Nr. 78 | Februar 2006

Schwerpunkt-Thema:

Zusammenarbeit Abschlussprüfer/ IT-Revisor

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Inhaltsverzeichnis

Editorial 4

Zusammenarbeit Abschlussprüfer/IT-Revisor – Bedeutung neuen der Schweizer Prüfungsstandards (PS) 5

Zusammenarbeit Abschlussprüfer/IT-Revisor – Processus informatiques et audit financier, une interaction de plus en plus importante 8

Zusammenarbeit Abschlussprüfer/IT-Revisor – Zusammenarbeit zwischen Abschluss-prüfer und Informatikrevisor 10

Zusammenarbeit Abschlussprüfer/IT-Revisor – Are We Just Below the Summit? 12

CobiT – Erfüllt CobiT 4.0 die Erwartungen des PCAOB? 13

The ISACA Crossword Puzzle 18

Express Line 20

DACH-News 22

Veranstaltungen 26

Vereinsadressen 28

Impressum

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

Redaktion:
Max F. Bretscher
KPMG Fides Peat
Badenerstrasse 172
8026 Zürich
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 5 Mal jährlich
Auflage: 1350 Exemplare

Nächste Ausgabe (Thema: PS 240 – IT-Deliktische Handlungen): April 2006, Redaktionsschluss: 30. März 2006

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Editorial

L'audit: une plus-value essentielle

Le Conseil fédéral a déclaré 2005 « Année de la technique ». Un « Jour de la technique 2006 » sera introduit et c'est là l'occasion idéale de se pencher sur la plus-value que peut apporter l'audit. Sous le titre « ePower », l'objectif est d'amener la Suisse à occuper une position de pointe dans des domaines comme eHealth, eGovernment, Recherche et Développement.

Les promoteurs de ce projet sont conscients de l'importance à accorder à la protection des données et à la sécurité informatique. Ces deux thèmes sont en effet essentiels pour convaincre les citoyens et les clients d'adhérer à ces e-solutions. C'est une excellente occasion d'examiner la plus-value que peuvent apporter à ce projet « ePower » les spécialistes de la gouvernance informatique de l'ISACA/ITGI.

Ce thème, mais aussi la manière de collaborer et les effets positifs que notre profession peut attendre de cette collaboration sont abordés dans ce numéro.

L'amélioration de plusieurs référentiels de contrôle (CobiT 4.0 et COSO) constitue une bonne occasion de repenser les modalités de la collaboration entre l'audit interne et l'audit externe, mais également entre les auditeurs informatiques et les auditeurs financiers.

La communication et la collaboration entre les auditeurs et les audités représentent cependant un défi peut-être encore plus important que ces instruments. La croissance des exigences réglementaires, organisationnelles et techniques ne pourra être maîtrisée qu'en clarifiant les rôles respectifs et en améliorant la coopération entre les acteurs suivants:

- Conseil d'administration, direction, comité d'audit
- Management (gestion des risques, qualité, sécurité, compliance)
- Audits interne et externe
- Chambre fiduciaire et ISACA/ITGI (IT Governance Institut).

D'une manière générale, seule une approche globalisante de l'entreprise permet de concevoir et de mettre en place un système de contrôle interne et une gouvernance informatique efficaces.

Jusqu'à ce jour les auditeurs se sont essentiellement intéressés aux actions (quoi ?) et aux justifications (pourquoi ?) des opérations informatiques. Ce qui va changer est l'intérêt croissant des auditeurs pour la performance des systèmes d'information (comment ? quels indicateurs de prestations ? quelle plus-value apporte l'informatique ?)

Nous devons accompagner cette innovation en faisant évoluer les relations entre la politique, l'économie, la science et les organisations professionnelles. Un défi ambitieux mais motivant si nous arrivons à faire évoluer les mentalités !

Bruno Wiederkehr

Zusammenarbeit der Revision

Im Jahre 2005 hat der Bundesrat das Patronat „Jahr der Technik 2005" übernommen. Ein „Tag der Technik 2006" wird weitergeführt – der ideale Rahmen, um über das Thema „ePower" und die Zusammenarbeit nachzudenken. Das Ziel ist: Die Schweiz soll in folgenden Bereichen der ICT-Branche eine Spitzenposition einnehmen können: eHealth, eGovernment, Forschung und Entwicklung.

Die Initianten sind sich einig, auch dem Datenschutz und der Sicherheit genügend Rechnung zu tragen: Nur so haben eLösungen die notwendige Akzeptanz und das Vertrauen. Mit der Initiative „ePower für die Schweiz" wurden konkrete Ziele definiert. Eine gute Chance, die ePower-Umsetzung mit ISACA/ITGI-Know-how und Professionalität in IT Governance zu unterstützen.

Dies wiederum ist mit positiven Auswirkungen auf unseren Berufsstand der Informatikrevision verbunden. In diesem ***NewsLetter*** werden sowohl die Notwendigkeit der Aufgaben und Zuständigkeiten, als auch die Aspekte der reibungslosen Zusammenarbeit angesprochen.

Diesbezüglich wurde die Basis der Kontrollmodelle von anerkannten Institutionen weitgehend verbessert. Dies trifft insbesondere auf die neue Edition von CobiT 4.0 (IT-Modell) im Zusammenspiel mit COSO (Business-Modell) zu. Das heisst aber auch, dass die Zusammenarbeit zwischen der internen und externen Revision sowie des Finanz- und Informatik-Revisiors gefördert werden muss.

Trotz der weltweit bekannten Kontrollmodelle bestehen immer noch Mängel bezüglich der ausgewogenen Anwendung. Die steigenden Anforde-

rungen in gesetzlicher, organisatorischer und technischer Hinsicht verlangen eine bessere Zusammenarbeit und Kommunikation von allen Beteiligten (Prüfer und Geprüfte).

Handlungsbedarf besteht im Wesentlichen in der angemessenen und gemeinsamen Umsetzung der angesprochenen Kontrollmodelle. Eine bedeutende Rolle spielen dabei die Kompetenz und Zuständigkeit der folgenden Partner:

- Verwaltungsrat, Geschäftsleitung und Audit-Komitee
- Management (u.a. Risiko, Qualität, Sicherheit, Compliance)
- Interne und Externe Revision (Revisionsgesellschaften)
- Treuhand-Kammer und ISACA/ITGI (IT Governance Institut).

Zur Gewährleistung der Gestaltung und Einhaltung des internen Kontrollsystems (IKS) sowie der dazu notwendigen Ausbildung müsste das Zusammenspiel auf allen Stufen und Ebenen harmonisiert werden.

Um der angestrebten Corporate und IT-Governance gerecht zu werden, ist eine ganzheitliche Sicht in Bezug auf die Kontrollziele und deren Prüfung bzw. Zusammenarbeit dringend notwendig.

In der Vergangenheit befasste man sich bei den Prüfungen hauptsächlich mit dem ***Was*** und ***Warum***. Vermehrt kommt nun die Beurteilung des ***Wie*** d.h. Leistungsmessung (KGI, KPI) und die Wertschöpfung (Value@IT) hinzu.

Die Innovation bei der wachsenden Dienstleistungsbranche sehe ich im Engagement für eine bessere Kooperation und Koordination zwischen der Politik, Wirtschaft, Bildung und den Berufsorganisationen. Dabei ist das Leistungsergebnis die beste Motivation.

Bruno Wiederkehr

Zusammenarbeit Abschlussprüfer/ IT-Revisor

Bedeutung neuen der Schweizer Prüfungsstandards (PS)

Einleitung

Für die Mitglieder der Treuhand-Kammer sind die neuen Schweizer Prüfungsstandards (PS)[1] nun verbindlich. Sie gelten für Abschlüsse, die am 1. Januar 2005 oder später beginnen, betreffen aber nicht alle geprüften Gesellschaften. Die neuen Standards sollen die Qualität der Abschlussprüfungen und der damit verwandten Dienstleistungen erhöhen sowie den Anschluss an die internationale Entwicklung gewährleisten.

1. Beschreibung der PS

Die Prüfungsstandards (PS) behandeln das Wesen, die Grundsätze und die Verfahren der Abschlussprüfung und damit verwandter Dienstleistungen, die im Zusammenhang mit Abschlüssen oder anderen Finanzinformationen erbracht werden. Sie äussern sich zur konkreten Ausgestaltung der Prüfung, wohingegen die gesetzlichen Bestimmungen im Obligationenrecht zur Prüfung nur grundsätzliche Aspekte regeln.

Als Mitglied der International Federation of Accountants (IFAC) hat sich die Treuhand-Kammer verpflichtet, die International Standards on Auditing (ISA)[2] umzusetzen. Die Treuhand-Kammer hat deshalb beschlossen, die ISA als gesamtes Regelwerk zu übernehmen und, falls notwendig und sinnvoll, mit schweizerischen Normen zu ergänzen.

2. Geltungsbereich

Der Geltungsbereich und das Inkrafttreten der PS sind in der Richtlinie zu Abschlussprüfung Nr. 5 (RzA 5)[3] verbindlich festgehalten.

Die neuen PS gelten für Abschlussprüfungen und damit verwandte Dienstleistungen in Bezug auf Abschlussperioden, die am oder nach dem 1. Januar 2005 beginnen. Die im Dezember 2005 von den Räten beschlossene Neuregelung der Abschlussprüfung sieht Erleichterungen vor, sofern bestimmte Grössenkriterien nicht überschritten werden. Vor diesem Hintergrund gelten die PS vorläufig nur für Unternehmen und Organisationen einer gewissen Grösse. Es sind dies Unternehmen, die Anleihensobligationen ausstehend haben, deren Aktien an einer Börse kotiert sind oder zwei Grössenkriterien bezüglich Bilanzsumme (CHF 20 Mio.), Umsatzerlös (CHF 40 Mio.) und Arbeitnehmern (200 im Jahresdurchschnitt) erfüllen. Es ist vorgesehen, die PS für die ordentliche Revision verbindlich zu erklären, während für die eingeschränkte Revision eigene Regeln gelten sollen, welche die Grundsätze zur Abschlussprüfung (GzA) ablösen werden.

Die PS finden auch für sämtliche Unternehmen und Organisationen Anwendung, die dem Bundesgesetz über Banken und Sparkassen, dem Bundesgesetz über die Börsen und den Effektenhandel, dem Bundesgesetz über die Anlagefonds sowie dem Bundesgesetz über die berufliche

Bei der Anwendung der GzA zu berücksichtigende PS	*Durch PS ersetzte GzA*
PS 290 – Pflichten der gesetzlichen Revisionsstelle bei Kapitalverlust und Überschuldung	GzA 15 – Verhalten der Revisionsstelle bei Kapitalverlust und Überschuldung
PS 570 – Unternehmensfortführung (Going Concern)	GzA 13 – Fortführung der Unternehmenstätigkeit (Going Concern)
PS 700 – Bericht des Abschlussprüfers	GzA 17 – Bericht der Revisionsstelle und des Konzernprüfers
PS 910 – Review (prüferische Durchsicht) von Abschlüssen	GzA 20 – Review (prüferische Durchsicht)

Alters-, Hinterlassenen- und Invalidenvorsorge unterstehen. Bei allen anderen Organisationen behalten die GzA grundsätzlich ihre Gültigkeit. Jedoch für zentrale Bereiche der Wirtschaftsprüfung werden einzelne GzA durch die entsprechenden Prüfungsstandards ersetzt. Damit wird für wichtige Bereiche eine einheitliche Berufsausübung gewährleistet.

Die nun vorliegenden PS umfassen sämtliche am 30. Juni 2003 publizierten ISA. Der International Auditing and Assurance Standards Board (IAASB) hat in der Zwischenzeit eine umfassende Überarbeitung seiner Standards eingeleitet und seine Verlautbarungen neu systematisiert. Dies führt dazu, dass die vorliegenden PS und die ISA in ihrer Gesamtheit während einer Übergangsphase nicht vollständig deckungsgleich sind.

3. Wichtige Neuerungen

Mit dem Inkrafttreten der PS werden zahlreiche Lücken der GzA geschlossen. Die Tabelle gibt Aufschluss über die Gebiete der Abschlussprüfung und damit verwandter Dienstleistungen, die bis jetzt in den GzA nicht geregelt waren.

Nachstehend wird auf einen Aspekt der neuen PS eingegangen, der für den Informatikprüfer von besonderem Interesse ist.

4. Prüfung im Umfeld der Informations- und Kommunikationstechnologie

Der Prüfer muss sich Kenntnisse der Tätigkeit und des Umfelds des zu prüfenden Unternehmens machen (PS 310). Von besonderem Interesse ist PS 401 „Prüfung im Umfeld der Informations- und Kommunikationstechnologie“, welcher Anleitungen zur Prüfung im Umfeld von Systemen der Informations- und Kommunikationstechnologie (fortan: ICT) gibt. Für den Prüfer werden dadurch vor allem folgende Bereiche beeinflusst: Beurteilung des Rechnungswesen-

PS	*Thema*
PS 120	Konzeptioneller Rahmen der PS
PS 250	Gesetzliche und andere Vorschriften – Berücksichtigung bei der Abschlussprüfung
PS 260	Kommunikation über die Abschlussprüfung mit den Verantwortlichen für die Leitung und Überwachung
PS 300	Planung
PS 310	Kenntnisse der Tätigkeit und des Umfelds des Unternehmens
PS 320	Wesentlichkeit bei der Abschlussprüfung
PS 401	Prüfung im Umfeld der Informations- und Kommunikationstechnologie
PS 500	Prüfungsnachweise
PS 501	Prüfungsnachweise – Zusätzliche Überlegungen zu bestimmten Positionen
PS 510	Erstprüfungen – Eröffnungsbestände
PS 520	Analytische Prüfungshandlungen
PS 530	Stichproben- und andere Auswahlverfahren bei der Abschlussprüfung
PS 540	Prüfung von Schätzungen im Abschluss
PS 545	Prüfung von Fair Values (Bewertungen und Angaben)
PS 550	Nahe stehende Parteien
PS 710	Vergleichsinformationen
PS 720	Andere Informationen in Dokumenten, die den geprüften Abschluss enthalten
PS 800	Berichte über Spezialprüfungen
PS 810	Prüfung zukunftorientierter Finanzinformationen
PS 920	Vereinbarte Prüfungshandlungen bezüglich Finanzinformationen
PS 930	Erstellung von Finanzinformationen (Compilation)

Systems, der internen Kontrolle und der Risikolage sowie Planung und Durchführung der Prüfungshandlungen.

Von einem ICT-Umfeld ist im Sinne der PS die Rede, wenn ein ICT-System, gleich welcher Art oder Grösse, bei der Verarbeitung wesentlicher Finanzinformationen durch das Unternehmen eingesetzt wird. Dabei spielt es keine Rolle, ob das System vom Unternehmen selber oder von einem Dritten betrieben wird.

Will der Prüfer einen wirkungsvollen Prüfungsansatz entwickeln, muss er bei ICT-Anwendungen, die für das Rechnungswesen relevant sind, Bedeutung und Komplexität der ICT-gestützten Verarbeitungsprozesse verstehen, aber ebenso das ICT-Umfeld, samt der in den Prozessen und im Umfeld enthaltenen Risiken. Dem finanziell orientierten Abschlussprüfer fehlt möglicherweise die notwendige Sachkenntnis oder Ressourcen im ICT-Bereich. Um den Auswirkungen beizukommen, hat der Prüfer nötigenfalls einen IT-Spezialisten (CISA, CISM) oder externen Experten ins Prüferteam aufzunehmen, der ihn von der Planung bis zur Berichterstattung fachtechnisch unterstützen kann.

Die spezifischen Prüfungsziele hängen dabei nicht davon ab, ob Daten manuell oder ICT-gestützt verarbeitet werden. Trotzdem verlangt die Prüfungseffizienz, den Grad der ICT-Verarbeitung zu berücksichtigen. Bei manchen Anwendungen kann es für den Prüfer schwierig oder gar unmöglich sein, relevante Informationen zu erlangen, ohne selber mit Computerunterstützung (Computer-assisted audit techniques, CAAT) vorzugehen.

5. Ausblick

Durch die Nutzung von ICT Anwendungen durch die zu prüfenden Kunden sind die Anforderungen an den Abschlussprüfer die Jahresrechnung als Ganzes oder besondere Bestandteile zu beurteilen immer komplexer. Der Informatikprüfer kann mit seinem Spezialwissen in technischen und organisatorischen Belangen wertvolle Unterstützung und Hinweise liefern.

Deshalb ist die Einbindung ins Prüfteam weiterhin von Bedeutung und wird zur Sicherstellung der Qualität einer ordnungsgemässen Prüfung künftig weiter zunehmen.

Hanspeter Plozza, PWC, Basel

Endnoten

[1] Schweizer Prüfungsstandards (PS), Treuhand-Kammer, Zürich 2004 (auch abrufbar von www.treuhand-kammer.ch)

[2] Handbook of International Auditing, Assurance, and Ethics Pronouncements, International Federation of Accountants, New York 2005

[3] Richtlinie zur Abschlussprüfung Nr. 5 (RzA 5): Übergang von den Grundsätzen zur Abschlussprüfung (GzA) zu den Schweizer Prüfungsstandards (PS), Treuhand-Kammer, Zürich 2004 (auch abrufbar von www.treuhand-kammer.ch)

ISACA Serving IT Governance Professionals Switzerland Chapter
www.isaca.ch

Drei spannende Kurse!

ITIL Foundation mit Apollo 13
inkl. int. Zertifizierung
1. - 3 März 2006 in Zürich

ITIL Foundation Training
Service Management auf der Basis des de-facto Standards ITIL
7. - 9. Juni 2006 in Zürich

BS 15000 Consultant & Internal Auditor
Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung
12. - 14. Juni 2006 in Zürich

Weitere Informationen erhalten Sie in unserem Kurssekretariat:

ISACA Switzerland Chapter
c/o ITACS Training AG, Stampfenbachstr. 40
8006 Zürich, Schweiz, kurse@isaca.ch,
Tel. 044 444 11 01, Fax 044 444 11 02, www.isaca.ch

ISACA®
Serving IT Governance Professionals
Switzerland Chapter

Zusammenarbeit Abschlussprüfer/ IT-Revisor

Processus informatiques et audit financier, une interaction de plus en plus importante

Aujourd'hui, la plupart des sociétés ont informatisé leurs principaux processus; ceux liés à l'information financière ne font pas exception à cette règle. Cette automatisation a permis une forte augmentation du volume d'informations traitées, mais a également considérablement augmenté la complexité et, par conséquent, la maîtrise des processus financiers.

La pertinence et la fiabilité de l'information utilisée pour l'élaboration des états financiers dépendent donc directement de la qualité du processus informatisé sous-jacent.

Conscients de cette réalité, les professionnels de l'audit fixent au travers de normes et de standards nationaux ou internationaux en perpétuelle évolution un cadre d'exigence qui inclut la dimension informatique comme un élément indispensable de la réflexion. Nous pouvons relever, à titre d'exemple, la Norme d'audit suisse (NAS) 401 ***Audit réalisé dans un environnement informatique***, qui fixe à l'auditeur les « règles à suivre lorsqu'un audit est réalisé dans un environnement IT ». Cette norme exige également de l'auditeur « qu'il acquiert une connaissance suffisante des systèmes comptables et de contrôle interne pour planifier l'audit et concevoir une approche d'audit efficace ».

Bref historique

Avec l'émergence de l'informatique, les auditeurs financiers ont rapidement fait appel à du personnel spécifique pour apprécier l'organisation informatique des sociétés auditées. Ces spécialistes IT ont pu, grâce notamment à un standard comme le CobiT®, apprécier et communiquer sur les risques liés à l'environnement de contrôle informatique.

Dès lors, des problèmes de compréhension mutuelle sont naturellement apparus, avec des perspectives et un langage différents, les comptables et les techniciens ne se comprenaient pas toujours. Progressivement, ce fossé culturel a été comblé, phénomène rendu obligatoire par la complexité toujours plus grande des entreprises modernes (groupes internationaux, multiplicité des reportings, réduction des délais de traitement, etc.)

Un exemple de synergie est l'utilisation des compétences techniques dans le traitement des données de masse. Les auditeurs financiers ont vite su utiliser les compétences disponibles pour effectuer des contrôles systématiques sur des volumes importants de données ou de transactions. La réussite dans ce domaine est telle que dorénavant, ils disposent d'un outil et de formations appropriées pour effectuer eux-mêmes les traitements.

Evolution de la relation

Avec le temps, les attentes envers les spécialistes IT se sont intensifiées. Leurs connaissances et leurs compétences ne sont plus simplement utiles mais nécessaires à chaque étape d'un audit financier.

Dans la phase de ***préparation d'un audit*** (notamment lors de la collecte de l'information et de l'appréhension des cycles d'activités), il est nécessaire pour l'auditeur de pouvoir s'imprégner rapidement du fonctionnement des processus, pas uniquement en terme de métier de l'entreprise mais également en terme de fonctionnement propre. Dans ce contexte, l'auditeur informatique est également sollicité pour sa compréhension de la fonction informatique.

Lors de la ***planification stratégique de l'audit,*** le spécialiste informatique aide l'auditeur financier à identifier les risques dans les processus d'élaboration des états financiers. Par exemple, seul un auditeur possédant des compétences informatiques sera à même d'identifier des interfaces entre des applications et de mesurer l'impact que pourrait avoir ces interfaces (transfert d'informations sur des technologies ou plateformes différentes) sur la planification de l'audit.

Dans cette phase, l'expert IT devra également documenter et apprécier la fonction informatique dans son ensemble. Les points relevés dans son analyse devront être appréciés selon 2 axes :

1. Non-conformité avec un ou plusieurs standards de la profession ayant un impact sur l'étendue des travaux des auditeurs financiers ;
2. Amélioration potentielle de la fonction informatique pour la faire tendre vers les meilleures pratiques du secteur.

Le spécialiste IT doit dès lors identifier en premier lieu les faiblesses ayant un impact significatif pour l'auditeur financier, celles-ci ayant une influence sur la stratégie d'audit et, potentiellement, sur la quantité de travaux nécessaires.

L'audit informatique prend de plus en plus d'importance lors de la ***documentation et de l'appréciation des contrôles.*** En effet, il est encore parfois difficile pour des auditeurs purement financiers de pouvoir rapidement, sur base des risques relevés, d'identifier tous les contrôles clés au sein de l'organisation et d'en apprécier la pertinence (design) et l'existence (implémentation). En effet, de plus en plus de contrôles sont directement liés à des traitements informatiques ou découlent de ceux-ci.

Dans la phase d'***exécution de l'audit***, les auditeurs informatiques seront également sollicités pour tester l'efficacité opérationnelle des contrôles, qu'ils soient informatisés ou non. Par exemple, certains contrôles-clés ne pourront être appréciés uniquement au travers d'un test de « re-performance » d'un échantillon pour valider le contrôle. Ils peuvent également apporter leur support technique pour effectuer des extractions des systèmes d'informations qui serviront notamment à la sélection d'échantillons statistiques pour les tests d'implémentation.

Au-delà de simples extractions, directement exploitables par les auditeurs, les spécialistes IT sont de plus en plus sollicités pour effectuer des extractions complexes et produire ainsi des informations spécifiques après de multiples traitements.

Développement actuel

La complexité toujours grandissante des produits et des services proposés par nos clients, nous a naturellement conduits vers une nouvelle définition des rôles de chacun au sein de l'équipe d'audit.

La répartition des tâches de documentation des processus par spécialisation technique entre les auditeurs financiers et informatiques ne correspond plus au mode de fonctionnement actuel des entreprises. Les équipes d'audit sont principalement composées sur la base d'une approche métier de l'entreprise. Indépendamment de la formation ou de la spécialisation originelle des auditeurs, le développement d'une expertise s'effectue au profit d'une connaissance des métiers et des processus de nos clients. C'est à travers cette approche que nous pouvons assurer une évaluation pertinente des risques de nos clients.

Figure 1 : Synthèse de l'évaluation des risques sur la planification d'audit

En conclusion

Nous mesurons mieux à présent l'évolution des attentes des auditeurs financiers envers leurs collègues informaticiens. Le spécialiste IT a pris une place de plus en plus prépondérante dans les audits financiers. C'est ce judicieux équilibre qui permettra aux professionnels de l'audit de répondre aux exigences réglementaires de la profession et aux attentes de leurs clients.

Alexandre Buga, ESSEC, Certified Public Accountant, Partner Audit, Deloitte SA, Genève

Nicolas Heiniger, licence HEC Lausanne, expert-comptable diplômé, Manager Audit, Deloitte SA, Genève

ISACA®
Serving IT Governance Professionals
Switzerland Chapter

Zusammenarbeit Abschlussprüfer/ IT-Revisor

Zusammenarbeit zwischen Abschluss-prüfer und Informatikrevisor

Historie und Positionierung

Nach wie vor ist das Gedankengut der schweizerischen Pioniere der IT-Revision gültig und Massstab auch für die heutige Arbeit der IT-Revisoren. Die Checklisten der Schweizerischen Treuhand-Kammer (TK) und weitere Standardwerke gaben damals Antwort auf die Frage wo und wie sich die Zusammenarbeit zwischen IT-Revision und Fachrevision entwickeln sollte. Man sprach damals noch von „applikationsabhängiger und -unabhängiger EDV-Revision". Man sprach also fast nur davon, was man prüfen müsse. Das Warum trat unverdienterweise in den Hintergrund, obwohl die damaligen Autoren immer und eindeutig davon gesprochen haben.

Letztlich will (und wollte) der Abschlussprüfer seit jeher wissen, ob er sich auf das Zahlenmaterial verlassen kann. Ganz einfache Fragen stellen sich: Werden die Informationen effizient und effektiv aufbereitet? Ist die Vertraulichkeit geregelt? Sind die Daten integer? Haben die Fachabteilungen die nötigen Daten zur Verfügung? Entsprechen diese Gesetz und Regelungen? Kann man sich auf die Daten abstützen?

Kommt Ihnen das bekannt vor? O ja! CobiT hat ca. 1996 zum ersten Mal formuliert, was der Abschlussprüfer von uns IT-Revisoren erwarten kann. Eine Aussage nämlich auf die oben gestellten Fragen! Wenn der Abschlussprüfer die Sache noch ein bisschen genauer angeht, könnte er seine Fragen ganz genau stellen. Zum Beispiel:

- Werden die Versicherungsleistungen in der korrekten Höhe, dem richtigen Empfänger zur richtigen Zeit ausbezahlt?
- Ist sichergestellt, dass alle Konten in die jeweils vorgesehene Bilanzposition fliessen werden?
- Können Zahlungen doppelt ausgelöst werden?
- Erfolgen die Bestandesbewertungen zum vorgesehenen Kurs und sind die Berechungen korrekt?
- Kann eine Buchung die Jahresrechnung wesentlich verfälschen?
- Ist das Projekt zu teuer bzw. gefährdet das Projekt die Fortführung des Unternehmens?
- Wird das IKS von der Informatik gestützt oder gar unterlaufen?
- Ist die Firma wegen nicht sachgemässem Informatikbetrieb gefährdet? (Sicherheit, Physisches, Verfügbarkeit, etc.)
- Stellt das Archivierungskonzept die Einhaltung von Aufbewahrungsvorschriften sicher?
- Ist das Personal in der Lage, die IT-Probleme zu lösen?
- Erfolgt der tägliche Betrieb der Informatik nach den Regeln der Kunst?
- Etc.

Erkennen Sie, dass nach wie vor die zentrale Frage des Abschlussprüfers nach Prüfungssicherheit im Raum steht? Er möchte schlicht und einfach Gewissheit, dass seine Arbeit ein gutes und sicheres Fundament hat. Nicht mehr und nicht weniger! Genau daran hatte und hat sich unsere Arbeit zu orientieren.

Situation heute

Mit Fug und Recht darf heute, nach vielen Jahren IT-Revision, von einer gewissen Ernüchterung gesprochen werden. Ich möchte dies anhand von drei – persönlichen – Feststellungen erläutern:

Die IT-Revision hat die Erwartungen nicht erfüllt

Etwas ketzerisch behaupte ich, wir IT-Revisoren hätten den Abschlussprüfern nur in der Minderheit aller Prüfungen wirkliche Antworten auf obige Fragen geliefert. Dies lag zum Teil daran, dass wir IT Revisoren schlicht und einfach keine Ahnung vom Geschäft hatten! Und schlimmer noch, die Auswirkungen auf das Geschäft wegen einer „schlechten" Informatik konnten wir gar nicht formulieren, weil uns der Blick auf das Geschäft von unserem Technologie-Know-how verstellt wurde.

Die Abschlussprüfer sind heute noch nicht in der Lage, adäquate Fragen zu stellen und zweckmässige Resultate einzufordern

Ach, wie gut kennen wir den so genannten „T.S.L. Auftrag". „Tüend Sie luege, ob…"! Wie oft hätten wir uns präzise Aufträge gewünscht und wie oft waren wir frustriert, weil sich niemand für die Erkenntnisse des IT-Revisors interessierte. Mit einem mitunter überraschenden Selbstbewusstsein (oder Naivität) wurde auf IT-Revision verzichtet oder wurde nicht zielgerichtete Arbeit akzeptiert.

Die „Ränder" der EDV-Revision fransen zunehmend aus

Betreffend Anwendungs-Know-how, z.B. in Sachen SAP, erhalten wir IT-Revisoren zunehmend „Konkurrenz"

von Abschlussprüfern, die das Metier der Anwendungsprüfung so gut verstehen wie wir selbst. Ferner können einfache Fragen betreffend Infrastruktur (Sicherheit, Notfall, Wartung, etc.) von einem gut ausgebildeten Revisionsassistenten ebenso gut beantwortet werden wie von einem IT-Revisor. Und: jede Informatikfrage hat einen Bezug zum Geschäft und niemals nur zu Technologie. In jedem Projekt ist dies klar zu sehen.

Ausblick

Wir jammern auf hohem Niveau

In der Zusammenarbeit zwischen Abschlussprüfer und IT-Revisor ist viel erreicht worden. Die Aufgeregtheit hat sich gelegt, Versuche wurden gemacht und sind gescheitert, der Blick auf Neues wird frei. Mit CobiT haben wir zudem ein Prüfungshandbuch mit dem sich in der Tat arbeiten lässt. Der Status quo ist ansprechend. Aber es wird Zeit, die nächsten Schritte anzugehen.

Ausbildung und Spezialisierung

Als erstes sind zwei Pfeiler der IT-Revision zu verstärken: ***Ausbildung und Spezialisierung.***

Die ***Ausbildung*** der IT-Revisoren soll so gestaltet werden, dass nebst einem fundierten IT-Know-how und Revisionswissen auch ein gehöriges Mass an Managementkompetenz und betriebswirtschaftlichem Wissen verfügbar ist. Vorstellbar sind Lehrgänge mit dieser Ausrichtung in Form von Nachdiplomstudien, wo die CISA-Ausbildung und das Diplom selbstverständlich „mitgenommen" wird. Wer weiss, vielleicht gibt es wieder mal, wie in früheren Zeiten, einen dipl. Wirtschaftsprüfer mit Spezialisierung auf IT Revision… CISA allein genügt nicht!

Die ***Spezialisierung*** sollte massiv vertieft werden. In groben Zügen schlage ich einerseits eine Ausrichtung auf Anwendungsprüfung (Softwarekonzepte, Lösungskonzepte) und andererseits eine Spezialisierung auf Technologieprüfung (Sicherheit, Infrastruktur, IT-Betrieb, Netzwerke, etc.) vor. Beide Spezialisierungen haben Überschneidungen, bieten aber je für sich genug Stoff für ein spezielles Nachdiplomstudium.

Damit wäre sichergestellt, dass wir IT-Revisoren im ganzen „Rösslispiel" der Revision und Wirtschaftsprüfung wirklich mitreden könnten. Wir wären ***wirklich*** in der Lage perfekte Arbeit zu liefern und – ganz wichtig – Aufmerksamkeit zu ***fordern***.

Planung und Management

Als zweites und zentrales Element der Zusammenarbeit sind die Planung und das Management der Mandate zu verbessern! Jede und jeder von uns hat diesbezüglich leidvolle Erfahrung. Schlechte Planung, unzureichende Absprachen zwischen IT-Revision und Abschlussprüfer, unbefriedigende Prüfungsergebnisse, ignorieren von Prüfungsergebnissen durch den Abschlussprüfer, unzureichende Arbeitspapiere, unrealistische Budgetvorgaben, etc. dürfen einfach nicht mehr hingenommen werden. Und zwar sowohl vom IT-Revisor als auch vom Abschlussprüfer!

Partnerschaft

Abschlussprüfung und IT-Revision gehören zusammen wie Bahn und Schiene, Skis und Schnee, Schiff und See. Die Zukunft ist nur möglich, wenn nicht mehr in „Hüben" und „Drüben" unterschieden wird. Besonders gut lässt sich diese Partnerschaft in der internen Revision leben. In der externen Revision wird der Entwicklungsprozess noch länger dauern und die Bedeutung der IT-Revision wird sich zugunsten der internen IT-Revision verschieben.

Interne Revision, externe Revision (Abschlussprüfer)

Traditionellerweise beschäftigt sich die interne Revision mit dem internen Kontrollsystem der Firma, mit den Verfahren und mit der Governance. Die externe Revision konzentriert sich auf die Abschlussprüfung, die Finanzrevision. Diese Arbeitsteilung wird sich akzentuieren, wobei die externe Revision die Arbeit der internen Revision beurteilt. Es liegt auf der Hand, dass sich die externe Revision auf die Arbeit der internen Revision, insbesondere betreffend Verfahren und IT-Revision abstützen wird.

Ueli Engler, Leiter IT Revision, Swiss Life, Zürich

Zusammenarbeit Abschlussprüfer/ IT-Revisor

Are We Just Below the Summit?

It has been an up-hill-battle all the way.

The first time I was called by an auditor in order to explain and help when he faced a computer was in 1968. As a former audit assistant and now programmer I was proud to be of use. I concluded that a new area had dawned and I was eager to help build this „new" profession ***EDP Audit***. I set out to develop courses for auditors and tried to teach them bits and bytes. My expectations were considerable, and I saw myself flooded by audit requests.

The disillusion set in pretty fast. As soon as conventional auditors were faced with the news that EDP auditing would not be an additional sale for them, but in the contrary might reduce their work, they started to fear that their jobs were in jeopardy. They probably realized that they were in a wrong movie and turned their backs to me. It took me some time to realize that missionary work was necessary. I had to sell my creed as the hostility I started to face was cannibalistic.

OK, more education and convincing was necessary. As generalized audit software (GAS) emerged, I embarked on a few experiments with the new tool. I offered to do some file analyses for free as „additional" audit service. One or two elderly auditors caught on (because it was „for free" and they hoped to get some „free" education – this was before the invention of continued education credits – on the side). We were quite successful in finding double payments and lost rebates in the accounts payable files. The auditors were at the same time enthused and angry. Enthused because they were able to tell their clients that they would have to improve their internal control system and their programs. Angry because they had not found out themselves over the last years. The result was that those „brave" auditors started to turn their back an us EDP auditors as well. It was the time when I was contemplating to shoot a few conventional auditors if they would not die a natural death pretty soon.

In the meantime a new generation of auditors was coming into view. Some of them had experienced the forerunners of Nintendo games in school. Computers no longer were a complete mystery to them. They therefore concluded that they would not need EDP auditors, either, because they knew all about „it". Unfortunately they were not educated as far as the intricacies of EDP was concerned. They failed to put the new tool into proper perspective. Above all, they were constantly looking for EDP deficiencies instead of realizing its benefits as well. Especially as far as the use in audit work was concerned. On the other hand they did not take into account that a new age had begun: The agricultural society had been replaced by the industrial one in the eighteenth century; the latter by the service economy in the middle of the nineteenth (as Fourastié had correctly formulated). But now, the complementary information society came into being. The qualities that go with it (benefits as well as dangers) were – and in some instances still are – not recognized.

One of the first disasters probably was the Equity Funding scandal, where millions of dollars had been lost due to computer fraud by employees (introducing fake policies in the files of insurance companies). Quite a few foreclosures followed due to lack of security measures, fraudulent bookkeeper, hackers, etc. I am pretty much convinced that the scandals of Parmalat, Worldcom, Enron, etc. would not have occurred as easily without computers. And probably not without proper EDP audit, and especially not without proper collaboration between conventional and IT auditors.

Whose fault is it? Is it just the conventional financial auditor? Most certainly not. We IT-auditors failed to a considerable degree to sell our services in a way that was convincing enough for the potential „buyer". Moreover, we too often tried to keep our accomplishments a secret, or insisting that our merits be respected in order to let the financial auditors decorate themselves with „our" laurels. The word collaboration implies a mutual understanding and consent. But who takes the first step? Maybe we should have done so more often than we did.

With the new audit standards (PS 240, 402, 620, etc – ISA 240, 401, 620 etc), a formal basis for such a fruitful collaboration has been set. However, those words remain dead literature if they are not followed in every-day life.

Let us make renewed effort. Even though the way to the top has been

uphill and full of thorns and setbacks, the summit cannot be to far away.

Max F. Bretscher,
Langnau a/A

CobiT

Erfüllt CobiT 4.0 die Erwartungen des PCAOB?

Ja, aber… ! CobiT 4.0 ist und bleibt das beste Instrument, um die IT-Kontrollen zu gestalten und zu revidieren. Schlecht eingesetzt kann aber CobiT zu überdimensionierten Audits führen. Die Anwendungskontrollen müssen zusätzlich und ohne CobiT behandelt werden.

Die Prüfung des Internen Kontrollsystems (IKS) hat wieder an Bedeutung gewonnen. Und es ist gut so. Die Umsetzung der Regeln des PCAOB[1], dem mit der Einhaltung des Sarbanes-Oxley-Gesetz (SOX) betrauten Aufsichtsorgan der amerikanischen Börse, zeigt allerdings, dass hinsichtlich des Einbezugs der Informatikrevision ins IKS noch viele Fragen offen sind. Es wäre falsch zu glauben, diese Fragen beträfen nur eine kleine Minderheit von in den USA börsenkotierten Schweizer Unternehmen. In Zukunft werden ***alle*** Unternehmen den Informatikrisiken und ihrer angemessenen Berücksichtigung im IKS vermehrt Beachtung schenken müssen; entweder weil neue europäische Richtlinien oder neue Bestimmungen im Obligationenrecht dies verlangen oder einfach, weil ihre Kreditinstitute entsprechenden Druck auf sie ausüben werden.

Es empfiehlt sich, sich in dieser Diskussion an die Typologie zu halten, die im Prüfungsstandard Nr. 2[2] des PCAOB angewendet wurde. Dort ist

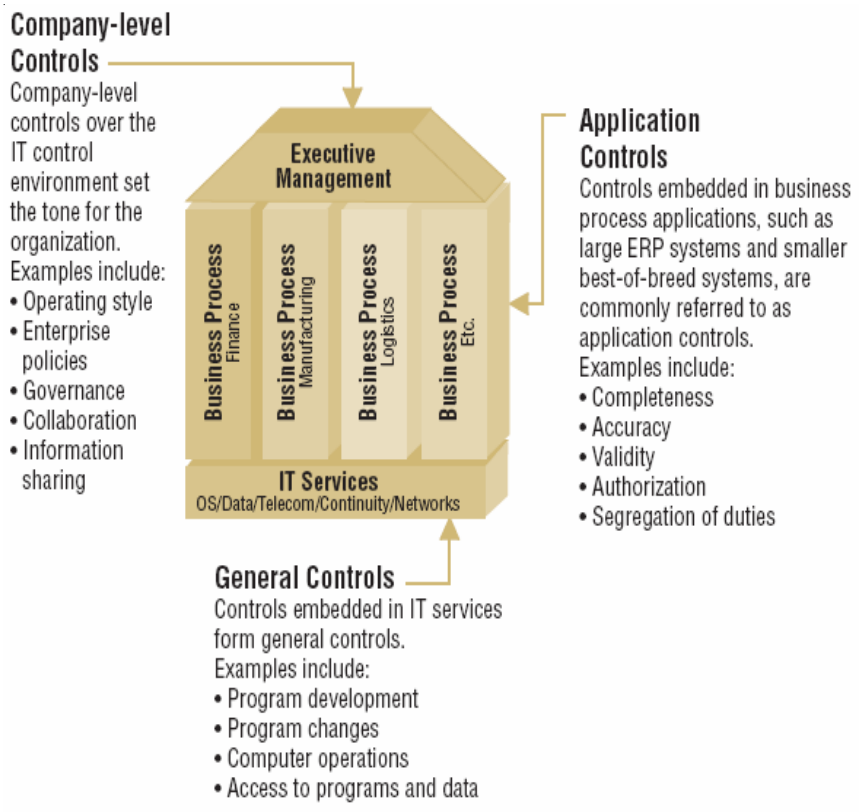


Abbildung 1: Die verschiedene Kontrolltypen gemäss der PCAOB-Terminologie

die folgende Unterscheidung zu lesen:

- allgemeine Kontrollen auf Stufe Unternehmen (***company***- oder ***entity-level controls***);
- Anwendungskontrollen (***application controls***) und
- allgemeine IT-Kontrollen (***IT general controls***).

Abbildung 1[3] zeigt, dass nur die zweitgenannte Kategorie direkt von den Geschäftsprozessen im Unternehmen abhängt.

Die Publikation der Version 4.0 von CobiT im Dezember 2005[4] bot Gelegenheit für einige Anpassungen (siehe Abb. 2) sowie für eine systematische Angleichung dieses Bezugssystems an die Vorschriften des PCAOB.

Sowohl die Europäische Kommission[5] als auch das Institute of Internal Auditors (IIA) bestätigen es: CobiT ist derzeit ***das*** Standardwerk, wenn es bei der Umsetzung europäischer Richtlinien oder im Rahmen des SOX-Ansatzes um die Einhaltung der IT Governance geht.

Dabei sind aber unbedingt folgende drei Regeln einzuhalten:

1. Direkte Integration der Informatik in die gesamte Analyse der Kontrollen auf Stufe Unternehmen (company- oder entity-level controls)

Um wirksam zu sein, müssen die Kontrollen auf Stufe Unternehmen umfassend sein. Die Kontrollsysteme müssen unbedingt ganzheitlich konzipiert sein:

- Sie müssen z.B. eine Risikoanalyse enthalten, die alle im Unternehmen existierenden Risiken umfasst, einschliesslich desjenigen von Informatikpannen.

CobiT 3	***CobiT 4.0***
Management Guidelines und Kontrollziele sind in zwei separaten Dokumenten enthalten.	Kontrollziele, Maturitätsmodelle (Reifegrade) sowie Erfolgsfaktoren und Erfolgsindikatoren für jeden der 34 IT-Prozesse sind in einem einzigen Dokument enthalten.
Die Prozesse AU5 «Sicherstellen der Systemsicherheit» und AU11 «Verwaltung der Daten» enthalten einige Anwendungskontrollen.	Aus den ehemaligen Prozessen AU5 und AU11 wurden 18 Anwendungskontrollen ausgewählt und von AC1 bis AC18 durchnummeriert. Sie werden nur in der Einleitung zu C***obi***T kurz beschrieben und in der Folge nicht mehr aufgegriffen (Abb. 3).
Der Prozess PO04 befasst sich mit der allgemeinen Definition der IT-Organisation.	Der neue Prozess PO04 setzt sich eingehend mit dem Thema des «Eigentums» an den Informatikanwendungen und den elektronischen Daten auseinander. C***obi***T beschränkt sich für jeden der 34 IT-Prozesse nicht mehr nur auf die EDV-Abteilung, sondern definiert unter Zuhilfenahme eines RACI-Modells (***who is Responsible, Accountable, Consulted and/or Informed***) die Rollen im ganzen Unternehmen.
Die 34 Prozesse stehen gleichrangig nebeneinander. Wie sie miteinander verknüpft sind, wird nicht explizit dargelegt.	C***obi***T 4.0 verdeutlicht die Kontinuität zwischen allen Prozessen, indem es darauf hinweist, dass z.B. ein Bericht über die Kosten einer Anwendung, der im Rahmen des Prozesses PO5 (Management der IT-Investitionen) erstellt wird, zur Beschaffung einer neuen Anwendungssoftware (Prozess BE2) führen kann, welche ihrerseits eine Anpassung des Sicherheitskonzepts (Prozess AU5) erforderlich macht.

Abbildung 2: Einige wichtige Neuerungen beim Übergang zu CobiT 4.0

- Die Regeln der Berufsethik müssen sowohl Korruptionsbekämpfung als auch ein Verbot des Zugriffs auf Pädophilen-Websites einschliessen.
- Die Kompetenzaufteilung muss sowohl den Abschluss von Verträgen als auch die Verantwortung für Daten und Anwendungen regeln.
- Die Überwachung der Sicherheit im Unternehmen muss sowohl den Kundenreklamationen Beachtung schenken, als auch Eindringungsversuche in einen Informatikserver aufdecken, usw.

Mehrere Prozesse der CobiT-Bereiche Planung und Organisation (PO) sowie Überwachung (ME) behandeln diese Art von Kontrollen bereits aufs Beste.

Die Prüfungshandlungen können sich auf oberflächliche Reviews, auf Selbstevaluationen, Interviews und das Sichten von Dokumenten beruhende Prüfungen beschränken. Der Abschlussprüfer muss aber einigen wesentlichen Fragen auf den Grund gehen; unter anderem der Frage nach der Definition des Eigentums an

einer Anwendung. Diese Frage verdient es, an dieser Stelle eingehend erörtert zu werden.

In einem älteren Artikel (Der Treuhänder 2004/10) wurde bereits darauf hingewiesen: Die vollständige Kontrolle über die Informatik setzt voraus, dass die Anwender ihre Verantwortung kennen und sie auch wahrnehmen. Die Anwender (Auftraggeber) sind die Eigentümer der elektronischen Daten und der Anwendungen, mit denen diese Daten bearbeitet werden. In ihrer Eigenschaft als Eigentümer sollten sie jede Änderung an ihrer Software vorgängig gutheissen, z.B. mit Hilfe geeigneter Tests. An zwei Beispielen lässt sich aufzeigen, dass die technologische Entwicklung diese Aufgabenteilung leider eher verkomplizieren wird:

a) EAI/SOA

Die beiden Integrationswege „EAI, Enterprise Application Integration" oder „SOA, Service oriented Architecture" (serviceorientierte Systemarchitektur) weisen den gleichen Mangel auf. In der lobenswerten Absicht, die Schnittstelle bzw. die IT-Abläufe zu vereinfachen und effizienter zu gestalten, wurden bestehende Schranken zwischen den Anwendungen aufgehoben. Identische Aufgaben, die in mehreren Anwendungen vorkommen, z.B. Routinearbeiten wie Zinsberechnung, Erstellen und Ausdrucken von Rechnungen, oder ganz einfach die Übermittlung von Daten zwischen verschiedenen Computerprogrammen, werden aus den Anwendungen herausgelöst und in einen gemeinsamen Raum gestellt, zu dem alle Anwendungen Zugriff haben (im EAI-Ansatz Middleware genannt). Diese Lösung bietet hinsichtlich des Unterhalts zweifellos grosse Vorteile. Als problematisch erweist sich jedoch in der Praxis das „Eigentum" an dieser Middleware. Eine Änderung der Routinearbeiten müsste nämlich im Prinzip in allen betroffenen Anwendungen getestet und vorgängig von desen Anwendungsverantwortlichen formell abgesegnet werden. Dieser Anspruch ist weder technisch noch organisatorisch leicht einzulösen (zum einen ist es schwierig, eine Testumgebung zu simulieren, zum andern bereitet auch die Bildung einer vernünftigen Vertretung von Anwendungsvertretern Mühe).

b) Patch Management[6]

Der Einsatz von Standardsoftware bringt dem Unternehmen zweifellos auch einen Effizienzgewinn. Die Praxis zeigt jedoch, dass die auf den Markt gebrachten Versionen noch zahlreiche Fehler aufweisen, die nachträglich mit Hilfe von Programmen korrigiert werden, die der Lieferant zur Verfügung stellt (so genannte Patches). Problematisch ist auch hier, dass die Anwender nicht ohne weiteres zu Unterhaltsarbeiten beigezogen werden können. Angesichts der Schwierigkeit, im grossen Massstab Tests durchzuführen, werden diese Patches oft übernommen, ohne dass die Anwender sich dessen überhaupt bewusst sind. Die Informatiker neigen dazu zu glauben, diese Vorgänge seien völlig risikolos und hätten keinen Einfluss auf die Verfügbarkeit oder das reibungslose Funktionieren der Anwendungen. In 99 Prozent der Fälle trifft dies wahrscheinlich auch zu, doch die Praxis hat auch gezeigt, dass in den wenigen Fällen, in denen diese Arbeiten eine Panne nach sich zogen, diese für das Unternehmen dramatisch sein konnte. Daher die Empfehlung, die Patches vor dem Herunterladen zu testen, sie nicht gerade in der hektischsten Zeit zu laden, in den ersten Stunden oder Tagen ein strenges Monitoring durchzuführen und auf jeden Fall die Anwender auf das erhöhte Risiko aufmerksam zu machen.

Diese Beispiele liefern den Beweis dafür, dass der Abschlussprüfer gut beraten ist, eingehend zu untersuchen, ob das Unternehmen die erforderlichen Massnahmen ergriffen hat, die es erlauben, die Prüfziele nach CobiT PO4.6 bis 4.9 zu erreichen. Er sollte sich insbesondere damit befassen, wem die Verantwortung für Qualitätssicherung und Risikomanagement sowie für Daten und Systeme übertragen wurde.

2. Die Geschäftsprozesse verstehen und die notwendige Anwendungskontrollen (application controls) identifizieren

Es ist wichtig zu wissen, dass die Anwendungskontrollen in CobiT 4.0 erwähnt werden (siehe Abb. 3), jedoch nicht in die 34 grundlegenden IT-Prozesse integriert sind. Diese Kontrollen unterstehen den Geschäftsprozessen. Deswegen sind sie weder in den Kontrollzielen, noch in den Management Guidelines enthalten.

„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."

Sie müssen unbedingt einem Verfahren unterzogen werden, das auf die Ermittlung der prozessbedingten Risiken ausgerichtet ist. Dafür ist CobiT nicht von grossem Nutzen.

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

Abbildung 3: Die 18 von CobiT identifizierten Anwendungskontrollen

3. Allgemeine IT-Kontrollen (IT general controls) nur insofern berücksichtigen, als sie für das reibungslose Funktionieren wesentlicher Applikationen von Geschäftsprozessen von Bedeutung sind

In Fachartikeln wurde thematisiert, dass manche Konformitätskontrollen nach SOX in einem völligen Missverhältnis zu den angestrebten Zielen stehen. Hat zum Beispiel die Dicke der Panzerung der Türen eines Rechenzentrums wirklich einen Einfluss auf die Zuverlässigkeit des Jahresabschlusses des betreffenden multinationalen Konzerns? Zweifel sind berechtigt und solche Übertreibungen tragen höchstens dazu bei, die Arbeit der Abschlussprüfer in Verruf zu bringen.

Solche Übertreibungen lassen sich mit dem vom PCAOB empfohlenen rückwirkenden Verfahren (oder „***Top-down Approach"***) vermeiden, das folgendermassen aufgebaut ist:

1) Wichtige Positionen im Jahresabschluss ermitteln.
2) Prozesse ermitteln, welche diese Positionen hervorbringen oder stark beeinflussen.
3) Informatikanwendungen ermitteln, die für diese Prozesse von Bedeutung sind.
4) Nur diejenigen allgemeinen IT-Kontrollen prüfen, die für das reibungslose Funktionieren der oben genannten Anwendungen wichtig sind.

Realisiert das Unternehmen z.B. nur einen äusserst geringen Anteil seines Umsatzes mit einer von seinen übrigen Informatikressourcen abgekoppelten eCommerce-Anwendung, so sollte der Prüfer den „Mut" haben, diesen Bereich einfach zu ignorieren. Ist dagegen der gesamte Fakturierungsbereich ausgelagert, muss z.B. die Zuverlässigkeit der Schnittstellen, die sowohl von den Anwendungskontrollen, als auch von den allgemeinen Kontrollen abhängt, umfassend geprüft werden.

Die Prüfung der allgemeinen IT-Kontrollen darf sich nicht auf Interviews beschränken, sondern sie muss auch Wirksamkeitsprüfungen umfassen. Diese Prüfungen sind in den Bereichen Beschaffung und Einführung (AI) sowie Auslieferung und Unterstützung (DS) von CobiT enthalten, das mit seinen Audit Guidelines[7] eine wertvolle Hilfe liefert.

Ich kann also nur empfehlen, CobiT 4.0 schnell herunter zu laden und wünsche Ihnen viel Erfolg mit dieser neuen Version!

Michel Huissoud, CISA, CIA,
Vizepräsident ISACA (Schweiz)

Endnoten

[1] Public Company Accounting Oversight Board

[2] Prüfungsstandard Nr. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements, Stand Februar 2005

[3] Die Abbildung stammt aus dem Dokument „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] Zum Beispiel der Beschluss vom März 2005: CobiT ist als eines der offiziell zugelassenen Instrumente anerkannt, mit welchem die

IT-Sicherheit der Agrarbeihilfenzahlstellen sichergestellt werden kann.

[6] Vgl. Dazu das ausgezeichnete Handbuch „Global Technology Audit Guide Change and Patch Management Controls: Critical for Organizational Success“, The Institute of Internal Auditors, 2005

[7] In der Version 4.0 noch nicht verfügbar.

ISACA Serving IT Governance Professionals Switzerland Chapter

www.isaca.ch

Alle Kurse mit hohem Labor-Anteil

Drei spannende Kurse!

Application Security Lab
Workshop für Sicherheit von Web-Anwendungen
19. - 21. April 2006 in Zürich

Evidence Lab
Workshop über die Spurensuche in Computersystemen
26. - 28. April 2006 in Zürich

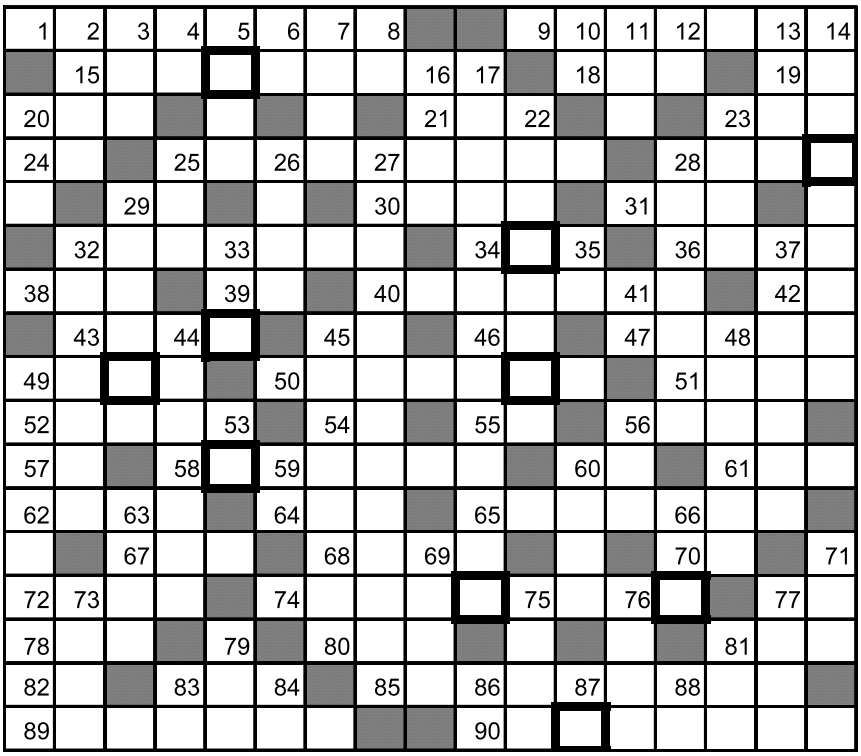
Content und Mobile Security Lab
Kritische Betrachtung moderner Perimeter-schutzmechanismen und deren Gefährdung
3. - 5. Mai 2006 in Zürich

Weitere Informationen erhalten Sie in unserem Kurssekretariat:

ISACA Switzerland Chapter
c/o ITACS Training AG, Stampfenbachstr. 40
8006 Zürich, Schweiz, kurse@isaca.ch,
Tel. 044 444 11 01, Fax 044 444 11 02, www.isaca.ch

The ISACA Crossword Puzzle 1/06

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



Across: 1 ***in Corporate Governance often mentioned in connection with checks***; 9 ***thing intended***; 15 inherent; 18 ***32 across is supposedly counting them*** (singular); 19 conjunction; 20 under which umbrella James Bond was acting on the mountain tops in Switzerland (abb.); 21 undergo natural decomposition; 23 credit rate stop; 24 form of to be; 25 ***where the evidence is to be found***; 28 lay hold of; 29 Ltd (F); 30 island (Rom); 31 nocturnal quadruped; 32 ***person carrying out reviews***; 34 suitable; 36 Egyptian Christian; 38 circle; 39 Southeast; 40 Egyptian politician; 42 egg (D); 43 catholic clergyman, causing lately a lot of trouble near Basel; 45 it (D); 46 conjunction; 47 celebrates her name day on the 12th of August; 49 with al added of air; 50 ***we all think we are*** (pl), ***don't we?!;*** 51 Swiss comedian; 52 trim; 54 aromatic beverage (E); 55 ancient yes; 56 these (E); 57 her (F); 58 lighted animal; 60 soundless beat; 61 rodent; 62 elm tree (D); 64 exclamation (F); 65 not according to the law; 67 ore (D); 68 answer to the pact of Warshaw; 70 article (I); 72 high playing cards; 74 equalizing; 77 Italian river; 78 meshed fabric; 80 soundless metric measurement; 81 coal product; 82 short Swiss bank; 83 obtain; 85 measuring device; 89 absolute being; 90 be reluctant.

Down: 2 targets; 3 natural logarithms; 4 preposition; 5 disturbed norm; 6 here (I); 7 biblical giant; 8 feared Nazi organization; 10 preposition; 11 colour; 12 short for father; 13 Scottish for hem – a such Cutty was once the fastest ship and today a tasteful Wiskey; 14 of primary importance; 16 part of the eye; 17 ***goals can be reached often only by this***; 20 score; 22 the one in Boston had serious consequences; 23 Roman writer; 25 small lump of soft material; 26 worth estimate; 27 company comparative advantage; 28 besides center, guards and ends in the front row of the football team; 29 Japanese auto producer; 32 the London „Gunners"; 33 International Standard Organization; 35 Turkish auto; 37 a t is missing for a muscular tic; 41 Share Capital (D); 44 smart blowers; 45 ***these auditors sign off***; 48 not of ethical value; 49 ***modern form of auditing***; 53 free information; 56 French summer; 59 rowing club; 60 lead (D); 63 gather; 66 one-horsed carriage; 69 the red earth that „went with the wind"; 71 preposition; 73 discontinue; 75 encryption; 76 country team (slang, D); 77 agreement (D); 79 mother chicken; 81 tennis club Aberdeen; 83 auto from Geneva; 84 tennis club; 86 blood factor; 87 double consonant; 88 ***our trade***.

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 Kreuzworträtsel 5/05:
Revisorengruppe

Waagrecht: 1 werken; 6 ***Vorjahr***; 11 Ma(ma); 13 EF; 14 Ilona; 16 AO; 17 Helau; 19 ***Regel***; 21 Stiche; 24 Bild; 25 Turm; 27 er; 28 Affe; 30 Kl; 31 vier; 33 Inka; 34 Mut; 35 Ernte; 39 ***Norm***; 41 RS; 42 starr; 43 Trara; 46 mess; 48 sit!; 49 SE; 51 (C)OSO; 52 Ibis; 54 Ea; 55 ***Richtschnur***; 56 Mi; 57 dick; 59 ETH; 59 Nr; 60 sec; 61 POCH; 62 traeg; 64 Gizeh; 66 GR; 67 Hege; 69 Ebert; 70 rio; 71 Rose; 72 Bier; 74 in; 75 Knut; 76 de; 77 Heli(kopter); 79 PZIA (Pizza); 81 tagaus; 84 Nonen; 85 Pille; 87 ta; 88 limes; 90 Ei; 91 EP; 92 Bloesse; 93 Moehre.
Senkrecht: 1 ***Wertmesser***; 2 Efeu; 3 Keim; 5 no; 6 Vater; 7 RAC; 8 Johanna; 9 HH; 10 Rebe; 11 Malkurs; 12 ***Audits***; 15 NS; 18 Li; 20 Granat; 22 ir; 23 EFKO; 26 Ai; 29 Farmburger; 31 versichern; 36 RTIA (Rita); 37 TR; 38 Mass(s)tab; 40 Meir; 44 Roter; 45 (Hoffmann La) Roche; 47 SS; 50 Eck; 52 Inn; 53 ***Richtlinie***; 55 Rich; 56 Meer; 57 Do; 60 Szenen; 61 ***Prinzip***; 62 ***Testate***; 63 gli; 65 IB; 66 Grippe; 68 gout; 72 Beule; 73 EU; 75 Kalb; 76 da; 77 Hose; 78 leer; 80 il; 82 Gas; 83 si; 84 neo; 86 el; 89 mm.

Watson: 34 senkrecht ist nur ein Buchstabe. Er wurde von ***Marc Bucher*** entdeckt, was ihm den Jackpot von US$ 150 in Büchergutscheinen des ISACA Bookstores einbringt. Herzliche Gratulation! Ein origineller Vorschlag war übrigens, dass das Bild des Kreuzworträtsels an die neue Beleuchtung der Zürcher Bahnhofstrasse erinnert. Eigentlich hätte dies einen Originalitätspreis verdient!

Aus den Einsendern mit richtiger Lösung wurde durch die Glücksfee Monika ***Stefan Ciecior*** gezogen, der damit einen Büchergutschein von US$ 50 beim ISACA Bookstore gewinnt. Auch hier herzliche Gratulation!

Somit beginnt der Jackpot wieder bei Null bzw. US$ 50.

An audit assistant was looking in vain for a mate.
All men she looked after with love, rather than hate.
When she found errors in the client's declarations,
This one suggested some sexual „collaborations".
She declined and said: „Buster, now it's too late!"

Ein Revisor fand die Arbeit beim Kunden immer nett.
Drum benützte er häufig Informationen ab Internet.
Seine Kollegin war eine EDV-Computerfachfrau.
Mit „Zusammenarbeit" lockte er sie in seinen Bau.
Und studierte mit ihr die neuen PS im Himmelbett.

Express Line

A Word From the Chair

Greetings! As a reminder, second invoices will be sent to members in late January. Members can also continue to renew online if they choose.

The Membership Board will be reviewing all chapter web sites in the coming months to recognize outstanding web sites.

Steve Thorsted
Chair, Membership Board

Nominations for ISACA Board of Directors

Maintaining a strong and devoted Board of Directors is crucial to ISACA's ongoing success. Recruitment of candidates for ISACA's Board of Directors reflects input from many sources, including nominations submitted by members. ISACA is looking to its members to recommend individuals for board leadership who can help carry the organization to new heights of excellence and innovation.

When considering nominations, members should review the specific responsibilities for each position listed on the nomination form. Each board member is expected to meet the following criteria:

- Attendance at three Board of Directors meetings per year
- Attendance at the leadership conference in his/her own geographic area
- Possession of strong leadership and strategic planning capabilities
- Possession of an energetic spirit of volunteerism and innovative thought process
- Maintenance of a global perspective on professional issues and ISACA matters
- Strong motivation to accomplish board-mandated initiatives
- Possession of a significant network of professional contacts
- Willingness and capability to participate in all aspects of fundraising activities
- Adherence to the ISACA Code of Professional Ethics

International board appointments are for one-year terms.

Invitation to Participate

ISACA's and ITGI's key boards and committees depend upon member participants to ensure that all members receive the high-quality resources they have come to expect from these organizations. Participants on key boards and committees help ensure successful certification programs, comprehensive professional conferences, timely education programs, insightful research, thorough and appropriate online resources, representative professional standards, and financially sound infrastructures. Serving on a key board or committee carries with it several benefits, including:

- A role in the future of the association and institute
- Influence on industry issues
- Networking with peers around the globe
- Enhancement of leadership and professional skills
- A forum for sharing expertise and learning from others

The selection of members for key board and committee service is based upon the current needs of those groups, the relevant professional background of the candidates and the need to reflect a global perspective. All appointments are for one-year terms and are ratified by the Board of Directors at the first meeting of the administrative year.

To apply to serve on a key board or committee, please complete the application form included with volume 1, 2006, of the ***Information Systems Control Journal***. You may also obtain a form from your local chapter or download it from www.isaca.org/participate. The deadline for applying is 15 May 2006.

ISACA
Serving IT Governance Professionals
Switzerland Chapter

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
CONTROLLA FEDERALA DA FINANZAS

Bringen Sie Ihr Know-how bei uns ein!

Die Eidg. Finanzkontrolle (EFK) ist das oberste Finanzaufsichtsorgan des Bundes. Sie unterstützt das Parlament und den Bundesrat bei der Wahrnehmung ihrer Aufsichtspflicht. Die EFK übt bei Bundesämtern, internationalen Organisationen, Subventionsempfängern und Institutionen mit öffentlichen Aufgaben die Finanzaufsicht aus.
Zur Ergänzung unserer Fachbereiche suchen wir eine/n

IT-Auditor/in

für Prüfung der Wirtschaftlichkeit grosser Informatikprojekte, der Betriebssicherheit von SAP R/3 Anwendungen und des internen Kontrollsystems informatikunterstützter Geschäftsprozesse sowie für Ausführung von Spezialaufträgen unserer Direktion und parlamentarischer Aufsichtsgremien.

***Ihr Profil:** Sie verfügen über das CISA Diplom oder eine gleichwertige Erfahrung und bringen SAP R/3 Kenntnisse mit. Sie sind gewillt, sich in interdisziplinäre Teams zu integrieren, komplexe Fragen zu bearbeiten und anspruchsvolle Berichte zu schreiben.*

Wenn Sie teamorientiert handeln, eine zweite Amtssprache beherrschen und eine flexible, initiative Persönlichkeit sind, freuen wir uns darauf, Sie kennen zu lernen. Nehmen Sie mit uns Kontakt auf!

Die Bewerbungsunterlagen richten Sie an Irène Strobel, Leiterin Personal der Eidg. Finanzkontrolle, Monbijoustrasse 45, 3003 Bern. Für weitere Auskünfte steht sie Ihnen unter 031 323 10 31 gerne zur Verfügung.

Ref. EFK FB Informatikprüfungen 001/06
16.01.2006

Eidg. Finanzkontrolle
Personaldienst
Monbijoustrasse 45
CH-3003 Bern
irene.strobel@efk.admin.ch
www.efk.admin.ch

ISACA Serving IT Governance Professionals
Switzerland Chapter

DACH-News

In eigener Sache

Geschmacksache?

Als ich 1977 erstmals mit der EDP Auditors Association (EDPAA) in Kontakt kam, trug sie Lochkarten, Magnetbänder und Diskpacks in ihrem Emblem. Höchst modern, und von vielen Leuten damals bewundert und nicht verstanden. Als erleuchtendes Merkmal trug die für die Ausbildung zuständige Stiftung (EDPAF) auch noch eine Öllampe auf dem Schild, was mich an Aladins Wunderlampe erinnerte.

Wie doch die Zeit vergeht! Inzwischen hat sich der Wortschatz und -gebrauch geändert und die EDPAA ihren Namen in Information Systems Audit and Control Association (ISACA) modernisiert. Längst war nicht nur „Electronic Data" ein Hauptthema, sondern Netzwerke, Kommunikation und nicht zuletzt das Internet hatten sich im Umfeld der technisierten Wirtschaftsprüfung etabliert. Parallel dazu wurde das Stichwort „Sicherheit" aufgewertet und praktisch gleichwertig neben Kontrolle und Revision gestellt. Das Logo musste entsprechend angepasst werden, was ein gewisses ***Streamlining*** bedeutete.

Ausdruck dieser Entwicklung waren die neu geschaffenen Titel des Certified Information Systems Auditor (CISA) und des Certified Information Security Managers (CISM). Der CISA hatte zudem noch einen kurzlebigen Vorgänger, der sich CDPA nannte. Dieser Titel wurde aber nach einem heftigen, aber relativ abrupt beendeten Rechtsstreit mit der damaligen amerikanischen Vereinigung der Certified Public Accountants (AAAC) fallen gelassen. Der CDPA war diesen Damen und Herren dem CPA nun doch etwas zu ähnlich.

Heute sieht sich die ISACA veranlasst, das Erscheinungsbild erneut zu modernisieren. Das ausgeschriebene ***Information Systems and Control Association*** ist aus dem Logo verschwunden und wurde durch den Zusatz ***Serving IT Governance Professionals*** ersetzt. Damit soll der Zweck der Vereinigung verbessert zum Ausdruck gebracht werden. Nämlich, dass sich die ursprünglich 1967 lose gegründete Interessengemeinschaft von Herstellern, Benützern und Revisoren bezüglich EDV zu einem in ihrem Tätigkeitsgebiet führenden Gremium gemausert hat. Einem Gremium, das Standards setzt und internationale Anerkennung geniesst.

Das ISACA Switzerland Chapter hat diesen Steilpass aus dem Hauptquartier erkannt, erlaufen, angenommen und das Erscheinungsbild des ***News-Letters*** den internationalen Vorgaben angepasst. Das Redaktionsteam hofft, die Änderungen seien im Sinne der Leser. Verbesserungsvorschläge sind übrigens jederzeit willkommen. Zu einer letzten Klarstellung: Das Redaktionsteam hat darauf verzichtet, den Zusatz ***Serving IT Governance Professionals*** auf Deutsch, Französisch und Italienisch zu übersetzen (was zwar für die letzten zwei Sprachen angeblich verfügbar sei).

Für das Redaktionsteam:
MadMax, CINE

D: Aktivitäten des German Chapter

Ein weiteres Jahr der Vorstandsarbeit ist vorüber und in Kürze steht die Mitgliederversammlung des ISACA German Chapters an. Diese wird am 10. März 2006 in Frankfurt am Main stattfinden. Der Vorstand möchte alle Mitglieder hierzu ganz herzlich einladen und hofft auf eine rege Teilnahme. Wie in den Vorjahren wird allen Mitgliedern noch eine entsprechende schriftliche Einladung per Post zukommen. Bis dahin wird der Vorstand natürlich weiter aktiv den Verein vorantreiben.

Auch in diesem Jahr werden wir CISA Kurse in Frankfurt am Main sowie Hamburg anbieten. Den Anfang macht hier Frankfurt am 8. April 2006, gefolgt von Hamburg am 22. April 2006. Ergänzt werden diese Kurse wieder durch das Testexamen in Frankfurt am 20. Mai 2006. Da die Kurse in der Teilnehmerzahl begrenzt sind, sollte sich jeder Interessierte schnellstmöglich anmelden.

Unsere Webseite hat im letzten Jahr ein vollständiges Facelifting erfahren und bietet seitdem neue interessante Funktionalitäten. Hierbei möchte ich allen Mitgliedern das Forum des ISACA German Chapters ans Herz legen, um sich dort über diverse Themen auszutauschen.

Abschließend möchten wir wieder einmal alle diejenigen Mitglieder ansprechen, die interessante Projekte oder auch wissenschaftliche Themen bearbeiten oder bearbeitet haben. Schreiben Sie doch einfach einmal einen Artikel für den ***News-Letter*** und lassen Sie andere auch ein wenig an Ihren Praxiserfahrungen oder dem erworbenem Wissen teilhaben. Wenn Sie Fragen dazu haben sollten, können Sie mich jederzeit gern kontaktieren

(ingo.struckmeyer@pf.comdirect.de). Sie werden sehen, es ist gar nicht so schwer, einen interessanten Artikel zu schreiben. Allen Autoren des letzten Jahres danken wir an dieser Stelle nochmals für ihre wirklich gelungenen Artikel.

Ingo Struckmeyer
Vorstand German Chapter

CH:

After Hour Seminar

Das letzte ***After Hour Seminar*** (AHS) 2005 vom 29. November war trotz (oder vielleicht gerade infolge) des unsicheren Themas erstaunlich gut besucht. Peter Bitterli berichtete über seine „Sicherheits"-Eindrücke aus Australien in Form einer Lichtbildershow. Er setzte gewisse Schwerpunkte bezüglich der Verantwortung der Eltern gegenüber ihren Kindern, des Strassenverkehrs, der Tiere, der Sonneneinstrahlung, des Badens in quallen- und krokodilverseuchten Gewässern usw. Vielfach waren erheiternde Einzelheiten eingestreut, welche entsprechend kommentiert wurden (z.B. Schulkinder sind zu beaufsichtigen – was ist mit den Vorschulkindern??? usw.). In der anschliessenden Diskussion wurde die völlig unnötige Frage gestellt, was das Ganze mit IT bzw. IT-Sicherheit und -revision zu tun hätte. Obschon Peter Bitterli ausdrücklich festhielt, dass er keine Parallele ziehen wollte, meinte er, die vielen angetroffenen Schilder und Affichen hätten mehrheitlich Hinweise enthalten, „wie man sich verhalten sollte" und nicht blosse Warnungen und Verbote (obschon es diese auch hatte). Nehmen wir uns ein Beispiel daran und versuchen wir immer, Verhaltensmassnahmen vorzuschlagen, anstatt falsches Verhalten anzuprangern!

Gespannt darf man auf die AHS 2006 sein. Die Mitglieder der ISACA und Besucher der AHS sind aufgefordert, den Veranstaltern Themen und Referenten vorzuschlagen. Wenn die Ausgabe 2006 so vielfältig, lehrreich und spannend wie 2005 wird, darf man sich schon heute freuen.

Nachtrag: Die Erwähnung des Autors des AHS vom 30.8.2005 (Corporate & ICT Performance Management) ist in der letzten Nummer leider untergegangen. Es ist Bruno Wiederkehr. Interessenten zum Thema melden sich direkt bei ihm.

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

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

Letzte Sitzung: 7. November 2005 bei EFK, Bern
Besprechung Entwurf Domäne „Beschaffung und Implementierung neuer Systeme"
Weiteres Vorgehen: gemäss Sitzungsprotokoll

Nächste Sitzung: 24. Januar 2006, 08.45–12.00 Uhr, Ort wird den IG Mitgliedern noch mitgeteilt.

Traktanden:
1. Abnahme Domäne Beschaffung und Implementierung neuer Systeme
2. Detailbesprechung der Domäne Service Delivery.
Weiteres Vorgehen

IG Romandie

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

IG Outsourcing/Insourcing

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

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

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

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 keinen 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

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

Letzte Sitzung: 28. November 2005, EFK, Bern
1. Begrüssung
2. Daten finden Sicherheit und Schutz im Swiss Vault® (Hr. Christoph A. Oschwald, Delegate of the Board of Directors, SIAG)
3. Releasestrategie, was ist bei einem Releasewechsel (z.B. 4.6 —> 4.7) zu machen (und zu prüfen!) (Hr. Walter Bremer, Leiter Applikationsbetrieb CCSAP BV)
4. Tipps und Tricks für die FI-Revision (Hr. Roland Giger, Revisionsexperte, EFK)
5. Governance & Compliance Massnahmen für IT Betrieb & Controlling (Hr. Peter Zgraggen, Account Director, CA)
6. Erfahrungen und News (alle)
7. Diverses
8. Gemeinsames Mittagessen und anschliessendem Besuch der Session der eidgenössischen Räte im Parlamentsgebäude

Nächste Sitzung: gemäss Protokoll der Sitzung vom 28.11.2005

IG (Self) Assessement mit CobiT 4.0

Neue IG

Leitung
Luc Pelfini, Bitterli Consulting AG
Tel: +41 44 444 11 00
prb@bitterli-consulting.ch

Ziele der IG: Diese IG konstituiert sich neu. An einer ersten Sitzung wird gemeinsam das Vorgehen definiert und verabschiedet. Ziel der IG ist die Erarbeitung eines Vorgehens und aller notwendigen Arbeitshilfen, um ein qualitativ hochstehendes (Self) Assessment basierend auf CobiT 4.0 durchführen zu können. Schwerpunkt wird dabei sein, grösstmöglichen Nutzen aus den neuen Bestandteilen von CobiT (z.B. RACI-Matrix) zu ziehen und die inhaltlich teilweise massiv überarbeiteten IT-Prozesse sowie deren Maturity Level für das (Self) Assessment zu verwenden. Grundsätzlich sollen aus CobiT 4.0 möglichst viele quantitve und qualitative Faktoren herausgeschält werden, so dass Assessment-Ergebnisse nachvollziehbar und objektiv sind. Die Arbeitsergebnisse werden voraussichtlich in MS-Office erstellt und sollen sowohl die Arbeit mit Papierexemplaren als auch die elektronische Erfassung und Auswertung der Assessment-Ergebnisse weitgehend unterstützen.

Datum der ersten IG-Sitzung:
Montag 27.2., 16.00–18.00
Ort : Im Raum Zürich, ausnahmsweise auch in Basel oder Bern. Erste Sitzung an der Stampfenbachstrasse 40 (Bitterli Consulting AG)

Traktanden der ersten IG-Sitzung mit Interessenten:
1. Vorstellung der (potentiellen) Mitglieder
2. Spielregeln der Arbeitsgruppe (z.B. Verwendung der Resultate)
3. IG-Ziele (Diskussion, detailierte Ausgestaltung und Verabschiedung)
4. Diskussion des Vorgehens und Definition von ersten Arbeitspakten
5. Etablierung der IG (Mitgliederliste, Planung der Sitzungen, etc.)

Mitglieder der IG (Self) Assessment mit CobiT 4.0: Angesprochen sind primär Personen, die bereits mit CobiT (3rd Edition oder 4.0) gearbeitet haben. Ebenfalls willkommen sind Personen, die CobiT nur kennen aber nicht selber damit gearbeitet haben, sofern sich der Anteil der „Newcomer“ in angemessenem Rahmen hält.

ISACA
Serving IT Governance Professionals
Switzerland Chapter

Veranstaltungen

CISM-Vertiefungskurs	12. Januar–16. Mai 2006 Zürich, 12 Tage, ISACA/ITACS
CISA-Vertiefungskurs	16. Januar–15. Mai 2006 Zürich, 14 Tage, ISACA/ITACS
Formation à l'audit des systèmes d'information	23 janvier au 26 avril 2006 Lausanne, 18 soirées, ISACA
ISO/IEC 27001 Auditor Lehrgang mit Zertifizierung	20.–24. Februar 2006 Zürich, 5 Tage, Infosec
Technische Sicherheit	27. Februar – 2. März 2006 Zürich, 4 Tage, Infosec
After Hour Seminar: Thema noch nicht bekannt	28. Februar 2006 16.40–17.40, Zürich, ISACA
ITIL Foundation mit Apollo 13 inkl. int. Zertifizierung	1.–3. März 2006 Zürich, 3 Tage, ISACA/Glenfis
EuroCACS	19.–22. März 2006 London, 4 Tage, London
IT-Sicherheit: erfolgreiche Integration in das Risikomanagement	22. März 2006 Zürich, 1 Tag, Vereon AG
IT-Revision aus Sicht des Managements	29. März 2006 Zürich, 1 Tag, Vereon AG
CISM-Prüfungsvorbereitungskurs	30. März–16. Mai 2006 Zürich, 4 Tage, ISACA/ITACS
CISA-Prüfungsvorbereitungskurs	3. April–15. Mai 2006 Zürich, 5 Tage, ISACA/ITACS
Application Security Lab – Workshop zum Thema Sicherheit von Web-Anwendungen	19.–21. April 2006 Zürich, 3 Tage, ISACA/Compass
Evidence Lab – Workshop über die Spurensuche in Computersystemen	26.–28. April 2006 Zürich, 3 Tage, ISACA/Compass
Préparation à la certification internationale CISA	1 mai au 8 juin 2006 Lausanne, 18 soirées, ISACA
Anwendungssicherheit: Risiko-orientierte Entwicklungsmethoden	22.–24. Mai 2006 Zürich, 3 Tage, ISACA/ITACS
Content- und Mobile-Security Lab – Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung durch mobile Tech. und aktuelle Malware	3.–5. Juni 2006 Zürich, 3 Tage, ISACA/Compass
Service Management – ITIL Foundation Training – Auf der Basis des de facto-Standards ITIL mit Links zur BS 15000 Zertifizierung	7.–9. Juni 2006 Zürich, 3 Tage, ISACA/Glenfis
BS 15000 Consultant & Internal Auditor, inkl. int. Zertifizierung	12.–14. Juni 2006 Zürich, 3 Tage, ISACA/Glenfis

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 CH Kurssekretariat
c/o ITACS Training AG
Stampfenbachstrasse 40
CH-80006 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 61 697 72 41
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
Paul Wang
Tel. +41 22 748 56 01
paul.wang@ch.pwcglobal.com

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

www.isaca.ch