung erreicht.
- Bottom up: Zusammenstellung eines internen Anforderungskatalogs welcher die Mindestanforderungen an Prozesse, Standards, Verhaltensweisen, etc. für die Swiss Re beschreibt. Diese Übersicht wollten wir von einem weltweit anerkannten „Best-Practice“-Standard ableiten, der möglichst breit angelegt ist und sämtliche IT-Prozesse umfasst. COBIT bot dazu die ideale Basis. Die bei der Swiss Re gültigen Standards, etc. wurden entsprechend in die Übersicht eingefügt, bzw. müssen noch erstellt werden. Dieses sogenannte „Repository“ ist auf dem Intranet verfügbar.



Einführung von IT-Governance und bisherige Erfahrungen

IT-Governance-Prozesse an sich sind nicht neu. Vieles hat vorher schon bestanden. Vieles ist in ständigem Fluss. Wir sind deshalb auch in nächster Zukunft damit beschäftigt, die IT-Governance zu verbessern.

Was ist nun bei der Einführung zu beachten? Unsere Erfahrungen haben folgendes gezeigt:

- Der Buy-in des Managements ist von grösster Wichtigkeit (top-down). Nur so können Mitarbeiter in ihrem Tun unterstützt und Verantwortung wahrgenommen werden.
- Der Buy-in der Mitarbeiter: Bei unserem Bottom-up-Approach ist es wichtig, dass der Einzelne einen Sinn in diesen Aktivitäten sieht. Im ersten Moment glauben viele, dass es einen Mehraufwand bedeutet, was berechtigt sein kann, dort, wo noch nicht viele Prozesse, Standards, etc. definiert sind. Langfristig gesehen vereinfachen sich die Prozesse und sie werden verlässlicher. Dies kommunizieren wir bei jeder Gelegenheit, in Sitzungen, Einzelgesprächen, Präsentationen, etc.
- Messbarkeit: Vor allem, wenn es sich um qualitative Faktoren handelt, ist Messen nicht trivial. Eine Universallösung haben wir keine, sondern versuchen, uns schrittweise an die für uns ideale Vorgehensweise heranzutasten. Wir fokussieren uns auf die wichtigsten Ziele zuerst – was wichtig ist, wird vom Management entschieden.
- Überblick und Steuerung: Es sind bereits verschiedenste Abteilungen mit Governance-Aktivitäten beschäftigt. Wichtig ist es, eine Übersicht und einen „Fahrplan“ zu haben sowie die Tätigkeiten richtig zu priorisieren. Wie beim Project-Portfolio-Management ist es wichtig, das IT-Governance-Activity-Portfolio richtig zu steuern und die Ressourcen richtig einzusetzen.
- Schnittstellen: Mit dem Überblick verbunden ist auch die Koordination der Schnittstellen zu anderen Abteilungen. Hier möchte ich speziell das Internal Audit erwähnen. Da wir uns beim Aufstellen der Basisregeln an einen internationalen Standard angelehnt haben, gab es bezüglich Inhalt praktisch keine Diskrepanzen.

Obiges nützt alles nichts, wenn IT-Governance nicht „gelebt“ wird. Die Umsetzung fordert ein bestimmtes Umdenken. Wo Verhaltensänderungen gewünscht sind, erfolgen sie meist nicht von heute auf morgen. Im Sinne von „Steter Tropfen höhlt den Stein“ versus „Holzhammermethode“ möchte ich Sie ermuntern, den für Ihre Unternehmung richtigen Mix für die Umsetzung der (IT)-Governance zu finden.

Daniela Gschwend, Swiss Re, Zürich

IT-Governance

Le débat « Maîtrise d'ouvrage / Maîtrise d'œuvre » du système d'information est-il toujours d'actualité ?

L'Association Française de l'Audit et du conseil Informatique AFAI a organisé le 21 octobre 2003 une présentation débat autour du thème des rôles respectifs de la maîtrise d'ouvrage (MOA) et de la maîtrise d'œuvre (MOE). Cette dualité issue de l'univers du bâtiment engage l'ensemble du corps de métier sur la bonne issue des travaux. Elle pouvait être considérée jusqu'à l'année dernière comme une spécificité française . En effet, la culture anglo-saxonne gomme singulièrement cette dichotomie contractuelle dans la notion de « sponsor ». Pourtant il ne viendrait à l'idée de personne, d'affirmer que ce modèle « vertueux » satisfait constamment le besoin des entreprises. Pour autant le modèle est-il incorrect ou insuffisamment redécouvert?

Michel Volle et Jean-Marie Faure du Club MOA imputent une grande part des échecs à un défaut de « maîtrise de l'ouvrage », ce qui laisse songeur compte tenu de la proportion des projets non réalisés, réduits ou remis hors des délais. Afin de transformer ces revers en succès, trois facteurs de réussite sont évoqués avant tout. Le premier de ceux-ci est la nécessaire professionnalisation de la fonction. Le deuxième est la distinction claire des rôles et responsabilités. Et enfin, le dernier, qui n'est que le prolongement naturel des deux premiers, est le facteur humain et organisationnel, fondé sur le respect mutuel des rôles de chacun.

La professionnalisation de la MOA : une étape indispensable

L'étendue et la complexité croissante des Systèmes d'Information (SI), ne peuvent être correctement appréhendées que si tous les intervenants d'un projet, partagent un même langage de représentation. Claude Sissmann, du Syntec Informatique, a d'ailleurs souligné cette carence et principalement au niveau de la fonction architecture. Il est donc nécessaire d'instaurer un esprit de modélisation au niveau de la MOA (cahier des charges, recettes, plan d'assurance qualité).

Ainsi, Michel Volle du Club MOA, lors de la table ronde, préconise que la MOA doit être capable d'urbaniser et modéliser les processus. Cette professionnalisation, comme l'indique Serge Yablonsky, Président de l'AFAI, pourrait passer par une formation adaptée. Il a rapporté les premiers résultats du programme du MITI japonais de professionnalisation massive du métier d' « IT conductor ». Ce programme initié en 2001, forme et certifie chaque année plus de 1500 candidats. La certification de ces rôles vise à fiabiliser la relation de confiance entre les différents intervenants et à s'assurer de la conformité des stratégies business et IT.

Une distinction claire des rôles et responsabilités

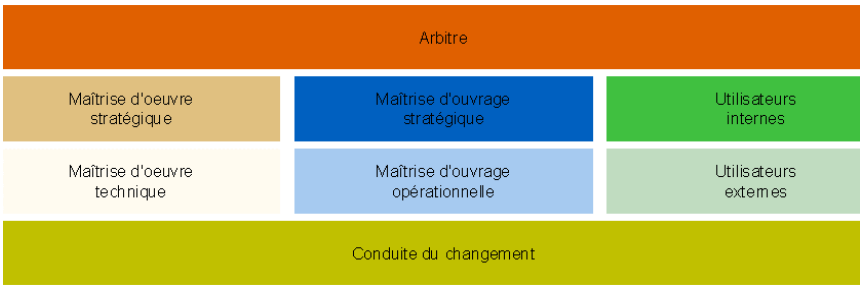
Nathan Hattab (expert judiciaire AFAI) a dressé un panorama de la pathologie des relations MOA/MOE, confirmant le chemin qui reste à parcourir. La confusion des rôles et responsabilités est un facteur de risque. Ainsi, la profusion des intervenants (MOA, MOA fonctionnelle, MOA technique, MOA déléguée, MOE, MOE déléguée, éditeurs, intégrateurs, partenaires) est source de confusion dans la lisibilité des périmètres d'intervention et favorise ainsi les incompréhensions qui peuvent éventuellement dégénérer en conflits. Toutefois, l'absence totale de toute MOA conduit tout aussi sûrement à l'échec.

La distinction claire des rôles et responsabilités passe par une rationaisation de l'organisation, comme l'explique Georges Epinette du Club Informatique de Grandes Entreprises Françaises (CIGREF) en proposant une cartographie des rôles (8 macro-rôles) qu'il convient d'articuler avec une matrice croisée de 24 interfaces. Un éclairage tout particulier est porté sur l'existence des trois domaines d'intervention de la MOA le système d'information, les projets et le fonctionnement.

Cette distinction permet une attribution du budget informatique à la MOA plutôt qu'à la MOE. En effet, la MOA, qui représente les intérêts de l'entreprise, joue en quelque sorte le rôle de client et la MOE de fournisseur. D'ailleurs, cette répartition du budget est pratiquée à la Poste comme en témoigne Marie-Noëlle Gibon, responsable DSI du Groupe La poste, lors de la Table Ronde.

Ainsi, la précision du cadre contractuel du projet (enjeux, risques et coûts, rôles et responsabilités, qualité des attendus et des livrables) nécessite du professionnalisme. La mise en œuvre du cadre contractuel s'assouplit au sein d'une véritable collaboration.

Dans ce qui pourrait apparaître comme une simple séparation des pouvoirs (MOA qui détient la connaissance métier et commande l'exécution d'un ouvrage / MOE qui détient la connaissance technique et exécute les travaux), il est important de ne pas opposer ces deux savoirs. Il est donc primordiale de renforcer ce partenariat en clarifiant les rôles et les responsabilités de chacun. La professionnalisation du métier MOA peut être envisagée comme l'aboutissement de ce processus.



Les 8 macro-rôles identifiés par le CIGREF.

La nécessité d'une bonne collaboration MOA/MOE

Tous les intervenants s'accordent pour dire que l'un des principaux Facteurs Clé de Succès du projet passe par une vision commune pour la MOA et la MOE. Ce qui se traduit par une bonne collaboration MOA/MOE.

Claude Sissmann du Syntec Informatique prend l'exemple du modèle de « plateau-projet » emprunté du mode de la construction automobile, carrefour des compétences et de la communication autour du projet, pour illustrer cette logique de partenariat. La notion de transversalité, qui implique une coopération et une complémentarité des acteurs, est donc un facteur important pour la réussite d'un projet.

L'avenir des MOA est encore largement devant nous…

Propos recueillis par l'équipe des étudiants du DESS 242, Jean Luc Loubeyre, Matthieu Bellamy, Sandrine Do Celeiro, Nadia Amri, Samuel Galbois, Romain Violier, David Hauptschein, Sonia Kim

Repris avec l'autorisation de l'AFAI

IT-Governance

Rosinen aus dem euroCACS2004-Kuchen

gepickt von Max F. Bretscher

What is IT-Governance? (Dr. Jean Pernet)

„Im Westen nichts Neues“ könnte man beinahe Remarque bemühen. Einerseits verstehen verschiedene Leute darunter unterschiedliche Dinge, andrerseits ist es für viele nur ein neues Schlagwort für Altbekanntes. Allerdings erhielten mit diesem Ausdruck doch etliche in der Vergangenheit ein Mauerblümchendasein führende Aspekte vertiefte Beachtung:

- Betonung der Vorschriftentreue (Compliance)
- Transparenz
- Ethisches Geschäftsverhalten
- Beachtung des Risikomanagements

Der Referent tritt sodann noch auf einige wichtige Punkte ein, die heute oft eine ausschlaggebende Rolle spielen:

- Outsourcing
- Projektmanagement
- Rolle des (IT)-Revisors

Structures, processes and relational mechanisms for IT Governance (Wim van Grembergen/Steven De Haes)

Die Referenten platzieren den Terminus „IT-Governance“ anhand diverser früherer Modelle in der heutigen Verständniswelt. Als illustratives Beispiel sei eine Ansicht von Peterson aus dem Jahr 2003 herausgegriffen. Dazu ist mit Sicherheit zu bemerken, dass sich IT-Governance natürlich nicht auf zukünftige (strategisch unzweifelhaft entscheidende) und äussere (ebenfalls eher strategisch orientierte) Dimensionen beschränken darf, sondern das IT-Management ebenso intensiv beobachten und überwachen muss.

Wie dies auf der strategischen Ebene üblich ist, versuchen sich die Führungsleute in sogenannten *committees* und *councils* auf Marschrichtungen zu einigen, wobei sie sich mit Resultaten aus diversen taktischen (z.B. business partnerships, monitoring, usw.) und prozeduralen (z.B. Strukturen durch Organigramme, IT job rotation, usw.) Mitteln alimentieren. Unweigerlich spielt bei den Betrachtungen als wichtiges Instrument eine auf die Belange der IT-Governance zugeschnittene Balanced Scorecard bzw. gleich deren mehrere eine bedeutende Rolle. Die Autoren zeigten, wie sie letztlich in ihre Überlegungen auch COBIT mit den verschiedenen Reifegraden einbeziehen.

A Framework for Designing IT Governance (Johan Marnewick)

Der Präsentator teilt mit der Zuhörerschaft seine Erfahrungen und nennt sie einen Bericht aus den „Schützengräben“. Es mutet denn auch nach einem langen Krieg an, der über drei Drittel führt (Anmerkung des Redaktors: Ist dies der Grund, weshalb Eishockeyspiele, die ja oft in eine Schlacht ausarten, auch in drei Dritteln ausgetragen werden?!).

Im Kern des ersten Drittels steht die Erkenntnis, dass bezüglich IT-Governance ein Verbesserungspotential vorhanden ist. Somit ist das Festlegen von Grundlagen in Übereinstimmung mit der (eventuell zu korrigierenden) Kultur unter Einbindung einer Scorecard von Wichtigkeit. Der Verbesserungsplan wird oft nicht ohne Konflikte (und deren ultimativ geforderte Lösung) über die Bühne gehen.

Im zweiten Drittel werden die zur Umsetzung beauftragten Körperschaften gebildet, die auch mit Kompetenzen zur Beschlussfassung ausgerüstet sein müssen. Der gesamte Prozess muss strukturiert werden, Kontrollen sind zu definieren und Instrumente sind bereitzustellen.

Im dritten Drittel wird ein Reifegrad erreicht, in welchem erkannt wird, dass ein stures Befolgen der früher festgelegten Regeln nicht einge-

halten werden kann. Dennoch dürfen nun die unweigerlich erzielten Erfolge nicht über Bord geworfen werden, sondern Ergänzungen zum Bewältigen von Ausnahmeregelungen (Overrides) sind zu definieren und die Detailprozesse, inklusive Kontrollen, erfahren eine Anpassung. Dazu sind Ressourcen, aber auch Lernprozesse und Kapazitäten, gefragt.

Die aus der Übung gemachten Erfahrungen sollen die Tagungsteilnehmer einerseits „trösten“, dass die Welt nicht in einem Tag erschaffen wurde, andererseits ermutigen, sich in ähnlicher Art und Weise ans Werk zu machen.

Contribution of Supervision on IT to the IT Governance of Financial Institutions (Paul W. Osse)

Die Erfahrungen und Einsichten aus der Niederländischen Bank haben sehr wohl allgemeine Gültigkeit. Dies, auch wenn gewisse „Kleinigkeiten“ länderspezifisch bleiben. Ein zentrales Element der Präsentation sind die drei Säulen des Modells von „Basel II“:

Die Kapitalgrundsätze

- Wenn sich die Risiken in der Welt vermehren, wird *mehr* Kapital benötigt.
- Wenn das Geschäftsvolumen zunimmt wird *mehr* Kapital benötigt.
- Wenn die Komplexität der Geschäftstransaktionen zunimmt, wird *mehr* Kapital benötigt.
- Wenn sich das Kontrollniveau erhöht, wird *weniger* Kapital benötigt.

Überwachung durch Bank- und Marktaufsicht
Zentralbanken

- Basel Committee
- Börsenaufsichten
- Aktionäre
- Analysten
- Rating Bureaux

Ziele

- Transparenz der operationellen Risiken
- Verminderung der operationellen Verluste
- Verminderung des Risikokapitals
- Imagepflege

Tools for Implementing IT-Governance (Derek Oliver)

Wir haben die richtigen Werkzeuge vor unserer Nase, teilweise auf unseren Fingerspitzen:

- COBIT
- ISO17799 (BS7799)
- Information Technology Infrastructure Library (ITIL)

Wie der erfahrene IT-Security-Fuchs Oliver eindrücklich darlegt, ist das COBIT-Framework voll von unterstützenden Hinweisen auf wirksames Initialisieren (PO), Umsetzen (AI), Betreiben (DS) und Überwachen (M). Dabei unterstreicht der Präsentator mehrfach, dass ohne ein schriftliches Formulieren der Sicherheitspolitik keine Sicherheit, die den Namen verdient, erreicht werden kann. Ohne eine solche Ausrichtungs- und Messlatte ist auch nicht festzustellen, ob das gewünschte Sicherheitsniveau erreicht ist, oder ob, und insbesondere wo, Defizite vorhanden sind, die durch geeignete Massnahmen eliminiert werden müssen.

Aufbauend auf eine solche Politik können erst Standards und Verarbeitungsregeln definiert werden, auf denen wiederum (sozusagen pyramidenförmig) die Detailaspekte der physischen und logischen Sicherheit behandelt, kontrolliert und revidiert werden können.

Ein besonderes Augenmerk hat der Referent auf die personellen Elemente, insbesondere der logischen Sicherheit, geworfen. Sind es doch immer wieder die Menschen, welche sich als schwächste Glieder einer Sicherheitskette erweisen. Dazu gehören u.a. Standards, welche das Einstellen und Entlassen von Personal umfassen.

Nicht zu vergessen sind branchen- und nationalitätenspezifische Elemente, die es zu beachten gilt. Gerade im Finanzsektor sind die Regulative länderspezifisch ausgedehnt und nicht überall identisch.

IT-Governance

Outsourcing der IT: Chancen und Risiken aus Sicht der Revision

Der Trend zum Outsourcing und speziell zum Outsourcing von IT-Leistungen ist in Zeiten schwacher Konjunktur besonders ausgeprägt. Unternehmen besinnen sich auf Kernkompetenzen und versuchen in peripheren Bereichen Kostenersparnisse zu erzielen. Kaum eine andere IT-Branche geht von gleich hohen Steigerungsraten wie die Outsourcing-Dienstleister aus. Aber Outsourcing bietet nicht nur Chancen. Outsourcing beinhaltet besondere Risiken und damit Tätigkeitsfelder für interne und externe Revisoren.

Trends des IT-Outsourcing

Aktuell geht der Trend im IT-Outsourcing in zwei Richtungen. Zum einen spezialisieren sich immer mehr Dienstleister auf bestimmte Branchen. Klassisches, wenn auch nicht ganz typisches, Beispiel ist hier der Bankensektor. Zum anderen wird auch der Mittelstand, der sich bisher als relativ Outsourcing-resistent gezeigt hat, ins Visier der Vertriebsstrategien genommen. Dies gilt besonders vor dem Hintergrund des zum Teil gesättigten Marktsegments der Großunternehmen.

Begriffe

Beim Outsourcing der IT werden verschiedene Typen unterschieden:

- Internes Outsourcing – beinhaltet die Ausgliederung von Tochter- oder Servicegesellschaften. Beim internen Outsourcing gab es speziell seit Beginn der achtziger Jahre einen starken Anstieg. Hintergrund war damals die Hoffnung, teure EDV-Ressourcen anderen Unternehmen gewinnbringend verkaufen zu können. Diese Hoffnung hat sich in einigen Fällen bestätigt, in anderen Fällen endete das ganze allerdings in einem teuren Desaster.
- Externes Outsourcing – beim externen Outsourcing werden Leistungen an einen Dritten ohne Unternehmensverflechtungen abgegeben. Eine besondere Variante des externen Outsourcings ist das Management-Buy-Out der Datenverarbeitung. Eine Zeit lang sehr beliebt bei deutschen Unternehmen war das Konzept, aus im Nachhinein offensichtlichen Gründen in der überwiegenden Mehrzahl der Fälle zum Scheitern verurteilt. Ein DV-Leiter kauft mit wenig Kapital und viel Herrschaftswissen seine Abteilung und beliefert seinen alten Arbeitgeber. Die Folge scheint logisch: Die Kapitalschwäche beim Dienstleister führt zu einer überlebensorientierten Preisgestaltung und die Abhängigkeit vom jetzt Externen wird größer.
- Totales Outsourcing – bezeichnet die vollständige Ausgliederung eines Funktionsbereichs, wie z.B. die Ausgliederung der kompletten Datenverarbeitung.
- Partielles Outsourcing – bezeichnet die Ausgliederung von Teilfunktionen. Partielles Outsourcing beginnt z.B. bereits mit der externen Vergabe der Reinigung von Peripheriegeräten. Speziell im Bereich der Internet-Dienste, z.B. Hosting der Homepage, ist partielles Outsourcing stark verbreitet.

Outsourcing im Mittelstand

Weniger als ein Drittel des deutschen Outsourcing-Marktes wird vom Mittelstand[1] bestimmt. Dies ist auf den ersten Blick gerade in einem mittelstandsorientierten Land wie der Bundesrepublik Deutschland erstaunlich, bietet doch das Outsourcing der IT dem Mittelstand Zugang zu Technologien (z.B. e-Commerce), die in Verbindung mit dem Aufbau eigener personeller Ressourcen extrem teuer wären.

Einer der wesentlichen Gründe, warum das Outsourcing der IT im Mittelstand unterrepräsentiert ist, resultiert aus dem fehlenden Vertrauen der Kunden zu den Dienstleistern. Mittelständische Kunden verlangen häufig ein beziehungsorientiertes Marketing. Die typische Vertriebsstrategie der Outsourcing-Dienstleister war bisher eher funktionsorientiert. Hier entwickeln sich allerdings erste Ansätze, den Bedürfnissen des Mittelstandes weit stärker entgegen zu kommen als bisher.

Andere Probleme ergeben sich aus den fehlenden Vorraussetzungen bei vielen Unternehmen. Um ein erfolgreiches Outsourcing der IT durchführen zu können, muss neben einer

Firmenphilosophie, die im Regelfall sogar vorhanden ist, eine explizite IT-Strategie definiert sein, die sich (hoffentlich) in Übereinstimmung mit der Unternehmensstrategie befindet. Vielleicht noch wichtiger für die Entscheidungsfindung ist die Existenz detaillierter und vollständiger Informationen über die Kosten und Leistungen der eigenen Datenverarbeitung.

Chancen des Outsourcings – Die Versprechen der Dienstleister

Welche Gründe sprechen für ein Outsourcing der IT?

Neben der mittelfristigen Kostenersparnis ist das Hauptargument für das Outsourcing der IT die Konzentration auf die Kernkompetenz eines Unternehmens. Dadurch, dass „nebensächliche" Funktionen an Fremde, die diese Aufgaben in der Regel besser und kostengünstiger wahrnehmen können, vergeben werden, können eigene Ressourcen effizienter eingesetzt werden.

In der Argumentationskette folgt, wie beschrieben, der Kosteneffekt. Durch eine bessere Ressourcenauslastung können externe Dienstleister IT-Leistungen günstiger anbieten. Zudem sind die Kosten transparent (zumindest auf den ersten Blick), weil sie in der charmant simplen Form der Eingangsrechnung beim Unternehmen in Erscheinung treten.

Des Weiteren hat ein spezialisierter Dienstleister in der Regel IT-Know-how, das einem „normalen" Unternehmen nicht zur Verfügung steht. Dies ermöglicht es, Prozesse zu optimieren und wettbewerbsfähiger zu machen und dabei insgesamt den Service-Level zu erhöhen.

Ein weiterer, nicht zu unterschätzender, Effekt, der besonders in der IT zum Tragen kommt, ist der Risikotransfer. Die Risiken im Rahmen der IT nehmen durch steten Wandel, erhöhte Komplexität und zunehmende Systemintegration exponentiell zu. Hier kann natürlich ein Großteil der notwendigen Maßnahmen in Verbindung mit der Gewährleistung der notwendigen Reaktionszeit an den Dienstleister transferiert werden.

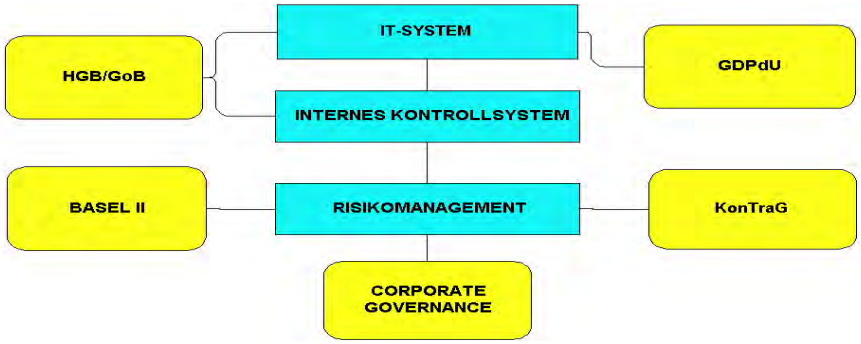


Abb. Übersicht Unübertragbare Verantwortung für Systeme und ihre Quellen

Verantwortung

Eines sollte jedoch niemals unterschätzt werden: Ein Risikotransfer kann noch so explizit und umfangreich im Outsourcing-Vertrag geregelt sein; die schlussendliche Verantwortung verbleibt beim Unternehmen und ist nicht übertragbar!

Dies betrifft im Wesentlichen die Ordnungsmäßigkeit der Buchführung (GoB/GoBS), die Anforderungen an das Risikomanagementsystem (KonTraG), die entsprechenden Regelungen im Bundesdatenschutzgesetz (BDSG) und die Anforderungen an qualitative Faktoren, die Banken im Rahmen eines Ratings nach Basel II stellen.

Als weitere Entwicklung ist das Unternehmen auch im Rahmen der Sicherstellung der Zugriffsmöglichkeiten auf die steuerlich relevanten Daten durch die Betriebsprüfung (GDPdU) in der Pflicht. Eine Aussage, dass sich die Daten bei einem fremden Dritten befinden, wird das Finanzamt kaum zufrieden stellen.
Aus der fehlenden Möglichkeit der Übertragung der Verantwortung ergeben sich hohe Anforderungen an die Überwachung der Leistungen des Outsourcing-Partners. Die outgesourcten Leistungen sind in das interne Kontrollsystem des Unternehmens einzubetten und unterliegen dementsprechend der Prüfungspflicht. Dies ist im Rahmen der Vertragsgestaltung zu berücksichtigen.

Risiken

Das Outsourcing der IT ist kein neues Feld. Seit den sechziger Jahren ist Outsourcing der IT verbreitet und

jeder Fehler, der gemacht werden kann, wurde mehrfach wiederholt!
Die folgenden Abschnitte widmen sich detailliert den Problembereichen bezüglich der Wahl des Dienstleisters, der IT-Sicherheit und der Leistungskontrolle.

Veränderung der Kernkompetenz

Gilt als Hauptargument für das Outsourcing die Konzentration auf das Kerngeschäft, so muss doch berücksichtigt werden, dass der Marktdruck und die technologische Entwicklung auch Kerngeschäfte verändern können.

Abhängigkeiten und Know-how-Verlust

Einer der schlimmsten und verbreitetsten Fehler ist die Abhängigkeit von Externen und der Know-how-Verlust im eigenen Unternehmen. Je spezieller die ausgelagerte Dienstleistung, desto größer die Abhängigkeit. Das fehlende ausgelagerte Know-how führt zu

- einer Verstärkung der Abhängigkeit von Externen,
- Informationsdefiziten bezüglich der Angemessenheit von Leistungen und
- fehlenden Entscheidungsgrundlagen für notwendige Umorientierungen.

U.a. um Abhängigkeiten zu vermeiden und notwendiges Wissen zu konservieren, ist es zwingend erforderlich, kompetente Schnittstellenpositionen im Unternehmen aufzubauen.

Reibungsverluste

Der Outsourcing-Dienstleister hat ein spezielles Geschäft, das üblicherweise das Kerngeschäft des Unternehmens maximal administrativ berühren sollte. In der Zusammenarbeit zwischen Outsourcing-Partner und Fachabteilung kommt es deshalb immer wieder zu Reibungsverlusten. Es ist deshalb wichtig, verlässliche Ansprechpartner beim Dienstleister zu haben, die sich zeitnah, auf Basis eigener Erfahrungen und in der gleichen Sprache mit den Problemen der Fachabteilungen auseinandersetzen können.

Verlust der Flexibilität

Aus dem fehlenden Know-how, der Abhängigkeit vom Dienstleister und den Reibungsverlusten folgt zwangsläufig auch ein Verlust an Flexibilität. Die Umgestaltung von extern vergebenen Prozessen kann zu einer zeit- und kostenintensiven Angelegenheit werden.

Sicherheitsrisiken

Viele Unternehmen verstehen die Rolle des Dienstleisters als Black-Box. Dies ist grundsätzlich, bei aller Konzentration auf das Kerngeschäft, ein Fehler. Vor dem Hintergrund der Unübertragbarkeit liegt die schlussendliche Verantwortung für die IT-Sicherheit nicht beim Outsourcing-Partner.

Abrechnungsproblematik

Ein weiteres großes Problem des Outsourcings der IT ist die Abrechnung, bzw. die Leistungskontrolle. In der Regel werden bestimmte Leistungen, z.B. Antwortzeiten oder Verfügbarkeit messbar sein müssen. Doch wer misst die Werte und wer kann die Messergebnisse vor dem Hintergrund des angesprochenen Know-how-Verlustes nachvollziehen?

Bonitätsrisiko

Die Krise in der IT-Branche führt zur Vergrößerung des Bonitätsrisikos. Die Gefahr der Insolvenz des Partners, mit unabsehbaren Folgen für die Aufrechterhaltung der Dienstleistung, ist aktueller denn je. Hier muss das Unternehmen Maßnahmen ergreifen, um den DV-Betrieb auch in dem Fall sicherzustellen, wenn der Partner ausfällt.

Kosten

Outsourcing kann, muss aber nicht, kostengünstiger sein, als der Unterhalt einer eigenen IT. An dieser Stelle mussten und müssen viele Unternehmen einsehen, dass der Weg zum Partner der falsche Weg war. In der Praxis wird eine solche Entscheidung aber in den seltensten Fällen korrigiert. Eine genaue Kostenplanung im Rahmen des Outsourcing-Projekts, die auch Sekundärkosten, wie z.B. Kosten für Schnittstellenpersonal, enthält, ist zwingend erforderlich. Dies gilt auch für eine zeitnahe und dauerhafte

Kontrolle der Kosten im laufenden Betrieb.

Auswahl des Dienstleisters

Frei nach dem Motto „Darum prüfe, wer sich ewig bindet“ lassen sich einige der genannten Risiken durch eine sachgerechte und nicht nur an Kosten orientierte Auswahl des Dienstleisters verringern.

Einer der wesentlichen Punkte bei der Auswahl des Dienstleisters, der häufig eine entscheidende Rolle spielt, sind Eigentumsverhältnisse und andere Verflechtungen. Ein Outsourcing-Partner in Form einer Schwestergesellschaft im Konzern ist im Normalfall einem völlig Fremden vorzuziehen; dies gilt im Besonderen, wenn Verflechtungen mit der Konkurrenz existieren.

Wichtig bei der Beurteilung ist die Kompetenz und Professionalität des Anbieters. Der Outsourcing-Anbieter sollte ausreichend Erfahrung mit genau der Dienstleistung besitzen, die angefragt wird. Dabei sind, über die Papierlage hinaus, auch Referenzen von anderen Kunden des Anbieters von entscheidender Bedeutung. Viele Outsourcing-Projekte sind gescheitert, weil der Anbieter in einem ganz bestimmten Teilsegment, der für das Unternehmen besonders wichtig war, z.B. Web-basiertes EDI, keine Erfahrung und keine Ressourcen besitzt.

Die Kosten sind natürlich wichtig, besonders im Vergleich mit kalkulatorischen IT-Kosten einer Inhouse-Lösung, dürfen aber, speziell wenn die Bonität des Anbieters in Frage steht, auch bei nachgewiesen guter Servicequalität nicht entscheidend sein.

IT-Sicherheit

Wie bereits angesprochen, liegt die Verantwortung für die Sicherheit der IT schlussendlich beim Unternehmen selbst. Der logische Schluss ist, dass die Sicherheit der IT im Outsourcing-Prozess besondere Aufmerksamkeit erfordert.

Dies beinhaltet eine Vereinheitlichung von Sicherheitskonzepten auf dem notwenigen Niveau. Beispiel: Für einen Finanzdienstleister ist der Zugang zu aktuellen Aktienkursen über das Internet von entscheidender Bedeutung. Um signifikante Vermögensverluste zu vermeiden, darf der Internetzugang maximal eine Stunde gestört sein. Im Service-Level-Agreement (SLA) mit dem Outsourcing-Partner sind diese Anforderungen oft nicht spezifiziert. Aufgrund der sonst üblichen Geschäftstätigkeit anderer Kunden, hat der Outsourcing-Partner das notwendige Schutzniveau für den Internetzugang auf „mittel“, d.h. eine garantierte Behebung der Störung innerhalb von 24 Stunden, festgelegt. Sobald es zu einer Systemstörung kommt, ist der signifikante Vermögensverlust wahrscheinlich.

Eine besondere Rolle spielen bestimmte vertrauliche Daten. Personenbezogene Daten, Daten aus Forschung & Entwicklung, Krankenakten, Daten von Rechtsanwälten oder Wirtschaftsprüfern sollten im Einzelfall auf die Tauglichkeit zum Outsourcing untersucht und wenn rechtlich möglich ggf. zusätzlich abgesichert werden, z.B. durch kryptographische Verfahren.

Bereits mehrfach angesprochen wurde die Verantwortung des Unternehmens und die damit in Verbindung stehende Prüfungspflicht. Die Prüfung sollte durch die Innenrevision des Unternehmens ggf. mit externer Unterstützung oder durch einen sachverständigen Dritten erfolgen. In jedem Fall sollten gegenseitige Prüfungsrechte und -pflichten von Anfang an und im vorhinein festgelegt werden. Vorgelegte Gutachten des Outsourcing-Partners können verwendet werden, entbinden aber nicht von der Prüfungsverpflichtung.

Ein weiterer Gesichtspunkt ist die Notfallplanung beim Ausfall des Dienstleisters. Hier sollten in Zusammenarbeit mit dem Dienstleister, der in der Regel mehrere Kunden mit dem gleichen Problem hat, entsprechende Szenarien entwickelt und dokumentiert werden.

Leistungskontrolle

Um eine sinnvolle Leistungskontrolle des Outsourcing-Partners durchführen zu können, muss ein spezifizierter Service-Level existieren. Voraussetzung sind messbare Kenngrößen. Verbreitete Kenngrößen sind z.B. Verfügbarkeit, Antwortzeiten, Kundenzufriedenheit, Prozesseffizienz.

Wie die letzen beiden Kenngrößen zeigen, besteht nicht nur das Problem, dass die gelieferten Informationen in der Regel alleinig vom

Partner kommen (von sinnvollen Konzeptionen wie „Mess-PCs“ einmal abgesehen), sondern dass viele durchaus entscheidende Kenngrößen ein gewisses Maß an Unschärfe beinhalten. Deswegen ist die Festlegung der Kenngrößen und des Messverfahrens von entscheidender Bedeutung für den Erfolg des Outsourcings der IT. Eine entscheidende Rolle können an dieser Stelle die Funktionsträger der Schnittstellenfunktion im Unternehmen spielen.

Festgelegt werden sollte die Bewertung des Einflusses der vom Unternehmen geäußerten zusätzlichen Anforderungen auf die vereinbarten Messgrößen, z.B. der Einfluss von zusätzlichen Reportingfunktionen auf die Antwortzeiten des Systems. Ein Schlichtungsverfahren bei Unstimmigkeiten in der Bewertung der Messgrößen sollte ebenfalls festgelegt werden.

Die verbleibende „Rumpf“-Datenverarbeitung

Das Outsourcing der IT und die oft damit einhergehende räumliche und psychologische Trennung zwischen Fachabteilung und zentraler Datenverarbeitung führt in vielen Fällen zu einem erhöhten Aufkommen der individuellen Datenverarbeitung (IDV oder End-User-Computing).

Aufgrund von (plötzlich) transparenten Zusatzkosten, langen Realisierungszeiten bei Anforderungsumsetzungen und des fehlenden persönlichen Kontaktes entscheiden Fachabteilungen häufig neue (manchmal auch alte) Probleme mit Hilfe von entsprechenden Tools, wie z.B. Microsoft Excel™ zu lösen.

Frei nach dem Motto „Karthago muss zerstört werden“ an dieser Stelle noch einige oft wiederholte Anmerkungen zum Einsatz von End-User-Computing. Die individuelle Datenverarbeitung beinhaltet i.d.R. erhöhte Risiken:

- Es fehlen vernünftige Tests und ein Qualitätsmanagement;
- Der End-User hat weniger Fachkenntnis, als ein Anwendungsentwickler;
- Es fehlt an Dokumentation;
- Die Anwendungen sind nicht revisionssicher;
- Es fehlen Kontrollen!

Ein Fehler in einem Excel-Programm macht alle vorgelagerten Kontrollen in den Quellsystemen unwirksam! Einige Spezialisten gehen davon aus, dass ca. 40 % aller Excel-Anwendungen Fehler enthalten[2]. Qualitätssicherung ist beim Einsatz von End-User-Computing von wesentlicher Bedeutung für die Sicherheit der Information.

Fazit

Outsourcing der IT ist auch in Zukunft ein wesentlicher Faktor in der Landschaft der Informationstechnik. Der Trend zielt dabei auf branchenspezifisches Outsourcing, speziell auch im Mittelstand. Unabhängig vom Verbreitungsgrad erfordert jede Entscheidung für oder gegen Outsourcing der IT eine individuelle Auseinandersetzung mit den Chancen und Risiken des Outsourcings.

Die Verantwortung für die Sicherheit der Daten und das Risikomanagement verbleibt aber in jedem Fall beim Unternehmen. Insofern ist der Outsourcing-Partner in das eigene interne Kontrollsystem einzubinden und regelmäßigen Prüfungen zu unterwerfen.

Spezielle Problemfelder, die sich aus einer Outsourcing-Entscheidung ableiten, sind die Auswahl des richtigen Dienstleisters, die Prüfung der IT-Sicherheit bei einem externen Unternehmen und die Kontrolle der mit dem Outsourcing verbundenen Leistungsabrechnung.

Literaturhinweise:
ZIR Zeitschrift für interne Revision, Ausgabe 6/2002
„Leitsätze für die Prüfung von IuK-Outsourcing“
ZIR Zeitschrift für interne Revision, Ausgabe 5/2001
„Prüfung des Outsourcing“
ZIR Zeitschrift für interne Revision, Ausgabe 6/1994
„Prüfungsaspekte beim Outsourcing von DV-Leistungen“
E/3 , Ausgabe Juli / August 2003
“Mega-Trend Outsourcing”

Endnoten
1 Quelle E/3 Magazin, Juli/August 2003
2 Quelle: HM Customs & Excise

Holger Klindtworth
Susat & Partner

Information Systems Audit and Control Association®

ITACS Training AG
Konradstrasse 1
CH-8005 Zürich
Telefon 01 440 33 64
Fax 01 440 33 61

CISA-Testprüfung 2004 in Zürich

Samstag, 15. Mai 2004; 8:30-13:00, ganztägige Besprechung am 24. Mai 2004

Als Vorbereitung auf die echte CISA-Prüfung vom 12. Juni führen wir in Zürich eine möglichst realistische Testprüfung durch. Am Samstag Morgen wird eine "normale" CISA-Prüfung gelöst (also 200 Fragen in 4 Stunden). Diese kann dann mit einem Lösungsschlüssel selber korrigiert werden. Alle Fragen werden ausgewertet und dann am 24. Mai während einem ganzen Tag besprochen. Die schwierigen Multiple-Choice-Aufgaben sind – wie in der echten Prüfung – nicht nach CISA-Areas geordnet. Mit einem riesigen Aufwand haben wir auch dieses Jahr weitere Fragen auf Deutsch übersetzt, so dass Sie erneut eine volle Testprüfung in dieser Sprache ablegen können. Eine Garantie, dass die Testprüfung eine Ähnlichkeit zur diesjährigen CISA-Prüfung aufweist, wird jedoch weder von der ISACA noch von unserem Chapter abgegeben. Alle Teilnehmer erhalten eine weitere Testprüfung ausgehändigt, so dass zu Hause noch ein zweiter Versuch absolviert werden kann, der von uns ebenfalls ausgewertet wird. Ebenfalls abgegeben werden alle Lösungen (z.T. mit kurzen Erläuterungen).

Deutsch oder Englisch

Ihre Anmeldung ist an unser Sekretariat zu schicken. Sie erhalten rechtzeitig genaue Angaben zum Kurslokal und den Prüfungsbedingungen sowie eine Rechnung über CHF 650.- (Nicht-Mitglieder von ISACA CHF 750.-), welche innert 10 Tagen zu bezahlen ist. In diesem Betrag sind zwei Testprüfungen (in Deutsch ***oder*** Englisch), zwei Prüfungsauswertungen sowie Mittagessen am 15. Mai + 24. Mai 04, alkoholfreie Getränke inklusive. Die Mehrwertsteuer wird zusätzlich verrechnet.

Anmeldung — Offizielle CISA-Testprüfung des ISACA Switzerland Chapter

Diesen Talon bis zum **30. April 2004** einschicken an:
ITACS Training AG,
Konradstrasse 1, 8005 Zürich, Fax: 01 / 440 33 61.

Ich melde mich für die CISA-Testprüfung am **15. Mai 2004** an.

Ich bin/bezahle
❏ Mitglied ISACA CHF 650.- (exkl. 7,6% Mwst.) (ISACA Mitglied Nr .....)
❏ Nicht-Mitglied ISACA CHF 750.- (exkl. 7,6% Mwst.)

Name Vorname

Mehrwert- konforme Rechnungsadresse

E-Mail

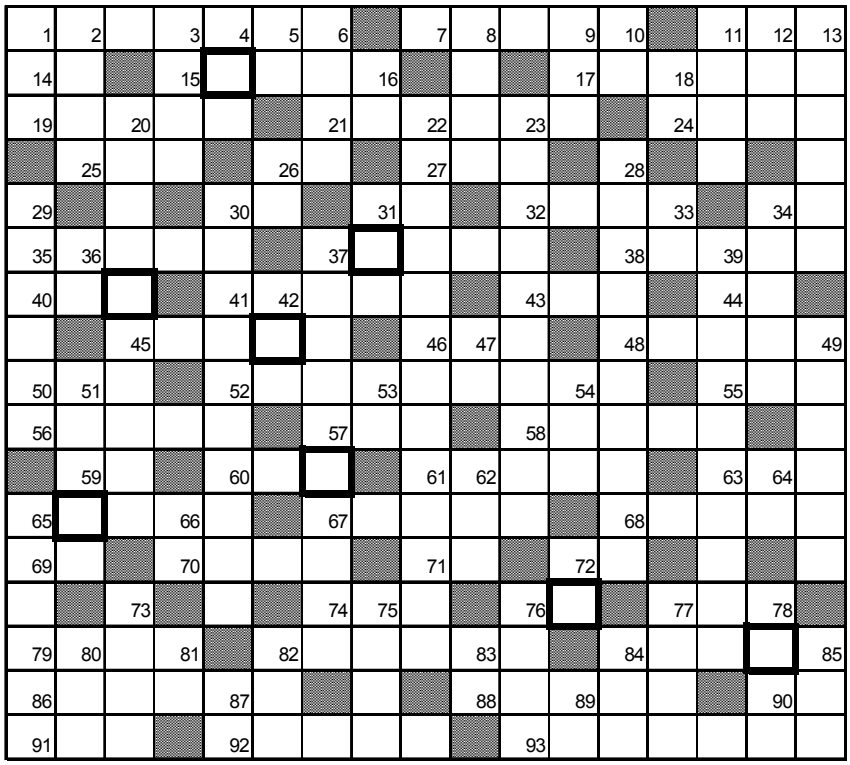
Tel. (P) Tel. (G)

Ort, Datum Unterschrift

Ich absolviere die CISA-Testprüfung ❏ in Deutsch ❏ in Englisch

The ISACA Crossword Puzzle 2/04

This puzzle is in English and relates to the key elements of this issue (*Schwerpunktthema*).



Across: **1 object of IT Governance (sg);** 7 part of Roman dress; 11 occupation; 14 two equal vowels; 15 “southpaw”; 17 blood vessel; 19 Asian country; 21 in trust; 24 device to catch animals; 25 soundless apprehension; 26 surgery room; 27 over the bend (abb); 30 short for former Vaudoise football club; 31 F article; 32 french name; 34 auto plate from Nothern Switzerland; 35 if bald, a coin or an emblem of the USA; 37 infamous Miss Wong; 38 part of the face (pl); 40 oil product; 41 clever, missing the last character; 43 US (counter) espionage; 44 your (F); 45 inspiration; 46 rodent; 48 bed and breakfast; 50 summer festival master (abb); **52 together with 93 across: responsible for IT-Governance;** 55 American Standard Nucleus; 56 clock; 57 nervous reaction; 58 violent stomach reaction; 59 auto plate from Western Switzerland; 60 so (L); 61 bitch (G); 63 summer (F); 65 fast (G); 67 former ice skating champion (Carol), 68 river and country in Africa; 69 article (A); 70 product from Mendrisio; 71 overtime; 72 and (F); 74 F negation; 76 iron football club; 77 victorious General in the US secession war; 79 if completed with “que”, a city in Northern Chile; 82 US tennis ace; 84 catching rope; 86 egg form; 88 belonging to Hitler's preferred race; 90 Southeast; 91 former small F coin; 92 at the end of the row; **93 see 52 across**.

Down: 1 writing instrument and club; 2 film roll; 3 family group; 4 snakelike fish; 5 auto plate from Finland; 6 dancing pas; 8 wrong; 9 rule; 10 auto plate from Eastern Switzerland; 11 jolt; 12 command to pray (L); 13 heart operation; 16 soundless agreement; 18 two equal consonants; 20 plans or instructions; 22 building (pl); **23 goals for IT Governance;** 26 bone (L); **28 collective responsibility for IT Governance;** 29 abhor; **30 part of IT Governance;** 31 three equal vowels; 33 negation; 34 vegetable (pl); 36 stream name from central Switzerland; 37 warm-up for sportsmen; **39 part of IT Governance (pl);** 42 Clinton’'s cat has gotten a completely new meaning; 47 preposition; 49 type of medical doctor; 51 ultimate; 53 here (I); 54 flight (F); 62 East (G); 64 aromatic beverage in Spain; 65 wireless (pl); 66 carriage return; 72 European Community; 73 African tribe; 75 a rowboat cannot do without (pl); 76 steadfast; 77 film star Turner’s first name; 78 this G imperative could also be a G oven; 80 Queen’s body order (abb); 81 one of Zeus' conquests; 82 era; 83 her (F); 84 local area network; 85 Nordic coin; 87 Dutch auto plate; 89 donkey sound.

The solution is to be found in the marked fields. The ISACA Switzerland chapter awards a prize of $US 50 in ISACA bookstore credits each issue for the winner (who is drawn by lots from the correct answers) on a postcard. Address
M.F. Bretscher, Oberrenggstrasse 8,

CH-8135 Langnau a/A
or e-mail mbretscher@kpmg.com.
Deadline may 14, 2004

If there are less than 5 answers, or the solution has not been found, the $US 50 go into the Watson Jackpot to be carried forward to the next issue. Watson: Each puzzle contains some anomaly that is to be detected. If correctly identified, the Watson Jackpot is broken and replenished with $US 50 for the next issue.

Solution Crossword Puzzle 1/04: *Table Tennis*

Across: 1 guest; 6 Jamsession; 13 steel; 18 lemurs; 20 gate; 21 gloria; 22 Al, 23 reason; 25 so; 26 pillar; 28 es; 29 ride, 31 der; 32 état; 34 Oos; 35 être; 38 aeon; 40 cans; 43 germen; 46 SC; 48 EERGRM; 52 ensign; 53 ***customer***; 57 Lionel; 59 ***response***; 61 Irre; 62 omoplate; 64 rice; 65 ***relationship***; 66 fray; 67 so; 68 dill; 69 NN; 70 asex(ual); 72 -ol; 74 doe; 75 ***management***; 78 emu; 80 ice; 81 CIA; 83 S(wissai)R; 84 yen; 86 nil; 94 in; 96 or; 97 eel; 98 UU; 100 LXX, 101 PE; 102 le; 103 neural; 104 slapshot; 105 Chopin; 106 GI; 107 Mt; 108 Ito; 109 sa; 110 deo; 111 OP; 112 St; 113 their; 115 ISO; 117 pen; 118 abaft; 119 SH; 120 Noëls; 122 NSJA; 125 tapir; 127 IA; 129 chestnut; 132 tu; 134 trading; 136 orts; 137 humanity; 141 saga; 142 separation cell; 146 Lands (end); 147 it; 148 Neon; 149 LL; 150 urban.

Down: 1 glare; 2 Ueli; 3 EM; 4 sure; 5 tre; 7 amore; 8 SG; 9 east; 10 Stoa; 11 SE; 12 onion; 13 *SLA*; 14 tore; 15 -er; 16 Eier; 17 laser; 19 sad; 21 GLS; 24 Sean; 27 lose; 30 dresscodes; 32 en; 33 TC, 36 ***turnaround***; 37 (L)emgo; 39 ONU; 41 Abe; 42 trip; 43 Gneis; 44 ripe; 45 ENNRI; 46 strings; 47 coroner; 49 elope; 50 golf; 51 metal; 52 err; 53 cella; 54 sit; 55 men; 56 Rohan; 58 ley; 60 Selma (Lagerlöf); 63 misty; 68 decorations; 71 xenophobia; 73 ***timing***; 76 niellos; 77 explode; 79 ***client***; 82 IP; 85 EC; 88 torments, 89 testis; 91 extent; 93 leopards, 95 neither; 98 UPS; 99 USA; 102 listing; 114 reuse; 116 on; 117 Pa; 118 April; 119 school; 121 L(ieutenan)t; 124 junio; 126 at; 128 again; 130 Stan; 131 Hur; 133 FTN; 135 iamb; 137 hat; 138 man; 139 ion; 140 YCL; 142 SS; 143 pi; 144 el; 145 LU.

The winner is Marc Bucher, who wins $US 50. Congratulations!

Watson: The intended anomaly was that this puzzle was not (as all others) symmetric as far as the center – point symmetry – is concerned, but symmetric according to the vertical axis) *and* the solution had nothing do with the focus of the issue. Both qualities have been detected by Ingo Borchardt, who has thus broken the Watson jackpot of $US 200. Congratulations! This reduces the Watson jackpot to $US 50.

Ein Revisor hatte in Bern eine Bekannte,
Die all' ihre Schreibmaschinen verbrannte.
Sie sagt dem Revisor: „Mein Guter,
Heute hat jeder einen Computer."
Sie ist jetzt immerhin IT-Gouvernante.

There is a young swinger who really knows how to dance,
No question, as everyone can realize it with a single glance,
The rumba, the samba, the tango,
The waltz, the twist and the mambo,
Lately, they say, she practicing the IT-IT-IT-Governance.

Express Line

A Word from the Chair

The annual membership purge takes place every April. Following the purge, members who have not yet renewed with ISACA® International Headquarters will no longer receive member benefits, including the *Information System Control Journal*™, K-NET™ and all member-protected areas of the ISACA web site.

An exit survey will be sent to non-renewing members in May. In addition to obtaining information on the decision not to renew, the survey provides a final opportunity for renewal.

On behalf of the Membership Board, I am pleased to congratulate the following 2003 Newsletter Award winners for their outstanding chapter newsletters:

- Adelaide – small chapter
- Denver – medium chapter
- Milan – large chapter
- Mumbai – very large chapter

(Note by the editor: The Swiss Chapter did not participate)

Howard Nicholson
Chair, Membership Board

Certification UpdateNew CISA® Job Practice Analysis Begins

ISACA has begun a CISA job analysis study to update the criteria used to certify and examine CISA candidates. The work is scheduled to be completed by the end of the year and results will be implemented beginning with the 2006 exam.

As a part of this process, a series of task force meetings and focus panels has been scheduled to gather information from experienced practitioners.

Chapter leaders interested in participating in focus panels or in recommending subject matter experts for future reviews should contact Kim Cohen at *kcohen@isaca.org* or +1.847.253.1545, ext.409.

ISACA Celebrates 35th Anniversary

The Information Systems Audit and Control Association celebrates its 35th anniversary this year. The association began as the EDP Auditor's Association in 1969. Today, its members number more than 28,000 from 100 countries. In addition, ISACA has more than 170 chapters worldwide.

More than 34,000 professionals have earned ISACAs globally recognized Certified Information Systems Auditor (CISA) designation since its inception in 1978. Within its first two years, ISACAs Certified Information Security Manager (CISM) designation is on track to certify 5,000 professionals.

For the past 35 years, ISACA has been the leading association of professionals in IS audit, control, security and governance.

Forum

ERFA-Bericht zum Kurs: ITIL Foundation Training (inkl. internationale Zertifizierung)

Dreitägiger Service Management Workshop auf der Basis des „de-facto"-Stanfards ITIL (mit übersichtlichem Prozessmapping ITIL – COBIT).

So die Ausschreibung der ISACA (Switzerland Chapter) für die vom 22. bis 24. Oktober 2003 in Zürich und in Zusammenarbeit mit der Firma Glenfis AG (mit Firmensitz in Hünenberg, ZG) durchgeführte Veranstaltung.

Mit einem Mix aus Theorie und praktischen Übungen sollten – gemäss Ausschreibung – die begrifflichen Grundlagen vermittelt und Einblick in die IT-Service-Management-Prozesse gegeben werden. Aktives Lernen und aktive Beteiligung, sprich Einbringen eigener Erfahrungen, sollten den Wissenstransfer unterstützen und die Vernetzung festigen. Mit den erworbenen Fachkenntnissen könnten eigene Serviceorganisationen nach ihrer Servicefähigkeit beurteilt und IT-Kernprozesse nach ITIL konzipiert werden.

Das alles liest sich gut, ist aber weiter nicht spektakulär. Viele Beratungs- und Schulungsfirmen partizipieren an der ITIL-Hype und werben, mit dem international anerkannten „best-practices"-Standard ITIL („Information Technology Infrastructure Library") die IT-Herausforderungen aktiv und strukturiert angehen zu können. Schliesslich war es der Zusatz: „ITIL und COBIT – im Kurs werden die Service-Management-Prozesse nach ITIL mit den korrespondieren COBIT-Prozessen verglichen", welcher ausschlaggebend war für meine Anmeldung.

Meine Erwartungen, einerseits einen Überblick über das Thema IT-Service-Management nach ITIL zu gewinnen und andererseits COBIT-Erfahrungen auszutauschen, schienen gegeben. Wie sind die Referenzmodelle COBIT und ITIL positioniert? Welches sind die Unterschiede, welches die Gemeinsamkeiten? Wie grenzen sie sich ab? Welches bringt den höheren Nutzen für die IT-Organisation und das ganze Unternehmen? Kurz, welches ist – soweit sich dies überhaupt beurteilen lässt – das bessere Modell? Diese und ähnliche Fragen waren es, über die ich mir eine Diskussion erhoffte. Erwartungen, die sich durchaus erfüllen sollten. Aber – dieses Fazit seit vorweggenommen – es gibt keine digitale Antwort zu ITIL oder COBIT.

IT-Service-Management-Initiativen

ITIL und COBIT sind beileibe nicht die einzigen Bemühungen, um die IT in den Griff zu bekommen. Die nachfolgende Übersicht des Instituts für Wirtschaftsinformatik (IWI) der Universität St. Gallen zeigt sehr schön die verschiedenen Initiativen um das IT-Service-Management.

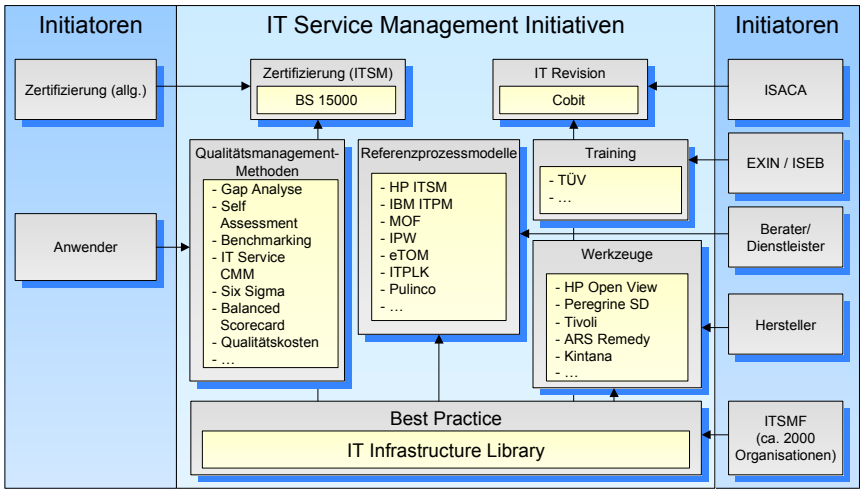


Abb. 1: IT Service Management Initiativen

Es ist unschwer zu sehen, dass einige Software-Lieferanten ihre Produkte auf die Prinzipien von ITIL ausgerichtet haben.

ITIL und seine Historie

Der IT-Dienstleistungsstandard ITIL wurde 1989 von der CCTA (Central Computing and Telecommunications Agency) für die britische Regierung mit dem Ziel entwickelt, Best Practices für 24 unterschiedliche Dienstleistungs- und IT-Support-Bereiche

zu definieren. Dazu gehören unter anderem Help Desk, Problem Management, Change Management und Softwareverteilung.

Was ist itSMF

Um sicherzustellen, dass ITIL auch die Anforderungen der realen Geschäftswelt erfüllt, brachte das OGC (Office of Government Commerce vormals CCTA) verschiedene nicht staatliche Gruppen in einer Stiftung namens itSMF (IT Service Management Forum) zusammen. Das itSMF ist eine lieferanten- und produkteunabhängige weltweite Vereinigung, deren Mitglieder den Erfahrungsaustausch zwischen IT-Dienstleistungsanbietern pflegen und fördern. Dazu gehören insbesondere die Verbesserung und Weiterentwicklung des de-facto-Standards ITIL sowie die Mitarbeit bei der Schaffung von Grundlagen für die Berufsausbildung im Bereich des IT-Service-Management. Die Aktivitäten von itSMF Switzerland sind auf der Homepage www.itsmf.ch publiziert.

Für wen wurde ITIL entwickelt?

Die IT Infrastructure Library wurde in erster Linie für Leute geschrieben, die für die Planung, Überwachung und Steuerung von qualitativ hochstehenden IT-Services verantwortlich sind. Die Bücher beschreiben hauptsächlich, was getan werden muss und weniger, wie es getan werden soll. Sie vermitteln jedoch insgesamt einen guten Überblick und ein gutes Verständnis der Zusammenhänge innerhalb einer IT-Serviceorganisation. Die Anleitung ist für Organisationen jeder Grösse, ob öffentliche Hand oder Privatwirtschaft, hilfreich und wird heute rund um den Erdball eingesetzt.

Die ITIL-Philosophie

Zusammengefasst werden die auf ITIL bezogenen Aktivitäten oft als die „ITIL-Philosophie“ bezeichnet. Darunter wird das Angebot an Dienstleistungen und Produkten verstanden, mit dem der de-facto-Standard im IT-Service-Management unterstützt wird. Dieses Angebot bietet dem Kunden die zur Entwicklung eines IT-Service-Management erforderlichen konsistenten Hilfestellungen. Die Bücher stellen heute lediglich noch einen Anteil von 1 % an den weltweit verkauften ITIL-Produkten und -Dienstleistungen dar (siehe auch Abb. 2).

Prozessmodell des IT-Service-Management nach ITIL

ITIL beschreibt ein systematisches und professionelles Vorgehen für das Management von IT-Dienstleistungen. Dabei stellt die Library nachdrücklich die Bedeutung der wirtschaftlichen Erfüllung der Unternehmens-Anforderungen in den Mittelpunkt. Das IT-Service-Management nach ITIL gliedert sich in die Kernbereiche IT Service Support und IT Service Delivery.

Kernprozesse des IT-Service-Supports dienen der Betriebsunterstützung und sind der operativen Ebene zuzuordnen:

- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release Management

Planende und steuernde Prozesse werden im IT-Service-Delivery-Set zusammengefasst, der taktischen Ebene des IT-Service-Management.

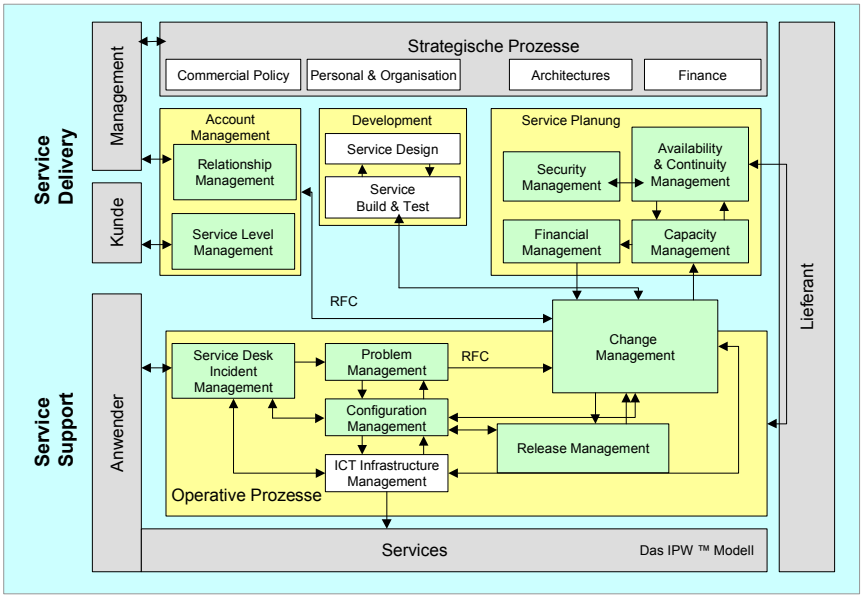


Abb. 2: IT-Service-Management-Architektur nach ITIL

- Service Level Management
- Financial Management
- Capacity Management
- Availability Management
- Continuity Management

IT-Security-Management wie auch das Qualitätsmanagement sind nicht als eigenständige Kernprozesse beschrieben. Als Querschnittsfunktionen sind sie auf der strategischen Ebene anzusiedeln und damit den Führungsaufgaben zugeordnet.

ITIL-Foundation-Kurs: Klare Struktur und adäquate Methodik

Im Mittelpunkt der dreitägigen Schulung standen natürlich die ITIL-Kernprozesse. Diese sind absolut technologie-unabhängig und deshalb weitgehend gültig für alle IT-Service-Management-Organisationen.
Ausgehend vom einem Prozessraster wurden die Prozesse von Service-Support und Service-Delivery erarbeitet, was dank der aktiven Beteiligung der Teilnehmer zu einer ausserordentlich kreativen und interessanten Arbeit wurde. Die allerseits eingebrachten IT-Service-Erfahrungen führten zu einem gelegenen Erfahrungsaustausch und zu angeregten Diskussionen.

Aufgrund des unterschiedlichen Backgrounds der Beteiligten kamen viele Aspekte ins Spiel, ja sogar internationale (ein Teilnehmer kam aus Wien). Alle Anwesenden hatten irgendwelche Erfahrungen mit Informatikprozessen und den allerorts initiierten Bestrebungen, diese zu optimieren. Schon bald war allgemein klar, dass mit ITIL das Rad

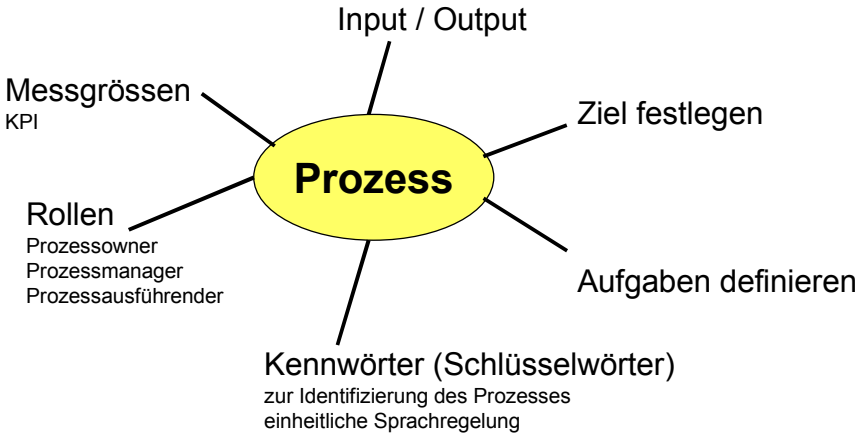


Abb. 3: Mindmap eines Prozesses

nicht neu erfunden wurde. Die Erkenntnis war, dass sich der de-facto-Standard als Regelwerk für einen strukturierten Aufbau eines IT-Service-Managements bestens eignet. Die Sollprozesse nach ITIL erlauben es, gaps in der eigenen IT zu identifizieren und Optimierungspotenziale auszuschöpfen. Die IT-Leistungen werden transparent und messbar (Benchmark).

Mir hat die Unterrichtsgestaltung sehr gepasst, nicht zuletzt deshalb, weil die Leiter des Workshops, Martin Andenmatten und Daniel Frutschi, sich gegen die Methode Powerpoint-Bombardement entschieden hatten. Mit bewährter Methodik wurden die Themen im Dialog erarbeitet, die Kernpunkte mittels Mindmap visualisiert und gefestigt und anhand von ergänzenden Beispielen aus Literatur und Praxis veranschaulicht und vernetzt.

Die beiden Moderatoren haben sich nicht nur sprachlich – echter Walliser Dialekt (Hr. Andenmatten) und Bünder/Berner-Gemisch (Hr. Frutschi) –, sondern auch inhaltlich ideal ergänzt. Sei es durch ihre breite Berufserfahrung, sei es durch die Art und Weise der Wissensvermittlung. Mehr Details seien an dieser Stelle nicht verraten.

ITIL COBIT Prozess Mapping

Dieser in der Ausschreibung speziell beworbene Punkt konnte aufgrund der Stoffdichte und der zur Verfügung stehenden Zeit nicht sehr tief angegangen werden. Es liegt in der Sache der Natur, dass für einen Vergleich zumindest Grundwissen über die zu vergleichenden Objekte vorhanden sein sollte. Da dem – verständlicherweise – nicht so war, war ein COBIT-Schnellabrieb angesagt. Ein echter Vergleich im Sinne einer Beurteilung der beiden Prozessmodelle gegenüber bestimmter Kriterien lag aufgrund des erwähnten Zeitfaktors in diesem Einführungskurs schlicht nicht drin. Für denjenigen, der sich tiefer mit dem Mapping befassen möchte, stellt der Kursordner ein geeignetes Nachschlagewerk dar. Er enthält das gesamte Mapping der ITIL- und COBIT-Prozesse, und zwar in beiden Richtungen. Nachfolgend ein Auszug:

DS	Auslieferung und Unterstützung	ITIL Prozesse
DS1	Definition und Management von Dienstleistungsgraden	ITIL Service Level Management
DS 1.1	Rahmen der Dienstleistungsvereinbarung	ITIL Service Level Management
DS 1.2	Aspekte von Dienstleistungsvereinbarungen	ITIL Service Level Management
DS	…	
DS2	Handhabung der Dienste von Drittparteien	ITIL Capacity & ITSCM & Security Mgmt
DS 2.1	Schnittstellen zu Lieferanten	ITIL Capacity Management
DS 2.2	Beziehungen zu Eignern	ITIL Capacity Management
DS 2.3	Verträge mit Drittparteien	ITIL Service Level Management
DS 2.4	Qualifikationen von Drittparteien	ITIL Capacity Management

Abb. 4: Auszug Kursordner

Das Mapping ist übrigens auch auf der Glenfis Homepage (www.glenfis.ch) als Download zugänglich.

ITIL und COBIT im Vergleich

Bezüglich des Vergleichs bin ich später dennoch fündig geworden. Das Institut für Wirtschaftinformatik (IWI) der Universität St. Gallen hat die Referenzmodelle die COBIT, ITIL und weitere nach formalen und pragmatischen Gesichtspunkten verglichen.

Meine eingangs aufgeworfene Frage nach dem besseren Referenzmodell lässt sich – wen wundert's – auch mit dem IWI-Vergleich nicht beantworten. Selbst wenn aufgrund der Kriterienliste ein klarer Sieger resultieren würde, wäre eine Antwort schwierig. Hinter den Modellen stehen unterschiedliche Initiatoren, dies ist klar. In der Zielsetzung, im Inhalt/Zweck aber liegen sie nicht sehr weit auseinander. Sowohl ITIL als auch COBIT bieten Praktiken, mit denen die vielfältigen Anforderungen der Stakeholder an die Informatik eines Unternehmens erfüllt

	Public-Domain		**Non-Public-Domain**	
Formale Kriterien	**ITIL**	**COBIT**	**IBM ITPM**	**HP ITSM Reference Model**
Ziele	**Ja**	**Ja**	Ja	Ja
Detaillierungsgrad	**hoch**	**hoch**	hoch	hoch
End-to-End	**Ja**	**Ja**	Ja	Ja
Konsistenz	**Nein**	**Ja**	Ja	Ja
I/O-Schema	**Hinweise**	**Nein**	Ja	Ja
Rollen/Verantwortlichkeiten	**Ja**	**Hinweise**	Ja	Ja
Instrumente	**Ja**	**Nein**	Ja	Ja
Pragmatische Kriterien				
Erfolgsfaktoren	**Hinweise**	**Ja**	Nein	Nein
Effektivitätskennzahlen	**Hinweise**	**Ja**	Nein	Nein
Effizienzkennzahlen	**Nein**	**Ja**	Nein	Nein
Implementierungshinweise	**Ja**	**Ja**	Ja	Ja
Klarheit/Einfachheit	**Nein**	**Ja**	Ja	Ja
Flexibilität	**Ja**	**Ja**	Ja	Ja
Weiterentwicklung	**Ja**	**Ja**	Ja	Ja
Verbreitung und Nutzung	**hoch**	**mittel**	mittel	mittel

Abb. 5: ITIL-COBIT-Vergleich (Quelle: IWI, HSG)

werden können. Einen Zauberkasten, mit dem sich, quasi per Zauberspruch, alle IT-Wünsche erfüllen lassen, ist weder das eine noch das andere Modell. Entscheidend ist die Umsetzung. ITIL und COBIT bieten dazu Unterstützung und zeigen einen Weg zur Einführung auf. Abhängen wird die erfolgreiche Implementierung von der Fähigkeit eines Unternehmens, Veränderungsprozesse zu managen. In diesem Fall gilt es, in der Informatik und weit darüber hinaus, eine Servicekultur aufzubauen. Das heisst u.U. weg von einer hierarchisch dominierten Führungsstruktur zu einem teamorientierten Aufbau mit motivierten, unternehmerisch und zielorientiert denkenden Mitarbeitenden. Die Theorie ist das eine, die Praxis das andere. Eine 1:1-Übertragung von theoretischen Modellen – ob ITIL oder COBIT – wird genauso zum Scheitern führen, wie die Unterschätzung von „kulturellen" Aspekten oder eine allzu euphorische Toolgläubigkeit. Ansonsten dürften für die erfolgreiche Realisierung gleiche oder ähnliche Schlüsselfaktoren gelten, wie wir sie aus anderen Veränderungsprojekten kennen: „Kritische" Kunden ins Boot, Fokussierung auf wenige aber wichtige Services, Support durch das Top Management (IT und Business) und Visualisierung des Status der IT.

Worauf der gegenwärtige ITIL-Boom zurückzuführen ist, kann ich nur vermuten. So war beispielsweise ITIL etlichen Mitarbeitern unseres Instituts ein Begriff, lange bevor ITIL oder COBIT offiziell zur Sache wurden. Vielleicht liegt es an der Vermarktung. Tatsache ist, dass zu ITIL ein breites Schulungs- und Beratungsangebot (inkl. Literaturangebot in deutsch) existiert. Vielleicht liegt es auch am Image: COBIT hat das Image des Kontrollmodells für die IT-Governance. ITIL hingegen stellt den Service-Management-Gedanken ins Zentrum. Es markiert daher einen idealen Bezugspunkt für unterschiedlichste Anbieter von Produkten und/oder Dienstleistungen. Ich denke da beispielsweise an all die Tools und Konzepte zur Einführung, Steuerung und Überwachung von Service Level Agreements (SLA). Diese Philosophie ist auch im Foundation-Kurs klar zum Ausdruck gekommen. Als Beispiel sei das Service Desk (Help Desk) erwähnt, welches im Workshop wie in Pausengesprächen häufiges und beliebtes Thema war. Als zentrale Verbindung zwischen IT und Fachabteilung kommt ihm eine Schlüsselfunktion zu. Viele Unternehmen haben die Wichtigkeit dieser „Visitenkarte" der Informatik erkannt und die Prozesse um diese First-Level-Supportorganisation zu verbessern begonnen. Dass ITIL in diesem Bereich ein starkes Gerüst mit klar definierten Rollen, Aufgaben und KPI bietet, mag ein weiterer Grund sein für die nach wie vor steigende ITI-Hype.

Qualifikation – ITIL Foundation-Zertifikat

Und weil auch hier galt: „No work is done until paperwork ist done", gab es am Schluss die international anerkannte ITIL-Foundation-Zertifikatsprüfung. Anlass genug, den TÜV auffahren zu lassen, welcher im Auftrag der beiden Prüfungszertifizierer EXIN (eine von der holländischen Wirtschaft geförderten Stiftung) und ISEB (Information Systems Examination Board) autorisiert ist, Prüfungen im deutschsprachigem Raum durchzuführen.

Die Prüfung hatte bei mir starke Erinnerungen an die CISA-Prüfung geweckt: Multiple-Choice, Verstehen der Logik, Prüfungssituation etc. aufgrund der Dauer von einer Stunde aber der Kategorie CISA-light oder -beginners zugeordnet werden konnte. Last but not least: An den Rahmenbedingungen (Technopark als Kursort, Räumlichkeiten, Verpflegung etc.) wie auch der Betreuung nach Kursabschluss gab und gibt es nichts zu bemängeln.

Oskar Stenz, Aarau

DACH-News

D: Aktivitäten des German Chapter

Das herausragende Ereignis der letzten Monate war wie jedes Jahr zu dieser Zeit die Mitgliederversammlung des ISACA German Chapter am 12. März im Frankfurter Hilton Hotel.

Auch dieses Jahr haben wieder viele interessierte und engagierte Mitglieder den Weg zu unserer Mitgliederversammlung gefunden, obwohl ein Punkt erstmalig nicht auf der Agenda zu finden war. Da im vergangenen Jahr der Vorstand erstmalig für zwei Jahre gewählt wurde, entfiel die Wahl in diesem Jahr. Somit startete die Veranstaltung am Vormittag zuerst mit einem Vortrag unseres Vorstandsmitglieds Markus Gaulke zu dem Thema „Risikomanagement in IT-Projekten“. Nach der Beantwortung und Diskussion von Fragen zum gehörten Vortrag setzten sich die Gespräche beim folgenden Mittagessen im Hotel fort.

Auf der am frühen Nachmittag beginnenden Jahresmitgliederversammlung wurden die Vereinsaktivitäten des letzten Jahres sowie die angedachten Vorhaben durch den Vorstand präsentiert. Der bisherige Vorstand wurde für das abgelaufene Jahr entlastet, aber eine Neuwahl musste nicht stattfinden. Somit war die einzige Wahl des Tages die des Kassenprüfers. Als nächster Punkt stand die Vorstellung der Workgroup zum Thema Linux, der Herr Neuy vorsteht, auf dem Programm. In diesem Rahmen wurden erstmalig Arbeitsergebnisse präsentiert, die sowohl inhaltlich als auch von der Präsentation der Oberfläche her alle Anwesenden beeindruckte. Man kann sicherlich sagen, dass hier ein erster Erfolg der Arbeitsgruppe nach nur einem Jahr deutlich sichtbar gemacht werden konnte. Für alle anderen ISACA-Mitglieder wird in naher Zukunft auch eine Möglichkeit der Einsicht in die Arbeitsergebnisse bestehen. Abschließend stellte uns Herr Rolf von Rössing das „Betriebliche Kontinuitätsmanagement“ der BCI vor. Das Thema ist für viele unserer Mitglieder besonders interessant, da es Schnittmengen zu den Themengebieten des ISACA beinhaltet und diese Bereiche noch weiter vertieft.

Die Mitgliederentwicklung mit einer Tendenz zu fast 600 Mitgliedern sowie die Kassensituation des Vereins sind sehr erfreulich. Dies ermöglicht dem German Chapter auch die Unterstützung aktiver regionaler Arbeitsgruppen sowie von bestehenden oder neuen Workgroups. Eine Workgroup zum Thema SAP ist derzeit im Entstehen und interessierte Mitglieder werden hiermit aufgerufen, sich gern daran zu beteiligen. Weitere Informationen zu Arbeitsgruppen oder Workgroups sowie die Unterstützung durch das German Chapter finden sich in unserem Mitgliederbereich unter www.isaca.de oder lassen sich über Herrn Wojtyna erfragen.

Das Protokoll der Mitgliederversammlung wird demnächst noch separat an alle Mitglieder versandt.

Die diesjährigen CISA-Vorbereitungskurse des German Chapters werden in Hamburg und Frankfurt stattfinden. Die im vorletzten Jahr überarbeitete Struktur in der Form von Wochenendseminaren an jeweils zwei Wochenenden und einem abschließenden CISA-Testexamen als Generalprobe in Frankfurt wird beibehalten. Weitere Informationen (auch für Nachzügler) sind unter www.isaca.de zu finden.

Zum Schluss möchten wir noch alle Mitglieder dazu auffordern, den *NewsLetter* verstärkt als Basis für den Wissens- und Erfahrungsaustausch zu nutzen sowie die Möglichkeit in den neuen Workgroups mitzuarbeiten oder auch eine Workgroup ins Leben zu rufen zu nutzen, da der Berufsverband letztlich von den Aktivitäten seiner Mitglieder lebt.

Ingo Struckmeyer

CH:

Aus der Generalversammlung des Switzerland Chapters vom 18. März 2004 in Bern

Vorgängig der GV präsentierte Tobias Murer für seinen Chef Stefan Arn – Entrepreneur of the Year 2003 – der Firma Adnovum Informatik AG die praktizierte Vorgehensweise beim „Relay-Programming“ (24-Stunden-Entwicklung). Die kompetenten und illustrativen Darlegungen

wurden mit diversen Beiträgen und Fragen von den anwesenden Mitgliedern bereichert, so dass sich eine rege und interessante Diskussion ergab. Eigentlich schade, dass nur gerade 32 Leute den Weg nach Bern fanden. Die Abwesenden haben etwas versäumt! Angeregt wurde eine IG, die sich mit dem Referatsthema befasst. Interessierte melden sich bitte bei Rolf Merz.

Wie gewohnt berichteten die Vorstandsmitglieder über ihre Ressorts; zum einen legten sie Rechenschaft über das verflossene Geschäftsjahr ab, zum andern zeigten sie ihre Absichten in einem Ausblick für 2004.

- Im Zentrum steht eindeutig die erfolgreiche Durchführung der euroCACS 2004 in Zürich-Kloten.
- Die Präsidentin Daniela Gschwend gab die Absicht des Vorstandes bekannt, sich 2004 nach der euroCACS vermehrt „nach innen“, d.h. zugunsten der Mitglieder des Chapters, zu orientieren.
- Der für die Publicity zuständige Ressortleiter Bruno Wiederkehr wird dies durch Werbung für die CH-Mitglieder unterstützen.
- Die homepage wurde überarbeitet und aktualisiert. Ein Besuch lohnt sich.
- 42 Teilnehmer der CISA-Prüfung haben bestanden, was über 87 % entspricht. Eine beachtliche Rate.
- Derzeit sind in der Schweiz 31 CISM registriert, von denen einer die Prüfung bestand, die übrigen sich mit der „Grandfather-Clause“ qualifizierten.
- Die neue IG Forensics war im vergangenen Jahr nur in der Romandie aktiv. Eine Ausdehnung „schweizweit“ ist geplant.
- Auch dieses Jahr soll ein Seminar in Zusammenarbeit mit der Kammer stattfinden (23. Juni 2004). Das Thema ist „Professional Judgement bei Informatikanwendungen“.

Einige Unruhe bewirkte der Umstand, dass das Chapter 2003 einen beträchtlichen Verlust einfuhr. Grund dafür ist der Einbruch der Teilnehmerzahlen bei der Ausbildung, die in der Vergangenheit nicht nur selbsttragend, sondern sehr gewinnbringend, war. Dieser Rückgang seinerseits ist auf die Konjunkturlage mit dem Zusammenstreichen der Budgets der Firmen zurückzuführen. Nach Ansicht nicht nur des Ressortleiters Peter Bitterli vielerorts eine falsche, wenn nicht fatale, Entscheidung. Die Mitglieder waren mehrheitlich der Ansicht, dass die Ausbildung ein wichtiger Bestandteil des Chapterlebens ist und genehmigten entsprechend ein erneut negatives Budget. Die Details werden durch den Vorstand ausgearbeitet, der sich einstimmig bestätigen liess.

Trotz nicht so sehr rosiger, wohl eher roter, Finanzlage offerierte der Vorstand auch dieses Jahr das anschliessende Mittagessen. Die Gelegenheit wurde intensiv für ein erfolgreiches „Networking“ benutzt. Für etliche Mitglieder war die ganze Veranstaltung sicher mehr als eine CPE-Stunde wert.

Auszeichnung

Die beiden Chairs vom euroCACS 2004 Conference Programme Committee (Daniela Gschwend) und vom Conference Partnering Chapter Committee (Thomas Bucher) haben von ISACA „international“ je eine Auszeichnung für Ihren erfolgreichen Einsatz erhalten. Überreicht wurden die Awards von Robert Bergquist, ISACA Staff Liaison für das Programme Committee.

Ohne die Unterstützung der jeweiligen Teamkollegen wäre die euroCACS2004 nicht so positiv ausgefallen. Wir möchten uns bei allen Kolleginnen und Kollegen ganz herzlich für Ihr Mitmachen bedanken.

News aus den Interessengruppen

IG Operational IT-Risk/Basel II

Neu!

Peter R. Bitterli
Bitterli Consulting AG
Konradstrasse 1
8005 Zürich
Tel. + 41 1 440 33 60
Fax. +41 1 440 33 61
prb@bitterli-consulting.ch

Interessenten melden sich bitte bei Peter R. Bitterli

IG Government IT-Audit („Closed user group“)

Michel Huissoud, CISA, CIA
Eidg. Finanzkontrolle/
Contrôle fédéral des finances
Monbijoustr. 45
3003 Bern
Tel. +41 31 323 10 35
Fax. +41 31 323 11 00
Michel.Huissoud@efk.admin.ch

Programme 2004 :

- 4.5.2004 : Risiken und Best practices bei einer SAP-Einführung
- Les séances suivantes auront lieu les 24.8.2004 et 16.11.2004.

La participation à ce groupe est réservée aux collaborateurs des organes de contrôle.

IG Computer Forensics

Nouveau!

Paul Wang
PricewaterhouseCoopers
Avenue Giuseppe-Motta 50
1211 Geneva 2
Tel. +41 22 748 56 01
Fax. +41 22 748 53 54
Mobile: +41 79 220 54 07
Paul.Wang@ch.pwc.com

L’objectif de ce groupe de discussion lié aux « Computer Forensics », est de fournir un forum d’intérêt et d’information sur les méthodologies et les outils de ce qu’on appelle communément en français « Assistance informatico-légale » Ce forum offre la possibilité de partager des idées, des technologies, des outils et certainement aussi des notions juridiques de ce domaine en constante évolution. Ce groupe de discussion abordera également des discussions techniques et procédurales sur les prérequis en matière de recherche de preuves informatiques. Même si les participants doivent être familiers avec la recherche, l’acquisition et l’analyse de preuves informatiques, tous les intéressés de tout niveau de connaissance sont les bienvenus.

IG Einführung von IT-Governance

Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
rolf.merz@ch.ey.com

Letzte Sitzung: Kick-off Sitzung am 4. März 2004, bei Ernst & Young AG, Zürich

Nächste Sitzung: Donnerstag, 6. Mai 2004, 09.00 bis ca. 12.00 Uhr, Ernst & Young AG, Bleicherweg 21, 8022 Zürich, Sitzungszimmer Rom

Traktanden:

- Präsentation der beiden Pilotprozesse PO1 und PO10
- Festlegen Weiteres Vorgehen

IG Romandie

Vacant : touts personnes intéressées à participer ou animer un groupe de travail ou tous ceux qui aimeraient proposer un thème de réflexion peuvent s’annoncer auprès de M. Paul Wang.
paul.wang@ch.pwcglobal.com

IG Outsourcing/Insourcing

Ulrich Engler
Swiss Life
CF/REV HG 3151
General-Guisan-Quai 40
Postfach, 8022 Zürich
Telefon +41 43 284 77 58
Telefax +41 43 284 47 33
ulrich.engler@swisslife.ch

Nächste Sitzung: Offen. Interessenten melden sich bei Ueli Engler.

Mögliche Themen: Kontiniuität des Insourcers, Abhängigkeit vom Insourcer (Konkurs), Überarbeitetes Rundschreiben EBK, Fernwartung, etc.

Geplant sind *Gespräche* zum Thema „Grounding“ eines IT Service Providers mit ausgewählten Gesprächspartnern aus den Bereichen Legal, Service Provider, Industrie und Financial Services.

IG MIS/EIS/DWH

Leitung:
Daniel Oser
Ernst & Young AG
Badenerstrasse 47
Postfach 5272
8022 Zürich
Tel. +41 58 286 34 39
Fax. +41 58 286 32 76
daniel.oser@ch.ey.com

Letzte Sitzung: Die letzte Sitzung fand am 16. Januar 2004 bei Ernst & Young am Bleicherweg statt.

Traktanden:
- Referenzmodell Data Load
- Risk Matrix
- Fact Sheets

Nächste Sitzungen: Anfang April 2004 bei Ernst & Young AG, Bleicherweg 21, 8022 Zürich
Für Informationen melden Sie sich bitte bei Daniel Oser.

IG SAP R/3

Monika E. Galli Mead
Eidg. Finanzkontrolle
Monbijourstrasse 51a
3003 Bern
Tel. +41 31 324 9495
Fax. +41 31 323 1101
monika.galli@efk.admin.ch

Letzte Sitzung: Donnerstag, 13. November 2003, 10.00 Uhr, PwC, Stampfenbachstrasse 73, 8035 Zürich

Traktanden:
1. Begrüssung
2. Vorstellung des Implementierungs-Review Tool „TeamMate“ (Fr. F. Seheri, PwC)
3. Enterprise oder die neue Architektur der SAP (Hr. Ch. Winzer, BIT)
4. Neues Berechtigungskonzept BV (M. Galli)
5. Java und ABAP (Hr. X, BIT)
6. Neues aus der Arbeitsgruppe SAP-Security (FGSec SAP) (M. Galli)
7. Erfahrungen und News (alle)

Nächste Sitzung: Donnerstag, 13. Mai 2004 in Bern

Vorläufige Themen:
- Java und ABAP
- Erfahrungen und News

WILDHABER Consulting

Unternehmensberatung & Unternehmensführung
IT Governance & Compliance
Strategic IT Auditing
Electronic Archiving
Datenschutz
IT Security
Consult the Consultant

Welche Rolle soll die IT im Unternehmen einnehmen ?
Was ist IT Governance?
Wie kann man mit IT Werte generieren?
Was bedeutet Sarbanes-Oxley für uns?
Welchen IT Risiken sind wir ausgesetzt?
Wie soll man technische, organisatorische und rechtliche Massnahmen kombinieren und messen?
Wie kann man IT Governance dem Top Management kommunizieren?

Sind ihre Berater oder Revisoren diesen Fragen gewachsen?

Wenn nicht, sollten sie uns kontaktieren:

Wildhaber Consulting
Zimikerried 15
8603 Schwerzenbach / Schweiz
Tel. +41 1 826 21 21
info@wildhaber.com / www.wildhaber.com

Veranstaltungen

Vertiefung BS7799	22.–23. April 2004 Zürich, 2 Tage, Infosec
Grundkurs für Informations- und IT-Sicherheitsbeauftragte	26.–30. April 2004 Zürich, 5 Tage, Infosec
Forensic Investigation – Aufdeckung und Analyse von Wirtschaftsdelikten	28.–30. April 2004 Zürich, 3 Tage, ISACA CH
Testprüfung CISA und CISM (Besprechung CISA am 24.5.2004/CISM am 25.5.2004)	15. Mai 2004 Zürich, 1 Tag, ITACS Training AG
SSI Fachtagung: Arbeitssicherheit und… wo bleibt der Gesundheitsschutz?	26. Mai 2004 Zürich, 1 Tag, MediaSec
PRINCE2 – Planung und Organisation mit flexibler Projektmanagement-Methode	2.–4. Juni 2004 Zürich, 3 Tage, ISACA CH
Intensivlehrgang für Informations- und Sicherheitsbeauftragte	14.–18. Juni 2004 Zürich, 5 Tage, Infosec
BS7799 Implementation	16.–18. Juni 2004 Zürich, 3 Tage, InfoGuard
Auditorenkurs nach BS7799	21.–25. Juni 2004 Zürich, 5 Tage, Infosec
Securing and Auditing Windows 2000 Server	6.–9. Juli 2004 London, 4 Tage, MIS
SAP R/3 – Workshop „Grundlagen“ für Wirtschafts- und Informatikprüfer	17.–20. August 2004 Stuttgart, 4 Tage, ISACA CH
SAP R/3 – Workshop „Prüfung von Geschäftsprozessen“ für Wirtschafts- und Informatikprüfer	23.–25. August 2004 Stuttgart, 3 Tage, ISACA CH
Evidence Lab – Workshop über die Spurensuche in Computersystemen	30. August – 1. September 2004 Zürich, 3 Tage, ISACA CH
Application Security Lab – Workshop zum Thema Sicherheit von Web-Anwendungen	7.–9. September 2004 Zürich, 3 Tage, ISACA CH
Internet Security Lab – Workshop mit Angriffsszenarien und Abwehrmassnahmen	28.–30. September 2004 Zürich, 3 Tage, ISACA CH

Kontaktadressen Veranstalter

Der *NewsLetter* empfiehlt folgende Veranstalter (weitere Kurse und Unterlagen direkt anfordern):

AFAI
Tel. +33 1 55 62 12 22
afai@afai.asso.fr
www.afai.asso.fr

advanced technology seminars
Grundgasse 13
CH-9500 Wil
Tel. +41 71 911 99 15
Fax. +41 71 911 99 16
Maurer@inf.ethz.ch

Stiftung für Datenschutz und Informationssicherheit
Dr. Beat Rudin
Kirschgartenstrasse 7
Postfach
CH-4010 Basel
Tel. +41 61 270 17 70
Fax +41 61 270 17 71
beat.rudin@privacy-security.ch
www.privacy-security.ch

e-tec Security
PO Box 54
Wilmslow Chesire SK9 6FU
United Kingdom
info@a-tecsecurity.com

Euroform Deutschland GmbH
Hans-Günther-Sohl-Strasse 7
D-40235 Düsseldorf
Tel. +49 211 96 86 300
Fax. +49 211 96 86 509
info@euroforum.com

Hochschule für Technik Rapperswil
Institut für Internet Technologien und Anwendungen
Oberseestrasse 10
8640 Rapperwil
Tel. +41 55 222 41 11
Fax. +41 55 222 44 00
office@hsr.ch

IIR-Akademie
Ohmstr. 59
D-60468 Frankfurt/Main
Tel. +49 69 7137 69-0
Fax. +49 69 7137 69-69
iir.academie@iir-ev.de

InfoGuard AG
Feldstrasse 1
CH-6300 Zug
Tel. +41 41 749 19 00
Fax +41 41 749 19 10
www.infosec.com

Integralis GmbH
Gutenbergstr. 1
D-85737 Ismaning
Tel. +49 89 94573 447
Fax +49 89 94573 199 fx
schulung@integralis.de

ISACA CH
Kurssekretariat
c/o. ITACS Training AG
Konradstr. 1
8005 Zürich
Tel. +41 1 440 33 64
Fax. +41 1 440 33 61
kurse@isaca.ch

ISACA USA
3701 Algonquin Rd #1010
USA_Rolling Meadows IL 60008
Tel. +1 847 253 15 45
Fax. +1 847 253 14 43
www.isaca.org

Marcus Evans
Weteringschans 109
1017 SB, Amsterdam
The Netherlands
Tel. +31 20 531 28 13
Fax. +31 20 428 96 24
www.marcusevansnl.com

MIS Training Institute
Nestor House
Playhouse Yard P.O. Box 21
GB-London EC4V 5EX
Tel. +44 171 779 8944
Fax. +44 171 779 8293
www.misti.com

MediaSec AG
Tägernstrasse 1
8127 Forch/Zürich
Tel. +41 1 360 70 70
Fax. +41 1 360 77 77
it@mediasec.ch

Secorvo Security Consulting GmbH
Secorvo College
Albert-Nestler-Strasse 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455
info@secorvo.de
www.secorvo.de

Treuhand-Kammer
Jungholzstrasse 43
Postfach
CH-8050 Zürich
Tel. +41 1 305 38 60
Fax. + 41 1 305 38 61

ZfU Zentrum für Unternehmensführung AG
Im Park 4
CH-8800 Thalwil
Tel. +41 1 720 88 88
Fax. +41 720 08 88
info@zfu.c

Germany Chapter

Vereinsadressen

Geschäftsstelle
ISACA e.V., German Chapter
Eichenstr. 7
D-46535 Dinslaken
Tel. +49 2064 733191
Fax. +49 2064 733192
isaca.dinslaken@t-online.de

Präsidentin
Karin Thelemann
Ernst & Young AG
Wirtschaftsprüfungsgesellschaft
Mergenthalerallee 10–12
65760 Eschborn/Frankfurt am Main
Tel. +49 6196 99626 488
Fax. +49 6196 99626 449
karin.thelemann@de.ey.com

Konferenzen
Markus Gaulke
KPMG
Marie-Curie-Str. 30
D-60439 Frankfurt
Tel. +49 69 9587 2313
Fax. +49 69 9587 192313
MarkusGaulke@kpmg.com

Mitgliederverwaltung und Kassenwart
Norbert Gröning
PwC Deutsche Revision AG
Friedrich-List-Str. 20
D-45128 Essen
Tel. +49 201 438 0
Fax. +49 201 438 1000
Norbert.Groening@
de.pwcglobal.com

Public Relations
Heinrich Geis
Deutsche Börse AG
Neue Börsenstrasse 1
D-60487 Frankfurt
Tel. +49 692 101 5149
Fax. +49 692 101 4396
heinrich.geis@deutsche-boerse.com

Arbeitskreise und Facharbeit
Bernd Wojtyna
WLSGV-Prüfungsstelle
Regina-Portmann-Strasse 1
D-48159 Münster/Westfalen
Tel. +49 251 288 4253 oder
+49 251 210 4539
bernd_wojtyna@gmx.net

Publikationen
Ingo Struckmeyer
comdirect private finance AG
Pascalkehre 15
25451 Quickborn
Tel. +49 4106 704 2336
Fax. +49 4106 704 2301
ingo.struckmeyer@pf.comdirect.de

CISA-Koordinator
Michael M. Schneider
Deloitte & Touche
Schumannstraße 27
60325 Frankfurt am Main
Tel. +49-69 75606 121
Fax. +49-69 75695 84448
michaelschneider@deloitte.de

Austria Chapter

Vereinsadressen

Vorsitzender (Präsident)
Ing. Mag. Dr. Michael Schirmbrand, CIA, WP, StB
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 211 70-2831
michael.schirmbrand@at.eyi.com

Stellvertretender Vorsitzender I (Vizepräsident I)
Dipl.-Ing. Maria-Theresia Stadler,
Österreichische Kontrollbank Aktiengesellschaft
Strauchgasse 1–3
1010 Wien
Tel: +43 1 531 27-857
maria-theresia.stadler@oekb.co.at

Stellvertretender Vorsitzender II (Vizepräsident II)
Mag. Josef Renner, StB
GRT Price Waterhouse
Prinz-Eugen-Straße 72
1040 Wien
Tel: +43 1 50188-0

Sekretär
Mag. Gunther Reimoser, CISA
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 21170-4113
gunther.reimoser@at.eyi.com

Kassier
Mag. Helmut Zodl
IBM Österreich
Obere Donaustraße 95
1020 Wien
Tel: +43 1 21145-0
helmut_zodl@at.ibm.com

CISA/CISM-Koordinatorin
Mag. Ulrike Knödlstorfer-Ross, MBA
Certified Internal Auditor
Certified Information System Auditor
Interner Revisionsdienst
Agrarmarkt Austria
Dresdner Str. 70
1200 Wien

Public Relations/Newsletter-Koordination
Rolf von Rössing
MA, D.E.s.s, CBCP, MBCI
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 211 70-2812
dk@cos-ag.de

E-Mail ISACA Austria Chapter:
office@isaca.at
Homepage ISACA Austria Chapter:
www.isaca.at

Switzerland Chapter

Vereinsadressen

Präsidentin
Daniela S. Gschwend
Swiss Re
Mythenquai 50/60
8022 Zürich
Tel. +41 43 285 69 36
Fax. +41 43 285 33 69
daniela_gschwend@swissre.com

Vizepräsident
Michel Huissoud, CISA, CIA
Eidg. Finanzkontrolle/
Contrôle fédéral des finances
Monbijoustr. 45
3003 Bern
Tel. +41 31 323 10 35
Fax. +41 31 323 11 00
Michel.Huissoud@efk.admin.ch

Kassier
Pierre A. Ecoeur, CISA
Thurgauer Kantonalbank
Bankplatz 1
8570 Weinfelden
Tel. +41 71 626 64 61
Fax. +41 71 626 63 60
pierre-alain.ecoeur@tkb.ch

Ausbildung/Kurssekretariat
Peter R. Bitterli, CISA
Bitterli Consulting AG
Konradstr. 1
8005 Zürich
Tel. +41 1 440 33 60
Fax. +41 1 440 33 61
prb@bitterli-consulting.ch

CISA/CISM-Koordinator
Thomas Bucher
Ernst & Young AG
Postfach
8022 Zürich
Tel. +41 58 286 42 90
Fax. +41 58 286 40 14
thomas.bucher@ch.ey.com

Sekretär
c/o Präsidentin

Information & Kommunikation
Monika Josi
Novartis Animal Health
Global Information Technology
WRO-1032.1.90
4022 Basel
Tel. +41 61 697 72 41
Fax. +41 61 697 78 44
monika.josi@ah.novartis.com
Adressmutationen bitte hier melden.

Koordinator Interessengruppen
Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
Rolf.Merz@ch.ey.com

Représentant Suisse Romande
Paul Wang
PricewaterhouseCoopers
Avenue Giuseppe Motta 50
1211 Genève 2
Tel. +41 22 748 56 01
Fax. +41 22 748 53 54
paul.wang@ch.pwcglobal.com

Marketing
Bruno Wiederkehr
Rigistrasse 3
CH-8703 Erlenbach
bru.wiederkehr@bluewin.ch

Homepage ISACA Switzerland Chapter: www.isaca.ch