Nr. 80 | Juli 2006
Juillet 2006
July 2006

Focus:

COBIT 4.0

Liebe ***NewsLetter*** Leserinnen und Leser: ***Texte français voir au verso***

Der Entschluss des ISACA Chapter Germany, die Zusammenarbeit bezüglich ***NewsLetter*** mit dem Schweizer Chapter einzustellen, ergibt eine neue Situation. Wir ergreifen die Gelegenheit, Sie nach Ihrer Meinung zu unserem Publikationsorgan in der heutigen Form zu fragen.

Nehmen Sie sich bitte fünf Minuten Zeit, um den folgenden Fragebogen auszufüllen und zurückzuschicken an:

Max F. Bretscher, KPMG, Badenerstrasse 172, CH-8004 Zürich (Schneckenpost) bzw. 044 249 20 29 (Fax), bzw. mbretscher@kpmg.com (e-Mail). Fragebogen in elektronischer Form auf www.isaca.ch verfügbar.

Name und Adresse:
……

……

……

ISACA Chapter: ……

Ich möchte den Switzerland Chapter ***NewsLetter*** jährlich erhalten
☐ 1 Mal
☐ 2 Mal
☐ 3 Mal
☐ 4 Mal
☐(wie bisher) 5 Mal

☐ Ich wünsche den ***NewsLetter*** in Papierform
☐ Download von der ISACA Switzerland Homepage in einer Closed User Group
☐ Beides

Ich bevorzuge Artikel in
☐ Deutsch
☐ Français
☐ English

Ich habe folgende Vorschläge zur Verbesserung des ISACA Switzerland ***NewsLetters***:

……

……

……

……

Zusätzliche Fragen für Leserinnen und Leser in Deutschland und/oder Österreich:
☐ Ich möchte auch in Zukunft den ***NewsLetter*** des ISACA Switzerland Chapters erhalten
☐ Ich wäre bereit, einen Beitrag von EUR 20 für Druck und Porto zu leisten

Zusätzliche Fragen für unsere französisch sprechenden Leserinnen und Leser:
Siehe bereits versandte Umfrage betreffend ***Revue de l'AFAI*** (ankreuzen, wenn nicht erhalten)

Chère lectrice et cher lecteur, ***Deutscher Text auf Rückseite***

Suite à la décision du chapitre allemand de l'ISACA d'émettre sa propre publication périodique, une nouvelle situation se dessine pour nous. Ainsi, nous profitons de cette opportunité pour lancer une enquête sur vos attentes concernant la ***NewsLetter*** afin de pouvoir, nous l'espérons, répondre au mieux à vos attentes.

Nous vous remercions d'avance de nous accorder 5 minutes afin de remplir le questionnaire ci-dessous et de nous le retourner à : Max F. Bretscher, KPMG, Badenerstrasse 172, CH-8004 Zürich (courrier), 044 249 20 29 (Fax), ou mbretscher@kpmg.com (e-Mail). Questionnaire électonique disponible chez www.isaca.ch.

Nom et adresse

……

……

……

Chapitre de l'ISACA: ……

1. A quelle fréquence souhaiteriez-vous recevoir notre ***NewsLetter***

☐ 1 x par an
☐ 2 x par an
☐ 3 x par an
☐ 4 x par an
☐ 5 x par an (statu quo)

2. Quel est votre média préféré?

☐ Format papier
☐ Download depuis la page principale ISACA (closed user group)
☐ Format papier et électronique

3. Langue***:*** je préfère des articles en

☐ Allemand
☐ Français
☐ Anglais

4. Ce que je propose pour améliorer la ***NewsLetter*** :

……

……

……

Pour nos lecteurs de l'Allemagne et de l'Autriche:

☐ Je désire de recevoir la NewsLetter Suisse aussi à l'avenir.
☐ Dans ce cas serais préparé de contribuer EUR 20 pour les frais

Questions supplémentaires pour nos lecteurs en français concernant la Revue de l'AFAI voir questionnaire séparé déjà envoyée(indiquez si pas reçu).

✂

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Inhaltsverzeichnis

Editorial 6

CobiT 4.0 – CobiT 4.0 apporte-t-il une réponse aux attentes du PCAOB ? 7

CobiT 4.0 – Bringt CobiT 4.0 eine Antwort auf die Erwartungen des PCAOB? 13

CobiT 4.0 – Von CobiT 3rd edition zu CobiT 4.0 in 30 Sekunden? 18

CobiT 4.0 – Vergleich CobiT 3 vs. CobiT 4 19

The ISACA Crossword Puzzle 24

Express Line 26

DACH-News 27

Veranstaltungen 32

Vereinsadressen 34

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o Monika Josi
Novartis International
WSJ 210.12.31
4002 Basel

Redaktion:
Max F. Bretscher
KPMG Fides Peat
Badenerstrasse 172
8026 Zürich
mbretscher@kpmg.com

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.

Preise:
Mitglieder gratis
Abonnement CHF 35.–/Jahr
Einzelnummer CHF 10.–

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

Erscheint 4 Mal jährlich
Auflage: 1350 Exemplare

Nächste Ausgabe (Focus: e-Mail): November 2006, Redaktionsschluss: 10. Oktober 2006

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Editorial

Der Schock sitzt tief. Der Entschluss des Germany Chapters, die Zusammenarbeit mit dem Switzerland Chapter bezüglich ***NewsLetter*** aufzukündigen, zeigte Wirkung.

Bei der Redaktion gingen diverse Reaktionen aus Deutschland ein, welche den Entschluss bedauerten. Daneben wurden Stimmen laut, welche am Fortbestehen des ***NewsLetters*** Zweifel aufkommen liessen. Der Vorstand des Switzerland Chapters beschloss in Zusammenarbeit mit der Redaktion, eine Umfrage bezüglich Bedürfnis nach einem Publikationsorgan zu starten.

Eine Umfrage – siehe Beilage – soll nun klären, wie es mit dem ***NewsLetter*** (wenn überhaupt) weiter gehen soll. Dabei soll jenen Interessenten aus Deutschland die Möglichkeit geboten werden, den Schweizer ***NewsLetter*** mit relativ geringen Kostenbeiträgen weiter zu erhalten. Verschiedentlich war auch angeregt worden, dass der ***NewsLetter*** in elektronischer Form versandt oder zur Verfügung gestellt werden könnte. Leider scheint wenig bekannt zu sein, dass dies seit einiger Zeit der Fall ist, allerdings mit einer Zeitverzögerung von etwa zwei Monaten. Auch dieser Aspekt wird mit der Umfrage beleuchtet.

Die Redaktion bittet Sie, die beiliegende Umfrage so schnell wie möglich zu beantworten, damit den echten Bedürfnissen der ISACA-Mitglieder nachgekommen werden kann.

Der ***NewsLetter*** hatte sich in den letzten Jahren bemüht, auch den Französisch sprechenden Lesern in ihrer Muttersprache zur Verfügung zu stehen. So wurden verschiedene Artikel übersetzt, teilweise auch solche nur in Französisch abgedruckt. Leider musste immer wieder zur Kenntnis genommen werden, dass die Romands den ***NewsLetter*** gar nicht beachteten. Als einstweilige Massnahme wurde den francophonen Mitgliedern des Switzerland Chapters letztes Jahr ***zusätzlich*** zum ***NewsLetter*** gratis die Publikation ***Revue de l'AFAI*** zugestellt. Obschon dies bei vielen Empfängern geschätzt wurde, konnte die Auswahl nicht befriedigen, weil sie nach Postleitzahl erfolgte (ein anderes Kriterium stand nicht zur Verfügung). Es ist aber wohl unbestritten, dass auch Romands in der Deutschschweiz (oder Deutschland) leben; umgekehrt Deutschschweizer im Welschland tätig sind. Als weitere Massnahme wurde die Titelseite neu mehrsprachig gestaltet, um die „Nichtdeutsch" sprechenden Leser weniger abzuschrecken.

Die vorliegende Nummer hat den Schwerpunkt CobiT 4.0. Es scheint, dass die Erfahrungen in dieser Hinsicht noch mager sind, weshalb die Beiträge spärlich eingingen. Oder liegt es an den Zweifeln über das Fortbestehen des ***NewsLetters***? Wie auch immer: Viel Spass bei der Lektüre und besten Dank für die Rücksendung des Fragebogens!

Herzlichst,

MadMax Bretscher

Le choc est rude. La décision du chapitre allemand de l'ISACA d'interrompre sa collaboration avec notre ***NewsLetter*** a entraîné de nombreuses réactions.

Plusieurs lecteurs allemands ont regretté cette décision, d'autres personnes ont émis des doutes sur l'opportunité de poursuivre la publication de notre périodique. Afin de pouvoir décider en connaissance de cause, le comité suisse de l'ISACA a décidé en accord avec la rédaction de lancer une enquête pour connaître les attentes des lecteurs.

Cette enquête que vous trouverez en annexe va nous permettre de décider de l'avenir de la ***NewsLetter***. Il s'agit d'une part de réfléchir au contenu, mais également de sonder nos lecteurs allemands pour savoir s'ils sont disposés à payer une modeste contribution pour continuer à recevoir notre revue. Un autre point concerne le mode de diffusion : papier, forme électronique, les deux ? C'est l'occasion de rappeler que les ***NewsLetters*** sont aujourd'hui déjà disponibles sous forme électronique sur le site www.isaca.ch, avec un décalage temporel d'environ deux mois.

La rédaction vous remercie de répondre rapidement à cette enquête, dont les résultats devraient nous permettre de prendre les bonnes décisions.

Un dernier mot sur le bilinguisme de notre revue. La ***NewsLetter*** s'est efforcé ces dernières années d'offrir aux lecteurs francophones des articles dans leur langue maternelle. Des articles ont été traduits, certains n'ont même été publiés qu'en français. Malheureusement souvent sans grand succès. Le comité a alors décidé d'offrir gratuitement aux membres habitant la Suisse romande – en plus de la ***NewsLetter*** suisse – ***la Revue de l'AFAI***. Cette mesure a été

très appréciée mais elle présentait l'inconvénient de ne reposer que sur une sélection du code postal de l'adresse de nos membres, ignorant de fait les romands établit en Suisse allemande. La dernière mesure destinée à capter l'attention de nos lecteurs romands est de produire une page de titre en deux langues, afin de signaler plus clairement le caractère bilingue du contenu du journal.

Le présent numéro est consacré à CobiT 4.0. Un sujet d'actualité mais qui n'a pas suscité beaucoup de réactions de la part des membres. Il semble manquer d'auteurs disposant d'expériences dans ce domaine. Ou la rareté des articles tient-elle à l'incertitude quant à l'avenir de la ***NewsLetter*** ? Dans tous les cas, bonne lecture et merci de nous renvoyer votre questionnaire !

Cordialement,

MadMax Bretscher

CobiT 4.0

CobiT 4.0 apporte-t-il une réponse aux attentes du PCAOB ?

Oui, mais…! CobiT 4.0 est l'instrument privilégié pour concevoir et auditer les contrôles informatiques. Mal utilisé, il peut cependant conduire à des audits surdimensionnés. Il doit en outre être complété par une analyse des contrôles applicatifs. Ce domaine réserve encore et toujours des surprises qu'un auditeur averti devrait découvrir avant la presse spécialisée…

L'audit du système de contrôle interne (SCI) est revenu en force et c'est tant mieux. La mise en œuvre des règles du PCAOB[1], l'organe de surveillance de la Bourse américaine chargé de faire respecter les exigences de la loi Sarbanes-Oxley (SOX), montre cependant que l'intégration de l'informatique dans le SCI pose encore de nombreuses questions. Il serait faux de penser que ces questions qui nous viennent des Etats-Unis ne concernent qu'une petite minorité de sociétés suisses cotées à la bourse américaine. Que ce soit par le biais des futures directives européennes, des nouvelles dispositions du Code des Obligations ou finalement sous la pression des bailleurs de fonds de l'entreprise, les entreprises vont devoir porter dans le futur une plus grande attention aux risques informatiques et à leur prise en compte correcte dans le SCI.

Il est pour la discussion utile de suivre la typologie adoptée par le Standard d'audit no 2[2] édicté par le PCAOB. Celui-ci distingue :

- les contrôles généraux établis à l'échelon de l'entreprise (***company-*** ou ***entity-level controls***),
- les contrôles applicatifs (***application controls***) et
- les contrôles généraux informatiques (***IT general controls***).

L'illustration 1[3] montre que seule la seconde catégorie est directement liée aux processus métiers de l'entreprise.

Premier constat : CobiT 4.0 permet de prendre en compte les contrôles informatiques, mais à l'exception des contrôles applicatifs

La publication en décembre 2005 de la version 4.0 de CobiT[4] a été l'occasion de procéder à quelques remaniements (voir illustration 2) et d'aligner systématiquement ce référentiel sur les règles du PCAOB.

Tant la Commission européenne[5] que l'Institute of Internal Auditors (IIA) le confirment : CobiT est aujourd'hui l'outil de référence privilégié pour la prise en compte de la gouvernance de l'informatique dans la mise en œuvre des directives européennes ou pour une démarche SOX.

Il est cependant nécessaire de prendre en compte les trois règles suivantes :

Intégrer directement l'informatique dans toute l'analyse des contrôles à l'échelon de l'entreprise (***company-*** ou ***entity-level controls***)

Les contrôles établis à l'échelon de l'entreprise ne sont efficaces que s'ils sont globaux. Il est donc essentiel que les systèmes de contrôle adoptent une démarche intégrante :

- ils doivent par exemple comprendre une analyse des risques qui porte sur l'ensemble des risques de l'entreprise, y compris les risques de panne informatique,
- les règles déontologiques doivent traiter aussi bien la lutte anti-corruption que l'interdiction d'accéder aux sites pédophiles,
- la répartition des compétences doit régler tant la conclusion des contrats que la responsabilité des données et des applications,
- la surveillance de l'entreprise doit détecter aussi bien les réclamations des clients que les tentatives d'intrusion dans un serveur informatique,
- etc.

Plusieurs processus des domaine Planning et organisation (PO) et Surveillance et évaluation (ME) de CobiT sont parfaitement adaptés à ce type de contrôles.

Les travaux d'audit peuvent se limiter à des vérifications superficielles, fondées sur des autoévaluations, des interviews et la consultation de documents. L'auditeur doit cependant vérifier quelques questions essentielles, dont celle de la définition de la propriété d'une application, qui mérite d'être abordée ici plus en détail.

Comme relevé dans un article précédent (Expert-comptable 2004/10), la maîtrise de l'informatique implique que les utilisateurs connaissent et assument leurs responsabilités. Les utilisateurs (les maîtres d'ouvrage) sont les propriétaires des données et des applications informatiques qui traitent celles-ci. A ce titre ils doivent par exemple valider par des tests adéquats toute modification apportée à leurs logiciels. Deux exemples montrent que l'évolution technologique vient malheureusement singulièrement compliquer cette répartition des tâches :

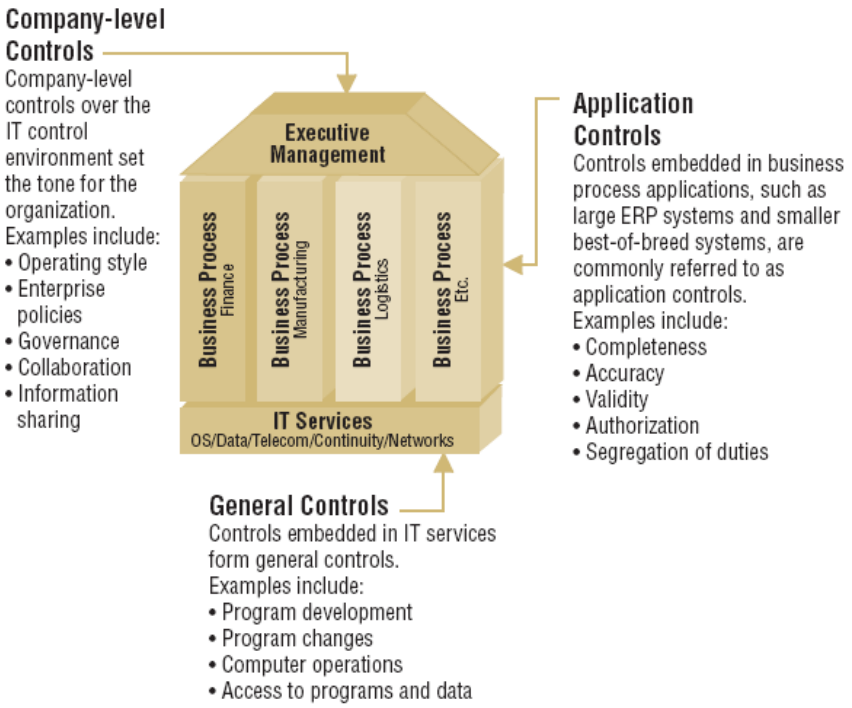


Illustration 1 : les différentes catégories de contrôles selon la typologie du PCAOB

a) EAI/SOA

Les démarches d'intégration (Enterprise Application Integration, EAI) ou d'architecture orientée service (Service oriented Architecture, SOA) présentent le même défaut. Dans un louable but de simplification et d'efficacité, elles brisent les anciennes barrières entre applications. Des tâches identiques, présentes dans plusieurs applications, comme les routines de calcul des intérêts, l'édition et l'impression des factures, ou plus simplement le transfert de données entre logiciels, sont extraites des application et placées dans un espace commun auquel accèdent l'ensemble des applications (middleware dans l'approche EAI). Si les avantages en terme de simplification de la maintenance sont incontestables, la pratique montre que la « propriété » de ce middleware est plus problématique. Une modification de ces routines devrait en principe être testée dans l'ensemble des applications qui y ont recours et formellement acceptée par les responsables de toutes ces applications. Une exigence complexe à remplir, tant techniquement (difficulté à simuler en environnement de tests) qu'organisationellement (difficulté à rassembler un pool de représentants d'application).

b) Patch Management[6]

Le recours à des logiciels standard apporte incontestablement un gain d'efficacité pour l'entreprise. La pratique montre que les versions misent sur le marché comportent encore de nombreuses erreurs qui sont corrigées ultérieurement par des programmes livrés par le fournisseur (patches). Le problème réside là aussi dans la

CobiT 3	***CobiT 4.0***
Le Guide du management et les objectifs de contrôle font l'objet de deux ouvrages séparés	Un ouvrage rassemble pour chacun des 34 processus informatiques, les objectifs de contrôle, les niveaux de maturité, ainsi que les facteurs et les indicateurs de succès
Certains contrôles applicatifs sont compris dans les processus DS5 « gestion de la sécurité » et DS11 « gestion des données »	18 contrôles applicatifs ont été identifiés (numérotés AC1 à AC18), extraits des processus DS05 et DS11, et font l'objet d'une brève description en introduction de CobiT. Ils ne sont par la suite plus traités dans CobiT (voir illustration 3).
Le processus PO04 traite de l'organisation générale de la fonction informatique	Le nouveau processus PO04 aborde en détail le thème de la « propriété » des applications et des données informatiques. Pour chacun des 34 processus informatiques, CobiT ne se limite plus à la division informatique mais définit les rôles au sein de l'ensemble de l'entreprise en recourant à un modèle RACI (***who is Responsible, Accountable, Consulted and/or Informed***).
Les 34 processus sont placés sur un même niveau leurs liens ne sont pas explicites	CobiT 4.0 indique les liens de continuité entre tous les processus, en mentionnant par exemple qu'un rapport sur les coûts d'une application, produit dans le cadre du processus PO5 (gérer les investissements informatiques), peut conduire à l'acquisition d'une nouvelle application (processus AI2) qui va nécessiter une adaptation du concept de sécurité (processus DS5).

Illustration 2 : quelques importants changements entre les versions 3 et 4.0 de CobiT

difficulté pour les utilisateurs d'être associés à ces travaux de maintenance. Vu la difficulté de réaliser des tests à grande échelle, ces patches passeront souvent en production sans que les utilisateurs en soient conscients. Les informaticiens auront en effet tendance à considérer que ces opérations ne présentent pas de risques et n'ont pas d'impact sur la disponibilité ou le bon fonctionnement des applications. Cela est probablement vrai dans 99% des cas, mais la pratique montre que dans les rares cas où ces travaux entraînent une panne, celle-ci peut se révéler dramatique pour l'entreprise. D'où la recommandation de tester les patches avant de les charger, de les passer en production en période calme, d'effectuer un monitoring étroit les premières heures ou les premiers jours et dans tous les cas d'informer les utilisateurs de l'augmentation des risques.

Ces exemples montrent que l'auditeur sera bien inspiré de vérifier en détail que l'entreprise a pris les mesures nécessaires pour atteindre les objectifs de contrôle selon CobiT PO4.6 à 4.9, en particulier la détermination des responsabilités pour l'assurance qualité, pour la gestion des risques, ainsi que pour les données et les systèmes.

Comprendre les processus métiers et identifier les contrôles applicatifs (***application controls***)

Il est important de savoir que CobiT mentionne les contrôles applicatifs (voir illustration 3) mais ne les intègre pas dans les 34 processus informatiques de base. Ces contrôles relèvent en effet des processus métiers. Ils ne sont donc compris ni dans les Objectifs de contrôle, ni dans le Guide du management.

Ils doivent absolument faire l'objet d'une démarche complémentaire centrée sur l'identification des risques liés aux processus, démarche pour laquelle CobiT n'est pas d'une grande utilité.

Le chiffre 2 ci-dessous revient en détail sur ce type de contrôles.

Ne traiter les contrôles généraux informatiques (***IT general controls***) que dans la mesure où ils conditionnent le bon fonctionnement d'applications sensibles des processus métiers

Des articles spécialisés se sont fait l'écho d'audits de conformité SOX qui avaient perdu toute proportionnalité avec les objectifs à atteindre. L'épaisseur du blindage de la porte d'accès à un centre de calcul a-t-elle réellement une influence sur la fiabilité des états financiers d'une compagnie internationale ? On peut en douter et de tels excès contribuent à discréditer le travail des auditeurs. Certaines critiques doutent à juste titre de la valeur ajoutée de tels audits et relèvent que SOX a de facto trans-

formé les dividendes autrefois versés aux actionnaires en honoraires versés aux cabinets d'audit.

Ces excès peuvent être évités en adoptant la démarche rétrograde (ou « ***Top-down Approach*** ») préconisée par le PCAOB:
1) identifier les positions importantes des états financiers,
2) identifier les processus qui génèrent ou conditionnent ces positions,
3) identifier les applications informatiques sensibles pour ces processus,
4) n'auditer que les contrôles généraux informatiques essentiels au bon fonctionnement de ces applications.

Si l'entreprise ne réalise par exemple qu'une part infime de son chiffre d'affaires avec une application e-commerce découplée de ses autres ressources informatiques, l'auditeur devrait avoir le « courage » d'ignorer purement et simplement ce domaine. Si en revanche, l'ensemble de la facturation est externalisée, c'est toute la fiabilité des interfaces (conditionnée par des contrôles tant applicatifs que généraux) qui devra par exemple être examinée.

L'audit des contrôles généraux informatique ne peut se limiter à des interviews mais doit comprendre des vérifications de l'efficacité des contrôles. Ceux-ci sont essentiellement compris dans les domaines Acquisition et implémentation (AI) et Distribution et support (DS) de CobiT, qui fournit avec son Guide d'audit[7] une aide précieuse.

Second constat : les contrôles applicatifs demeurent aujourd'hui le principal gap

Un fait divers a récemment illustré l'importance de ces contrôles applicatifs : un négociant en titres a saisi un ordre en inversant le nombre de titre et leur valeur. Il a ainsi vendu 610'000 actions pour 1 Yen au lieu d'en vendre une pour 610'000 Yens. Une erreur qui a coûté 290 millions de francs à la banque et qu'une simple plausibilisation à la saisie (comparaison avec les valeurs précédentes, avertissement vu le nombre d'actions offertes, etc....) aurait permis d'éviter.

Deux exemples montrent que ces risques importants sont aujourd'hui encore trop souvent négligés, aussi bien par les entreprises que par certains auditeurs.

Le programme standard de comptabilité des assurances suisses

Depuis le 1er janvier 2005, les assurances privées actives dans le domaine de la prévoyance professionnelle doivent établir à l'attention de l'autorité de surveillance (l'Office fédéral des assurances sociales) une comptabilité annuelle (Betriebsrechnung) permettant de délimiter ce type d'assurances du reste de leurs affaires. Une exigence raisonnable si l'on considère que le total de ces engagements s'élève fin 2004 à 118 milliards de francs à répartir entre 2,3 millions d'assurés…

Cette comptabilité constitue un instrument essentiel à la surveillance étatique, mais regroupe également les données qui pour la plupart des assurances permettent de justifier l'attribution au fonds d'excédents et la distribution des parts excédents. Elle doit donc être considérée comme un système alimentant les états financiers des assurances.

En outre, et selon l'article 140 (devoir d'information) de la nouvelle Ordonnance sur la surveillance des assurances privées en vigueur dès le 1.1.2006 , « ***L'entreprise d'assurance transmet aux preneurs d'assurance,***

„Therefore, the COBIT IT processes cover general IT controls, but not application controls, because these are the responsibility of business process owners and, as described previously, are integrated into business processes."

	DATA ORIGINATION/ AUTHORISATION CONTROLS
AC1	Data Preparation Procedures
AC2	Source Document Authorisation Procedures
AC3	Source Document Data Collection
AC4	Source Document Error Handling
AC5	Source Document Retention
	DATA INPUT CONTROLS
AC6	Data Input Authorisation Procedures
AC7	Accuracy, Completeness and Authorisation Checks
AC8	Data Input Error Handling
	DATA PROCESSING CONTROLS
AC9	Data Processing Integrity
AC10	Data Processing Validation and Editing
AC11	Data Processing Error Handling
	DATA OUTPUT CONTROLS
AC12	Output Handling and Retention
AC13	Output Distribution
AC14	Output Balancing and Reconciliation
AC15	Output Review and Error Handling
AC16	Security Provision for Output Reports
	BOUNDARY CONTROLS
AC17	Authenticity and Integrity
AC18	Protection of Sensitive Information during Transmission and Transport

Illustration 3: les 18 contrôles applicatifs identifiés par CobiT

dans les cinq mois qui suivent la date du bilan: (a.) la comptabilité des assurances de prévoyance professionnelle, (b.) les indications concernant l'attribution au fonds d'excédents et la distribution des parts excédents, … ».

Il est réjouissant d'apprendre que l'autorité de surveillance et ses partenaires ont mis au point à l'échelon national une comptabilité standard.

Il est revanche pour le moins préoccupant de constater qu'il est prévu dans un premier temps de tenir cette comptabilité standard grâce à des tableaux EXCEL.

Comment l'organe externe de révision considérera-t-il les données émanant de ces tableaux EXCEL, qui pour certaines influencent directement certaines positions au bilan des sociétés ? Quelle augmentation des honoraires sera-t-elle nécessaire pour donner une assurance raisonnable sur ces chiffres ? La situation sera-t-elle appréciée différemment si la compagnie d'assurance est soumise à SOX ? On peut dans tous les cas penser que les compagnies d'assurance suisses, qui devraient être les premières intéressées à disposer de données fiables, auraient été mieux inspirées de développer directement leur standard dans un langage de programmation sérieux permettant de mettre en place les contrôles applicatifs appropriés.

Une fréquente absence de contrôles applicatifs dans les processus de bouclement comptable et d'établissement des comptes

Les auditeurs ont vérifié que les processus métiers alimentent correctement les logiciels de comptabilité et que ceux-ci digèrent et traitent avec fiabilité les informations reçues. Les contrôles appropriés sont en place, tant dans les applications essentielles aux processus métiers que dans les logiciels de comptabilité. Tout est donc pour le mieux.

Ce serait oublier d'une part que le bouclement va nécessiter un certain nombre d'écritures et d'opération dans l'application comptable et, d'autre part, qu'un logiciel comptable n'est généralement pas en mesure de livrer à un imprimeur une version imprimable des comptes annuels. En pratique, les données vont passer à travers de nombreuses opérations informatiques : elles sont extraites de l'application comptable, transitent éventuellement par un tableur (en particulier s'il s'agit d'établir les comptes consolidés d'un groupe…), sont ensuite reprises dans un programme du type PageMaker ou InDesign, retravaillées en vue de leur publication et finalement transmises à l'imprimerie. Tous ces produits informatiques ont en commun une absence de gestion sérieuse des droits d'accès et de traçabilité des modifications. Compte tenu de cette absence de contrôles applicatifs, ce processus présente donc au moins autant de risques de fraudes et d'erreurs de présentation comptable que l'ensemble des processus situés en amont.

Le PCAOB confirme à cet égard dans une évaluation de novembre 2005[8] que « ***Some auditors did not perform sufficient testing of the controls over preparing financial statement disclosures. The controls in this area are among the most important in the financial reporting process because of the relatively high risk of material misstatement or omission due to fraud or error.*** »

Efficacité du contrôle interne, qui doit auditer quoi et quand?

Le malentendu relevé par le PCAOB vient-il d'une interprétation trop rigide de la notion de « période » ? Le PCAOB est-il lui-même suffisamment clair[9] ? Les Normes d'audit suisses[10] partent de l'idée qu'un audit du système de contrôle interne couvre l'exercice sous revue, alors que la réalité montre qu'en terme de risques de fraudes et d'erreurs c'est le laps de temps couvrant le bouclement et la préparation à la

Erfolgsrechnung - Teil 1 — Zahlen in Tausend CHF, BJ = Berichtsj

a	b	c	d
	Gesamtgeschäft		+/- in %
	BJ	BJ-1	
1 **Bruttoprämien gebucht**	0	0	
2 Veränderung Bruttoprämienüberträge (Zunahme = +)	0	0	
3 **Bruttoprämien verdient = 1 - 2**	0	0	
4 Anteil Rückversicherer an den verdienten Prämien	0	0	
5 **Verdiente Prämien für eigene Rechnung = 3 - 4**	0	0	
6 Sonstige versicherungstechnische Erträge	0	0	
7 Zahlungen für Versicherungsfälle	0	0	
8 Leistungsbearbeitungsaufwendungen	0	0	
9 Anteil Rückversicherer an Aufw. für Versicherungsfälle	0	0	
10 **Total Zahlungen netto für Versicherungsfälle = 7 + 8 - 9**	0	0	
11 Veränderung Deckungskapital (Zunahme = +)	0	0	
12 Veränderung der Verstärkungen	#VALEUR!	#VALEUR!	#######
13 Veränderung sonstige versicherungstechn. Rückstellungen	12'345	0	
14 Veränderung der Rückstellung für eingetretene, noch nicht erledigte Versicherungsfälle (+=Zunahme)	0	0	
15 Anteil Rückversicherer an Veränd. der vt. Rückstellungen	0	0	
16 **Veränderung der versicherungstechn. Rückstellungen (netto) = 11 + 12 + 13 + 14 - 15**	#VALEUR!	#VALEUR!	#######

Illustration 4 : le programme de comptabilité standard (Betriebsrechnung) des assurances privées suisses, réalisé provisoirement avec EXCEL

publication des comptes qui est la période de tous les dangers, donc bien après la fin de l'exercice.

En situation d'externalisation de services, quelle valeur accorder à un rapport d'audit (par exemple SAS70) qui n'étant pas daté du 31 décembre ne démontre pas que le prestataire de service disposait d'un SCI efficace durant toute la période ? Dans le même contexte, comment interpréter l'opinion de l'AICPA[11], qui semble admettre que les vérifications chez le prestataire de service ne puissent porter que sur six mois[12] ? Ces questions du périmètre temporel des contrôles mériteront probablement d'être encore approfondies.

La seconde question, toujours plus sensible dans l'audit du SCI, est la délimitation des tâches incombant à l'audit interne. Si le PCAOB règle de manière relativement précise les tâches que l'auditeur externe peut déléguer à l'audit interne[13], la délimitation des tâches entre la ligne et l'audit interne est plus floue.

L'IIA a récemment plaidé pour un renforcement de la surveillance continue de l'efficacité des contrôles en place. Il s'agit en réalité de mettre en place et d'institutionnaliser sous la responsabilité des auditeurs internes une batterie de contrôles détectifs, souvent développés en recourant à des logiciels d'audit[14]. On doit cependant se poser la question: les contrôles détectifs relèvent-ils de la surveillance du SCI ou sont-ils partie intégrante du SCI ? L'avenir nous montrera si les auditeurs internes auront pu éviter que la direction de l'entreprise saisisse cette perche tendue pour se débarrasser de la responsabilité du contrôle interne et la transférer aux auditeurs. Ce risque ne devrait pas être négligé.

Michel Huissoud, CISA, CIA

Vice-président ISACA (Suisse)

Footnotes

[1] Public Company Accounting Oversight Board

[2] Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements, état février 2005

[3] extraite de l'ouvrage « IT Control Objectives for Sarbanes-Oxley », IT Governance Institute (www.itgi.org), 2004

[4] „Control Objectives for Information and related Technology (CobiT®)", IT Governance Institute (www.itgi.org)

[5] Voir par exemple, la décision prise en mars 2005 reconnaissant CobiT comme un des instruments agréés pour assurer la sécurité des données des agences chargées du payement des aides agricoles.

[6] Voir sur ce thème l'excellent guide « Global Technology Audit Guide Change and Patch Management Controls: Critical for Organizational Success », The Institute of Internal Auditors, 2005

[7] Pas encore disponible en version 4,0

[8] « Report on the initial implementation of Auditing Standard no 2», PCAOB, 30 novembre 2005

[9] Voir par exemple le chiffre 101 de AS2: „***For controls over significant nonroutine transactions, controls over accounts or processes with a high degree of subjectivity or judgment in measurement, or controls over the recording of period-end adjustments, the auditor should perform tests of controls closer to or at the „as of" date rather than at an interim date***."

[10] Voir par exemple le chiffre 37 de la NAS 400 : « ***L'auditeur doit déterminer si les contrôles internes ont été appliqués tout au long de la période*** »

[11] American Institute of Certified Public Accountants

[12] „***Testing should be applied to controls in effect throughout the period covered by the report. To be useful to user auditors, the report should ordinarily cover a minimum reporting period of six months***.", AICPA Professional Standards, AU 324.02

[13] Voir par exemple l'annexe E (chiffres 29 à 50) de AS2

[14] L'entreprise ACL est le sponsor officiel du Guide (GTAG 3) publié par l'IIA sur ce thème

CobiT 4.0

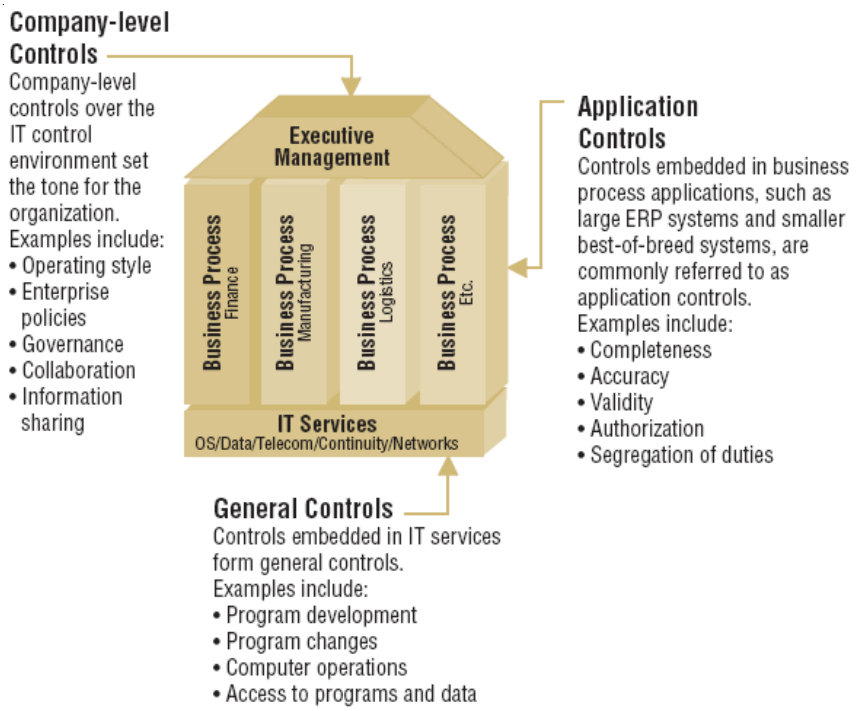
Bringt CobiT 4.0 eine Antwort auf die Erwartungen des PCAOB?

Ja, aber…! CobiT 4.0 ist ein Instrument, um Informatikkontrollen zu schaffen und zu prüfen. Falsch eingesetzt, kann es zu überdimensionierten Prüfungen führen. Es muss zudem durch applikationsorientierte Prüfungen ergänzt werden. Hier zeigen sich immer wieder Überraschungen.

Die Prüfung des Internen Kontrollsystems (IKS) wurde durch das PCAOB wieder aktiviert, und das ist gut so. Damit sollen die Forderungen des Sarbanes-Oxley Acts (SOX) durchgesetzt werden. Es stellen sich jedoch bei der Einbindung der Informatik in das IKS etliche Fragen. Es wäre falsch anzunehmen, dass die Bestimmungen aus den Vereinigten Staaten nur einige wenige (in den USA kotierte) Schweizer Gesellschaften betreffen. Zukünftige Europäische Vorschriften werden sich daran anlehnen und auch das Schweizerische Obligationenrecht wird sich am Ende nicht vor den Anforderungen drücken können. Somit ist die richtige Integration der Informatik in das IKS auf mittlere Sicht unabdingbar.

Für Diskussionszwecke ist es nützlich, der Terminologie des Revisionsstandards Nr. 2[1] zu folgen. Das PCAOB unterscheidet:

- Generelle Kontrollen auf Unternehmungsebene (***company-*** oder ***entity-level controls***),
- Applikationskontrollen (***application controls***) und
- Applikationsunabhängige Kontrollen (***IT general controls***).



Darstellung 1: Arten der Kontrollen nach PCAOB

Darstellung 1[2] zeigt, dass nur die zweite Art der Kontrollen direkt auf die Geschäftsprozesse einwirken.

Erste Feststellung: CobiT 4.0 erlaubt mit Ausnahme der Applikationskontrollen die IT-Kontrollen zu berücksichtigen.

Die Veröffentlichung vom Dezember 2005 der Version 4.0 von CobiT[3] nahm einige Begradigungen vor, die sich auf die Forderungen des PCAOB zurückführen lassen.

Sowohl die EU-Kommission[4] als auch das Institute of Internal Auditors (IIA) bestätigen diese Ansicht. CobiT ist heute das wichtigste Instrument zur Beherrschung (Governance) der Informatik um die Direktiven der EU und des SOX umzusetzen.

Dabei sind allerdings die folgenden drei Regeln zu beachten:

Integration der Informatik bei der Analyse der Kontrollen auf Unternehmens-ebene (***company-*** oder ***entity-level controls***)

Die Kontrollen auf Unternehmensebene sind nur wirksam, wenn sie globaler Natur sind. Es ist deshalb wichtig, dass die Systemkontrollen umfassend sind.

- Sie müssen z.B. eine Risikoanalyse enthalten, welche auf die Geschäftsrisiken bei einer Informatikpanne eintreten.
- Die Abwehrmechanismen müssen sowohl die Veruntreuungsversuche als auch die pädophil/pornographischen Elemente umfassen.
- Die Aufsicht muss sowohl die Kundenreklamationen als auch die unberechtigten Zugriffsversuche berücksichtigen.
- etc.

Mehrere Prozesse der Domäne Planung und Organisation (PO) und Aufsicht (ME) von CobiT sind bestens für diese Zwecke geeignet.

Die Revisionstätigkeiten können sich auf oberflächliche Prüfungen, die auf Selbsanalysen beruhen, beschränken.

Immerhin muss der Revisor einige zentrale Fragen eingehend prüfen. Eine davon ist jene der Eigner von Anwendungen und Daten.

In einem Artikel im Schweizerischen Treuhänder (2004/10) wurde festgehalten, dass die Beherrschung der Informatik durch die Benützer wahrgenommen wird. Diese sind Eigner der Daten und Anwendungen. Als solche müssen sie sich z.B. durch geeignete Tests bezüglich der Richtigkeit jegliche Änderung der Software vergewissern. Zwei Beispiele mögen dies illustrieren.

a) EAI/SOA

Die Enterprise Application Integration (EAI) und die Service Oriented Architecture (SOA) weisen die gleiche Schwäche auf. Durch die Eliminierung von redundanten Informationen werden die Grenzen zwischen den Anwendungen niedergerissen. Zinsberechnungen, die Fakturierung, etc. werden nicht mehr von Applikation zu Applikation weitergegeben, sondern sind in der so genannten Middleware enthalten und stehen verschiedenen Anwendungen zur Verfügung. Daraus ergibt sich die Problematik, dass eine allfällige Änderung durch sämtliche Anwendungen getestet werden müsste. Eine sehr sowohl auf technischer als auch auf organisatorischer Seite komplexe Angelegenheit.

CobiT 3	***CobiT 4.0***
Der Management-Guide und die Kontrollziele sind separat festgehalten.	Ein einziges Werk definiert für jeden der 34 Informatikprozesse die Ziele, den Reifegrad und ihre Erfolgsindikatoren.
Vereinzelte Applikationskontrollen sind in den Kontrollzielen DS5 «Systemsicherheit» und DS11 «Datenmanagement» enthalten	18 Applikationskontrollen wurden identifiziert (AC1 bis AC18), die aus den Prozessen DS5 und DS11 stammen. Sie werden von CobiT nur kurz beschrieben und nicht weiter behandelt (siehe Darstellung 3).
PO04 befasst sich mit der allgemeinen IT-Organisation.	Der neue Prozess PO04 geht detailliert auf das Thema «Dateneigners» ein. Bei jedem der 34 Kontrollziele beschränkt sich CobiT nicht mehr auf die Informatik, sondern folt deinem RACI-Modell (***who is Responsible, Accountable, Consulted and/or Informed***).
Die 34 Prozesse sind gleichberechtigt und die Verknüpfungen werden nicht explizit behandelt.	CobiT 4.0 weist auf die Abhängigkeiten hin. Z.B. können die Kosten für die Fortführung im Rahmen von PO5 zur Beschaffung einer neuen Anwendung führen (AI2) und diese wiederum kann eine Adaption des Sicherheitskonzeptes (DS5) nach sich führen.

Darstellung 2: Einige wichtige Änderungen der Version 3 zu 4.0 von CobiT

b) Patch Management[5]

Das Zurückgreifen auf Standardsoftware ist eine wirtschaftlich gute Lösung für viele Anwender. Die Praxis zeigt, dass die auf dem Markt angebotenen Produkte oft Fehler enthalten, deren Behebung durch die Lieferanten mittels so genannten Patches realisiert werden. Das Problem liegt nun darin, dass beim Programmunterhalt nur in Ausnahmefällen darauf geachtet wird, dass vor Einspielen in die Produktion ein eingehendes Testen vorangehen sollte. Die Informatiker haben die Tendenz zu unterstellen, dass diese Patches richtig funktionieren und kein Risiko für die Produktion darstellen. Dies ist wahrscheinlich für 99% der Fälle zutreffend. Wenn aber eine Panne eintrifft, hat sie oft schlimme Folgen. Daher die Empfehlung, Patches vor dem Einspielen in die Produktion eingehend zu testen und in den ersten Tagen der Produktion die Ergebnisse aufmerksam zu verfolgen, um das Risiko einschätzen zu können.

Diese Beispiele zeigen deutlich, dass der Revisor gut daran tut, sich zu vergewissern, ob die Unternehmung angemessene Massnahmen ergriffen hat, um den Forderungen gemäss CobiT PO4.6 bis 4.9 gerecht zu werden.

Verstehen der Geschäftsprozesse und Identifikation der Anwendungskontrollen (*application controls*)

Es ist wichtig zu erkennen, dass CobiT zwar die Applikationskontrollen erwähnt (siehe Darstellung 3), sie aber nicht in die 34 Basisprozesse intergriert hat.

Diese Kontrollen sind dennoch rudimentär und bedürfen einer Ergänzung der mit den Prozessen verbundenen Risiken, weil CobiT hier nicht sehr hilfreich ist.

Punkt 2 nachstehend geht auf diese Arten von Kontrollen im Detail ein.

Die allgemeinen Informatik-Kontrollen ***(IT general controls)*** nur in dem Sinne behandeln, als sie für die Richtigkeit der Anwendungsfunktionen von Bedeutung sind.

Fachartikel beanstanden, dass SOX-Revisionen oft jedes Mass an Vernunft überschreiten. Die Dicke der Brandmauern im Rechenzentrum hat wohl kaum einen direkten Einfluss auf die Richtigkeit der Jahresrechnung einer internationalen Unternehmung. Solche Fragestellungen nagen an der Glaubwürdigkeit des Revisionsstandes und lassen die Aktionäre zu Recht daran zweifeln, ob die Höhe der Revisionshonorare angemessen ist.

Derartige Auswüchse können durch einen ***Top-down Approach***, wie er vom PCAOB vorgesehen ist, vermieden werden.
1) Bestimmen der wichtigen Posten der Jahresrechnung.
2) Identifikation der Anwendungen, welche diese Positionen generieren.
3) Identifizieren der Informatikanwendungen, welche für diese Anwendungen wesentlich sind.
4) Revision lediglich jener allgemeinen Kontrollen, die für das Funktionieren dieser Anwendungen verantwortlich sind.

Wenn z.B. eine Unternehmung nur einen geringen Teil des Umsatzes durch eine isolierte Anwendung im e-Commerce erzielt, sollte der Revisor den «Mut» aufbringen, diesen Teil der Anwendungen ganz zu ignorieren.

Die Revision der allgemeinen Informatikkontrollen sollte sich nicht auf Interviews beschränken, sondern umfasst auch Einhalteprüfungen. Sie sind in den Domänen Acquisition und Implementation (AI) sowie Distribution and Support (DS) von CobiT wichtig, wobei der Audit-Guide[6] wertvolle Hinweise bietet.

Zweite Feststellung: Die Anwendungskontrollen bleiben auch heute noch die grösste Lücke

Eine Geschichte machte letzthin die Runde: Ein Wertschriftenhändler erfasste einen Auftrag, wobei er Betrag und Anteile verwechselte. Er verkaufte 610'000 Aktien für einen Yen anstatt eine für 610'000 Yen zu verkaufen. Der Fehler, der durch eine leichte Plausibilitätskontrolle hätte vermieden werden können, kostete die Bank 290 Millionen Franken.

Zwei Beispiele illustrieren, dass heute noch viele wichtige Risiken vernachlässigt behandelt werden. Und dies sowohl durch die Anwender als auch durch die Revisoren.

Das Finanz-Standardprogramm der Schweizer Vorsorgeeinrichtungen

Seit dem 1. Januar 2005 müssen die Vorsorgeeinrichtungen zuhanden der Sozialversicherungsaufsicht eine Betriebsrechnung vorlegen, welche sich von den übrigen Teilen des Unternehmens abgrenzt. Ein sinnvolles Verlangen, wenn man bedenkt, dass Ende 2004 118 Milliarden Franken 2,3 Millionen Versicherten «gehörten».

Diese «Buchhaltung» ist ein wichtiges Instrument für die Staatsaufsicht, welche die Deckungen der Versicherten zu kontrollieren hat. Das System wird deshalb vielerorts als Ergänzung zur Finanzbuchhaltung der Vorsorgeeinrichtungen verstanden.
Im weiteren hält die seit 1.1.2006 in Kraft stehende Verordnung in Art 140 (Informationspflicht) fest: «***Das Versicherungsunternehmen stellt fünf Monate nach Bilanzerstellung (a.)***

„Therefore, the COBIT IT processes cover general IT controls, but not application controls, because these are the responsibility of business process owners and, as described previously, are integrated into business processes."

	DATA ORIGINATION/ AUTHORISATION CONTROLS
AC1	Data Preparation Procedures
AC2	Source Document Authorisation Procedures
AC3	Source Document Data Collection
AC4	Source Document Error Handling
AC5	Source Document Retention
	DATA INPUT CONTROLS
AC6	Data Input Authorisation Procedures
AC7	Accuracy, Completeness and Authorisation Checks
AC8	Data Input Error Handling
	DATA PROCESSING CONTROLS
AC9	Data Processing Integrity
AC10	Data Processing Validation and Editing
AC11	Data Processing Error Handling
	DATA OUTPUT CONTROLS
AC12	Output Handling and Retention
AC13	Output Distribution
AC14	Output Balancing and Reconciliation
AC15	Output Review and Error Handling
AC16	Security Provision for Output Reports
	BOUNDARY CONTROLS
AC17	Authenticity and Integrity
AC18	Protection of Sensitive Information during Transmission and Transport

Darstellung 3: Die 18 durch CobiT identifizierten Kontrollen

das Versichertenkonto der Berufsversicherung, (b.) die Kennzahlen zur Deckung…».

Es ist zwar erfreulich festzustellen, dass die Aufsichtsbehörde ein Hilfsmittel zur Unterstützung der Bilanzerstellung zur Verfügung stellt. Es ist anzunehmen, dass die Berechnungen einige Zeit auf EXCEL-Tabellen bleiben.

Wie verhält sich nun die externe Revisionsstelle bezüglich der aus EXCEL resultierenden Tabellen, welche direkt Positionen der Bilanz des geprüften Unternehmens beeinflussen? Welche Erhöhung der Honorare wird notwendig sein, um die Richtigkeit der Zahlen zu überprüfen? Was sind die Auswirkungen auf Unternehmen, welche SOX unterliegen? Es wäre eigentlich anzunehmen gewesen, dass sich die Vorsorgeunternehmen (die ja ein vitales Interesse daran haben müssen, dass die Zahlen zuverlässig sind) sich einer Programmiersprache bedient hätte, welche strengere Applikations-Plausiblitäten zulässt als EXCEL.

Häufiges Fehlen von Applikations-Kontrollen beim Abschluss und beim Erstellen der Jahresrechnung

Die Revisoren prüfen oft das richtige Funktionieren der Kontrollen in den Anwendungen. Die Zuverlässigkeit des Datenmaterials in den Anwendungen und zwischen den Anwendungen scheint gegeben. Desto besser.

Oft geht vergessen, dass für die Darstellung in Bilanz und Erfolgsrechnung noch Abschlussbuchungen notwendig sind, die nicht direkt in den Anwendungen vorgesehen sind, jedoch über die Informatik laufen. In der Praxis werden diese Zahlen vielfach direkt via PageMaker oder InDesign eingegeben, ohne entsprechende Plausibilitätskontrollen zu durchlaufen, von Zugriffssicherheiten ganz zu schweigen.

Das PCAOB bestätigt in diesem Zusammenhang in einer Feststellung vom November 2005[7], «***Some auditors did not perform sufficient testing of the controls over preparing financial statement disclosures. The controls in this area are among the most important in the financial reporting process because of the relatively high risk of material misstatement or omission due to fraud or error*** ».

Wirksamkeit des IKS: Was ist zu prüfen und in welchen Fällen?

Durch das PCAOB hervorgerufene Missverständnisse können auf der engen Interpretation des Wortes «period» beruhen. Das PCAOB drückt sich in dieser Hinsicht leider nicht sehr klar aus[8]. Der Schweizerische Prüfungsstandards[9] gehen davon aus, dass eine Prüfung des IKS die Periode der Jahresrechnung umfasst. Viele Fehler entstehen jedoch auf Perioden ausserhalb dieses engen Zeitraumes, etliche nach Abschluss.

Bei Outsourcing (beispielsweise bei Anwendung von SAS70) kann man sich die Frage stellen, ob bei Datierung des Revisionsberichtes ausserhalb des 31. Dezembers der Berichtsperiode ein wirksames IKS während der Berichtsperiode bestand. Im gleichen Zusammenhang ist die Frage berechtigt, wie die Meinung der AICPA[10] zu interpretieren ist, wonach eine entsprechende Prüfung nur eine Gültigkeit von sechs Monaten haben soll. Hier sind wohl noch tiefer gehende Überlegungen angebracht.

Eine weitere Frage drängt sich bezüglich der durch die Interne Revision hinischtlich des IKS auf. Das PCAOB regelt die Delegationsmöglichkeit der externen Revision an die Interne[11] in sehr beschränktem Ausmass.

Die IIA hat kürzlich für ein stärkeres laufendes Überwachen des IKS plädiert. Dabei soll zugunsten der Internen Revision vermehrt Audit Software[12] zum Einsatz kommen. Dabei darf man sich die Frage stellen, ob

Erfolgsrechnung - Teil 1 — Zahlen in Tausend CHF, BJ = Berichtsj

	a	b	c	d
		Gesamtgeschäft		+/- in %
		BJ	BJ-1	
1	**Bruttoprämien gebucht**	0	0	
2	Veränderung Bruttoprämienüberträge (Zunahme = +)	0	0	
3	**Bruttoprämien verdient = 1 - 2**	0	0	
4	Anteil Rückversicherer an den verdienten Prämien	0	0	
5	**Verdiente Prämien für eigene Rechnung = 3 - 4**	0	0	
6	Sonstige versicherungstechnische Erträge	0	0	
7	Zahlungen für Versicherungsfälle	0	0	
8	Leistungsbearbeitungsaufwendungen	0	0	
9	Anteil Rückversicherer an Aufw. für Versicherungsfälle	0	0	
10	**Total Zahlungen netto für Versicherungsfälle = 7 + 8 - 9**	0	0	
11	Veränderung Deckungskapital (Zunahme = +)	0	0	
12	Veränderung der Verstärkungen	#VALEUR!	#VALEUR!	########
13	Veränderung sonstige versicherungstechn. Rückstellungen	12'345	0	
14	Veränderung der Rückstellung für eingetretene, noch nicht erledigte Versicherungsfälle (+=Zunahme)	0	0	
15	Anteil Rückversicherer an Veränd. der vt. Rückstellungen	0	0	
16	**Veränderung der versicherungstechn. Rückstellungen (netto) = 11 + 12 + 13 + 14 - 15**	#VALEUR!	#VALEUR!	########

Darstellung 4: Standardisierte Betriebsrechnung der Vorsorgeeinrichtungen, realisiert mit EXCEL

diese detektiven Kontrollen ein Mittel der Überwachung des IKS oder Teil des IKS selbst sind. Die Zukunft wird zeigen, ob die Internen Revisoren den Ball dem Management zugespielt haben, oder ihre Verantwortlichkeit wahrnehmen. Auf jeden Fall darf das Risiko einer ungenügenden Kontrolle bzw. Prüfung nicht vernachlässigt werden.

Michel Huissoud, CISA, CIA
Vice-président ISACA (Suisse)

Übersetzung durch die Redaktion

Endnoten

[1] Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements, état février 2005

[2] extraite de l'ouvrage « IT Control Objectives for Sarbanes-Oxley », IT Governance Institute (www.itgi.org), 2004

[3] „Control Objectives for Information and related Technology (COBIT®)", IT Governance Institute (www.itgi.org)

[4] Z.B. der Beschluss vom März 2005, CobiT als ein Instrument der Datensicherheit bei der Auszahlung der Landwirtschaftshilfe anzuerkennen.

[5] Siehe zu diesem Thema «Global Technology Audit Guide Change and Patch Management Controls: Critical for Organizational Success», The Institute of Internal Auditors, 2005

[6] Noch nicht verfügbar in Version 4.0

[7] « Report on the initial implementation of Auditing Standard no 2», PCAOB, 30 novembre 2005

[8] Siehe Ziffer 101 AS2: „For controls over significant nonroutine transactions, controls over accounts or processes with a high degree of subjectivity or judgment in measurement, or controls over the recording of period-end adjustments, the auditor should perform tests of controls closer to or at the „as of" date rather than at an interim date."

[9] Sieh Ziffer 37 AS 400 : « ***L'auditeur doit déterminer si les contrôles internes ont été appliqués tout au long de la période*** »

[10] American Institute of Certified Public Accountants

[11] Siehe Anhang E, Ziffer 29 bis 50) AS

[12] ACL ist Sponsor des Guide (GTAG 3) des IIA

In einer mondänen Manager-Bar da stand ein Klavier.
Getrunken wurde Rum, Wodka, Gin aber auch Bier.
Von CobiT wurde geflunkert
Und Whiskey gebunkert.
Der Takt des Manns am Klavier ist seither eher bei Vier.

An astronaut auditor trained for a longer discovering trip.
She thought to have all board members firm in her grip.
When finally off the launch pad in orbit,
She encountered a new version of CobiT,
Made a space walk and lost contact with the mothering ship.

CobiT 4.0

Von CobiT 3rd edition zu CobiT 4.0 in 30 Sekunden?

Vor sieben Monaten wurde der Schleier gelüftet: die komplett überarbeitete Version CobiT 4.0 war die ersten Tage exklusiv für die ISACA-Mitglieder und danach für alle Interessierte frei von www.isaca.org herunterladbar. Wahrscheinlich hat sich unterdessen jeder Leser ein eigenes Exemplar beschafft. Der erste Eindruck? Die Struktur erscheint uns (zum Glück) im Grossen und Ganzen bekannt; die einzelnen Elemente wie CobiT Kontrollziele, CobiT IT-Prozesse, CobiT Management Guidelines und CobiT Maturity Modell sind uns ebenfalls erhalten geblieben – wenn auch deutlich entschlackt und ganz nett in einem einzigen „Buch" verpackt.

Da mein CISA-Kurs immer wieder auf die relevanten CobiT Kontrollziele verweist, war ich für den im Januar gestarteten Kurs gezwungen, die Kontrollziele genauer anzuschauen – und da kam ich auf die Welt: Kaum ein einziges Kontrollziel ist textlich erhalten geblieben; einzelne Kontrollziele sind verschwunden, andere bis zur Unkenntlichkeit (positiv) überarbeitet und einige mit anderen Kontrollzielen zu einem einzigen neuen Ziel verschmolzen. Eigentlich toll, wenn es nur nicht so viel Aufwand für die Anpassung der Skripte bedeutet hätte.

Auf der anderen Seite zwang mich der CISA-Kurs dazu, auch die anderen Elemente von 4.0 genauer anzuschauen, und ich entdeckte einige ganz interessante Neuigkeiten: So z.B. die RACI-Chart und die Input/Output-Referenzen für alle CobiT IT-Prozesse. Wer CobiT 3rd ed. gut kennt, wird einige der Informationen aus den (noch nicht) überarbeiteten Audit Guidelines von CobiT 3 wieder erkennen. Sie sind aber viel anschaulicher präsentiert, wesentlich erweitert und in der aktuellen Form sehr nützlich.

Unsere ersten Erfahrungen in der Revisions- und Beratungspraxis sind ebenfalls positiv. Zwar ist CobiT 4.0 immer noch ein Framework, mit dem man sich intensiv auseinandersetzen muss. Die Kombination aller wesentlichen, nach den IT-Prozessen sortierten, Informationen in einem einzigen Buch hilft dabei, dass die verschiedenen Elemente wie Kontrollziele und Management Guidelines als zusammengehörig erkannt werden, was dem Verständnis von Leser und Anwender sehr förderlich ist. Die bessere Ausrichtung auf ITIL hat uns als Berufsstand viel näher zur „Fraktion" der Management Systeme wie BS15000/ISO20000, ISO27001 (vormals BS7799-2) usw. gebracht, da die verwendeten Begriffe und die wesentlichen Inhalte angeglichen wurden. Einzelne IT-Verantwortliche sehen daher CobiT bereits als Erweiterung des ITIL-Frameworks …

Dass der Markt auch sehr an CobiT 4.0 interessiert ist, erkennt man an den zahlreichen Referenzierungen z.B. in Seminaren oder Tagungen: Kaum ein Anlass, ohne dass CobiT nicht mindestens einmal auf der Ausschreibung erscheint. Und bereits gibt es mehrere Anbieter, welche CobiT-Kurse im Programm haben. Hier zeigt sich nun eine typische Auffassung auch unserer Mitglieder (hoffentlich nicht bei zu vielen!): Man ist der Ansicht, dass man die frei vom Internet herunter ladbaren Unterlagen auch ohne weiteres in einem kommerziellen Kurs verwenden darf. Dem ist aber nicht so: Das Urheberrecht liegt nach wie vor beim IT Governance Institute (ITGI) und dieses vergibt (in der Regel sehr kostengünstige) „Lizenzen" an die Ausbildungsinstitute, welche CobiT im Unterricht einsetzen wollen. Gemäss unserem Kenntnisstand gibt es in Europa (inkl. Schweiz) erst ganz wenige Unternehmen, welche so eine offizielle Erlaubnis haben.

Übrigens – in einem guten Monat wird die deutsche Version von CobiT auf den Markt kommen; wahrscheinlich von den Webseiten von ISACA Deutschland, Oesterreich und der Schweiz frei herunterladbar. Aber auch hier gilt: Das Urheberrecht bleibt beim ITGI; eine Verwendung im Rahmen kommerzieller Veranstaltungen muss vom ITGI vorgängig bewilligt werden. Die massgeblich von unseren Kollegen in Oesterreich vorangetriebene Übersetzung wird als „Neuheit" die strikte Verwendung von bestimmten CobiT-Begriffen im Original bringen: Controls, High-Level Control Objective, KPI, Best Practice, Information Criteria usw. werden grundsätzlich nicht mehr übersetzt. Auch andere Fachbegriffe werden im Original verbleiben, wenn sie beispielsweise auch bei uns oft in Englisch verwendet werden. Das Ganze ist derzeit in einer Phase des „Fine Tuning" und sieht sehr vielversprechend aus.

Schauen Sie doch mal wieder bei den Webseiten www.isaca.de, www.isaca.at und www.isaca.ch vorbei. Viel Erfolg mit der Anwendung von CobiT 4.0 wünscht Ihnen

Peter R. Bitterli, CISA

CobiT 4.0

Vergleich CobiT 3 vs. CobiT 4

Im Dezember 2005 wurde vom IT Governance Institute (ITGI) die aktuellste Version 4.0 von CobiT veröffentlicht, die einige wesentliche Änderungen und Erweiterungen gegenüber der Version 3 aufweist. CobiT 4 ist eine Weiterentwicklung von CobiT 3. Durch die neue Version sind bisherige Arbeiten nicht in Frage gestellt oder gar obsolet werden. Auf Grund der vorgenommenen Änderungen muss der Anwender beim Umstieg von CobiT 3 auf CobiT 4 allerdings doch mit einem gewissen Anpassungsaufwand rechnen.

Mit CobiT 4 wird die international anerkannte Rolle von CobiT als übergreifendes Framework für IT-Governance betont. Es wurde eine bessere Abstimmung mit dem COSO Framework vorgenommen, indem die Verbindung von Geschäftszielen zu IT-Zielen und zu den einzelnen Kontrollzielen mit den Informationskriterien klar aufgezeigt wird (die entsprechenden Referenztabellen befinden sich im Anhang I zu CobiT 4). Ausserdem wurden verschiedene Anpassungen vorgenommen, um die Integration der verbreitetsten internationalen Standards wie

- ISO 17799,
- ITIL,
- CMM/CMMI,
- PMBOK,
- ISF Standard of Good Practice for Information Security

zu verbessern.

Die Unterschiede zwischen den beiden Versionen sind teilweise substantiell und werden im Folgenden dargestellt.

Physischer Aufbau

Während in CobiT 3 die unterschiedlichen Informationen in verschiedenen Dokumenten (Executive Overview, Framework, Control Objectives, Management Guidelines) zu finden sind, wurden die wesentlichen Elemente in CobiT 4 in einem einzigen Dokument zusammengefasst. Executive Overview und Framework sind nun als die ersten beiden Kapitel im CobiT 4 Manual enthalten. Der Inhalt der ehemaligen Management Guidelines ist in Form von Maturity Modellen in die einzelnen übergeordneten Kontrollziele integriert. Ausserdem sind in einem umfassenden Anhang Querverweistabellen aufgeführt, die einen guten Überblick über die Zusammenhänge zwischen CobiT und den übergeordneten Frameworks geben sowie einen Vergleich zwischen den detaillierten Kontrollzielen von CobiT 3 und CobiT 4 ermöglichen.

Executive Overview

In diesem Übersichtskapitel werden Struktur und Ziele von CobiT 4 generell vorgestellt, wobei die Aspekte des IT-Governance mit den Schwerpunkten

- Strategische Ausrichtung
- Wertschöpfung
- Ressourcenverwaltung
- Risikomanagement
- Messung der Ergebnisse

speziell betont werden und der Zusammenhang zwischen den Geschäftszielen und den IT-Zielen sowie den Kontrollzielen hergestellt wird.

Framework

Das CobiT 4 Framework beschreibt die Elemente von CobiT 4 im einzelnen. Neu ist, dass in CobiT 4 nur noch vier IT-Ressourcen existieren: der Ausdruck „Daten“ aus CobiT 3 wurde ersetzt durch den allgemeineren Begriff „Informationen“ und die beiden Elemente „Technologien“ und „Anlagen“ wurden zusammengefasst zu „Infrastruktur“. Die sieben Informationskriterien blieben unverändert. Eine weitere Änderung gegenüber CobiT 3 besteht darin, dass allgemein geltende Prozess- und Applikationskontrollen aus den einzelnen Kontrollzielen herausgelöst wurden und in zwei Gruppen PC1 bis PC6 und AC1 bis AC18 separat im Framework aufgeführt werden. Dadurch konnten die 34 CobiT-Kontrollziele wesentlich gestrafft werden, was in der Reduktion der Zahl der detaillierten Kontrollziele von 318 auf 215 zum Ausdruck kommt.

Prozesskontrollen

Die nachfolgenden Prozesskontrollen beschreiben allgemein gültige Kontrollen, die für sämtliche Prozesse gelten und die als Ergänzung zu den jeweiligen detaillierten Kontrollzielen zu verstehen sind:

PC1 Prozess Eigentümer
PC2 Wiederholbarkeit
PC3 Vorgaben und Ziele
PC4 Aufgaben und Verantwortlichkeiten
PC5 Prozess-Leistung
PC6 Richtlinien, Pläne und Arbeitsanweisungen

Applikationskontrollen

Die 18 folgenden Applikationskontrollen sind aus der Sicht von CobiT keine eigentlichen IT-Kontrollen, sondern liegen in der Verantwortung der Geschäftsbereiche und sind daher im

Rahmen von CobiT als Empfehlung aufzufassen:
AC1 Datenaufbereitung
AC2 Genehmigung von Originalbelegen
AC3 Erfassung der Originalbelege
AC4 Fehlerbehandlung bei Originalbelegen
AC5 Aufbewahrung von Originalbelegen
AC6 Ermächtigung zur Dateneingabe
AC7 Prüfung der Richtigkeit, Vollständigkeit und Genehmigung
AC8 Behandlung fehlerhaft eingegebener Daten
AC9 Integrität der Datenverarbeitung
AC10 Überprüfung und Überarbeitung der Datenverarbeitung
AC11 Fehlerbehandlung bei der Datenverarbeitung
AC12 Handhabung und Aufbewahrung von Output
AC13 Output-Verteilung
AC14 Abgleich und Abstimmung des Outputs
AC15 Output-Überprüfung und Fehlerbehandlung
AC16 Sicherheitsvorschriften für Output
AC17 Authentizität und Integrität
AC18 Schutz sensibler Informationen während der Übertragung oder beim Transport

Struktur des Hauptteils

Der Hauptteil von CobiT 4 besteht aus der detaillierten Beschreibung der 34 CobiT-Prozesse, die jeweils in die vier Abschnitte
1. High-Level Control Objective,
2. Detailed Control Objectives,
3. Management Guidelines und
4. Maturity Model

gegliedert sind.

High-Level Control Objectives

Der Abschnitt Control Objectives verbindet das Framework mit detaillierten Kontrollzielen aus im wesentlichen sechs primären Quellen (entsprechend Anhang IV), welche ***de facto*** und ***de jure*** internationale Standards und Verordnungen in Bezug auf die Informatik umfassen. Er enthält Aussagen zum gewünschten Ergebnis oder zum Ziel, das mit der Implementation von spezifischen Kontrollverfahren innerhalb der IT-Aktivität erreicht werden soll. Er stellt damit eine weltweit und für alle Industrien klare Politik und bewährte Praktiken für IT-Kontrolle zur Verfügung.

Für jeden IT-Prozess werden die übergeordneten Kontrollziele sowie deren Beziehung zu den
- IT Governance Schwerpunktthemen (Strategische Ausrichtung, Wertschöpfung, Ressourcenverwaltung, Risikomanagement und Leistungsmessung)
- COSO Komponenten (Kontrollumfeld, Risikobeurteilung, Kontrollfunktionen, Information und Kommunikation, Überwachung)
- CobiT 4 IT-Ressourcen (Menschen, Informationen, Applikationen, Infrastruktur)
- CobiT 4 Informationskriterien (Wirksamkeit, Wirtschaftlichkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Konformität, Zuverlässigkeit)

Die übergeordneten Kontrollziele (High Level Control Objectives) sind alle in einer strukturierten Form gemäss der Wasserfall-Darstellung in Abbildung 1 formuliert.

Detailed Control Objectives

Der zweite Abschnitt enthält, wie bereits in CobiT 3, zu jedem Prozess die detaillierten Kontrollziele in Form von generisch formulierten Aktivitäten.

Die Informationen in diesem Teil sind gegenüber CobiT 3 deutlich verdichtet und prägnanter formuliert. Durch die Auslagerung der Process Controls und der Application Controls in den Teil „Framework“ wurden vielfältige Redundanzen beseitigt. Ausserdem wurde die Formulierung deutlich gestrafft, so dass von den ehemals 318 Kontrollzielen nur noch 215 übrig geblieben sind, die zudem noch wesentlich treffender formuliert sind.

Management Guidelines

Der dritte Abschnitt „Management Guidelines“ ist in CobiT 4 vollständig neu gestaltet und enthält die drei Elemente „Input-Output“, „RACI-Chart“ sowie „Goals and Metrics“.

In der Input-Output-Tabelle wird das Zusammenwirken der einzelnen Prozesse aufgezeigt. Es wird beschrieben, welche Ergebnisse aus anderen Prozessen als Input für den betreffenden Prozess dienen und welche Ergebnisse dieser Prozess für die anderen Prozesse bereitstellen muss. Abbildung 2 zeigt ein Beispiel für den Prozess DS 5 „Sicherstellen der Systemsicherheit“.

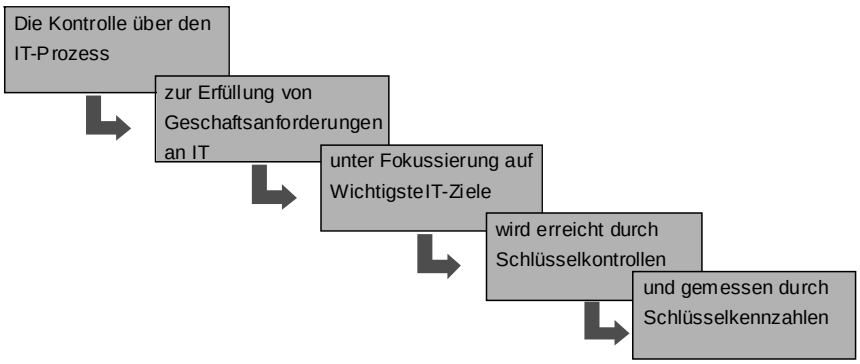


Abbildung 1: Wasserfall

DS5 Sicherstellen der Systemsicherheit

From	Inputs
P02	Information architecture; assigned data classifications
P03	Technology standards
P09	Risk assessment
AI2	Application security controls specification
DS1	OLAs

Outputs	To
Security incident definition	DS8
Specific training requirements on security awareness	DS7
Process performance reports	ME1
Required security changes	AI6
Security threats and vulnerabilities	P09

Abbildung 2: Sicherstellen der Systemsicherheit.

Als zweites neues Element zu den Management Guidelines gibt es zu jedem Prozess eine „RACI-Chart", in der zu den wesentlichen Aktivitäten, die zu dem Prozess gehören, den verschiedenen Jobfunktionen zugeordnet werden. In Form einer Matrix werden einerseits die Aktivitäten und andererseits die beteiligten Jobfunktionen dargestellt. An den Schnittpunkten der Matrix wird jeweils angegeben, welche Rolle die betreffende Funktion in der jeweiligen Aktivität spielt. Es wird hier angegeben R=resposable (zuständig für die Durchführung), A=accountable (verantwortlich für das Ergebnis), C=consulted (wird zur Beratung beigezogen), I=informed (wird informiert).

Das dritte Element der Management Guidelines ist eine Zusammenstellung von prozessspezifischen Zielen und Metriken und hilft bei der Festlegung konkreter Ziele (Was soll erreicht werden?) sowie der Metriken zur Feststellung des Zielerreichungsgrades (Wie kann die Zielerreichung gemessen werden?). In einer kaskadierten Darstellung werden Tätigkeitsziele, Prozessziele und IT-Ziele mit zugehörigen Kern-Ziel-Grössen (***key goal indicators*** – KGI) und Prozess-Ziel-Grössen (***key performance indicators*** – KPI) aufgeführt. Damit kann zwischen Leistungsmessung für den Prozess (KPI) sowie Zielerreichung (KGI) für den jeweiligen Prozess und für die IT insgesamt unterschieden werden.

RACI Chart PO10

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit Risk ans Security
Define a programme/portfolio framework for IT investments	C	C	A	R						C	C
Establish and maintain an IT project management framework	I	I	I	A/R	I	C	C	C	C	R	C
Establish and maintain an IT project monitoriing , measurement and management system	I	I	I	R		C	C	C	C	A/R	C
Build project charters, schedules, quality plans, budgets, and communication and risk management plans.			C	C	C	C	C	C	C	A/R	C
Assure the participation and commitment of project stakeholders.	I		A	R	C						C
Assure the effective control of projects and project changes.			C	C		C	C	C		A/R	C
Define and implement project assurance and review methods.			I	C				I		A/R	C

Functions

Responsible | Consulted
Accountable | Informed

Abbildung 3: RACI Chart

Dieses System ersetzt die aus CobiT 3 bekannten Elemente ***Critical Success Factors***, ***Key Goal Indicators*** und ***Key Performance Indicators.***

Maturity Model

Der jeweils vierte und letzte Abschnitt zu den einzelnen CobiT-Prozessen enthält die sechsstufige Beschreibung der „Reifegrade" des Prozesses. Es werden jeweils die Situationen beschrieben, die typischerweise in der betreffenden Maturitätsstufe anzutreffen sind. Durch Vergleich mit tatsächlich vorgefundenen Situationen lässt sich damit relativ einfach eine Einstufung vornehmen, die eine Beurteilung des Prozessreifegrades in einem spezifischen Unternehmen erlaubt.

Die Maturitätsmodelle wurden an die neue Prozessstruktur angepasst und zur Beurteilung der Reifegrade wurden die folgenden Kriterien definiert:

- Awareness und Kommunikation
- Richtlinien, Standards und Prozesse
- Hilfsmittel und Automatisierung
- Fähigkeiten und Expertenwissen
- Zuständigkeit und Verantwortlichkeit
- Zielsetzung und Messung der Zielerreichung

Gegenüber CobiT 3 sind die Beschreibungen insgesamt stark überarbeitet und konkreter formuliert worden.

Die folgenden sechs generischen CobiT-Maturitätsstufen sind definiert:

0 Es existieren keine Managementprozesse

1 Prozesse sind spontan und nicht organisiert

2 Prozesse laufen geordnet nach Vorlagen ab

3 Prozesse sind dokumentiert und kommuniziert

4 Prozesse werden überwacht und gemessen

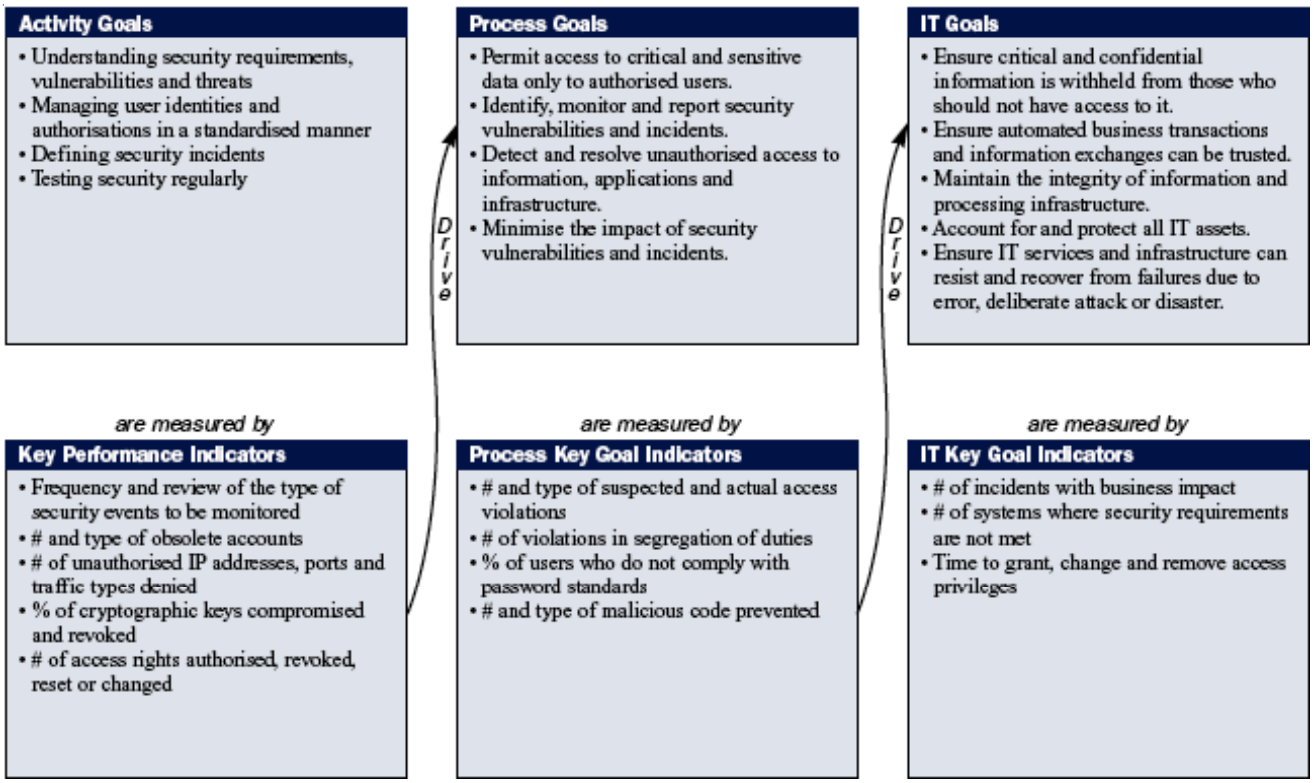


Abbildung 4: Key Goal Indicators

5 Bewährte Verfahren werden eingesetzt und automatisiert

Veränderungen in den Kontrollzielen

Wie auch in CobiT 3 gibt es unverändert vier Domains und 34 Prozesse. Da die Schwerpunkte teilweise neu gesetzt wurden, haben sich inhaltlich jedoch in den einzelnen Domains einige Änderungen ergeben, die im Folgenden beschrieben werden.

Plan and Organise

PO4 „Define the IT Processes, Organisation and Relationships“ wurde erweitert und deckt nun die IT-Prozesse, die Organisation und die Beziehungen ab.
PO5 „Manage the IT Investment“ beinhaltet verstärkt Aspekte der Wertschöpfung.
PO8 „Ensure Compliance with external Requirements“ wurde gestrichen und ist inhaltlich jetzt als ME4 in der Domain ME zu finden.
Der CobiT 3 Prozess PO11 wurde neu zu PO8 „Manage Qualitiy“, somit gibt es nur noch 10 Prozesse in der Domain PO.

Acquire and Implement

AI4 heisst neu „Enable Operation and Use“ und wurde gegenüber CobiT 3 erweitert.
Ein neuer Prozess AI5 „Procure IT Resources“ wurde eingefügt und das alte AI5 wurde verschoben nach AI7 und heisst neu „Install and Accredit Solutions and Changes“
AI6 „Manage Changes“ wurde an die ITIL Prozesse angepasst.

Deliver and Support

DS8 wurde in „Manage Service Desk and Incidents“ umbenannt und DS10 in „Manage Problems“; damit wurde die klare Trennung der Prozesse in Anlehnung an ITIL erreicht.
DS11 „Manage Data“ enthält nur noch Kontrollen bezogen auf das Datenmanagement, alle Applikationskontrollen wurden eliminiert. Diese finden sich jetzt in einem separaten Teil im Framework.

Monitor and Evaluate

Die vierte Domain wurde vollständig umgestaltet und heisst neu ME (Monitor and Evaluate)
ME1 „Manage IT Performance“ wurde präzisiert durch „Monitor and Evaluate IT Performance“
ME2 „Monitor Internal Control“ wurde ergänzt durch „Monitor and Evaluate Internal Control“
ME3 „Obtain Independent Assurance“ wurde ersetzt durch „Oversee IT Governance“
ME4 „Provide for independent Audit“ wurde ersetzt durch „Ensure Regulatory Compliance“ und ent-

spricht inhaltlich dem ehemaligen PO8.

Anhänge

Im Anhang I zu CobiT 4 finden sich drei Verweistabellen, die den Zusammenhang zwischen Geschäftszielen, IT-Zielen und den IT-Prozessen mit den zugehörigen Informationskriterien herstellen.

Die erste Tabelle verbindet 20 relevante Geschäftsziele, die in Form einer ***Balanced Scorecard*** mit 28 IT-Zielen und den zugehörigen Informationskriterien aufgeführt sind.

In einer zweiten Tabelle wird die Verbindung zwischen den 28 IT-Zielen und den 34 CobiT 4 IT Prozessen sowie den entsprechenden Informationskriterien hergestellt.

Die dritte Tabelle enthält die umgekehrte Darstellung wie Tabelle 2: Den 34 CobiT 4 IT-Prozessen werden die IT-Ziele zugeordnet.

Zur Orientierung über die detaillierten Änderungen in den Kontrollzielen und als Hilfe für die Umsteiger von CobiT 3 auf CobiT 4 sind ausserdem im Anhang V Verweistabellen von den Kontrollzielen CobiT 3 zu CobiT 4 und umgekehrt von CobiT 4 zu CobiT 3 aufgeführt. Darin enthalten ist auch die Zuordnung der Kontrollziele aus CobiT 3 zu den Prozesskontrollen und Applikationskontrollen.

Zusatzprodukte

CobiT 4 wurde Anfang Dezember 2005 veröffentlicht. Verschiedene Zusatzprodukte, die zu CobiT 3 zur Verfügung stehen, sind noch nicht an die Version 4 angepasst, können aber noch ohne weiteres verwendet werden. Die Adaption dieser Produkte an CobiT 4 ist vorgesehen und wird voraussichtlich schrittweise im Jahr 2006 erfolgen.
Dazu gehören

- die Audit Guidelines, (werden komplett überarbeitet als „IT Assurance Guide using CobiT“ zur Verfügung stehen)
- der Implementation Guide (neu „IT Governance Implementation Guide“),
- die CobiT Control Practices,
- CobiT Control Objectives for Sarbanes Oxley
- CobiT Security Baseline,
- CobiT Quickstart,
- CobiT Online.

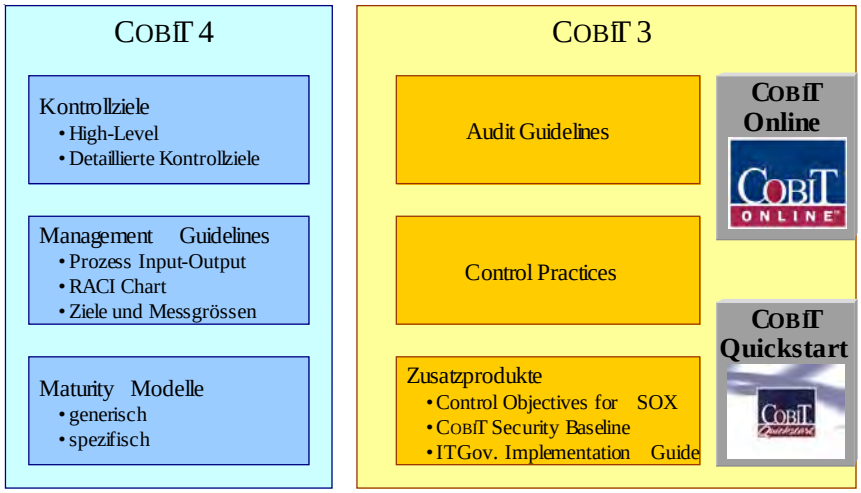


Abbildung 5: Dokumente

Literaturhinweise

CobiT 4.0: The New Face of CobiT; Gary Hardy and Erik Guldentops
Information Systems Control Journal, Vol. 6, 2005

CobiT's Management Guidelines Revisited: The KGIs/KPIs Cascade; Wim Van Grembergen and Steven De Haes
Information Systems Control Journal, Vol. 6, 2005

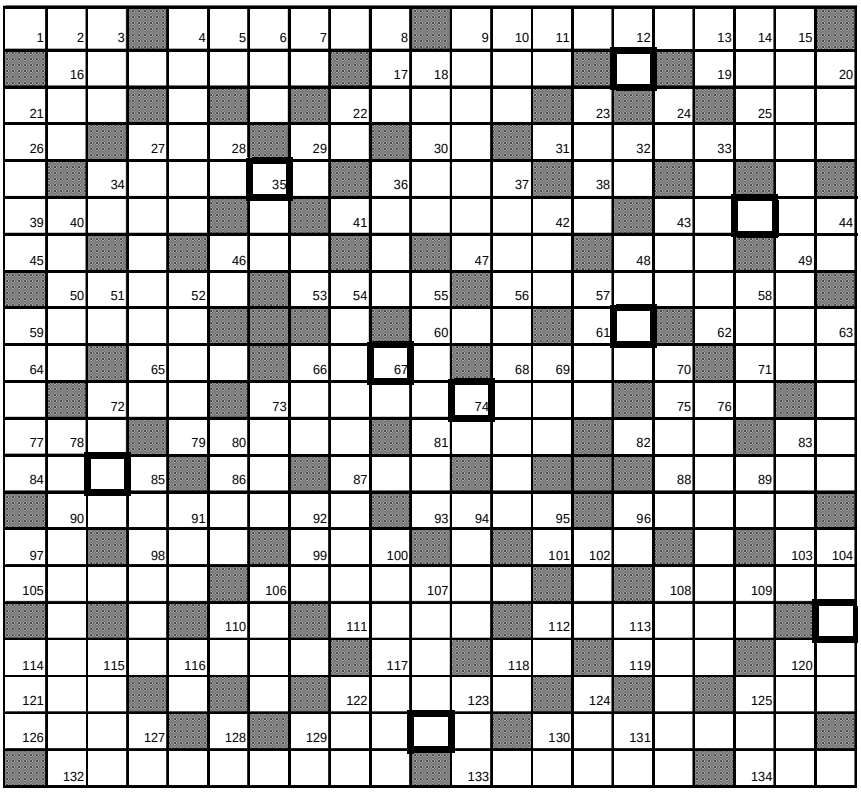
CobiT 4.0 Control Objectives, Management Guidelines, Maturity Models – ITGI 2005
ISBN 1-933284-37-4

Götz F. Hoffmann, CISA
Bitterli Consulting AG

ISACA
Serving IT Governance Professionals
Switzerland Chapter

The ISACA Crossword Puzzle 3/06

Dieses Rätsel ist auf englisch und hat mit dem Schwerpunktthema dieser Nummer zu tun. Autor ist der Redaktor. Lösungen, Kommentare und Reklamationen sind an ihn zu richten.



Across: 1 Wings from Nippon (abb); 4 Prodi's first name; 9 not suit; 16 Metropolis in India; 17 main bodies of trees; 19 biblical figure; 21 Master of Business Administration; 22 pull (Sp); 25 analysis of biological fingerprint; 26 Liliuokalani's Aloha; 27 trophy; 29 negation; 30 declined pronoun; 31 winter garment; 34 thing to be learnt; 36 comfortable; 38 Rubidium;39 dramatic music performance; 41 ***confirm***; 43 light brown; 45 king (It); 46 bag; 47 Joanne Woodward had three faces as such; 48 summer (Fr); 49 short mother; 50 hurling weapon; 53 artful flying (short word); 56 ***indication***; 59 ***main addressee***; 60 German preposition; 61 Southern Swiss license plate; 62 weight measurements; 64 conjunction; 65 the singing Jürgens; 66 chip in; 68 innocent; 71 between Salt and Marie on Lake Superior; 72 Greek character; 73 ***cascade***; 75 astrological sign; 77 ***norm body*** (abb); 79 ***transparent***; 81 transmit; 82 quality assurance verdict; 83 Barium; 84 place; 86 ***information system***; 87 to be heard by fans in Spain; 88 grabbed; 90 relating to the East; 93 always; 96 Greek letter; 97 he (Ge); 98 with (Ge); 99 they (Fr); 101 hour (It); 103 was once New Amsterdam; 105 remnant (pl); 106 woolly covering of sheep (pl); 108 deep voice or instrument; 110 Sp article; 111 bar; 112 order; 114 ***gain belief***; 117 left direction; 118 where the wizard lives, also used for Australia; 119 Kriemhild's mother; 120 auto plate from Herisau; 121 Palestinian Liberation Organization; 122 skies (Fr); 125 us (Ge); 126 relatively new currency; 129 textile trade mark; 130 currency (pl); 132 ***comparative measurement***; 133 ascertain; 134 not old.

Down: 2 French clergyman; 3 Jacob's first wife; 4 ancient Sicilian town; 5 conjunction; 6 males; 7 German ace; 8 operating system integration; 9 ***size***; 10 information management risk; 11 feared organization in WW II; 12 European Community; 13 two vowels; 14 Jap politician; 15 ***main addressee***; 18 dominating suit in card games; 20 King Cole's first name; 21 engine; 22 preposition; 23 drunk (Fr); 24 go (Sp); 27 watchdog in Greek mystic; 28 short post script; 29 no name; 32 European Union; 33 construction material; 34 French article; 35 wave (Sp); 36 pricking instrument; 37 ***control***; 40 currency (pl); 42 valid evidence value; 43 Greek goddess; 44 Egyptian god; 46 experienced a grounding; 48 French empty upside down; 51 short father; 52 with an additional t at the end devote; 54 ***business coxswain***; 55 ***supervise***; 57 ***benchmark organization***; 58 ***norm organization***; 59 ground; 63 hard top car; 66 three equal vowels; 67 aromatic beverage (Sp); 69 alternative level direction; 70 inspirit; 72 ill supplied; 73 cardinal point; 74 CS iron; 76 find numerical expression for; 78 recreational association; 80 soft material; 83 leguminous plant (pl); 85 wood; 89

the beginning and the end of every knight; 91 ice (Ge); 92 trouble; 94 much (Ge); 95 „Out of Rosenheim"; 96 yes (Ru); 97 it (Ge); 100 canal; 102 former Ethiopian noble;104 possessive pronoun; 106 French cop;107 fermented drink; 108 combat; 109 Southeast; 110 short for Edward; 112 short end zone; 113 French pronoun; 114 monkey; 115 kernel; 116 extra terrestrial; 118 bovine animal; 120 shallow bay; 122 automobile; 123 troubled French yes; 124 pronoun; 125 vase; 127 preposition; 128 Swiss auto plate; 129 short laughter; 130 data service; 131 lost right.

Die Lösung liegt in den markierten Feldern. Dieses Wort ist auf einer Postkarte zu senden an M.F. Bretscher, Oberrenggstrasse 8, 8135 Langnau a/A. Lösungen werden auch entgegengenommen unter der e-mail-Adresse mbretscher@kpmg.com. Einsendeschluss ist der 12. Januar 2006.

Lösung Crossword Puzzle 2/06: SCHIEBER

Waagrecht: 1 ***Erpressungen***; 11 Ganges; 16 (Kaul)Quappe; 17 Graben; 19 ile; 20 UEZ; 21 Iraki; 24 Ader; 25 bel; 26 EK; 27 Ra; 28 EC; 29 wer; 31 ***Betrueger***; 35 JL; 36 rio; 37 Me; 38 une; 39 RG; 40 jede; 42 Pan; 43 nur; 44 ir; 45 Assai; 47 Gaudi; 48 SU; 49 Hag; 51 Ola; 52 Leda; 54 Bo; 56 SG; 57 in; 58 Lt; 60 ***Boesewicht***; 64 Aiai (la-la); 66 ***faelschen***; 68 cher; 69 Mobilitaet; 71 NN; 72 ah; 73 re; 74 OK; 75 real; 77 Sau; 79 Tau; 80 la; 82 Yetis; 84 Hauer; 86 Aa; 87 und; 88 sie; 89 Flut; 90 EV; 92 (Big) Ben; 94 NE; 95 Rev; 96 ge; 97 ***Besserung***; 100 Ken; 101 SR; 102 te; 103 rr; 104 Lie; 105 Keil; 107 netto; 110 Sen; 112 Mae; 113 Sommer; 115 Ankern; 117 Palast; 118 ***Manipulation***.

Senkrecht: 1 Equ; 2 ***ruegen***; 3 paz; 4 Rp; 5 Epikur; 6 ser; 7 Ulk; 8 gg; 9 era; 10 Nadel; 11 Ger; 12 an; 13 Gier; 14 ell; 15 SE; 18 bec; 22 arg; 23 irreal; 25 Beo; 26 er; 29 ***window*** (dressing); 30 ***Veruntreuung***; 31 Buchsammlung; 32 Teig; 33 egal; 34 Eis; 35 je; 36 ***rauben***; 37 Mus; 41 ***Diebstahl***; 42 Pa; 46 Salat; 47 Gaehn; 50 Agio; 51 on; 53 Doc; 55 sch; 57 Ill; 59 tears; 62 ich; 63 Hera; 65 Abt; 66 ***fiktiv***; 67 Lee; 70 loesen; 72 Au; 76 Lauben; 78 Ares; 79 Tabu; 81 âne; 83 ie; 85 Ute; 89 Fe; 91 Verona; 93 entero; 95 Ree; 96 Grimm; 98 Set; 99 RR; 100 Kiel; 101 Sem; 104 Laa; 105 Kot; 106 Lea; 108 ERP; 109 Tal; 110 sei; 111 nnn; 112 MP; 113 ss; 114 RN; 116 K(en)t).

Watson: All letters of the alphabet appear at least once in the solution of the puzzle.

Der Gewinner ist Claus Reck, Hamburg. Er gewinnt damit $US 50 in Gutscheinen zum ISACA bookstore. Herzliche Gratulation! Der Watson wurde nicht entdeckt: Alle Buchstaben des Alphabets im Rätsel enthalten. Somit sind weiterhin $US 100 im Jackpot.

ISEIG Institut Suisse d'Enseignement de l'Informatique de Gestion

Nouveau et en exclusivité pour la Suisse romande,
animation par des pros de l'audit selon le modèle qui fait ses preuves depuis 13 ans à Zurich

Audit des systèmes d'information
Préparation à la certification internationale CISA

> formation complète : 18 soirées et 5 jours du 29 août au 25 novembre <
> Option « light » : 5 jours du 28 octobre au 25 novembre 2006 <

Pour plus d'informations : www.iseig.ch
ISEIG, av. des Boveresses 52, 1010 Lausanne
Tél : 021 654 40 60 – E-mail : info@iseig.ch

ISACA Serving IT Governance Professionals Switzerland Chapter

ISEIG Institut Suisse d'Enseignement de l'Informatique de Gestion

Nouveau et en exclusivité pour la Suisse romande

Audit des systèmes d'information
Préparation à la certification internationale CISA

> Excellent équilibre entre théorie et pratique <
23 soirées et 5 jours, dès le 29 août 2006

Pour plus d'informations : www.iseig.ch
ISEIG, av. des Boveresses 52, 1010 Lausanne
Tél : 021 654 40 60 – E-mail : info@iseig.ch

ISACA Serving IT Governance Professionals Switzerland Chapter

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Express Line

A Word from the Chair

Greetings!

ISACA's annual midyear dues incentive is now in place. Any new members joining between 1 June and 6 August will be charged only 50 percent of the international association dues, plus the new member processing fee and chapter dues, for membership through 31 December 2006. Keep in mind that the new member processing fee is reduced from US $30 to US $10 when new members join online at www.isaca.org.

Steve Thorsted
Chair, Membership Board

Fraudulent Web Site Alert

A web site (***www.cisaca.org***) originating in China and owned by the CISA Chinese Alliance is claiming to be authorized by ISACA to register candidates for the CISA exam and collect exam fees through its site. This same site also claims to sell a Chinese version of the ***CISA Review Manual*** and the ***CISA Review Questions, Answers & Explanations Manual.***

Please be advised that neither this web site nor its owner is affiliated in any way with or endorsed by ISACA. Nor has the web site or its owner been authorized as a registrar for the CISA exam or as a distributor of any CISA study materials. Please inform your members of this fraudulent operation. Please inform potential candidates that registration for the CISA or CISM exam can be done only through the ISACA web site.

International Headquarters has contacted this organization to advise it to cease and desist these infringements of ISACA intellectual property and fraudulent activities. If you are aware of any individuals who have been adversely impacted by this web site, please notify International Headquarters' certification department immediately (certification@isaca.org).

December 2006 Exam Registration and BOI

Registration for the 9 December 2006 CISA and CISM exams will open in July. More details will be provided as they become available. The English versions of the CISA and CISM bulletins of information for the December exam were mailed to the chapter CISA and CISM coordinators in May.

CISA and CISM Exam Recruitment and Training

We would like to thank you for your continued support in promoting the exams and offering CISA or CISM review courses for June exam candidates. The success of ISACA's programs can be attributed in large part to exceptional efforts from chapters.

Assistance Sought in Identifying IP Violations

ISACA International Headquarters is seeking the assistance of chapters to help identify potential violations of intellectual property. Please notify Joann Skiba, director of intellectual property, at ***jskiba@isaca.org***, if you become aware of web sites that are potentially misusing ISACA/ITGI trademarks and copyrighted materials.

DACH-News

Rückblick und Ausblick der IIR IT-Tagung 2006

Im Zeichen aktueller Entwicklungen, Methoden, Techniken und Werkzeuge

Rückblick

Rund 120 Teilnehmende (darunter ca. 50% ISACA-Mitglieder) trafen sich am 22. und 23. Mai 2006 im Arabella Sheraton Congress Hotel in Frankfurt am Main. Aus der Sicht des Gastreferenten und Teilnehmers Bruno Wiederkehr, ISACA Switzerland Chapter, kann ich auf den gut koordinierten Event (IIR e.V. und ISACA) und die beiden erfolgreichen Tage zurückblicken. Damit verbunden war auch die Kontaktnahme zwischen den beiden ISACA Chaptern (Deutschland – Schweiz), welche ich für die zukünftige Zusammenarbeit als sehr wertvoll betrachte.

Sehr positiv empfand ich auch die während der Tagung geplanten Diskussionsforen sowie den Gedanken- und Erfahrungsaustausch beim „Standing"-Nachtessen. Die grossen runden Tische erlaubten viel leichter, interessanten Diskussionen zu folgen und auch einmal den Platz zwischen den einzelnen Gängen sowie den Tischen zu wechseln. Wie von Herrn Dr. Peter Sporrer, Leiter der IIR-Akademie, zu erfahren war, hat bereits die Organisation für die nächste Tagung vom 04.–05. Juni 2007 in Frankfurt begonnen.

Das Rednerpult war denn auch mit prominenten Professoren, Visionären, Methodikern und Praktikern (Universität Freiburg, Universität Bremen, E&Y, KPMG, BSI, Deutsche Post AG etc.) besetzt. Nahe am Hörerinteresse wurden u.a. die folgenden Highlights thematisiert:

- CobiT 4 – ein neuer Meilenstein
- Implementierung ISO 27001 & Vorgehensweise BSI Standard 100-2
- Zertifizierung ISO 20000 – ITIL Norm im IT Service Management
- Joint Audits – Zusammenspiel IT- und Fach-Revision
- Risikoorientierte Audit-Planung und -Durchführung

Zusammenfassung des Referates

Nebst dem Fokus „Risikoorientierung" (Risk Management) darf bei der Audit-Vorbereitung, -Planung und -Durchführung die übrigen Domänen der IT-Governance durch den IT-Revisor nicht aus den Augen gelassen werden.

Wie auch aus dem IT Governance Status Report 2006 hervorgeht, steht die Security nicht an erster Stelle. Von den Befragten wurde das IT Staffing (Resource Management), also die Stellenbesetzung, als grösstes und wichtigstes IT Problem betrachtet. 87% der Befragten haben angegeben, dass die Erfüllung der Unternehmensstrategie durch die IT (Strategic Alignment) immer schwieriger werde. Beide Schwerpunkte betreffen wiederum die Leistungserbringung (Performance Management) und die Wertschöpfung (Value Delivery). Fazit: Bei einem Audit müssen alle fünf IT Governance Domänen in die Betrachtungen einbezogen werden.

Im Verlauf des Referates habe ich auf den Schlüssel des Erfolges, nämlich auf die Systematik hingewiesen. Es geht darum, Audit-Strategien, -Mittel und -Verfahren zu entwickeln, um strukturierte und unstrukturierte Informationen (u.a. Vorschriften, Standards und Prozeduren) zu handlungsrelevantem Auditwissen zu verknüpfen.

Weltweite Erfahrungen haben gezeigt, dass die von ISACA zur Verfügung gestellten IS Auditing Standards, Guidelines und Procedures in Verbindung mit CobiT „All in One, One for All" sehr hilfreich sind. CobiT-

basierte Werkzeuge zur Unterstützung der Audit-Systematik gibt es nebst ISACA bei einigen Beratungs-Unternehmen und Revisionsgesellschaften. Versuchen Sie begeistert damit die Vorgehensweise zu optimieren, Begeisterung soll ansteckend sein: Sie werden damit sicher Erfolg haben.

Schlusspunkt

Während der Tagung wurden vermehrt die Rolle des Revisors und die damit verbundenen Innovationsfragen diskutiert. Welche Voraussetzungen müssen gegeben sein? Wo können professionelle und systematische Innovationen der Revision einen Lösungsbeitrag für das Unternehmen leisten? Wann und wie sind ein Revisor und sein Manager innovativ?

Als Einstieg kann die aktuelle Diskussion über Sarbanes Oxley, Basel II und Solvency dienen. Die Chancen stehen gut, gemeinsame mit dem Management grundsätzliche Aussagen aufgrund anerkannter Rahmenwerke (COSO, CobiT 4) in Kombination mit neuen „Good Practice" Standards (u.a. Informationssicherheit ISO 27001, ITIL-Zertifizierung ISO 20000, IS Auditing Standards, Guidelines & Procedures) zu erarbeiten.

Es muss der Revision gelingen, sich den grossen Aufgaben im Audit Universe zu stellen und sich Ziele im Hinblick auf die Effizienz und Effektivität der Audit- und Control-Performance zu setzen.

Jeder muss über das eigene Potenzial im Klaren sein, um gemeinsam Chancen zu realisieren. Dazu braucht es den Willen und das Bewusstsein, innovativ zu agieren und zugleich die vorhandenen Revisionsmethoden und -werkzeuge professionell und angemessen einzusetzen.

Das visionäre und mit viel Schalk vorgetragene Referat von Prof. Dr. Günther Müller, Universität Freiburg, war der krönende Abschluss der IT-Tagung 2006.

Angaben zu Standards erhalten Sie unter www.iir-ev.de , www.isaca.de, www.isaca.org (engl.) CobiT Elemente www.isaca.ch (deut./engl.) und CobiT Werkzeuge www.isaca.org/bookstore.

Bruno Wiederkehr

AHS vom 25. April 2006

PD Klaus Peter Rippe referierte zum Thema „Mit der Brille der Ethik – Umgang mit ethischen Konflikten". Der Referent unterhielt die gegen 50 Teilnehmer in lockerem Stil über die Begriffe von Moral und Ethik. Sie sind seit den Skandalen von Enron, Worldcom und Co. aktuell wie kaum je zuvor. Peinlich ist dabei, dass Präsidenten der USA bei diesen Gelegenheiten in den Fettnapf traten.

Dabei ist jeweils zu unterscheiden, ob blosse Dummheit vorliegt, oder ob Manipulationen im Spiel sind. Delikat ist bei letzteren, ob sie ethisch verwerflich sind oder nicht. Ebenfalls sind kulturelle Unterschiede bei Moral und Ethik nicht unbedeutend. Wichtig ist, dass alle Teilnehmer am „Spiel" die „Spielreglen" kennen und akzeptiert haben. Ein „Über-den-Tisch-ziehen" ist immer dann verwerflich, wenn der Geschädigte die Regeln nicht kannte.

Die grosse Mehrheit der Teilnehmer war sich zu Beginn zwar einig, dass die Begriffe Zuverlässigkeit, Offenheit, Vertrauenswürdigkeit und Ehrlichkeit als Basis der Ethik eine Selbstverständlichkeit sein sollten. Die Standards der ISACA besagen ja genau dies. Die Darlegungen des Referenten stimmten alle jedoch nachdenklich, als offenbar wurde, dass die genannten Begriffe aber in Konfliktsituationen geraten können. Welcher Begriff hat wann Vorrang?

In der rege benützten Diskussion wurden Stimmen laut, die aussagten, dass der IT-Revisor immer unverblümt die Wahrheit sagen sollte. Kritische Beobachter führten dagegen ins Feld, dass die Wahrheit nicht immer sonnenklar ist (Unsicherheit) und dass bittere Pillen für den „Schluckenden" positiv darzustellen wären. Für Rippe bleibt aber auch eine bittere Pille mit Zuckerguss immer noch bitter. Auf die provokative Frage, ob eine unangenehme Tatsache verschwiegen werden dürfe, wenn dabei eigene Interessen einschneidend gefährdet werden könnten, war die im

Brustton der Überzeugung geäusserte Meinung, dass dies nicht verschwiegen werden dürfe. Ein Blick in die teilweise verlegenen Gesichter verriet hingegen, dass die Frage nicht leicht zu beantworten ist.

Ein Teilnehmer brachte beim anschliessenden Apéro die Sache wohl auf den Punkt, als er meinte, wichtig sei für ihn, dass er auch nach einer ethisch heiklen Diskussion gut schlafen könne.

AHS vom 30. Mai 2006: IT Risk Management.

Mario Walter der Firma Roche Diagnostics stellte den etwa 50 interessierten Teilnehmern die Elemente der Vorgehensweise bei seiner Firma vor. Als spezielle „goodies“ behandelte er auch die OSI-Levels 8 bis 10. Das Niveau 8 (eigentlich „people“) taufte er treffend in „Politik“ um. Damit sprach er natürlich die Firmenpolitik an, welche das Verhalten der mit den Applikationen (Level 7 des OSI-Modells) beschäftigten Leute bestimmt. Dass man sich mit dem Level 9 (Finanzen) schwer tun kann, illustrierte er mit dem Vergleich, was der monetäre Wert von beispielsweise CHF 5000 in diversen Ländern der Welt bedeuten kann. In Indien vielleicht ein Jahreslohn, in den USA „peanuts“. Auch der Level 10 (Gesetze und Regulatorien) kann in einigen Ländern zwar unproblematisch sein, in andern dagegen mit erheblichen Risiken verbunden sein: Wenn ein Land die Untreue eines Angestellten nicht unter Strafe stellt, können bei Outsourcing in dieses Land Fabrikgeheimnisse und anderes geistiges Eigentum (Source Code!) „problemlos“ verraten werden. Mario Walter erwähnte zwar, dass diese Elemente bei Roche Berücksichtigung finden, doch Details der Messelemente und -grössen konnte er in der kurzen Zeit nicht vorstellen. Ebenso blieb die Frage im Raum stehen, wie oft bisher aufgrund der operationellen Messungen Risikopunkte in der Risikomatrix (er nannte sie IT Risk Landscape) eliminiert, neu definiert oder verschoben werden mussten. Am Schluss gab er aus seiner Erfahrung jedoch wertvolle Hinweise an die Risk Manager und Revisoren, wie sie ihre Anliegen erfolgreich „verkaufen“, ohne „erschossen“ zu werden.

AHS vom 27. Juni 2006

Im AHS vom 27. Juni 2006 präsentierte Walter Sprenger der Firma Compass Security ein Frühwarnsystem für Phishing. Dabei erläuterte er die theoretischen Grundlagen, die sich an ein Frühwarnsystem einer Tsunamiwarnung anlehnen. Allerdings musste er zugestehen, dass echte Feldtests und deren Ergebnisse noch nicht vorliegen, weil offenbar das Interesse bei den möglichen Betroffenen (insbesondere Banken) nicht im notwendigen Umfang vorhanden ist. Dennoch demonstrierte er, wie das System funktionieren könnte. Zentral sind dabei erstens die zur Auswahl möglicher Phishingattacken zu definierenden Regeln, andererseits die Menge der zu untersuchenden e-Mails. Die Diskussionen im Anschluss an den Vortrag zeigten, dass ein sehr grosses Interesse am Thema der Abwehr von Phishing an sich besteht. Wie man mit den Attacken umgeht und darüber, ob eine allfällige Publizität bezüglich Attacken positive oder negative Imageeffekte für die angegriffenen Institute haben könnte, gingen die Meinungen stark auseinander.

News aus den Interessengruppen

IG Operational IT-Risk

Peter R. Bitterli
Bitterli Consulting AG
Stampfenbachstr. 40
8006 Zürich
Tel. + 41 44 444 11 01
Fax. +41 44 444 11 02
prb@bitterli-consulting.ch

Die Interessensgruppe „Operational (IT) Risk“ hat sich neu formiert und entwickelt ein Konzept resp. Vorgehensvorschlag für ein „Risiko Management Kochbuch“. Ziel ist, Geschäftsleitungsmitgliedern, Führungsverantwortlichen im Business und der IT, Risikomanagement-Spezialisten und anderen Personen Schritt für Schritt aufzuzeigen, wie man für ein mittleres Unternehmen (eventuell auch für ein grosses Unternehmen mit wenig eigenen Informatiktätigkeiten) ein Risikomanagement aufbauen und erfolgreich beibehalten kann.

Derzeit werden keine neuen Mitglieder aufgenommen. Wenn die Ergebnisse vorliegen, wird die Interessengruppe darüber informieren.

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

Le groupe de travail qui rassemble les auditeurs informatiques des collectivités publiques a élaboré des recommandations à l’égard des responsables de projet informatique. Ce document d’une douzaine de

pages est disponible en allemand, français et italien.

Les responsables de projet sont en effet soumis à de nombreuses contraintes et doivent conduire leurs projets au succès dans des conditions parfois difficiles. L'intervention d'un auditeur constitue un défi supplémentaire souvent perçu comme une inutile chicane par les responsables. Les Contrôles des finances estiment important de communiquer de manière ouverte et conséquente avec les responsables de projet. Cette brochure est là pour répondre à des questions qui sont fréquemment posées aux auditeurs. Elle contient également des informations intéressantes pour les décideurs, les responsables informatiques ou les personnes chargées de l'assurance-qualité.

L'objectif est notamment de déterminer la liste des documents les plus importants pour un auditeur et de définir les questions auxquelles ils doivent répondre. Cette brochure qui fait une large référence à CobiT se concentre sur la phase de projet qui constitue un passage important de la vie d'une application. Il existe en Suisse différentes méthodes de développement (y compris celles qui sont proposées par certains fournisseurs) et la terminologie peut varier de l'une à l'autre. Cette brochure se concentre sur le contenu des documents et fournit les références à ces différentes méthodes.

Ce document peut être téléchargé gratuitement aux adresses suivantes:
Deutsch : http://www.efk.admin.ch/pdf/novena_d.pdf
Français : http://www.efk.admin.ch/pdf/novena_f.pdf
Italien : http://www.efk.admin.ch/pdf/novena_i.pdf

Les membres de l'IG espèrent avoir grâce à cette brochure renforcé le dialogue entre les auditeurs et les responsables IT et contribué ainsi à un développement harmonieux et rentable des projets informatiques dans les administrations publiques suisses.

IG Computer Forensics

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

Cayan Oezguerol
Kügeliloostrasse 44
8050 Zürich
Mobile +41 79 401 01 81
Tel. +31 44 312 15 83
Fax. +41 86 079 401 01 81

Nächste Sitzung: Juli/August 2006.
Traktanden:
- Standortbestimmung der IG
- Erweiterung der Aufgaben (CobiT 4.0, Schnittstelle zur Corporate Governance, Leitfaden)
- Abnahme Domäne „Auslieferung und Unterstützung"
- Besprechung Entwurf zur Domäne „Planung and Organizsation"

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

Derzeit ruhend. Der Leiter sucht einen Nachfolger.

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

Nach einer längeren Pause hat die IG ihre Arbeit wieder aufgenommen.

■ Wrap-Up/Standortbestimmung

Es wurden alle bisher erstellten Dokumente aufgelistet und sofern sie noch finalisiert werden müssen, einem Verantwortlichen zur Bearbeitung zugeteilt.

■ Weiteres Vorgehen

Das Referenzmodell und die Risiko-Matrix sollen als Resultat der Phase I (Datenextrakt und Load) nochmals überarbeitet und bereinigt werden. Danach sollen sie auf der Website der ISACA öffentlich zugänglich gemacht werden. Die diversen Fact-Sheets werden zum Teil nochmals überarbeitet zum Teil neu erstellt und gelten als Resultat der Phase II (Projektvorgehen und weitere relevante Aspekte).

■ Wahl des neuen IG Leiters

Nach einer kurzen Besprechung ist der bisherige IG Leiter bestätigt worden. Es findet somit kein Wechsel statt.

■ Diverses

Die Resultate sollen im Rahmen einer ISACA-Abendveranstaltung präsentiert werden.

Neue Interessenten können sich bei Daniel Oser, IG-Leiter, anmelden.

IG SAP R/3

Jörg Altmeier
Wikima4 AG
Bahnhofstrasse 28
6304 Zug
Tel. +41 41 711 94 54
Fax. +41 41 711 94 54
joerg.altmeier@wikima4.com

Letzte Sitzung: 08. Mai 2006, ITACS Training AG, Zürich

1. Begrüssung
2. Sicherheitsstrategie SAP am Beispiel des Kompetenzzentrums der Bundesverwaltung was ist zu machen (und zu prüfen!) (Hr. Walter Bremer, Leiter Applikationsbetrieb CCSAP BV)
3. Tipps und Tricks zur Prüfung im SAP FI (Hr. Roland Giger, Revisionsexperte EFK)
4. Erfahrungen und News (alle)
5. Diverses

Nächste Sitzung: 27. November 2006 bei ITACS Training AG, Zürich

Monika E. Galli Mead hat die IG seit ihrer Gründung mit grossem Engagement geleitet und immer wieder sehr interessante IG Sitzungen organisiert. Nun tritt Sie in den Ruhestand und übergibt die IG-Leitung an Jörg Altmeier, Geschäftsführer der Wikima4 AG und fachlicher Leiter der Arbeitsgruppe „Sicherheit in SAP-Systemen" der Information Security Society of Switzerland (fgsec).

Monika, wir danken Dir und hoffen, Dich weiterhin an unseren Sitzungen begrüssen zu dürfen und wünschen Dir alle Gute.

Mit Jörg Altmeier ergeben sich sicherlich interessante Verbindungen zur fgsec.

IG (Self) Assessement mit CobiT 4.0

Luc Pelfini
Bitterli Consulting AG
Stampfenbachstrasse 40
CH-8006 Zürich
Tel: +41 44 444 11 00
lmp@bitterli-consulting.ch

Die Hälfte der Interessenten hat sich an einer ersten Sitzung am 29.5. in Zürich getroffen. Die restlichen Interessenten, die erst kurz vor der ersten Sitzung auf die IG aufmerksam wurden, werden an der zweiten Arbeitssitzung am 10. Juli dazu stossen. Weitere Interessenten können sich bei Luc Pelfini anmelden.

Die unterschiedlichen Arbeitgeber (Kanton, Consulting-Firma, internationaler Konzern, Telekom, etc.) der momentan sieben potentiellen IG-Mitglieder verspricht interessante Diskussionen und Arbeitsergebnisse. Möglicherweise kann auch ein Austausch von Arbeitsergebnissen mit einer CobiT Assessment Arbeitsgruppe in Deutschland weitere Horizonte eröffnen.

An der nächsten IG-Sitzung gilt es in möglichst vollständiger Zusammensetzung der IG vor Allem die folgenden drei Punkte zu klären:

1. Genaue Definition wie das Self Assessment gestaltet werden soll, insbesondere betreffend Hilfestellung für die Einteilung in einen Maturity Level sowie der pro Level mindestens verlangten Kontrollen.
2. Welche Kontrollziele werden als erstes angegangen, um eine Unterstützung zum (Self) Assessment zu erarbeiten?
3. Für welchen Personenkreis werden die vollständigen Arbeitsergebnisse oder Auszüge davon veröffentlicht? Diese Frage ist insbesondere zu klären, wenn die IG eine elektronische Unterstützung für das Assessment entwickelt (Beispielsweise mit Excel).

Nächste Sitzung: Die nächste IG-Sitzung findet am 10. Juli ab 16.00 in Zürich bei Bitterli Consulting statt.

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Veranstaltungen

CISA Vertiefungskurs 2006|2	14. Aug. 2006–27. Nov. 2006 Zürich, 14 Tage, ISACA/ITACS
CISM Vertiefungskurs 2006|2	21. Aug. 2006–28. Nov. 2006 Zürich, 12 Tage, ISACA/ITACS
Evidence Lab – Workshop über die Spurensuche in Computersystemen	23.–25. August 2006 Zürich, 3 Tage, ISACA/Compass
IT Security Forum	24. August 2006 Zürich, 1 Tag, Utimaco
After Hour Seminar: Mit Facetten des Business Continuity Management	29. August 2006 16:40–17:40, Zürich, ISACA
Anwendungssicherheit: Risikoorientierte Entwicklungsmethoden	30. August–1. September 2006 Zürich, 3 Tage, ISACA/ITACS
Intensivlehrgang für SIBE	4.–8. September 2006 Zürich, 5 Tage, Infosec
Application Security Lab – Workshop zum Thema Sicherheit von Web-Anwendungen	6.–8. September 2006 Zürich, 3 Tage, ISACA/Compass
Security over IP – Sicherheitstechnik der Zukunft	7. September 2006 Zürich, 1 Tag, SES
Einführungskurs in Systemhandling für SAP R/3 Workshop	12. September 2006 Stuttgart, 1 Tage, ISACA
SAP R/3 Workshop für Wirtschafts- und Informatikprüfer	13.–15. September 2006 Stuttgart, 3 Tage, ISACA
Content- und Mobile-Security Lab – Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung durch mobile Tech. und aktuelle Malware	27.–29. September 2006 Zürich, 3 Tage, ISACA/Compass
ITIL Foundation Training – Service Management Auf der Basis des de facto-Standards ITIL mit Links zur BS 15000 und ISO 20000 Zertifizierung	27.–29. September 2006 Zürich, 3 Tage, ISACA/Glenfis
Cryptography, Fundamentals and Applications	16.–19. Oktober 2006 Engelberg, 4 Tage, ATS
CISA Prüfungsvorbereitungskurs 2006|2	23. Okt. 2006–27. Nov. 2006 Zürich, 5 Tage, ISACA/ITACS
CISM Prüfungsvorbereitungskurs 2006|2	26. Okt. 2006–28. Nov. 2006 Zürich, 4 Tage, ISACA/ITACS
Forensic Lab	7.–9. November 2006 Karlsruhe, 3 Tage, Secorvo
ISO 20000 Consultant & Internal Auditor, inkl. int. Zertifizierung	20.–22. November 2006 Zürich, 3 Tage, ISACA/Glenfis

ISACA
Serving IT Governance Professionals
Switzerland Chapter

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

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

IIR-Akademie
Ohmstr. 59
D-60468 Frankfurt/Main
Tel. +49 69 7137 69-0
Fax. +49 69 7137 69-69
iir.academie@t-online.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 Switzerland Chapter
c/o ITACS Training AG
Stampfenbachstrasse 40
CH-8006 Zürich
Tel. + 41 44 444 11 01
Fax +41 44 444 11 02
info@isaca.ch
www.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

ITACS Training AG
Stampfenbachstrasse 40
CH-8006 Zürich
Tel. +41 44 444 11 01
Fax +41 44 444 11 02
info@itacs.ch
www.itacs.ch

Management Circle
Hauptstrasse 129
D-65760 Eschborn/Ts.
Tel. +49 6196 4722-800
anmeldung@managementcircle.de

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

Serview GmbH
The Business IT Alignment Company
Gartenstrasse 23
D-61352 Bad Homburg
Tel. +49 6172 177 44-0

Swiss Infosec AG
Weissensteinstrasse 2b
CH-3008 Bern
Tel. +41 31 300 73 73
Fax +41 31 300 73 78
infosec@infosec.ch

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

Vereon AG
Rosgartenstrasse 37
CH-8280 Kreuzlingen
Tel. +41 71 670 19 14
Fax. +41 71 670 19 13
info@vereon.ch
www.vereon.ch

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

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Vereinsadressen

Germany Chapter

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

Präsidentin
Karin Thelemann
Tel. +49 6196 99626 488
karin.thelemann@de.ey.com

Konferenzen
Markus Gaulke
Tel. +49 69 9587 2313
MGaulke@kpmg.com

Mitgliederverwaltung und Kassenwart
Norbert Gröning
Tel. +49 201 438 0
Norbert.Groening@de.pwcglobal.com

Public Relations
Heinrich Geis
Tel. +49 692 101 5149
heinrich.geis@deutsche-boerse.com

Arbeitskreise und Facharbeit
Bernd Wojtyna
Tel. +49 251 288 4253 oder
+49 251 210 4539
bernd_wojtyna@gmx.net

Publikationen
Ingo Struckmeyer
Tel. +49 4106 704 2336
ingo.struckmeyer@pf.comdirect.de

CISA-Koordinator
Holger Klindtworth
Tel. +49 (40)41522863
h.klindtworth@susat.de

www.isaca.de

Austria Chapter

Vorsitzender (Präsident)
Ing. Mag. Dr. Michael Schirmbrand
Tel: +43 1 31332 656
m.schirmbrand@kpmg.com

Stellvertretender Vorsitzender I (Vizepräsident I)
Dipl.-Ing. Maria-Theresia Stadler,
Tel: +43 1 53127 2857
maria-theresia.stadler@oekb.at

Stellvertretender Vorsitzender II (Vizepräsident II)
Mag. Josef Renner
PricewaterhouseCoopers
Tel: +43 1 501 88 1701
josef.renner@at.pwcglobal.com

Schriftführer, Mitgliederversammlung, Marketing
Mag. Gunther W. Reimoser
Tel: +43 1 12 111 701 032
gunther.reimoser@at.ey.com

Kassier, Webmaster
Mag. Jimmy Heschl
Tel: +43 1 31332 619
jimmy@heschl.at

CISA/CISM-Koordinator
Mag. Ulrike Knödlstorfer-Ross
Tel: +43 1 33151 145
ulrike.knoedelstorfer@ama.gv.at

NewsLetter-Koordination
Mag. Dieter Stangl-Krieger
Tel: +43 1 31332 619
DStangl-Krieger@kpmg.at

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

www.isaca.at

Switzerland Chapter

Präsidentin
Daniela S. Gschwend
Tel. +41 43 285 69 36
daniela_gschwend@swissre.com

Vizepräsident
Michel Huissoud, CISA, CIA
Tel. +41 31 323 10 35
Michel.Huissoud@efk.admin.ch

Kassier
Pierre A. Ecoeur, CISA
Tel. +41 71 626 64 61
pierre-alain.ecoeur@tkb.ch

Ausbildung/Kurssekretariat
Peter R. Bitterli, CISA
Tel. +41 44 444 11 00
prb@bitterli-consulting.ch

CISA/CISM-Koordinator
Thomas Bucher
Tel. +41 44 421 64 22
tbucher@deloitte.com

Sekretär
c/o Präsidentin

Information & Kommunikation
Monika Josi
Tel. +41 61 324 09 59
monika.josi@novartis.com
Adressmutationen bitte hier melden.

Koordinator Interessengruppen
Rolf Merz
Tel. +41 58 286 66 79
Rolf.Merz@ch.ey.com

Représentant Suisse Romande
Marc Barbezat
Tel. +41 79 56 55 666
marc.barbezat@b3b.ch

Marketing
Bruno Wiederkehr
Tel. +41 44 910 96 33
bru.wiederkehr@bluewin.ch

www.isaca.ch