Information Systems Audit and Control Association

News Letter

Nr. 70, September 2004

Thema

Professional Judgement in der IT

Switzerland Chapter
Germany Chapter
Austria Chapter

© 8.9.2004

Inhaltsverzeichnis

Editorial 4

Professional Judgement in der IT – Arbeiten und Ergebnisse Fachstab für Informatik 5

Professional Judgement in der IT – Les normes sont là mais tout (ou presque) reste à faire… 6

Professional Judgement in der IT – Die Richtlinien sind vorhanden, aber es bleibt noch viel zu tun 7

Professional Judgement in der IT – Approche d'audit d'une application bancaire standard 8

Professional Judgement in der IT – Integration IT Audit in Abschlussprüfung (Versicherung) 10

Professional Judgement in der IT – Intégration de l'audit informatique dans la révision annuelle des comptes (assurances) 12

eGovernment und Digitale Identität 14

The ISACA Crossword Puzzle 16

Express Line 18

Forum 20

DACH-News 21

Veranstaltungen 27

Germany Chapter 29

Austria Chapter 30

Switzerland Chapter 31

Impressum

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

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

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

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

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: 1100 Exemplare

Nächste Ausgabe (Thema: „Deutschland"): November/Dezember 2004, Redaktionsschluss: 12. November 2004

Editorial

Existe-t-il aujourd'hui un audit financier qui ne soit pas informatique ? Au terme du séminaire organisé le 23 juin dernier par l'ISACA conjointement avec la Chambre fiduciaire suisse, on peut en douter. Encore faudra-t-il en convaincre l'ensemble de la branche et surtout les clients qui ne seront pas toujours prêts à accepter de payer les honoraires nécessaires à une analyse sérieuse du contrôle interne. Les 50 participants du séminaire ont été appelés à définir les tâches d'audit à effectuer pour la révision annuelle des comptes (y compris comptabilité analytique) d'un hôpital de 600 lits occupant 2000 personnes. La fourchette d'honoraires estimée par les participants est révélatrice de ces écarts de perception : de 70 000 à 240 000 francs par année. Des différences que l'on retrouve dans de récentes attributions de marchés publics.

Ne nous leurrons pas : le chemin sera encore long. La Suisse n'a fait qu'adopter l'ancienne norme ISA 401 qui – pour des raisons que l'histoire n'a pas retenu – n'avait pas encore été transposée dans les normes suisses. Avec cette NAS 401, le principe de la prise en compte de l'informatique dans les travaux d'audit est posé. Il faudra cependant attendre la reprise des standards adoptés en octobre 2003 par l'IFAC, soit les ISA 315 « *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* », 330 « *The Auditor's Procedures In Response to Assessed Risks* » et 500 « *Audit Evidence* » pour réellement pouvoir parler d'une intégration de la dimension informatique dans la révision des comptes annuels.

La pression de la future institution de surveillance des organes de révision pourrait accélérer le mouvement. A moins que la législation américaine ne vienne à nouveau bousculer nos habitudes helvétiques. La Chambre des représentants traitera en effet prochainement un projet de *Corporate Information Security Accountability Act* qui obligerait les entreprises cotées « to hire an independent auditor to assess existing information security controls and ensure that they meet basic standards that the U.S. Securities and Exchange Commission has yet to determine ».

Certains en viendront peut-être à regretter le bon vieux temps de Sarbanes-Oxley…

Ce numéro de la *NewsLetter* nous apporte des résumés des présentations du séminaire. Bonne lecture!

Michel Huissoud
Vice-président ISACA (Suisse)

Gibt es heute überhaupt noch eine Finanzrevision, die nicht eine Informatikrevision beinhaltet oder sogar ist? Das vom ISACA Switzerland Chapter zusammen mit der Schweizerischen Treuhandkammer durchgeführte Seminar vom 23. Juni 2004 liess dahingehend Zweifel aufkommen. Es stellt sich zudem dem Berufstand und den Kunden die Herausforderung, die notwendigen Kosten für eine seriöse Revision des Internen Kontrollsystems aufzubringen. Die 50 Teilnehmer am Seminar hatten u.a. die Aufgabe, die aus ihrer Sicht notwendigen Revisionstätigkeiten für eine solche Revision eines Spitalbetriebes mit 600 Betten und 2000 Patienten aufzustellen. Die resultierende Bandbreite von CHF 70 000 bis CHF 240 000 spricht Bände, was unter einer solchen Revision verstanden werden kann. Die gleiche Bandbreite ist denn auch im Markt anzutreffen.

Machen wir uns nichts vor: Der Weg ist noch lang. Die Schweiz müsste nur die ISA-Norm 401 übernehmen – was sie aus historisch nicht näher untersuchten Gründen aber bisher nicht tat. So warten wir auf die Umsetzung der IFAC-Normen, die im Oktober 2003 übernommen wurden. Es handelt sich um die ISA-Normen 315 « *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* », 330 « *The Auditor's Procedures In Response to Assessed Risks* » und 500 « *Audit Evidence* » , damit wir von einer echten Integration der Informatikdimension in den Jahresrechnungen und -berichten sprechen können.

Der Druck der zukünftigen Aufsichtsinstitution des Bundes über die Revisionsgesellschaften könnte diese Entwicklung beschleunigen. Wenn uns nicht die amerikanischen Anstrengungen in dieser Hinsicht in unserer helvetischen Beschaulichkeit einmal mehr aufschrecken. In naher Zukunft wird die Treuhandkammer ein Projekt auf die Beine stellen, das unter dem Titel *Corporate Information Security Accountability Act* die kotierten Gesellschaften verpflichten soll, "to hire an independent auditor to assess existing information security controls and ensure that they meet basic standards that the U.S. Securities and Exchange Commission has yet to determine".

Einige unter uns werden sich wohl in nicht allzu ferner Zukunft an die guten alten Zeiten des Sarbanes-Oxley-Acts erinnern…

Diese Ausgabe des *NewsLetters* bringt Zusammenfassungen von den am Seminar vorgetragenen Referaten. Geniessen Sie die Lektüre!

Michel Huissoud
Vizepräsident ISACA (Schweiz)

Professional Judgement in der IT

Arbeiten und Ergebnisse Fachstab für Informatik

Hauptziel der Präsentation: Den Teilnehmern einen Eindruck vermitteln, was die neuen Prüfungsstandards (PS) und ISA ICT-seitig beinhalten und für jeden ICT-Prüfer bedeuten.

Gegenstand waren die folgenden Themen:

1. Mission, Ziele und Arbeiten des Fachstabs Informatik
2. Übersicht über neue PS aus Sicht Relevanz für ICT
3. Besprechung der wesentlichen Inhalte und Fragestellungen bei der Umsetzung der folgenden ISA/PS: PS 401, ISA 315; ISA 330, ISA 500, ISA 200
4. Übersicht über den Stand der Diskussionen betreffend ICT-relevanten IAPS
5. Kurze Einführung zu Sarbanes-Oxley aus Sicht ICT

Jürg Brun, E & Y, Bern

Professional Judgement in der IT

Les normes sont là mais tout (ou presque) reste à faire…

La Suisse a décidé de reprendre sans changement l'ensemble des normes ISA. Une décision quelque peu forcée, mais certainement un pas dans la bonne direction. Le séminaire de la Chambre fiduciaire du 23 juin 2004 a montré que le chemin pourrait être encore long avant que les nouvelles normes soient appliquées convenablement par l'ensemble de la branche.

Un premier constat : la pratique quotidienne montre que la branche a un urgent besoin d'outils permettant un *dialogue entre auditeurs financiers et auditeurs informatiques.* Si ces deux groupes professionnels n'apprennent pas à mieux communiquer ensemble, la mise en œuvre des nouvelles normes d'audit demeurera probablement lettre morte. Il s'agit en pratique de trouver la médiane entre le descriptif verbal d'une procédure et (à l'extrême) un schéma de câblage de bâtiment. La Compagnie (française) des commissaires aux comptes a fait œuvre de pionnier avec son excellent Guide d'application « Prise en compte de l'environnement informatique et incidence sur la démarche d'audit » (qui peut être commandé sur www.cncc.fr). On y trouve notamment des exemples réalistes de présentation du paysage applicatif d'une entreprise qui devraient permettre aux auditeurs de partager une perception identique des problèmes.

Au-delà de ces questions de communication, la branche devra se pencher attentivement sur quelques questions. Au nombre de celles-ci :

- Comment intégrer les contrôles généraux dans une démarche d'audit ? Cette question n'est pas nouvelle mais elle va prendre une acuité nouvelle avec les exigences accrues en matière d'audit du système de contrôle interne. L'existence d'un journal de mutation constitue souvent la pièce centrale d'un SCI. Comment être sûr de sa fiabilité sans avoir vérifié le processus de développement, de tests et d'acceptation du programme qui le génère ? Sans avoir examiné les droits d'accès du personnel d'exploitation sur les bibliothèques de programme ou les droits d'accès du gestionnaire de la base de données ?
- Comment s'assurer de la fiabilité des données générées par les innombrables tableurs qui se multiplient autour des dirigeants d'entreprise ? Une récente étude effectuée en Allemagne par Pricewaterhouse Coopers montre que « Die Tabellenkalkulations-programme sind selbst bei wichtigen Treasury-Aufgaben noch immer das dominierende Instrument. »
- Comment s'assurer de la fiabilité d'un logiciel standard, certifié ou non ? La Chambre fiduciaire a informé il y a quelques temps que les communications professionnelles n'étaient plus en vigueur. La communication no 9 « *Certification du logiciel* » disparaît ainsi en laissant un vide qu'il s'agira un jour de combler. Si l'on écarte la problématique de l'entreprise qui certifie les logiciels, il demeure le problème quotidien de l'auditeur confronté à un logiciel standard. Que doit-il faire ? Se renseigner sur une éventuelle certification, les réserves apportées à cette certification, les paramètres divergeant de la version certifiée ? Se renseigner sur les « bugs » de ce logiciel ? Prendre connaissance des tests effectués lors de la mise en place de ce logiciel standard ? Effectuer lui-même les tests qui n'ont pas été effectués ? L'expérience montre que les logiciels standards contiennent des erreurs mais comment convaincre un client de financer de tels tests ?
- Comment impliquer les fournisseurs et autres partenaires dans l'audit des interfaces ? La norme ISA 402, imparfaitement reprise dans la norme 18, pose les bases de l'audit de l'outsourcing. Il n'existe en revanche que peu de recommandations sur l'audit des interfaces, que celles-ci soient internes ou externes à l'entreprise. Un domaine ou tout ou presque est à définir.
- Quelles sont les bonnes pratiques en matière d'utilisation des outils d'audit informatiques ? L'IFAC a publié un Practice Statement sur ce thème (IAPS 1009). La question de la reprise, et dans l'affirmative de l'actualisation – de ce guide est à l'étude.
- Et enfin – la question probablement la plus importante mais également la plus délicate – que faire des conclusions d'un audit du SCI ? Est-il envisageable de proposer le renvoi des comptes en cas d'absence de SCI ? Qui paye les travaux

d'audit supplémentaires si le recours à des procédures orientées résultats est la seule voie permettant à l'auditeur de former son opinion sur les comptes ?

Il appartiendra au Comité informatique de la Chambre fiduciaire de proposer des réponses à ces questions. Un défi que les membres de ce comité sont prêts à relever avec le soutien de l'ensemble des auditeurs informatiques.

Michel Huissoud, CISA

Professional Judgement in der IT

Die Richtlinien sind vorhanden, aber es bleibt noch viel zu tun

Die Schweizerische Treuhandkammer hat beschlossen, grundsätzlich die ISA-Richtlinien tel quel zu übernehmen. Das Kammerseminar vom 23. Juni 2004 hat gezeigt, dass noch ein weiter Weg vor uns liegt, bis die Richtlinien eine einheitliche Anwendung im Berufstand finden.

Eine erste Erkenntnis: Der tägliche Umgang zwischen den Beteiligten lässt erkennen, dass dringend ein Mittel zur wirksamen *Kommunikation zwischen Finanz- und Informatik-Revisoren* benötigt wird. Wenn diese beiden Teilgruppen des Berufstandes nicht lernen, besser miteinander zu kommunizieren, laufen die neuen Richtlinien Gefahr, totes Papierwerk zu bleiben. Es ist demnach ein Mittel gefordert, das die Kommunikation erleichtert und sicherstellt, dass die Aussagen in allen Teilen richtig verstanden und interpretiert werden: Eine entsprechende Ausbildung ist wohl unumgänglich. Die (französische) Gesellschaft für Wirtschaftsprüfer hat m.E. Pionierarbeit mit der Leitplanke *Prise en compte de l'environnement informatique et incidence sur la démarche d'audit* (die auf www.cncc.fr abgerufen werden kann) geleistet. Man findet darauf insbesondere praktische Hinweise für die Zusammenarbeit zwischen Revisoren und geprüften Unternehmen.

Aus den vielen nützlichen Beispielfragen seien einige herausgegriffen:

- Wie soll das generelle Kontrollumfeld bei einer (Finanz-) Revision berücksichtigt werden? Die Frage ist nicht neu, erhält aber bei der heutigen Vertiefung der Wichtigkeit der Internen Kontrolle neue Akzente. So wird ein Mutationsprotokoll häufig als zentrales Element eines wirksamen IKS erkannt. Wie aber ist man sicher, dass dieses Mutationsprotokoll zuverlässig ist, wenn man das Umfeld, in welchem es entstand, nicht geprüft hat? Welche Gewissheit hat man über die Integrität des Protokolls, wenn man weder Zugriffsrechte noch deren Einhaltung kennt?
- Wie kann man sich über die Richtigkeit der generierten Daten ins Bild setzen, die durch ein Unzahl von Parametern und Tabellen gesteuert werden? Eine vor kurzem in Deutschland durchgeführte Studie von PricewaterhouseCoopers stellt fest: *Die Tabellenkalkulationsprogramme sind selbst bei wichtigen Treasury-Aufgaben noch immer das dominierende Instrument*.
- Wie kann man sich über die Zuverlässigkeit eines Standardpaketes überzeugen, ganz unabhängig davon, ob es ein Zertifikat besitzt, oder nicht? Die Treuhandkammer hat die Fachmitteilungen durch Grundsätze zur Abschlussprüfung (GzA) ersetzt. Wie verhält sich ein Revisor, der sich mit

Software, die aufgrund der Fachmitteilung Nr. 9 (*Software-Zertifizierung*) begutachtet wurde, konfrontiert sieht? Sich über die Hintergründe der Zertifizierung informieren? Sich über *bugs* dieser Software ins Bild setzen? Wo? Selber Tests durchführen? Die Erfahrung hat schon mehrfach gezeigt, dass Standardprodukte Fehler enthalten, aber wie soll man den Anwender überzeugen, dass Tests notwendig sind?

- Wie sollen Lieferanten und andere Geschäftspartner in die Prüfung von Schnittstellen eingebunden werden? Die Richtlinie 402, zwar unvollständig in die GzA 18 übernommen, legt einerseits Grundlagen für eine Outrsourcing-Revision. Auf der andern Seite bestehen aber wenig bis gar keine Hinweise zur Prüfung von *Schnittstellen*, weder interne noch externe. Ein Gebiet, das noch zu definieren ist.
- Welche Elemente gelten als *best practice* beim Einsatz von Audit-Software? Die IFAC hat zu dieser Thematik ein *Practice Statement (IAPS 1009)* verfasst. Es befindet sich in Überarbeitung.
- Und schliesslich – die wohl wichtigste und gleichzeitig heikelste Frage – was tut man mit den negativen Schlussfolgerungen einer IKS-Prüfung?! Rückweisung der Rechnung? Einschränkung(en)? Fussnot(en)? Ignorieren? *Management-Letter*? Wer zahlt allfällige Folgekosten (z.B. Kursverluste an der Börse), wenn Einschränkungen gemacht werden müssen?

Der Fachstab für Informatik der Kammer wird sich mit diesen Fragen auseinandersetzen müssen. Es wird eine Herausforderung für jedes Mitglied dieses Gremiums sein, entsprechende Hilfsmittel für den Berufstand zu erarbeiten.

Michel Huissoud, CISA

Professional Judgement in der IT

Approche d'audit d'une application bancaire standard

Résumé de la présentation

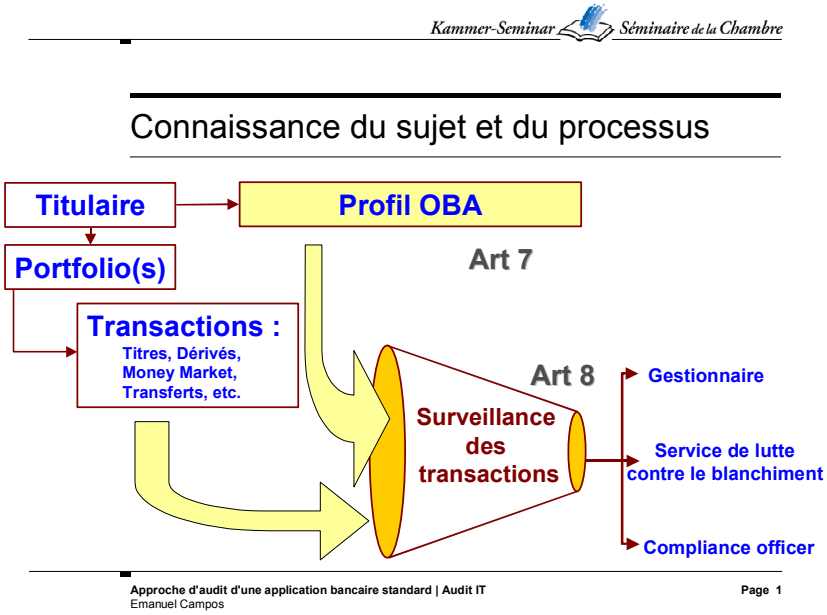
De nos jours la difficulté principale de l'auditeur informatique, est de cibler rapidement et efficacement les domaines à auditer afin de réduire les risques liés à son activité. Dans un même temps, il doit également apporter une assistance à ses confrères financiers et une opinion à ses clients.

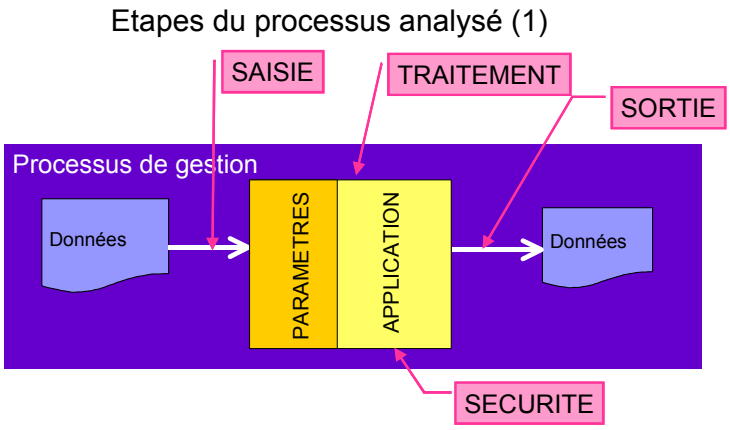
Les contraintes et pièges pour atteindre cet objectif ne manquent pas. En effet, au problème connu du budget restreint, viennent s'ajouter aujourd'hui la multiplication des plateformes à auditer et la complexité des nouveaux sujets.

Nous allons, durant cette présentation, montrer qu'une approche standard est toujours applicable quelque soit la plateforme et le sujet audité. Parallèlement à cette approche standard, nous essaierons d'illustrer à l'aide d'un exemple, la démarche qui pourrait être employée pour auditer la mise en place d'un système de surveillance des transactions bancaires dans le cadre des dispositions légales de l'Ordonnance sur le Blanchiment d'Argent, entrée en vigueur au 1er juillet 2003.

Rappelons que les établissements financiers soumis à cette ordonnance ont jusqu'au 1er juillet 2004, pour mettre en place ce système de surveillance informatisée.

L'approche d'audit IT d'une application requiert dans une première phase une prise de connaissance du sujet et du processus couvert par cette application. Une attention particulière doit être apportée à son importance parmi l'ensemble des processus de l'entreprise. Concrètement, l'auditeur devrait pourvoir répondre à une question essentielle : « quel est l'impact si le processus est défaillant ». La réponse à cette question détermine déjà une approche différenciée du processus. Par exemple, dans le cas du système de surveillance des transactions financières selon l'OBA, la défaillance apparaît clairement comme « non bloquante » pour les opérations de l'établissement financier, donc non stratégique pour l'entreprise. Néan-





moins, la défaillance prolongée ou l'inefficacité présentera un risque relatif au non respect d'une loi en vigueur.

Dans une deuxième phase un plan d'audit devra être défini en fonction d'objectifs de contrôle. Dans le cas de notre exemple, nous choisirons cinq objectifs de contrôle : L'intégralité, l'exactitude, la validité, la sécurité et la conformité.

Une fois ces objectifs de contrôle fixés, on peut orienter notre revue sur les étapes du processus analysés. Dans notre exemple, il s'agira d'analyser les paramètres mis en place, la saisie des opérations, leurs traitements, les rapports de l'application (sorties), les droits d'accès en place sur l'ensemble du processus et finalement la conformité de l'ensemble de l'application au respect de l'OBA.

Une fois le plan d'audit défini, il conviendra de déterminer les données à analyser. Dans notre exemple, l'ensemble des opérations sur une semaine d'un établissement financier possédant environ 5000 clients sera suffisant pour fonder une opinion. L'analyse de ces données consistera à effectuer à l'aide d'un outil séparé du système une simulation de la surveillance des transactions.

L'opinion devra conclure sur chacun des objectifs de contrôle à chaque étape du processus et finalement se résumer à répondre aux questions suivantes :

- La surveillance des opérations concerne-t-elle tous les clients de l'établissement (intégralité respectée des clients) ?
- La surveillance des opérations concerne-t-elle toutes les transactions présentant un risque de blanchiment d'argent (intégralité des transactions à risque) ?
- La surveillance des opérations couvre-t-elle des transactions valides et cohérentes ?
- La surveillance traite-t-elle des données exactes et fournit-elle des résultats exacts ?
- La surveillance est-elle effectuée par des personnes autorisées avec des droits d'accès adaptés aux besoins de leur fonction ?
- La surveillance est-elle conforme aux dispositions légales à respecter au 1er juillet 2004 ?

Une conclusion globale à ces réponses sera attendue par l'auditeur financier puis par l'autorité de surveillance dans les rapports de révision dès 2004. Cette opinion permettra à la CFB de s'assurer que les établissements ont mis en place un système de surveillance adéquat. Notons enfin que dans le cadre de cette Ordonnance, l'importance relative (matérialité) ne devra pas être considérée par l'auditeur lorsqu'il émettra son opinion.

Emanuel Campos
Lic. en informatique de gestion
Expert-comptable diplômé

Professional Judgement in der IT

Integration IT Audit in Abschlussprüfung (Versicherung)

Zusammenfassung

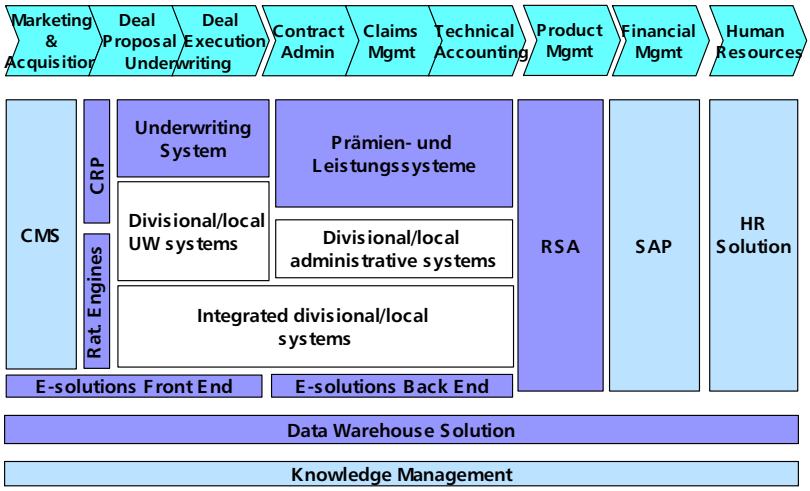
Einbezug von Informatik-Spezialisten

Buchführende Systeme werden in immer höherem Grad automatisiert und mit anderen Systemen der Wertschöpfungskette integriert. Schnittstellen werden dabei ebenfalls automatisiert und die enthaltenen Kontrollen sind nicht immer ohne weiteres zu erkennen und/oder zu testen. Daher wird es für den Abschlussprüfer immer wichtiger, dass er oder sie auch Revisoren mit IT-Kenntnissen beiziehen kann.

Die Mitwirkung des IT-Revisors bei der Abschlussprüfung kann verschieden gross sein: *beratend*, bei kleinen Mandaten mit Systemen von geringer Komplexität; *betreuend*, wenn für die Systemaufnahme und die Testarbeiten zwar keine IT Spezialisten notwendig sind, aber die Beurteilung der Ergebnisse IT-Fachkenntnisse erfordert; *ausführend*, wo Systeme integriert sind und Prozesse und Kontrollen automatisiert durchgeführt werden.

In jedem Fall muss eine enge Zusammenarbeit zwischen Abschlussprüfer und IT-Revisor bestehen. Der IT-Revisor ist sowohl an der Risikobeurteilung und Prüfungsplanung, als auch an der Durchführung beteiligt. Dabei hat der IT-Revisor neben Informatik-Kenntnissen auch Betriebswirtschafts- und Rechnungswesenkenntnisse und Erfahrung aus der Industrie des Kunden. Zusätzlich kennt sich der IT-Revisor mit Prozessrisiken und deren Kontrollen aus.

Systeme in der Wertschöpfungskette



Prüfung einer Gesamtlösung

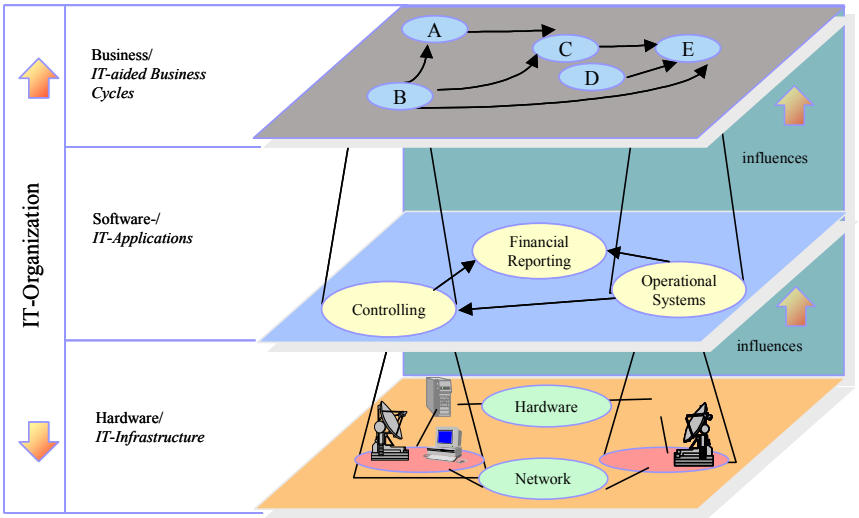
Ein kleineres Versicherungsunternehmen hat für die Abwicklung und Verwaltung seines Geschäfts ein neues Informationssystem entwickelt und eingeführt. Die Applikation umfasst das Underwriting und die Offertstellung, die Policenausstellung, Schadenabwicklung, Rückversicherung und technische Buchhaltung sowie auch die Finanzbuchhaltung.

Der Abschlussprüfer möchte sich bei der nächsten Jahresrevision auf die neuen Prozesse und Kontrollen abstützen können. Die beigezogenen Informatik-Revisoren haben nun die Aufgabe, das neu eingeführte Informationssystem und die Schnittstellen zu Benutzern und anderen Systemen aufzunehmen und zu beurteilen.

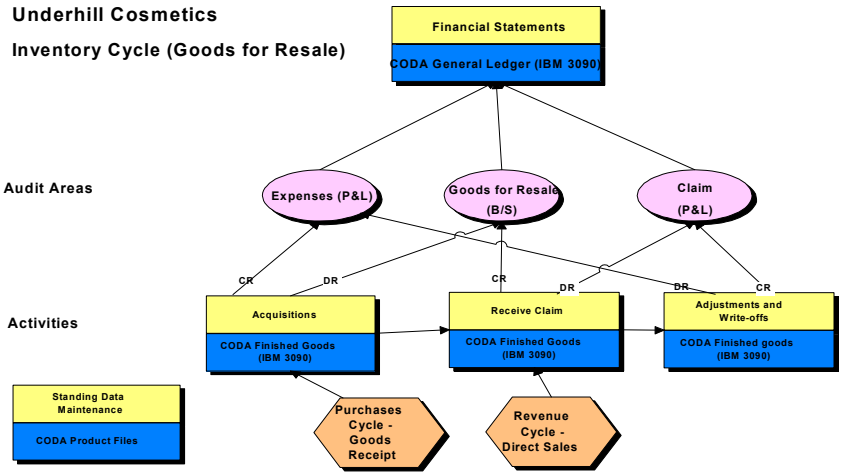
In einem ersten Schritt müssen die wesentlichen Geschäftsprozesse und die Einbindung der Informatik-Mittel verstanden werden. Sodann wird das Interne Kontrollsystem (IKS) aufgezeichnet und die Schlüsselkontrollen bestimmt. Diese werden getestet und die Wirksamkeit des IKS wird beurteilt. Ebenfalls wird durch die IT-Revision die Funktionalität der Applikation in bezug auf das IKS mittels Stichproben und Tests am System getestet. Dabei soll nach Möglichkeit auf die während dem Entwicklungsprojekt bereits durchgeführten Systemtests basiert werden.

Bei neu eingeführten Informationssystemen ist zusätzlich festzustellen, ob der Ausgangsdatenbestand voll-

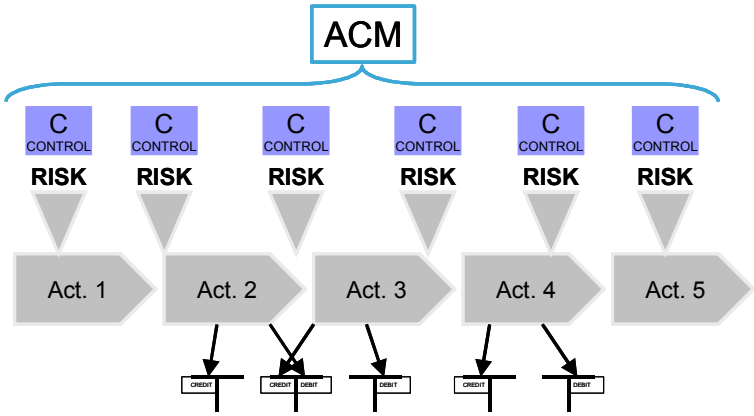
Risikobeurteilung und Prüfungsplanung



Ablauf der Prüfung: Audit Mapping



Ablauf der Prüfung: Audit Comfort Matrix



ständig und richtig ist. Da die Daten in vielen Fällen von Vorgängersystemen migriert werden, kann dies der IT-Revisor mittels automatisierten Verfahren (CAATs) prüfen und eine Aussage dazu machen.

Schliesslich werden die generellen Kontrollen im IT-Entwicklungs- und Produktionsbereich aufgenommen, beurteilt und allenfalls getestet. Dazu gehören auch systembezogene Zugriffskonzepte auf Daten und Funktionen und deren Implementierung.

Ergebnis

Das Ziel einer solchen Systemprüfung ist es festzustellen, dass die Grundsätze ordnungsmässiger Buchführung (GoB) eingehalten werden können. Dies beinhaltet die Umsetzung eines wirksamen IKS sowie die vollständige Aufzeichnung und Verbuchung der verarbeiteten Geschäftsvorfälle. Dem Abschlussprüfer wird dadurch die Möglichkeit gegeben, seine Einhalteprüfungen zu minimieren und damit seine Prüfung effizient durchzuführen.

Wo sinnvoll und möglich, werden durch den IT-Revisor konkrete Vorschläge zur Verbesserung des IKS und zur Sicherstellung der Ordnungsmässigkeit gemacht (z.B. fehlende Kontrollen einzuführen oder bestehende effizienter zu gestalten).

Fazit

Zunehmende Automatisierung von Geschäftsprozessen und Integration von Teilsystemen machen den Ein-

satz von Informatik-Spezialisten in der Abschlussprüfung immer bedeutender. IT-Revisoren helfen dem Abschlussprüfer bei der Risikobeurteilung von Prozessen und automatisierten Systemen und tragen zu einer effizienten Durchführung der Abschlussprüfung bei.

Während die IT-Revision in der Prüfung von Finanzdienstleistungsunternehmen kaum mehr wegzudenken ist, wird die Notwendigkeit des Einbezugs von IT-Spezialisten bei Prüfungen von kleinen und mittelgrossen Unternehmen (KMU) ebenfalls immer deutlicher.

In diesem Sinne ist auch der Standard ISA 401 „Auditing in a Computer Information Systems Environment“ und – in dessen Anlehnung – der von der Kammer neu entwickelte Prüfungsstandard PS 401 „Prüfung im Umfeld der Informations- und Kommunikationstechnologie“ zu verstehen.

Christoph A. Meier,
PricewaterhouseCoopers, Zürich

Professional Judgement in der IT

Intégration de l’audit informatique dans la révision annuelle des comptes (assurances)

Résumé

Recours à des spécialistes

Les systèmes comptables sont de plus en plus automatisés et intégrés à d’autres systèmes gérant les processus métier. Les interfaces entre ces systèmes sont également automatisées et il n’est pas évident d’identifier et de tester les contrôles qui y sont intégrés. Il est donc toujours plus important pour un auditeur financier de pouvoir s’adjoindre les services d’un auditeur disposant de connaissances en informatique.

L’intervention de l’auditeur informatique peut prendre différentes formes, *conseiller* pour de petits mandats et des systèmes de faible complexité, *expert* lorsque la collecte d’information et les travaux de validation ne requiert pas de connaissances informatiques particulières mais qu’une expertise est nécessaire pour tirer les conclusions de ces travaux, *exécutant* lorsque les systèmes sont intégrés et les contrôles automatisés.

Une étroite collaboration entre l’auditeur financier et l’auditeur informatique est dans tous les cas indispensable. L’auditeur informatique participe à l’analyse des risques et à la planification de l’audit. Il doit pour se faire disposer de connaissances économiques et comptables et d’expériences dans le domaine du client. Il apporte également sa maîtrise des risques liés aux processus et des contrôles automatiques.

Audit d’une solution intégrée

Une petite compagnie d’assurance a développé et introduit un nouveau système informatique pour l’ensemble de sa gestion. Cette solution intègre aussi bien la gestion des offres, l’établissement des polices, la gestion des sinistres, la réassurance, que les comptabilités technique et financière.

Le réviseur aux comptes souhaite ces prochaines années pouvoir se fier aux nouveaux processus et contrôles. L’équipe d’audit informatique doit comprendre et évaluer la nouvelle solution ainsi que ses interfaces avec les utilisateurs et les autres systèmes.

Dans un premier temps, les processus métiers et leurs liens avec l’informatiques sont analysés. Le système de contrôle interne (SCI) est ensuite représenté et les contrôles essentiels sont identifiés. Ils sont

testés et l'efficacité du SCI est évaluée. Les auditeurs informatiques examinent et testent également les fonctionnalités de l'application en matière SCI. Ils se fondent dans la mesure du possible sur les tests effectués lors de l'introduction du système.

L'examen de la qualité des données est essentiel pour de nouvelles applications. Ces données proviennent souvent des anciennes applications qui ont été remplacées et le recours aux techniques d'audit assistées par ordinateur (CAAT) permettra à l'auditeur de former son opinion sur la qualité de ces données. Les contrôles généraux de l'environnement informatique (développement, exploitation, etc.) seront enfin identifiés, évalués et testés. L'examen des concepts de droits d'accès ainsi que leur implémentation fait partie de ces travaux.

Résultat

L'objectif de cet examen de système est de s'assurer que les principes relatifs à la tenue régulière de la comptabilité sont respectés. Au nombre de ceux-ci : un SCI efficace, ainsi que l'enregistrement et la comptabilisation complets de toutes les transactions. Le réviseur aux comptes pourra ainsi réduire ses vérifications matérielles et travailler de manière rentable.

Si nécessaire (et possible) l'auditeur informatique formulera des recommandations pour améliorer le SCI et assurer la régularité de la tenue des comptes (par exemple afin d'introduire un contrôle nécessaire ou pour améliorer l'efficacité d'un contrôle existant).

Conclusion

L'informatisation croissante des processus métier ainsi que l'intégration grandissante des différents systèmes rendent le recours à un auditeur informatique toujours plus important. Celui-ci peut assister le réviseur aux comptes et lui permet de travailler de manière efficiente.

Cette évolution qui est déjà entrée dans la pratique quotidienne de l'audit des sociétés financières se fera de plus en plus sentir dans le domaine de l'audit des petites et moyennes entreprises (PME).

La reprise par la Chambre fiduciaire suisse du standard ISA 401 « Auditing in a Computer Information Systems Environment » dans les normes d'audit suisse constitue un pas important dans cette direction.

Christoph A. Meier
PricewaterhouseCoopers, Zürich

eGovernment und Digitale Identität

Wenn im elektronischen Behördenverkehr wichtige und heikle Transaktionen, wie z.B. der Abruf eines Strafregisterauszugs oder Wahlen und Abstimmungen online abgewickelt werden sollen, erhält das sichere gegenseitige Erkennen eine fundamentale Bedeutung. Die Privatperson muss sich über ein Netz wie das Internet einer staatlichen Stelle gegenüber ausweisen können und die Verwaltungsstelle muss diese Online-Person sicher als eine ihr bekannte, bestimmte Person identifizieren können.

Unter den aktuellen technischen Gegebenheiten besteht eine Digitale Identität aus einem PKI-Schlüsselzertifikat, gespeichert auf einer kreditkartengrossen Smartcard. Mit dieser elektronischen Identitätskarte (eID-Karte) kann die besitzende und berechtigte Person drei Grundfunktionen in einer Vielzahl von Anwendungsfällen durchführen:

- Ihre Identität einem System gegenüber beweisen (Authentifizierung);
- Eine Meldung digital signieren (elektronische Unterschrift);
- Eine vertrauliche, speziell für sie verschlüsselte, Meldung entschlüsseln.

eID-Karte und Public Key Infrastructure (PKI)

Die Digitale Identität kann die verlangten Sicherheitsfunktionen aber nur erbringen, wenn sie in ein ganz bestimmtes organisatorisches System – PKI genannt – eingebettet ist. So muss vorgängig eine vertrauenswürdige Instanz die Identität des Schlüsselinhabers, der zu diesem Zweck persönlich vorzusprechen hat, prüfen, die Zuordnung des Schlüssels zu dieser Person im erwähnten Schlüsselzertifikat bestätigen und dieses Zertifikat zudem in einem öffentlich zugänglichen Verzeichnis für Überprüfungen abrufbar halten.

Rechtliche Rahmenbedingungen

Im Einklang mit den europäischen Staaten hat der Bundesrat zuerst die rechtlichen Rahmenbedingungen für die Entwicklung eines Marktes von Zertifizierungsdiensteanbietern geschaffen. Durch Mindestanforderungen für ein Label als „staatlich anerkannter Anbieter“ wird ein Qualitätsstandard definiert, auf dem sich das ganze System von Vertrauen aufbauen kann. Diese Regelungen beinhaltet eine befristete Verordnung aus dem Jahr 2000 und nun das Bundesgesetz über die Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) vom 19.12.2003 (http://www.bj.admin.ch/themen/digsig/intro-d.htm), das am 1. Januar 2005 in Kraft treten wird. Im gleichen Gesetz wird ein neuer Artikel (Art. 15a) ins OR eingefügt, wonach alle Verträge, für die das Gesetz die Schriftform verlangt, künftig mit der anerkannten Elektronischen Signatur auch elektronisch geschlossen werden können. Für die Anwendung im eGovernment wird im Rahmen der Revision der Bundesrechtspflege (http://www.ofj.admin.ch/themen/bgg/intro-d.htm) im Verwaltungsverfahren des Bundes und im Verkehr mit den Bundesgerichten der elektronische Verkehr mit anerkannter Elektronischer Signatur der Schriftform gleichgestellt.

Das Projekt einer staatlichen eID-Karte

Angeregt durch die Bedürfnisse von eGovernment nach einer „Kundenkarte“, das Beispiel anderer Länder und die schwierigen Marktbedingungen für private Zertifizierungsdiensteanbieter stellte sich die Frage, ob der Staat selbst eine eID-Karte herausgeben soll. Im Juli 2002 hat der Bundesrat nach umfangreichen Abklärungen (http://www.ofj.admin.ch/themen/ri-ir/dig-id/intro-d.htm) den Auftrag gegeben, bis Ende 2003 ein Konzept und einen Gesetzesentwurf für eine elektronische Identitätskarte auszuarbeiten. Diese staatliche eID-Karte soll sowohl als konventionelle wie auch als elektronische Identitätskarte eingesetzt werden können und auch den Ausländerausweis ersetzen. Ansonsten sollte sie sich auf die Identität beschränken und keine weiteren Anwendungsdaten – z.B. Gesundheitsdaten – enthalten.

Aufgrund der aktuellen Sparbemühungen und geänderter Prioritäten sind die Arbeiten an diesem Vorhaben auf einen noch zu bestim-

menden Zeitpunkt aufgeschoben. Im Mai 2004 ist im Parlament eine Motion eingereicht worden (04.3228 Motion Noser Ruedi, E-Switzerland. Schaffung einer digitalen Identität), welche vom Bundesrat die speditive Schaffung einer digitalen Identität verlangt.

Einheitlicher oder sektorieller Personenidentifikator

Insbesondere bei einer staatlichen eID-Karte stellt sich die Frage, auf welche Identität sie sich denn genau beziehen soll. Aus organisatorischer Sicht wäre ein eindeutiger Personenidentifikator ideal; ein Nachfolger der heutigen AHV-Nummer, ohne ihre Mängel. Viele Länder, z.B. alle skandinavischen, verfügen über einen solchen Identifikator und verwenden ihn in den staatlichen Registern. In der Schweiz wird die Frage federführend vom Bundesamt für Statistik im Zusammenhang mit der Registerharmonisierung geprüft.

Was bringt die Zukunft

Wir gehen davon aus, dass sich in einer mittelfristigen Zukunft ein System von personenbezogenen Grundzertifikaten auf einer biometrisch abgesicherten Karte und darauf basierenden Attributszertifikaten (z.B. für Vertretungsbefugnisse), die nur als Datei existieren, durchsetzen könnte.

Eine einfache Erklärung all dieser Begriffe und Vorhaben rund um die Digitale Identität findet sich auf der Homepage des EJPD (www.ejpd.admin.ch) unter Themen → Wirtschaft → Elektronische Signatur.

Urs Bürge, Chef Informatik EJPD, Bern

Information Systems Audit and Control Association®
www.isaca.ch

Erlangen Sie weltweite Anerkennung als CISA® oder CISM®

Zwei spannende Kurse!

Informatik-Sicherheit und Informatik-Revision
CISA-Kurs 2004/2005, 17 intensive Tage
November '04 - Mai '05, Schweiz

Management der Informationssicherheit
CISM-Kurs 2004/2005, 13 intensive Tage
Dezember '04 - Mai '05, Schweiz

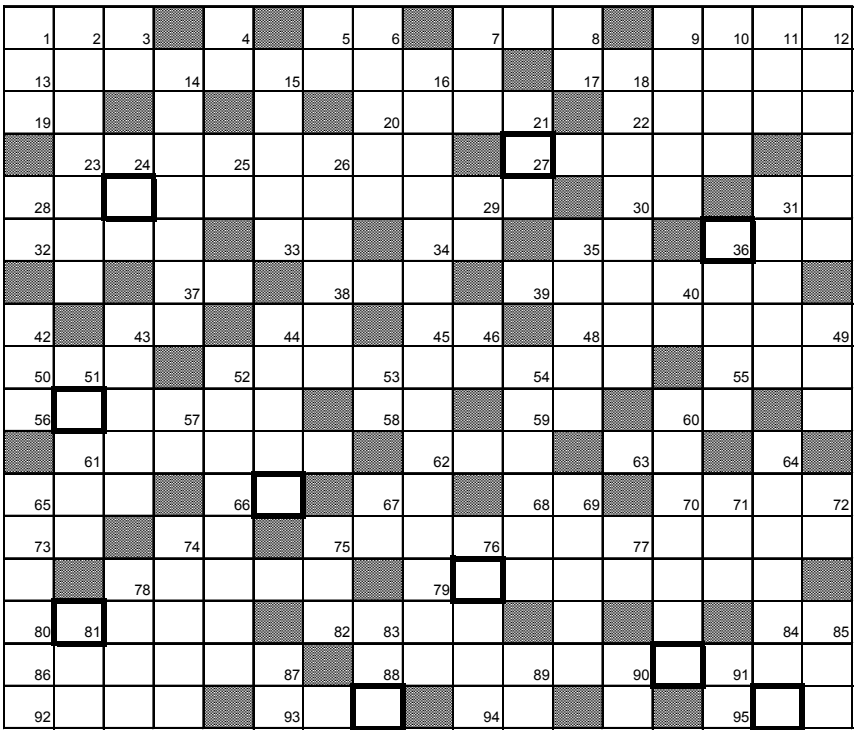
Informationsveranstaltung, 20. Oktober 2004, 18 Uhr
ITACS Training AG , Konradstrasse 1, 8005 Zürich, 1. Stock (bitte anmelden!)

Weitere Informationen erhalten Sie in unserem Kurssekretariat:

ISACA Switzerland Chapter
c/o ITACS Training AG, Konradstrasse 1, 8005 Zürich, Schweiz
kurse@isaca.ch, Tel. 01 440 33 64, Fax 01 440 33 61

The ISACA Crossword Puzzle 4/04

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.



Waagrecht: 1 Ausruf des Verstehens; 5 **AZ, woher auch 52 waagrecht kommt**; 7 Papstname; 9 Axt; 13 hängt in einem vielbesuchten Berner Turm; 17 Spielgerät (Mz); 19 tonloser Teil; 20 Kleidungsstück; 22 frz Komponist (y=i); 23 tilgen; 27 Drehkörper; 28 **bei Revisionen anzutreffende Skrupellosigkeit** (Mz); 30 zwei gleiche Vokale; 31 pers Fürwort; 32 Holzart; 33 AZ aus der Türkei; 34 CZ Radon; 35 früher sagte man PERS; 36 Wachholderschnaps; 37 frz Bindewort; 38 für (lat); 39 unterstützen; 43 CZ Zinn; 44 aromatisches Getränk (span); 45 it Artikel; 48 Frucht (Mz); 50 Bestand; 52 **internationale Vereinbarung**; 55 it Zahlwort; 56 **an der Börse gehandelt** (engl); 58 hohe Spielkarte; 59 Vorwort; 60 AZ aus der Westschweiz; 61 der Erdtrabant im Genitiv; 62 engl Bejahung; 63 sagt jeder Franzose von sich; 65 Blocher verliess es, um Bundesrat zu werden; 66 span Artikel; 67 Rekrutenschule; 68 welsche AG; 70 Drama von Ibsen; 73 CZ Xenon; 74 kurzer natürlicher Logarithmus; 75 **auch bei Revisoren praktizierte Verführung** (Mz); 78 religiöse Abspaltung; 79 **(Daten) erfassen**; 80 Ortsveränderung; 82 Zahnfleisch (engl); 84 launischer Ausruf; 86 hastig; 88 alkoholische Getränkearten; 92 Stange; 93 Gedichtart; 94 Auerochse; 95 Bindewort.

Senkrecht: 1 dem Mediziner fehlt das r; 2 Farbton; 3 Faultier; 4 kurze Wohngemeinschaft; 5 Vorname der Derek; 6 **wenn ein n angehängt wird, trügt er**; 7 frz Artikel; 8 russischer Strom; 9 Delle; 10 Armknochen; 11 flüssig in Vorarlberg und im Elsass; 12 eintönig vortragen; 14 **buchhalterisches Hindernis** (Mz); 15 Helligkeit; 16 **Überwachungsmittel** (Mz); 18 **von vielem etwas, auch bei Revisionen anzutreffen**; 21 Hausflur; 24 skand Münze; 25 AZ aus von ennet dem Rhein; 26 Virusinfektion; 28 Fussballklub; 29 schweizerisches Nass zum Schwarzen Meer; 31 Skiff; 35 in die Höhe bringen; 36 Reitpeitsche; 40 CZ Eisen; 42 verflüssigt (Abk); 43 Ostschweizer Schlachtort; 44 Rüge; 46 Land des amerikanischen Zauberers, auch von Australiern beansprucht; 49 damit wird der kurze Mailänder Fussballclub zum heute alltäglichen Kommunikationsmittel; 51 Total; 52 **kommen oft bei der Revision auf**; 53 babylonischer Erdgott; 54 **sei Macht, sagt man**; 57 kurzer Teilnehmer; 60 aufzuzählen; 64 **auch bei der Buchhaltung Weizen und Spreu auseinandernehmen**; 65 äusserst; 67 König (it); 69 **seine Aufmerksamkeit ist dem Revisor Vorbild**; 71 mit angehängtem r ein frz Menschenfresser; 72 Vorwort; 74 Aufforderung zur kollektiven Buchstabenerkennung; 75 bitten (engl); 76 wenn dies ins als fällt, entsteht der Urbaier auf der Wolke; 77 Umlaut; 78 sowohl im Domleschg als auch im Engadin anzutreffen; 81 kindlicher Ausruf; 83 der unvergessene Seeler; 85 Binde-

wort (engl); 87 Grundton der it Tonleiter; 89 kurze Nummer; 90 frz Gold; 91 halbes Ballettröckchen.

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 xx. Oktober 2004.

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

Lösung 3/04: *Assurance*

Der Gewinner des Lösungswortes ist Daniel Gläser.
Herzliche Gratulation!

Der beabsichtigte Watson war diesmal mehrfach: Ein englisches Lösungswort für ein deutsches Rätsel; Falschnumerierungen waagrecht (69/68) und senkrecht (14/13); eine fehlende Frage bei 44 senkrecht (EITEL). Marc Bucher hat alle entdeckt und damit den Watson-Jackport geleert! Der Autor wird sich bemühen, in Zukunft nur noch einen Watson zu platzieren. Ob es ihm gelingt?

Waagrecht: 1 warm; **4 drahtlos**; 11 Ali; 14 Migrol; 16 Salzseen; 18 RR; 20 grollt; 22 SA: 23 Sn; 24 Tod; 25 Plakatfarbe; 29 f(oo)t; 30 Giseh; 32 SE; 33 Dee; 35 win; 37 (seid einig, Brüder,) einig; 38 Ute; 40 de; 42 Erp; 44 Elfe; 45 surrend; 48 Oehi; 50 etc; **51 Kernkompetenz**; 55 AZV; 56 Edam; **57 Sendung**; 60 eist; 62 Sex; 63 Lt; 64 NLA; 65 Brust; 69 Erg; 70 Goa; 71 Cu; 73 titre; 75 BE; **76 gerichtlich**; 79 Sem; 80 or; 81 hu; 82 Schere; 85 NN; 86 Feingold; 90 Kessel; 92 TTT: 93 Erdbeere; 94 Lohn.

Senkrecht: 1 Wortfluss; 2 RM; 3 Mig; 4 Drops; 5 Roller; 6 Allah; 7 TS; 8 Laster; 9 Olaf; 10 SZ; 11 AE; 12 Lese; 14 Inn; 15 GR; 17 streifend; 19 rot; 21 TK; 26 As; 27 Adel; 28 Benetzung; 30 GI; 31 Inder; 34 ego; **35 Werkzeuge**; 36 Trommel; 39 tu; 41 ennet; 43 Pep; **46 Revisorin**; 47 DKD; 49 hes; 52 OAS; 53 Enter; 54 Agamemnon; 58 NL; 59 Abt; 61 stai!; 66 Schuld; **67 sicher**; 69 re; 72 ut; 73 ticke; 74 These; 75 Ben; 76 Gret; 77 Chor; 78 l(a/o)s; 80 rar; 83 RS; 83 eel; **87 IT**; 89 GE; 90 DB; 91 lo.

Express Line

A Word from the Chair

As the incoming chair of the Membership Board, I would like to welcome all new chapter officers. As many chapters hold elections and change officers during this time of year.

We are pleased to inform you that, in November 2004, ISACA International Headquarters will provide chapters with CISA and CISM pins free of charge. Chapters will receive pins for those fully certified from 1 January 2003 through 31 October 2004, along with a complete list of names/designations. Going forward, these pins will be provided to chapters every November.

Sunil Bakshi
Chair, Membership Board

Certification Update

CISA® and CISM™ Exams Attract Large Numbers

The ISACA Board of Directors and staff wish to thank ISACA chapters, members, and holders of the Certified Information System Auditor™ (CISA®) and Certified Information Security Manager™ (CISM™) designations worldwide for their efforts in supporting and promoting the CISA and CISM designations.

As previously reported, more than 14,000 candidates registered for the CISA exam, representing a nearly 20 percent increase over registrations in 2003, and in only its second year, the CISM exam generated 700 registrants, representing a 160 percent increase over registrations in 2003.

CISA and CISM Exam Results

CISA and CISM exam results will be mailed to candidates at the end of August. Please direct specific inquiries to ISACA International Headquarters at
certification@isaca.org
or +1.847.253.1545, ext. 471 or 474.

CISA Job Practice Analysis

Work continues on a CISA job analysis study to update the areas, task statements and knowledge statements used to certify and examine CISA candidates. This past month a focus group meeting was held in Boston, Massachusetts, USA, and was attended by ISACA members from around the world. The input from this meeting, and similar meetings held in Chicago, Illinois, USA, and Zurich, Switzerland, will be used to update the draft delineation earlier compiled by the CISA practice analysis task force. Next, there will be a series of subject expert reviews and, later in the year, approximately 3,000 CISAs will be surveyed.

Review Manuals

The CISA and CISM review manuals for the 2005 exam are currently being revised and updated. Numerous volunteers from around the world are participating in each project.

News Briefs

New IT Governance Education Program

The IT governance education program (slides and talking points) for chapters – in English and Spanish – was created by the ITGI Steering Committee as a benefit for ISACA chapters and members, as a way for chapters to offer their members low-cost education and a means to help communicate basic IT governance principles. The program covers the basics of IT governance:

- What it is
- What its components are
- Who is responsible
- Why it is important

This education program is based on the ITGI's *Board Briefing on IT Governance, 2nd Edition*, which is available from the ISACA Bookstore at www.isaca.org/bookstore.

Research Projects in Progress With Target Release Dates

- Cybercrime: Incident Response and Digital Forensics Services – third quarter 2004
- Managing Risk in the Wireless LAN Environment: Security, Audit and Control Issues – third quarter 2004

■ Managing Enterprise Information Integrity: Security, Control and Audit Issues – third quarter 2004
■ Linux Security and Control Features– third quarter 2004

Research Projects

COBIT Security Baseline

This guide is based on COBIT, which is a comprehensive set of resources that contains the information organizations need to adopt an IT governance and control framework. COBIT covers security in addition to all the risks that may occur with the use of IT. This guide focuses on the specific risks of IT security in a way that is easy to follow and implement for all users – small to medium enterprises, executives and board members of larger organizations as well as home users. This document is available for a limited time as a complimentary, member- and CISM-only download at www.isaca.org/cobitsecuritybaseline.

COBIT *Security Baseline* provides:
■ Useful reading:
– An introduction to information security – what does it mean and what does it cover?
– An explanation of why security is important, with examples of the most common things that can go wrong
– Thought-provoking questions to help determine the risks
■ The COBIT-based security baseline, which includes key controls
■ Six information security survival kits, with essential awareness messages for specific audiences
■ An appendix containing a summary of technical security risks

IT Control Objectives for Sarbanes-Oxley

The updated ITGI document is now available in the ISACA Bookstore for US $5 per printed copy. *IT Control Objectives for Sarbanes-Oxley* is also available as a complimentary download on both the ITGI and ISACA web sites (www.itgi.org and www.isaca.org). For convenience, ISACA members also have access to the appendices in Microsoft Word format on the ISACA web site.

ITGI first issued *IT Control Objectives for Sarbanes-Oxley* as a discussion document in the third quarter of 2003. It covered the importance of IT within the Sarbanes-Oxley compliance process. The positive responses received, as well as the number of new articles, web sites and third-party presentations that have referenced the document and its message, have served to meet the objective of the project – to provide IT-related guidance for Sarbanes-Oxley compliance.

The responses to the discussion document resulted in many enhancements to the new edition. This latest release addresses these suggested revisions, as well as the PCAOB pronouncement in March 2004.

Forum

Am letzten Tag des ersten Halbjahres 2004 fand in den heiligen Hallen des Landesmuseums in Zürich das erste After-Hour-Seminar des ISACA Switzerland Chapters statt. Bruno Wiederkehr präsentierte seine Ansichten zum Thema ICT-Risikomanagement. Dabei konnte er aus seinem Erfahrungsschatz bei seinen Tätigkeiten als Informatikrevisor schöpfen, bei welchen er zu diesem Thema verschiedentlich recht erfolgreich intervenierte. Er warnte davor, sich „wie wild" auf eine Risikoanalyse zu stürzen und gefährliche Geldbewertungen zu veranstalten (obschon diese bei den Verantwortlichen den nachhaltigsten Eindruck hinterlassen), sondern zuerst eine sorgfältige Vorbereitung zu treffen: „Understanding the Business" – ein altbekanntes und bewährtes Revisionskonzept. Interessant waren auch seine Ausführungen hinsichtlich Risiko*vergrösserung* – ein für Revisoren nicht sehr bequemes Konzept. Der Besuch der After-Hour-Seminare kann nur empfohlen werden. Auch wegen des Contact Hour Credits:

22.9., 20.10. und 17.11. 2004 jeweils 16:30 Uhr, Salon Bleu, Landesmuseum Zürich.

Nun, warum erscheint dieser Beitrag im Forum? Es ist das „C". Ich stosse mich daran. Nachdem der Ausdruck „EDP" (Electronic Data Processing) vor zwei Jahrzehnten durch „IT" (Information Technology) abgelöst wurde, stelle ich fest, dass ein „C" eingefügt wurde, das für „Communication" stehen soll. Ich persönlich finde dies eher überflüssig:

- Erstens wird durch die Hervorhebung der Eindruck erweckt, die Kommunikation als solche sei Thema der Betrachtungen. Dabei handelt es sich aber doch nur um jene des *elektronischen* Datenverkehrs in Computernetzwerken, oder? Die Kommunikation als solche war schon lange da, bevor es Computer auch nur auf dem Reissbrett gab.
- Zweitens ist unklar, ob der gewöhnliche Telefon- und Funkverkehr (zu Deutsch: Voice Mail) im neuen Begriff eingeschlossen ist oder nicht. In jenem Fall müsste auch die konventionelle Kommunikation in die Betrachtungen eingeschlossen werden, denn Verletzungen von Vertraulichkeit z.B. sind auf diesem Weg schneller und schlimmer begangen, als auf der elektronischen Schiene.
- Drittens beinhaltet gemäss meinem Verständnis der Ausdruck Information Technology bereits auch eben diesen elektronischen Datenverkehr. So, what's new? Ich bin dafür, das „C" wieder zu eliminieren.

Was meinen Sie? Alles nur Semantik, Schall und Rauch?

Max F. Bretscher

P.S. Das nächste Thema am After-Hour-Seminar ist übrigens ITIL, nicht ICTIL…

DACH-News

D:

Die Linux Audit Group – ein Erfahrungsbericht

Es fing alles damit an, dass ich bei einem bekannten Linux-Distributor anrief, um mich nach möglichen Unterstützungsmaßnahmen (z.B. Prüfungsleitfaden, Prüfprogramme etc.) für Revisoren zu erkundigen. Ich hatte mir nicht allzu große Illusionen über die zu erwartende Hilfe gemacht, aber es kam noch ärger: „Ein DV-Revisor? IT-Auditor? Was ist das denn, was machen Sie denn da so?“ Diese Rückfrage kam nicht nur einmal, sondern war über verschiedene Stationen und auch bei anderen Distributoren der durchgehende Tenor. Auch der Hinweis auf unseren Berufsverband brachte den Gesprächspartnern offensichtlich wenig Erhellung.

Da müsste was getan werden, und so wurde in Absprache mit dem Vorstand der Punkt bei der anstehenden Jahresmitgliederversammlung zur Sprache gebracht. Eigentlich war meine Vorstellung, dass es eine Art „Beauftragten“ des Chapters geben sollte, der als offizieller Repräsentant vielleicht leichter den Kontakt zu den maßgeblichen Institutionen knüpfen kann. Nun, vorgetragen und für gut befunden – ja, und schon hatte ich den Auftrag des Vorstands, eine Workgroup zum Thema zu gründen und die Sache voranzubringen.

Eine Workgroup hat ihrem Namen nach mehrere Mitglieder, und da fing das Problem natürlich an. Nun, zunächst waren wir zu Dritt, eine Art Triumvirat, das wie im alten Rom auszog, um große Taten zu tun. Die Praxis setzt diesem hehren Wunsch natürlich schnell Grenzen; aber immerhin hatten wir auf unser erstes Schreiben mit „offiziellem“ Briefkopf an einen großen süddeutschen LINUX-Distributor eine erste positive Resonanz. Es folgte ein freundliches Telefongespräch und die Vereinbarung eines festen Ansprechpartners für Fragen der Workgroup.

Auch dem Namen nach sollte die Workgroup etwas mit Work, also mit er*arbeiten* zu tun haben. Eine erste Idee war – naheliegend – die Erstellung eines Prüfungsleitfadens, einer Art Handbuch für die Kollegen, die nicht unbedingt LINUX-Experten sind, wohl aber im konkreten Fall ein solches System prüfen müssen. Drucklayout, Verteilung des Handbuchs, Austauschdienst, das waren allerdings alles Punkte, die für unsere kleine Gruppe nicht besonders gut zu handeln waren. Daher kam dann schnell der Gedanke, dieses Handbuch in eine Webseite zu packen, mit der die vorgenannten Probleme nicht verknüpft sind. Gesagt – getan, und so begannen wir im Sommer 2003 bei tropischen Temperaturen, eine Webseite aufzubauen, nach und nach Gliederungselemente zu entwickeln und diese mit Texten zu füllen. So werkelten wir bis Ende 2003 – meist im feierabendlichen Mailverkehr – fleißig vor uns hin; da inzwischen die Gruppe auf 6 Mitglieder angewachsen war, konnte auch der Input verstärkt werden, und unsere browserbasierte Prüfungshilfe wuchs heran.

Nun sollte es ja nicht schädlich sein, sich über die elektronische Kommunikation hinaus auch persönlich kennen zu lernen, und so verabredeten wir ein erstes Treffen in der Frankfurter Niederlassung einer großen WP-Gesellschaft. Anfang Februar ging es dann dort mit vereinten Kräften und konzentriert an den letzten Schliff unserer LINUX-Prüfungshilfe, damit wir diese zur Mitgliederversammlung Anfang März vorstellen konnten. Es zeigten sich bei der Diskussion natürlich die unterschiedlichen beruflichen Werdegänge und Kenntnisstände; dies sollte sich aber nicht als Hindernis, sondern eher als Bereicherung, erweisen. So ist es von großem Nutzen, in einer Workgroup Kollegen mit vertieftem technischen Know-how zu haben, die auch in der Lage sind, die „internen“ Zusammenhänge in einem Betriebssystem zu verdeutlichen. Aber auch Kollegen mit langjähriger Prüfererfahrung, die ein Verständnis für die Kommunikation und den Transfer von Informationen zum Geprüften aufweisen, bereichern die Entwicklungsarbeit, da man schließlich ein Werkzeug aufbauen möchte, dass von möglichst vielen Kollegen angenommen und verstanden wird.

Alles in allem, am 12. März 2004 war es dann soweit, und ich durfte das Ergebnis der Gruppe den anwesenden Mitgliedern vorstellen. Da unsere Prüfungshilfe (Linux Audit

Aid) weitgehend Gnade vor den gestrengen Augen von Vorstand und Mitgliedern fand, ist sie nun für jedermann (und jederfrau) als Prüfungshilfe auf der Webseite des ISACA aufrufbar. Sollte damit dem einen oder anderen Kollegen in einer Prüfungssituation geholfen sein, ist genau das erreicht, was wir beabsichtigt hatten, und dies würde uns natürlich sehr freuen.

Ein Fazit? Aller Anfang ist schwer, dies hat sich auch in unserer Gruppe bewahrheitet. Aber es hat sich vor allem gezeigt, dass man zusammen wirklich etwas schaffen kann, und das es höchst befriedigend ist, gemeinsam etwas zu entwickeln, dass dem Sinn eines Berufsverbandes Ausdruck verleiht: Gegenseitige Hilfe und Unterstützung im Kollegenkreis.

Ich kann dies als Anregung nur so weitergeben, und fände es toll, wenn wir uns – vielleicht schon zur nächsten Mitgliederversammlung – mit der Windows-Workgroup, der Oracle-Workgroup, der Novell-Workgroup, CISCO-, Firewall-, und … weiteren Kollegen, die sich ein Herz gefasst haben („da machen wir mit“) und eine Workgroup gegründet haben, unterhalten könnten.

Ingo Struckmeyer

CH:

Wir gratulieren Urs Fischer

Wir haben folgende Mitteilung erhalten, sind stolz und gratulieren Urs Fischer für die anspruchsvolle Aufgabe:

As a membership-based organization, ISACA is dependent on the quality and quantity of the contribution made by a large number of volunteers. In preparation for each new administrative year, the “Call for Key Board and Committees Volunteers” is sent to the general membership soliciting their applications to serve on the Association/ ITGI key boards and committees.

Based on these applications and recommendations from the Boards of Directors/Trustees, Key Board Chairs, and appropriate Chapter Presidents, the composition of each key board or committee is finalized and a balance sought between continuity of membership and the need for new vitality.

> It is with great pleasure that Marios Damianides, 2003-05 International President, invites you to serve on the Audit Committee for the upcoming administrative year.

In order for us to formalize your appointment, please signify your willingness to serve by replying to this e-mail.

You will soon be receiving various orientation materials from Scott Artman, the staff liaison assigned to this board. Included will be goals for the upcoming year, meeting/conference call schedules, minutes from previous meetings, and various other information to assist you throughout your 2004-05 year of service.

Best regards,

Monica Love
Executive Assistant to the CEO
Information Systems Audit and Control Association
IT Governance Institute

CISA/CISM Club

Liebe CISA/CISMs

In der Vergangenheit wurden jeweils Besichtigungen organisiert (Telekurs, Kriminalmuseum). Wer würde an der Besichtigung des Fernsehstudios SRG SSR idée suisse in Zürich teilnehmen?

Termin Donnerstag, 4. November 2004, 17.30 h

Falls ich bis zum 31. September 2004 nicht zwölf Anmeldungen erhalte, werden ich die Führung absagen müssen.

thomas.bucher@ch.ey.com

CISA/CISM-Koordinator
Thomas Bucher

Rückblick und Ausblick

Das ISACA After Hour Seminar vom 30. Juni 2004 hatte ICT-Risikomanagement zum Thema. Die Präsentation fand im modern eingerichteten Konferenzraum des Landesmuseums in Zürich (direkt neben dem Hauptbahnhof) statt.

Es wurden u.a. auf die folgenden Fragen eingegangen:

- Wie ist ein unternehmensweites Risikomanagement zu gestalten?
- Wer ist für den Risikoprozess verantwortlich – Business und ICT?
- Welche Aufgaben sind bei der Bewirtschaftung von ICT-Risiken massgebend?
- Welche Mittel, Methoden und Verfahren werden für die Beurteilung eingesetzt?
- Wie kann eine wirtschaftliche und wirksame Umsetzung sichergestellt werden?

Beim anschliessenden Apéro konnten sich die Teilnehmenden (auch Nicht-Mitglieder) näher kennen lernen und Erfahrungen austauschen.

Weitere Daten sind:

- 22. September 2004: ITIL, the Key to Operational Excellence, Martin Andermatten, Gastreferent
- 20. Oktober 2004
- 17. November 2004

Reservieren Sie sich bereits heute die Seminardaten, jeweils um 16.30–18.00 Uhr, Landesmuseum Zürich. Auch Nicht-Mitglieder der ISACA sind gegen einen kleinen Unkostenbeitrag (CHF 50.–) herzlich willkommen. Zusätzliche Information können der ISACA-Homepage entnommen werden. Die Anmeldungen sind an das ISACA-Kurssekretariat zu richten (siehe Kontaktadressen).

Bruno Wiederkehr, ISACA, Erlenbachs

After Hour Seminar vom 25. August 2004: Design a Self-Assessment Tool

Am bereits bekannten Ort im Landesmuseum Zürich trafen sich rund 20 Teilnehmer zum zweiten After Hour Seminar dieses Jahres. Ich kann nur sagen:

Die Abwesenden haben etwas verpasst!

Michel Huissoud präsentierte seine Erfahrungen als Moderator in einem Seminar der obersten Rechnungskontrollbehörden (SAI = Supreme Audit Institution) von Europa in Paris. Es ging darum, dass diese Institutionen (in der Schweiz: Eidg. Finanzkontrolle) sich zum Ziel gesetzt haben, ihre Tätigkeiten zu messen, zu vergleichen und zu optimieren.

Erkenntnisse:

- COBIT eignet sich ausgezeichnet für eine solche Übung.
- Neben COBIT muss aber gleichwertig eine Liste der Geschäftsprozesse (für jede Institution natürlich individuell) erstellt werden.
- Die Kombination von COBIT und Geschäftsprozesse kann in unterschiedlicher Tiefe vorgenommen werden (Michel empfiehlt je acht bis zehn Kernelemente).
- In der Selbstbeurteilung empfiehlt sich eine Kombination von Fragebogen und Workshops, damit unterschiedliche Meinungen in den (vorher unbekannten) Fragebogen an die Oberfläche gelangen und die Meinungsunterschiede in den Workshops besprochen und bereinigt werden können.
- Die gemeinsame Grundlage ermöglicht ein illustratives Benchmarking, das seinerseits zu einer Optimierung beiträgt.
- Grundsätzlich könnte jede Firma, jedes Unternehmen, jede Organisation eine solche Selbstbeurteilung bewerkstelligen.

Ich kann die Teilnahme an den After Hour Seminaren wärmstens empfehlen. Die an die Präsentationen anschliessenden Gespräche und Kontakte beim Apéro sind eine grossartige Ergänzung zu den vorgetragenen Themata.

Max F. Bretscher, CISM, CISA

ISACA Switzerland Chapter Website erhält einen Award für ihre Website!

Das ISACA Membership Board hat die hervorragend gestaltete Switzerland Chapter Website mit dem Silver Level Award ausgezeichnet. Der Award kann unter unserer Website

http://www.isaca.ch/ eingesehen werden.

Der Vorstand dankt Caroline M. Glauser der ITACS Trainings AG als Gestalterin unserer Website ganz herzlich für ihre Arbeit und gratuliert zu diesem Award.

CISA- oder CISM-Prüfung im 2004 in Zürich absolviert und erfolgreich bestanden?

Wir möchten Sie noch zu unserem CISA/CISM-Essen am Mittwoch, **20. Oktober 2004** einladen.

Bitte melden Sie sich bei unserem CISA/CISM-Koordinator Thomas Bucher unter tbucher@deloitte.com bis am 17. September 2004, wenn Sie am Abendessen teilnehmen möchten (Platzanzahl ist beschränkt).

Ort: Au Premier, im 1. Stock des Hauptbahnhofs in Zürich

Zeit: Ab 18.30 Apéro (Da Capo Bar) und ab 19.30 das Abendessen

Alle anderen CISAs und CISMs sind auch herzlichen zum Abendessen eingeladen, müssen das Essen/Trinken aber selbst bezahlen.
CISA/CISM Koordinator Thomas Bucher
tbucher@deloitte.com

Information Systems Audit and Control Association®

www.isaca.ch

Alle Kurse mit hohem Labor-Anteil

Drei spannende Kurse!

PRINCE2™
Planung und Organisation mit flexibler Projektmanagement-Methode
20. -22. September 2004 in Zürich

Internet Security Lab
Angriffsszenarien und Abwehrmassnahmen
28. - 30. September 2004 in Zürich

ITIL Business Continuity
Von Business Continuity zur IT Disaster Recovery auf der Basis des de facto-Standards ITIL
25. - 27. Oktober 2004 in Zürich

Weitere Informationen erhalten Sie in unserem Kurssekretariat:

ISACA Switzerland Chapter
c/o ITACS Training AG
Konradstrasse 1, 8005 Zürich, Schweiz,
kurse@isaca.ch, Tel. 01 440 33 64, Fax 01 440 33 61

News aus den Interessengruppen

IG Operational IT-Risk/Basel II

Neu!

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

Interessenten melden sich bitte bei Peter R. Bitterli

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

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

Programme 2004 :
La séance suivante aura lieu le 16.11.2004.

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

How closed is a Closed user group ?

Quelques personnes travaillant dans des banques cantonales ou des institutions para-étatiques ont demandé à pouvoir participer aux travaux du IG Government IT-Audit. Ces demandes ont malheureusement dû être repoussées pour les raisons suivantes : les communes, les cantons et la Confédération ont des processus communs et transversaux. Le but premier de ce groupe est d'analyser les risques de ces processus et d'organiser des audits conjoints des systèmes informatiques qui les gèrent. Cet objectif implique une confidentialité des travaux qui n'est pas compatible avec une ouverture du cercle des participants au-delà du « Konzern ». Les membres du groupe s'engage en revanche activement dans les différents groupes ERFA de l'ASAI/SVIR traitant d'audit informatique et y présentent leurs méthodes et expériences. Ces plate formes sont mieux adaptées aux demandes présentées.

Michel Huissoud

IG Computer Forensics

Nouveau!

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

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

IG Einführung von IT-Governance

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

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

Nächste Sitzung: Die für den 6. Mai 2004 vorgesehene Sitzung musste leider verschoben werden. Es wird ein neuer Termin festgelegt.

Traktanden:

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

IG Romandie

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

IG Outsourcing/Insourcing

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

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

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

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

IG MIS/EIS/DWH

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

Letzte Sitzung: Freitag, 16. Januar 2004, bei Ernst & Young AG, Zürich

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

Nächste Sitzungen: Für Informationen melden Sie sich bitte bei Daniel Oser.

IG SAP R/3

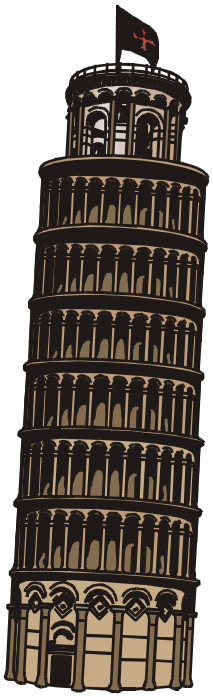
Monika E. Galli Mead
Eidg. Finanzkontrolle
Monbijoustrasse 51a
3003 Bern
Tel. +41 31 324 9495
Fax. +41 31 323 1101
monika.galli@efk.admin.ch

Letzte Sitzung: Donnerstag, 13. Mai 2003

Nächste Sitzung: Gemäss Protokoll der Sitzung vom 13. Mai 2004

Ein italienischer Computerfreak lebte am schiefen Turm in Pisa.
Er war unsterblicherweise verliebt in ein Internet-Girl namens Lisa.
Er schrieb ihr vom gemeinsamen Glück.
Sie aber wies ihn schroffstens zurück:
„Du bist mir zu wenig, nicht einmal CISM, geschweige denn CISA."

A globally operating auditor had in his sleep a wonderful vision:
All his clients had made for a million dollars a favorable decision.
He traveled around the globe ten thousand times.
And claimed to have found just as many crimes.
The regulatory agency put him immediately under supervision.



Veranstaltungen

Zweite deutsche IT Governance Konferenz 2004	13./14. September 2004 Berlin, 2 Tage, ISACA/marcevans
RACF – Info-Workshop für Revisoren	14.–16. September 2004 Ingelheim am Rhein, 3 Tage, F-IT
Symposium on Privacy and Security	15./16.September 2004 Zürich, 2 Tage, infosec
Basel II	17. September 2004 Zug, 1 Tag, infoGuard
PRINCE2 – Planung und Organisation mit flexibler Projektmanagement-Methode	20.–22. September 2004 Zürich, 3 Tage, ISACA CH/promavis
ITIL, the Key to Operational Excellence (After Hour Seminar im Landesmuseum)	22. September 2004 Zürich, ISACA CH
Internet Security Lab – Workshop mit Angriffsszenarien und Abwehrmassnahmen	28.–30. September 2004 Zürich, 3 Tage, ISACA CH
Sarbanes-Oxley – A Road Map top Compliance	7./8. Oktober 2004 London, 2 Tage, MIS
Service Management – ITIL Foundation Training Auf der Basis de facto-Standards ITIL mit Links zur BS 15000 Zertifizierung	18.–20. Oktober 2004 Zürich, 3 Tage ISACA CH/glenfis
IT-Security Area, SYSTEMS 2004	18.–22. Okt. 2004, Neue Messe München
Demonstrating the Value of IT in the 21st Century	24./25. Oktober 2004 London, 2 Tage, ITGI
ITIL Business Continuity and IT Service Continuity	25.–27. Oktober 2004 Zürich, 3 Tage, ISACA CH/glenfis
Thema noch offen: siehe www.isaca.ch (After Hour Seminar im Landesmuseum)	20. Oktober 2004 Zürich, ISACA CH
ITIL Business Continuity and IT Service Continuity Von Business Continuity zur IT Disaster Recovery auf der Basis des de facto-Standards ITIL	25.–27. Oktober 2004 Zürich, 3 Tage, ISACA CH/glenfis
How to Auddit SAP R/3 Basis	9.–12. November 2004 London, 4 Tage, MIS
Thema noch offen: siehe www.isaca.ch (After Hour Seminar im Landesmuseum)	17. November 2004 Zürich, ISACA CH
Network Security Conference	15.–17. November 2004 Budapest, 3 Tage, ISACA Intl.
CISA Vertiefungskurs	26. November 2004–23. Mai 2005 Zürich, 17 Tage, ISACA CH/ITACS
CISM Vertiefungskurs	3. Dezember 2004–24. Mai 2005 Zürich, 13 Tage, ISACA CH/ITACS

Kontaktadressen Veranstalter

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Germany Chapter

Vereinsadressen

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

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

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

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

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

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

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

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

Austria Chapter

Vereinsadressen

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

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

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

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

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

CISA-Koordinator
Mag. Maria Rieder
Münze Österreich AG
Am Heumarkt 1
1010 Wien
Tel: +43 1 71715-0
maria.rieder@aon.at

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

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

Switzerland Chapter

Vereinsadressen

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

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

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

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

CISA/CISM-Koordinator
Thomas Bucher
Deloitte & Touche AG
Klausstrasse 4
8034 Zürich
Tel. +41 44 421 64 22
Fax. +41 44 421 66 00
tbucher@deloitte.com

Sekretär
c/o Präsidentin

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

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

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

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

Homepage ISACA Switzerland Chapter: www.isaca.ch