Nr. 73 | Februar 2005

Schwerpunkt-Thema:

Sarbanes Oxley Basel II

Inhaltsverzeichnis

Editorial 4

Sarbanes Oxley/Basel II – Ein Meilenstein der Bankenregulierung 5

Sarbanes Oxley/Basel II – Nouveaux Règlements 6

Sarbanes Oxley/Basel II – SOX IT S404 in Novartis 7

Sarbanes Oxley/Basel II – Mit den Augen des Unternehmensstrafrechts: Welche Bedeutung haben der Sarbanes-Oxley Act & Co.? 9

Sarbanes Oxley/Basel II – SOX IT: The Challenge beyond Compliance 11

Sarbanes Oxley/Basel II – Bestmögliche IT-Unterstützung für Corporate Governance durch mySAP ERP 12

Sarbanes Oxley/Basel II – Basel II und die IT 13

Forensic – IT-Unterschlagungsprüfung 14

The ISACA Crossword Puzzle 18

Express Line 22

Forum 23

DACH-News 24

Veranstaltungen 30

Vereinsadressen 33

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: IT-Measurement):
April 2005, Redaktionsschluss: 14. März 2005

Editorial

Die drei Säulen von Basel II

Basel II baut auf drei sich ergänzenden Säulen auf. Die erste Säule knüpft an Basel I an und regelt die Mindestkapitalanforderungen. Die Bestimmungen der zweiten Säule haben die Überwachung des Risiko- und Kapitalmanagements durch die nationalen Aufsichtsbehörden im Brennpunkt. In der dritten Säule sind die Offenlegungspflichten der Banken enthalten.

Aus Sicht der IT und der potentiellen Kreditnehmer ist die erste Säule von Bedeutung. Dabei gelten neue Bemessungsansätze, wogegen die Einschätzung des Marktrisikos gegenüber Basel I unverändert bleibt. Ganz neu ist hingegen die Einschätzung des ***Operationellen Risikos***.

In der heutigen Umwelt ist der Einsatz der IT für Betriebe aller Arten und Grössenordnung wesentlicher Bestandteil der Operationen. Viele dieser Betriebe können ohne IT nicht funktionieren, vom Überleben ganz zu schweigen. Die Beurteilung dieses Risikos ist demnach für Kreditnehmer und Kreditgeber von erheblicher Bedeutung.

Wie schätzt nun eine Bank das Operationelle Kreditrisiko eines potentiellen Kreditnehmers ein? Bei nach Swiss GAAP FER, IFRS oder US GAAP abschliessenden Firmen wird eine solche Beurteilung aufgrund der im Geschäftsbericht veröffentlichten (und vom externen Revisor geprüften) Informationen „vom Pult aus“ einigermassen möglich sein. Bei der Vielzahl der „kleinen“ potentiellen Kreditnehmer dagegen liegen selten einschlägige Berichte (z.B. bezüglich Ordnungsmässigkeit und Kontinuität der Operationen) vor. Hier liegt m.E. ein erhebliches Potential an Beratungs- und Begutachtungsleistung für uns Informatikrevisoren vor.

Sind sich Banken und potentielle Kreditnehmer sich dessen bewusst?! Wir selber?!

Max F. Bretscher

Les trois piliers de Bâle II

Le concept de Bâle II est fondé sur trois piliers. Le premier reprend Bâle I et traite des exigences minimales en matière de capital propre. Le second se concentre sur la surveillance par les autorités nationales de la gestion des capitaux et des risques. Le troisième traite des exigences des banques en matière de transparence.

Le premier pilier est essentiel pour l’informatique et les débiteurs potentiels. Si les nouvelles règles de calcul reprennent sans modification l’estimation du risque de marché telle que Bâle I la prévoyait, il n’en est pas de même du ***risque opérationnel***.

L’informatique est aujourd’hui partie intégrante de la plupart des entreprises et peu d’entre elles pourrait survivre sans elle. L’estimation de ce risque informatique, intégré dans le « risque opérationnel », occupe désormais une place centrale dans l’examen des demandes de crédit.

Comment une banque estime-t-elle le risque de crédit opérationnel d’un débiteur potentiel ? Pour les entreprises qui se soumettent aux Swiss GAAP RPC, aux IFRS ou aux US GAAP, ce point sera compris dans le rapport de gestion (qui sera examiné par l’auditeur externe). Il sera ainsi possible de procéder à un examen « sur dossier ». Pour les autres entreprises, les « petits » débiteurs potentiels, pas de rapports externes, pas d’attestations de la régularité et de la continuité des opérations informatiques par un auditeur qualifié. Un domaine dans lequel il existe aujourd’hui un réel besoin, qui n’est pas couvert par le marché de l’audit et du conseil d’entreprise !

En sommes-nous conscients ?

Max F. Bretscher

Sarbanes Oxley/Basel II

Ein Meilenstein der Bankenregulierung

Das Kreditwesen der letzten Jahre hat im Bereich Risikomanagement – gerade in der Schweiz – grosse Fortschritte erzielt. Mit der Entwicklung von bankinternen Ratingsystemen und der dadurch stark verbesserten Identifikation und Messung der Risiken wurde der Grundstein für tiefgreifende Veränderungen im Kreditgeschäft gelegt.

Die Steuerung des Kreditportfolios nach Risikogesichtspunkten ist heute weit verbreitet, ebenso die Ausrichtung des Kreditzinssatzes nach der individuellen Kreditfähigkeit des Schuldners. Der Umgang der Banken mit Risiken ist effizienter geworden.

Mit dem raschen Wandel der Finanzmärkte und des Risikomanagements der Finanzinstitute nicht mitgehalten hat allerdings die Bankenregulierung. Die 1988 im Rahmen von Basel I eingeführten, noch weitgehend risikointensiven, Eigenkapitalvorschriften sind überholt. Die Revision – Basel II – tut Not.

Zukünftig steht den Banken für die Berechnung der regulatorischen Eigenmittelunterlegung von Kreditrisiken ein Menü von Ansätzen offen. Dabei sind grundsätzlich immer dieselben Faktoren relevant: Forderungsklasse (z.B. KMU-Kredit, Privathypothek), Kreditnehmerrating, eingebrachte Sicherheiten. Doch können Banken mit einem fortschrittlichen, die hohen Anforderungen der Regulatoren erfüllenden, Risikomanagement das geforderte Mindesteigenkapital stärker an den effektiven Risiken ausrichten und vermehrt Techniken der Kreditrisikominderung berücksichtigen.

Ob und in welchem Ausmass sich ein verändertes Eigenkapitalerfordernis auf die individuellen Kreditzinssätze niederschlägt, hängt wesentlich vom Risikomanagement einer Bank und von den Kräften auf dem Kapitalmarkt ab. Bei den Schweizer Finanzinstituten wurde mit den Fortschritten im Kreditrisikomanagment der letzen Jahre vieles von Basel II vorweggenommen. Die Auswirkungen der neuen Richtlinien dürften sich deshalb in Grenzen halten. Namentlich für viele Firmenkunden ist kaum mit veränderten Kreditkonditionen infolge des zukünftigen Eigenmittelerfordernisses zu rechnen.

Dies einerseits, weil (grössere) Banken ihre Eigenmittelunterlegung schon heute weniger nach regulatorischen als nach ökonomischen Gesichtspunkten gestalten und dies – neben Risikoprämien – in ihren Kreditsätzen entsprechend berücksichtigen. Andererseits bewegen sich die meisten Kunden im mittleren Bonitätsbereich, wo das zukünftige regulatorische Kapital im Rahmen der heutigen Anforderungen liegt. Überdies sieht Basel II bei kleinen und mittleren Unternehmen (KMU) unter bestimmten Voraussetzungen eine niedrigere Eigenmittelunterlegung vor.

Mit Entlastungen darf gegebenenfalls bei den Privatkrediten gerechnet werden, da in der geltenden Regelung die Eigenmittelvorschriften für die relativ sicheren Kredite eher zu hoch sind. Dies führt nicht zuletzt zu einer Verschärfung des Wettbewerbs um Kunden mit geringem Risiko.

Mit Basel II werden Ratings für Firmenkunden weiter an Bedeutung gewinnen. Dadurch werden Unternehmen vermehrt auf ihre Markt- und Zukunftsfähigkeit geprüft sowie deren Finanzierung stärker auf Risiko- und Rentabilitätsaspekte ausgerichtet. Für Banken werden Ratings zusehends zum kritischen Erfolgsfaktor. Für Kreditnehmer bieten sie die Chance, unternehmensinterne Einschätzungen mit einer externen Perspektive zu ergänzen.

Basel II ist ein Meilenstein auf dem Weg zu einer international harmonisierten Bankenregulierung und einem soliden Finanzsystem. Gewichtige Schwächen von Basel I werden – zumindest teilweise – korrigiert. Auch bei neuen Empfehlungen sind aber Bedenken erlaubt. Problematisch sind etwa Wettbewerbsverzerrungen, welche durch Nichtunterwerfung wesentlicher Finanzmarktteilnehmer ausserhalb der Bankenbranche unter die neuen Richtlinien, aber auch deren uneinheitliche nationale Umsetzung, entstehen werden. Schon heute ist absehbar, dass auf Basel II weitere Neuerungen in der Regulierung von Finanzinstituten folgen müssen.

Auszugsweiser Nachdruck des Economic Briefing Nr. 36 mit freundlicher Genehmigung der Autoren;
Herausgeber: Credit Suisse Economic Policy & Consulting Postfach 100, CH-8070 Zürich

Sarbanes Oxley/Basel II

Nouveaux Règlements

Voici plusieurs mois que la loi américaine Sarbanes-Oxley Act s'impose pour les modalité de gestion ou «gouvernance» des entreprises. L'Europe, de près ou de loin, suit ce courant réformateur.

C'est la première fois qu'une étude tente de chiffrer le coût de l'adaptation des nouvelles règles de transparence financière, de garantie sur l'intégrité des données au sein des entreprises.

1 million de dollars pour 1 milliard de chiffre d'affaires.

Le coût n'est pas négligeable. Il pourrait justifier l'adoption de solutions de migration particulières, d'autant que, même si la SEC a accepté d'accorder un délai supplémentaire d'un an aux entreprises qui le demandent, l'échéance est proche, et ses effets induits risquent de se révéler autrement plus onéreux.

Sarbanes-Oxley

C'est bien au-delà des Etats-Unis que les entreprises sont concernées par Sarbanes-Oxley Act (SOX), l'ensemble des lois américaines qui définissent les nouvelles règles de gouvernance, élaborées à la suite d'une multitude de scandales (Enron, Worldcom…) qui ont ébranlé une partie des fondements économiques de l'Amérique libérale.

Car il n'y a pas seulement les entreprises américaines qui sont concernées, mais aussi toutes leurs filiales, et les entreprises qui travaillent pour elles ou exportent vers l'Amérique du Nord.

Et si cela ne suffisait pas, les juridictions occidentales, en particulier européennes, travaillent à faire évoluer leurs propres législations, qui devraient se rapprocher de SOX. Et de toutes façons, SOX va rapidement influer sur les comportements des entreprises et devenir une part de leurs règles de bonnes pratiques !

La section 404 de SOX devrait être l'une des premières à être mises en application. Elle concerne l'auto-évaluation des contrôles internes des procédures de 'reporting' financier. Les données financières de l'entreprise doivent donc être correctement collectées, traitées et stockées.

Ces procédures concernent d'une manière ou d'une autre les services technologiques et de traitement de l'information dans l'entreprise. En particulier SOX prévoit la traçabilité de TOUS les mouvements financiers, donc obligatoirement de TOUS les processus IT partagés.

C'est tout le schéma directeur de l'information dans l'entreprise qui doit être validé, et peut être revu, ainsi que les responsabilités de chacun afin de s'assurer que les termes de SOX sont respectés.

Il ne faut pas oublier qu'en rupture avec les pratiques courantes de la gouvernance d'entreprise, SOX prévoit la responsabilité des maillons stratégiques de l'entreprise, avec des peines d'emprisonnement à l'appui en cas de poursuites ! Rien de mieux qu'un dirigeant en prison pour ternir la réputation d'une entreprise…

Les responsables informatiques, au cœur du traitement de l'information dans l'entreprise, figurent désormais au premier rang des personnes concernées par le Sarbanes-Oxley Act. En ont-ils conscience ?

Ils feraient sans doute mieux de s'assurer que leurs services et l'entreprise qui les emploie sont bien en conformité avec SOX, car désormais même le plus obscure sous traitant d'une entreprise américaine pourra être contrôlé… Sans risque, pensez-vous ? Et la perte d'un contrat pour non respect des règles de gouvernance, vous avez chiffré ce que cela représente ?

Repris avec la permission de l'AFAI

Sarbanes Oxley/Basel II

SOX IT S404 in Novartis

Hintergrund Information

Die Sarbanes-Oxley (SOX) Anforderungen werden oftmals nur aus Finanzsicht beurteilt und der Einfluss sowie die Anforderungen von SOX auf die Informatik eines Betriebes unterschätzt. Gemäss SOX müssen auch die Kontrollen über die Applikationen sowie der Infrastruktur eines Betriebes zur SOX Section 404 Attestierung mit einbezogen werden. Novartis hat sich als sogenannter Foreign Private Issuer freiwillig den Zeitvorgaben für amerikanische Firmen unterstellt, d.h. es wurde bereits ein vollständiger SOX-Attestierungszyklus durchgeführt. Um diesen Anforderungen Rechnung zu tragen, hat Novartis im März 2004 ein SOX-IT-Projekt ins Leben gerufen mit dem Ziel, Novartis zur Attestierung im IT-Bereich zu führen. Für 2004 betraf dies die wichtigsten globalen Lokationen von Novartis, deren 42.

Der nachfolgende Artikel beschreibt die Auswahl der Kontrollen, die Implementierungsstrategie sowie die dabei gemachten Erfahrungen.

Auswahl der Kontrollen

Als Grundlage für die zu implementierenden Kontrollen wurde das dannzumal aktuelle „IT Control Objectives for Sarbanes Oxley, Discussion Document“ des IT Governance Institute (ein aktualisiertes Dokument ist frei über www.itgi.org erhältlich) gewählt. Die darin vorgeschlagenen Kontrollen basieren auf dem CobiT Framework (erstellt durch und erhältlich bei Information System Audit and Control Association ISACA www.isaca.org), das als de facto Standard im Bereich IT Audit und IT Governance und als IT-Gegenstück zum COSO Framework gilt. Der Fokus bei der Auswahl wurde dabei auf die Kontrollen gelegt, die einen „High-Risk“ Bereich adressieren (Security Management, Change Management, Problem Management, Disaster Recovery, Service Level Management) oder generell die Qualität der implementierten Lösungen nachhaltig beinflussen (Corporate Policies, Project Management).

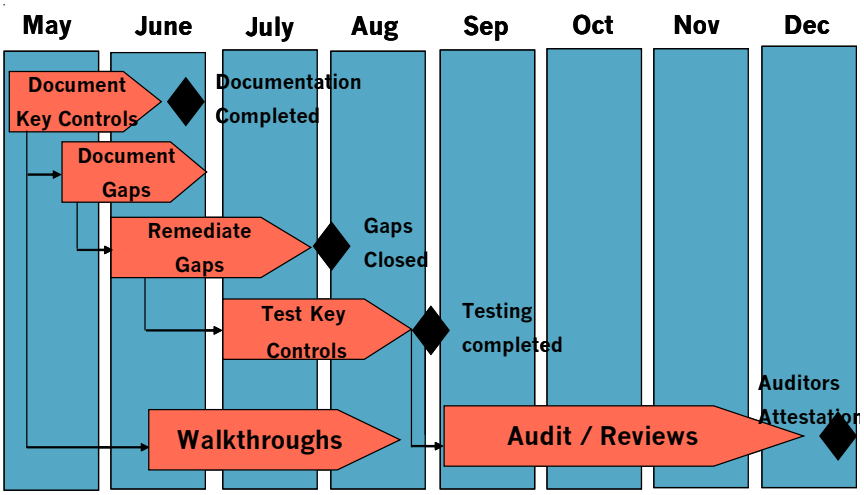
Implementierung

Für die Implementierung der Kontrollen in den Lokationen hat sich das SOX-IT-Projektteam, bestehend aus einem Projektleiter und fünf Kernteammitgliedern aus der gesamten Novartis-IT-Organisation, entschlossen, einen „Kochbuch“-artigen Ansatz zu wählen, d.h. es wurden zentral möglichst genaue Vorgaben bezüglich

- der abzudeckenden Applikationen und Infrastrukturkomponenten
- der geforderten Dokumention
- des Zeitrahmens
- des zu erreichenden Maturitätslevels der einzelnen Kontrollen sowie
- der Anforderungen an die Testaktivitäten

gemacht. Das notwendige „Rüstzeug“ gab das SOX-IT-Projektteam an weltweiten Workshops an die lokalen IT-SOX-Koordinatoren weiter. Zudem wurde ein enges Projektkontrolling und -management durchgeführt. Die kontinuierliche Überprüfung der Qualität der gelieferten Unterlagen sowie der monatlich eingeforderte Projektstatus jeder Lokation halfen, allfällige Probleme rasch zu adressieren und unterstützend einzugreifen. Als Ergänzung zum Reporting hat das SOX-IT-Projektteam von Juni bis August alle 42 Standorte aufgesucht und sich vor Ort über den Stand der Aktivitäten und des Projektstatus informiert. Die Verantworlichen für das gesamte SOX-Projekt, die Businessvertreter sowie das IT Management wurden zudem in regelmässigen Newslettern und Statusberichten über den Projekt-Stand sowie die nächsten Schritte informiert.

Nachfolgend eine Abbildung des Terminplanes für das SOX-IT-Projekt:



Herausforderungen

Die grössten Herausforderungen stellten sich vor allem in den folgenden Bereichen:

Verfügbare Resourcen

Zum Zeitpunkt der genauen Definition des SOX-IT-Projektes waren die meisten Resourcen bereits in Projekten und Initiativen verplant. Es galt, zusammen mit dem Business und den IT-Leitern Prioritäten neu zu definieren und die Wichtigkeit des SOX-Projektes deutlich zu machen.

Change Management innerhalb des Projektes

Während des Jahres wurden die Liste der Applikationen, die Lokationen und die Feinabstimmung der Kontrollen geändert. Es galt jeweils, schnell auf die veränderte Situationen einzugehen und die SOX-IT-Koordinatoren zu instruieren.

Umgang mit Outsourcern

In praktisch allen Lokationen waren Funktionen, wie zum Beispiel das Hosting von Applikationen, an Dritte outgesourced. Es galt, genaue Vorgaben bezüglich dem Umgang und der Kontrolle mit diesen Outsourcern zu definieren. In einigen Fällen wurde vorgeschrieben, diese in die SOX-IT-Aktivitäten einzubinden und ein Audit bei diesen durchzuführen.

Schnittstellen zwischen Systemen und Funktionen

Die Definition der Schnittstellen zwischen Applikationen und Geschäftsfunktionen bedurfte oft einer genauen Analyse und Feinabstimmung bezgl. des Umfanges und der Verantwortlichkeiten für die SOX-IT-Tätigkeiten.

Gemachte Erfahrungen

Positive Erfahrungen wurden in den folgenden Bereichen gemacht:

- Positive Rückmeldungen aus den Lokationen bezgl. des gewählten zentralen Ansatzes
- Gute Akzeptanz in den Lokationen (SOX-IT als genereller Verbesserungsprozess)
- Rückhalt und Kooperation durch/mit SOX-Business
- Unterstützung durch das Management
- Identifikation der „globalen“ Prozesse und somit Erleichterung für die einzelnen Lokationen
- Synchronisation mit anderen, SOX-IT überlappenden globalen Prozessen/Projekten, wie z.B. IT Security, ITIL-Initiativen und IT Quality Management

Alles in allem zeigen die bisherigen Erfahrungen, dass der Aufwand vor allem im Bereich des Testens der Kontrollen nicht zu unterschätzen und eine enge Zusammenarbeit zwischen Business und IT gefordert ist. Vor allem in der Phase des Testings war auch ein schnelles Reagieren vom SOX-IT-Projektteam gefordert, um rasch auf allfällig auftretende Probleme oder Fragen einzugehen. Das Zusammenrücken von IT und Business sowie das Realisieren, dass SOX-IT ein erster Schritt für eine kontinuierliche Verbesserung der gelebten Prozesse ist, sind wohl die positivsten Aspekte dieses ersten SOX-IT-Jahres, das im Dezember 2004 erfolgreich mit der SOX-IT-Attestierung abgeschlossen werden konnte.

Monika Josi
IT Compliance Officer
Novartis Animal Health
Mitglied des SOX-IT-Projektteams

Sarbanes Oxley/Basel II

Mit den Augen des Unternehmensstrafrechts: Welche Bedeutung haben der Sarbanes-Oxley Act & Co.?

Per 1. Oktober 2003 ist Art. 100quater StGB[1] in Kraft getreten, wonach ein Unternehmen für ein Verbrechen oder Vergehen, welches in Ausübung geschäftlicher Verrichtung im Rahmen des Unternehmenszwecks begangen wurde und keiner bestimmten natürlichen Person zugerechnet werden kann, mit Busse bis zu fünf Millionen Franken bestraft werden kann. Voraussetzung dafür ist die mangelhafte Organisation des Unternehmens.

Per 30. Juli 2002 ist der Sarbanes-Oxley Act – eine lex americana – [2] in Kraft getreten, ein Rahmengesetz, welches für korrekte und aussagekräftige Bilanzen sorgen, die Corporate Governance optimieren und das Vertrauen der Anleger stärken soll.[3] Überdies wird voraussichtlich per 31. Dezember 2006 die Vereinbarung Basel II in Kraft treten, die Eigenkapitalvereinbarung des Basler Ausschusses für Bankenaufsicht und Folgevereinbarung von Basel I[4] aus dem Jahre 1988. Basel II bezweckt mit seinem 3-Säulenkonzept (Mindesteigenmittelvorschriften, Aufsichtsverfahren, Marktdisziplin) die Stärkung der Sicherheit und Zuverlässigkeit des Finanzsystems, die Verbesserung der Wettbewerbsgleichheit und eine vollständigere Erfassung der Risiken. Operationelle Risiken sollen von Kreditrisiken getrennt werden.[5]

Noch unbestimmt ist der Zeitpunkt des Inkrafttretens der neuen Gesetzgebung zur Rechnungslegung und Revision[6].

Es mag erstaunen, jedoch haben die vier erwähnten Elaborate[7] einiges gemeinsam. Die Stichworte sind vorab: Risikomanagement, Corporate Governance, Vertrauensförderung.

Inwiefern hängen SOA und Basel II mit dem Unternehmensstrafrecht zusammen? Wer muss bei dieser Ausgangslage schlaflose Nächte haben? Die Strafrechtler? CEOs und CFOs? Die KMU? Wo schläft man besser? In den USA oder in der Schweiz? Wer schläft wohl ungestörter? Der Unternehmer oder die Strafrechtlerin? Nur einige wenige Aspekte sollen hier diskutiert werden.

SOA und 100quater StGB

Gemäss SOA haben CEO und CFO oder Personen mit ähnlichen Funktionen die Durchsicht des Finanzausweises (die korrekte und vollständige Wiedergabe der finanziellen Situation der Gesellschaft) eidesstattlich zu beglaubigen.[8] Wichtig im Zusammenhang mit Art. 100quater StGB ist die Verpflichtung dieser Personen, „interne Kontrollsysteme und deren wirksame Durchführung“ zu installieren und die Ergebnisse der Kontrollen zu unterzeichnen. Bei bewussten Falschangaben drohen strafrechtliche Sanktionen. Im schweizerischen Strafrecht (und nur dieses interessiert uns hier) wird diesen SOA-Anforderungen mittels Art. 152 StGB bereits Rechnung getragen.[9] Theoretisch kann Art. 152 StGB Anlasstat zu Art. 100quater StGB bilden, sofern grundsätzlich die Möglichkeit bejaht wird, dass Sonderdelikte Anlasstaten für die Strafbarkeit von Unternehmen bilden können. Fehlbares Verhalten kann aber – unabhängig vom SOA – in jedem Fall strafrechtlich verfolgt werden. Entweder in einem Strafverfahren gegen das Unternehmen (sofern Sonderdelikte als Anlasstaten anerkannt werden, was die Gerichte zu entscheiden haben werden) oder gegen natürliche Personen.

Fazit: Aus der Sicht des Unternehmensstrafrechts kann der SOA Bedeutung erlangen, und dies aus folgendem Grund: Die durch den SOA oktroyierte Installierung von internen Kontrollsystemen und die Verantwortung für deren wirksame Durchführung könnte ein Abwehr- bzw. Sicherheitsdispositiv sein, mittels welchem ein Organisationsmangel, welcher Grundlage für die Unternehmensstrafbarkeit bildet, erfolgreich abgewehrt werden könnte, sofern das Kontrollsystem dazu geeignet ist, die strafrechtlich fehlbare natürliche Person zu eruieren.

Allerdings könnte hier den KMU ein rauer Wind entgegenwehen, denn es werden vorab grössere, oekonomisch potentere, Unternehmen sein, welche sich ein Abwehrdispositiv in organisatorischer Hinsicht und entsprechende Kontrollsysteme schaffen können: Durch Erlass klarer Reglemente oder Organigramme. KMU-Betriebe (insbesondere die Klein- und Kleinstunternehmen) haben in der Regel weder das Geld noch das Know-how dazu.[10] Den KMU zum Trost sei jedoch eine ketzerische Bemerkung erlaubt: Der Erlass von allzu filigranartigen Reglementen kann auch zum Eigengoal werden, denn: Wer reglementiert, muss sich daran halten. Ein Beispiel: Ist in einem Organigramm ein „legal compliance officer“ vorgesehen und die Stelle bleibt vakant und genau während dieser Zeit kommt es zu Delikten, werden die Strafverfolgungsbehörden – bei Edition der Organigramme – un-

schwer feststellen können, dass ein Organisationsmangel vorliegt, die Unternehmensstrafbarkeit nach sich zieht.

Basel II und 100quater StGB

Basel I wurde in der Verordnung über die Banken und Sparkassen (BankV)[11] umgesetzt. Das selbe dürfte in Bezug auf Basel II zu erwarten sein. Was bedeutet das? Gesetzliche Grundlage für die BankV bildet das Bankengesetz,[12] welches auch Strafbestimmungen enthält:[13] Wer beispielsweise als anerkannte Revisionsstelle die ihm durch BankG und BankV auferlegten Pflichten grob verletzt, wird strafrechtlich verfolgt. Es mag vielleicht erstaunen, aber in diesem Bereich ist Art. 100quater StGB nicht anwendbar. Art. 51 Abs. 2 BankG erklärt nämlich bei Widerhandlungen nach Art. 46, 49, 50[14] und 50bis BankG die allgemeinen Bestimmungen des Verwaltungsstrafrechtsgesetzes (VStrR) vom 22. März 1974[15] (Art. 2 – 13) für anwendbar.

Wie in den meisten Fällen des Nebenstrafrechts ist somit – unter Ausschluss von Art. 100quater StGB – vorab Art. 6 VStrR anwendbar.[16] Es wäre ohnehin schwierig, für die vorgenannten Strafbestimmungen einen Fall zu konstruieren, in welchem eine Straftat vorliegt und die dafür verantwortliche natürliche Person nicht gefunden werden kann. Statt verwischte und unklare Verantwortlichkeiten mittels Art. 100quater StGB wieder aufzufangen, schafft Art. 6 VStrR klare Verantwortlichkeiten. Die teilweise unsorgfältig kritisierte Bundesgerichtspraxis zur Strafbarkeit des Unternehmens[17] darf sich – berechtigterweise – neuer Beliebtheit erfreuen. Sie schafft – dank Anwendbarkeit von Art. 6 VStrR – zumindest im Nebenstrafrecht klare Verantwortlichkeiten und griffige Kriterien für die Strafbarkeit von Unternehmern und damit des Unternehmens.

Fazit: Sofern die Bestimmungen von Basel II im Rahmen der Bankgesetz- und Verordnungsgebung niedergelegt werden, dürfte qua Verweis in der Bankengesetzgebung für strafbare Handlungen Art. 6 VStrR zur Anwendung kommen. Damit wird eine Unternehmensstrafbarkeit gemäss Art. 100quater StGB verdrängt. Das Regelwerk Basel II schafft allenfalls neue Straftatbestände, welche – bei fehlenden Abwehr- und Sicherheitsdispositiven und Kontrollsystemen – zur Strafbarkeit von Unternehmern (nicht des Unternehmens!) führen können.

Auf einen Punkt gebracht: Es bestehen Zusammenhänge zwischen dem Unternehmensstrafrecht und SOA und Basel II. Schlaflose Nächte braucht deshalb – bei guter Organisation – niemand – weder CEO, CFO, Strafrechtler oder Unternehmerin – zu haben. Bei den KMU könnte das Liegen beim Aufbau von Abwehr- und Kontrollsystemen mangels Finanzen und Know-how zeitweise etwas schmerzen. – Schlafstörungen? Die gibt es immer – und überall.

Natalia Schmuki
Fürsprecherin und Notarin
Assistentin von Prof. Dr. M. A. Niggli
Lehrstuhl für Strafrecht und Rechtsphilosophie

Endnoten

[1] Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (zit. StGB), Systematische Rechtssammlung (zit. SR) 311.0

[2] „An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes."

[3] Von der Crone, Hans Caspar/Roth, Katja: Der Sarbanes-Oxley Act und seine extraterritoriale Bedeutung, AJP 2/2003 (zit. Von der Crone/Roth), S. 131 f. – Dieses Gesetz ist nicht ohne Bedeutung für die Schweiz, da sich sein Geltungsbereich auch auf nicht amerikanische Unternehmen, welche in den USA zweitkotiert sind erstreckt (vgl. Von der Crone/Roth, S. 132). Zu den vom Sarbanes Oxley Act betroffenen Schweizer Unternehmen, vgl. Von der Crone/Roth, S. 132, FN 11).

[4] Basel I setzt einheitliche Mindestanforderungen für Kreditrisiken und soll die Stabilität des internationalen Bankensystems fördern.

[5] Befürchtet werden in diesem Zusammenhang Kredit- bzw. Zinsverteuerungen, Rückzug der Banken aus dem Kreditgeschäft, Verknappung der Kreditmittel. Amstutz/von Bhicknapahari sehen die KMU als grosse Verlierer solcher Globalisierungsgesetzgebung, cf. Amstutz, Marc/von Bhicknapahari, Sikander, Gesetzgebung auf verschlungen Wegen? Der Entwurf zu einem Revisionsaufsichtsgesetz, die KMU und die Globalisierung des Rechts (zit. Verschlungene Wege), NZZ vom 23. November 2004, S. 29.

[6] Davon soll aber hier im Detail nicht die Rede sein. Siehe zu diesem Bereich Amstutz/von Bhicknapahari, Verschlungene Wege.

[7] Unternehmensstrafrecht, Sarbanes Oxley Act, Basel II und die Gesetzgebung zu Rechnungslegung und Revision.

[8] Von der Crone/Roth, S. 133.

[9] A.a.O. (Section 906 des SOX)

[10] Immerhin machen die KMU in der Schweizer Wirtschaft 99, 7 Prozent aus. Die KMU beschäftigen zwei Drittel der Erwerbstätigen. Dabei sind 88 Prozent aller Unternehmen Mikro-Unternehmen, welche weniger als 10 Personen beschäftigen (nachzulesen auf www.economiesuisse.ch, Rubrik KMU-Fragen, besucht am 20.1.2005).

[11] SR 952.02, Verordnung vom 17. Mai 1972 über die Banken und Sparkassen (Bankenverordnung, zit. BankV)

[12] SR 952.0, Bundesgesetz vom 8. November 1934 über die Banken und Sparkassen (Bankengesetz, zit. BankG)

[13] Beispielsweise Art. 46 Abs. 1 lit. k BankG: Wer vorsätzlich als anerkannte Revisionsstelle bei der Revision oder bei Erstattung des Revisionsberichtes die ihm durch dieses Gesetz oder die Ausführungsbestimmungen auferlegten Pflichten grob verletzt, namentlich im Revisionsbericht unwahre Angaben macht oder wesentliche Tatsachen verschweigt oder eine vorgeschriebene Aufforderung an die revidierte Bank unterlässt oder einen vorgeschriebenen Bericht an die

Bankenkommission nicht erstattet, wird mit Gefängnis bis zu sechs Monaten oder mit Busse bis zu 50'000 Franken bestraft.

[14] Bei Art. 49 und 50 BankG käme das Unternehmensstrafrecht ohnehin nicht zur Anwendung, das es sich hierbei um Übertretungen handelt, welche von Art. 100quater StGB nicht erfasst werden.

[15] SR 313.0. Art. 6 VStrR (Widerhandlungen in Geschäftsbetrieben, durch Beauftragte u. dgl.) lautet:

(1) Wird eine Widerhandlung beim Besorgen der Angelegenheiten einer juristischen Person, Kollektiv- oder Kommanditgesellschaft, Einzelfirma oder Personengesamtheit ohne Rechtspersönlichkeit oder sonst in Ausübung geschäftlicher oder dienstlicher Verrichtungen für einen andern begangen, so sind die Strafbestimmungen auf diejenigen natürlichen Personen anwendbar, welche die Tat verübt haben.

(2) Der Geschäftsherr, Arbeitgeber, Auftraggeber oder Vertretene, der es vorsätzlich oder fahrlässig in Verletzung einer Rechtspflicht unterlässt, eine Widerhandlung des Untergebenen, Beauftragten oder Vertreters abzuwenden oder in ihren Wirkungen aufzuheben, untersteht den Strafbestimmungen, die für den entsprechend handelnden Täter gelten.

(3) Ist der Geschäftsherr, Arbeitgeber, Auftraggeber oder Vertretene eine juristische Person, Kollektiv- oder Kommanditgesellschaft, Einzelfirma oder Personengesamtheit ohne Rechtspersönlichkeit, so wird Absatz 2 auf die schuldigen Organe, Organmitglieder, geschäftsführenden Gesellschafter, tatsächlich leitenden Personen oder Liquidatoren angewendet.

[16] Ausführlich dargelegt von Niggli, Marcel Alexander und Schmuki, Natalia, anlässlich des Referates „Unternehmensstrafrecht: Fälle wie Von Roll und Schweizerhalle – Gestern, heute und morgen" vom 30. November 2004 vor der SEBWK in Bern (Publikation in Bearbeitung).

[17] Es sei an dieser Stelle nur exemplarisch auf BGE 122 IV 103 ff. in Sachen Von Roll verwiesen. Weitere Beispiele siehe Wiprächtiger, Hans: Strafbarkeit des Unternehmers. Die Entwicklung der bundesgerichtlichen Rechtsprechung zur strafrechtlichen Geschäftsherrenhaftung, AJP 7/2002, S. 754 – 762.

Sarbanes Oxley/Basel II

SOX IT: The Challenge beyond Compliance

Yes, the implementation of SOX IT is a major challenge for all IT organizations. The implementation consumes a substantial amount of resources within each IT organization. Key controls have to be documented, implemented, and gaps have to be remedied. Testing is time intense, and as it is new to many organizations to test their key controls it is also a journey to an unexplored land. Maintenance of SOX IT will become a substantial task for 2005, and the organizations are just about to learn the impact on their daily operations. And IT is also supporting the business to automate and implement key controls. Meanwhile it remains crucial for IT managers to meet all other deadlines and project milestones in 2005.

Thinking beyond meeting the requirements for SOX IT may sound premature for many IT managers, as the IT organization is still learning what impact on the daily business SOX IT has. However, it is truly important not to miss the opportunity to support the business in improving and automating processes to increase value and to reduce compliance workload. IT can become a real value adding partner if we can master maintaining operational controls and improving business processes meanwhile. IT should aim to understand finance key controls to support business in defining lean process frameworks and to provide effective and flexible IT solutions. 2005 will be the first year to maintain and retest key controls, and manual testing will be a major challenge for any business and IT organizations.

The implementation of Sarbanes-Oxley in 2004 was a compromise, as we could impossibly implement the new regulation at all IT sites, and as we had to focus on meeting critical key controls. Better understanding of the effect on financial reporting by managing IT will require quite some research over the next few months, and all the work will lead into a compliance framework to strongly support business to run in an effective, flexible and safe environment. Automation of key controls will reduce compliance costs over time for Business and IT.

Stefan Laux
Novartis SOX IT Projectleader

Sarbanes Oxley/Basel II

Bestmögliche IT-Unterstützung für Corporate Governance durch mySAP ERP

Das Thema ***Corporate Governance*** hat durch die Finanzskandale der vergangenen Jahre erheblich an Bedeutung gewonnen. Um das Vertrauen der Investoren zurück zu gewinnen, sind unter dem Druck von Finanz- und Börsenaufsichtsbehörden eine Reihe neuer Gesetze verabschiedet worden. Prinzipiell versteht man unter Corporate Governance die verantwortungsbewusste Unternehmensführung, die unter Beachtung geltender Gesetze und Vorschriften zu einer langfristigen Wertsteigerung des Unternehmens führen soll. Dabei werden die folgenden drei konkreten Ziele verfolgt:

- Compliance: Einhaltung von gesetzlichen Vorschriften bei der Erstellung von Quartals- und Jahresabschlüssen.

- Transparency: Zuverlässige, verständliche und nachweisbar richtige Berichte des Finanz- und Rechnungswesens.

- Speed: Einhaltung kurzer Fristen für die Erstellung von Quartals- und Jahresabschlüssen sowie die Möglichkeit zur Transformation externer Informationen basierend auf alternativen Rechnungslegungsvorschriften wie beispielsweise US-GAAP oder IAS.

Die Wirtschaftsprüfer analysieren neben den Systemen des Finanz- und Rechnungswesens auch alle Geschäftsprozesse, die in letzter Konsequenz die Bilanz, GuV und Kapitalflussrechnung beeinflussen. Bei der Abschlussprüfung wird daher genau untersucht, ob besonders sensible Prozess-Schritte gravierende Fehlerquellen aufweisen oder sogar betrügerische Aktivitäten zulassen.

mySAP ERP unterstützt die Corporate Governance Anforderungen durch eine Reihe von Anwendungen. Die moderne Softwarearchitektur erfüllt höchste Ansprüche an die Zuverlässigkeit und Überprüfbarkeit von Quartals- und Jahresabschlüssen. Im Finanz- und Rechnungswesen sind neben einem flexiblen General Ledger auch Anwendungen für die Abbildung von Transferpreisen und das Closing Cockpit für die Automatisierung von Abschlussarbeiten enthalten. Die Komponente SEM beinhaltet Anwendungen für die gesetzliche und Managementkonsolidierung, Bilanz-, GuV- und Cash Flow Planung, Strategie und Performance Management sowie Risiko Management. Anforderungen des Sarbanes-Oxley-Acts und vergleichbare Regelungen anderer Länder werden über Anwendungen zum Managen interner Kontrollen, Info-Systeme für Revisoren und Wirtschaftsprüfer sowie die Möglichkeit für Mitarbeiter anonyme Problemmeldungen zu erfassen zur Verfügung gestellt.

Konkret müssen sich CFOs den folgenden Herausforderungen stellen, für die ***mySAP ERP*** ausgereifte und robuste Lösungen bereitstellt:

1. IT Landschaft

mySAP ERP basiert auf der modernen Integrationsplattform ***SAP NetWeaver***, die eine dramatische Reduzierung der Komplexität von integrierten Systemen in einer heterogenen IT-Landschaft ermöglicht.

2. Einhaltung von gesetzlichen Vorschriften

Neben den bekannten Vorschriften unterliegen eine Vielzahl von Firmen seit diesem Jahr dem Sarbanes-Oxley-Act. ***mySAP ERP*** unterstützt die Anforderungen zum einen durch eine robuste Architektur mit einer Vielzahl von konfigurierbaren, Berichts- und Sicherheitskontrollen. Die Anwendung Management of Internal Controls unterstützt gezielt SOA 404 Projekte, mit dem Ziel das interne Kontrollsystem nicht nur zu dokumentieren, sondern auch Design und Effektivität interner Kontrollen zu bewerten und dem Management und Wirtschaftsprüfer transparent zu machen. Mit dem Whistle Blower können Mitarbeiter entdeckte Unregelmäßigkeiten anonym an das Audit-Board senden.

3. Unterstützung betriebswirtschaftlicher und System-Audits

mySAP ERP bietet internen und externen Prüfern mit dem Audit Information System eine Anwendung für die Prüfung in einem Umfeld von Massentransaktionen.

4. Einhaltung von Vorschriften zum Enterprise Risk Management

Die Auswirkung von Risiken auf wichtige Unternehmenskennzahlen können mit dem SEM Risk Management beurteilt werden. Eine Anwendung zum Managen operativer Risiken (ORM) ist in Vorbereitung. Es ist geplant, ORM bereits in 2004 auf Projektbasis einzelnen Firmen zur Verfügung zu stellen.

5. Transparenz für Basel II

Die SEM Komponenten von ***mySAP ERP*** unterstützen Industrieunternehmen, die als Konsequenz aus Basel II ihre Kapitalkosten nur dann verringern können, wenn Finanzinformationen inklusive Planzahlen transparent gemacht werden,

6. Parallele Bewertung

Das General Ledger von ***mySAP ERP*** erlaubt die Erstellung paralleler Abschlüsse resultierend aus der gleichzeitigen Anwendung mehrerer Rechnungslegungsvorschriften wie zum Beispiel IAS/IFRS und HGB.

7. Fast Close

Das Closing Cockpit von ***mySAP ERP*** ermöglicht durch die Automatisierung von Abschlussarbeiten eine deutliche Verringerung des Aufwands für die Erstellung von Quartals- und Jahresabschlüssen.

Weitergehende Informationen können bei karin.weis@sap.com angefordert werden.

Marcus Wefers, Director Solution Management mySAP ERP, Waldorf

Sarbanes Oxley/Basel II

Basel II und die IT

Erik Guldentops bespricht in der Ausgabe Nr. 6/2004 des ***Information System Controls Journals*** die Zusammenhänge zwischen Basel II und der Informationstechnologie. Besonders beeindruckt hat mich die Gegenüberstellung der Prinzipien der Basel II Vereinbarung mit den Auswirkungen auf die IT. Ich versuche an dieser Stelle, die ersten drei Prinzipien des Positionspapiers aus meiner Sicht mit provokativen Fragen und konkreten Beispielen zu ergänzen.

Prinzip 1

Der Verwaltungsrat muss sich der operationellen Risiken bewusst sein und ein ***operational risk management framework*** genehmigen und periodisch einer Review unterziehen.

Beinahe schon in Vergessenheit geraten: In den späten neunziger Jahren des vergangenen Jahrhunderts waren viele Leute durch das Millenniumgespenst aufgeschreckt. Ich bin sicher, dass dies bis in die Chefetagen und zu den Verwaltungsräten durchdrang. Letztlich mussten ja Tausende, wenn nicht Millionen von Geldeinheiten gesprochen werden, um der Drohung rechtzeitig zu begegnen. Damals befasste man sich also mit diesem einen Aspekt des IT-Risk-Managements ausgiebig. Und heute? Sind jene Notpläne in der Verstaubung versunken?! Ich hoffe nicht. Denn auch heute muss damit gerechnet werden, dass im Umfeld der IT-Phänomena auftreten, welche eine Normalverarbeitung des Datenmaterials verunmöglichen: Stromausfälle, Verarbeitungsfehler und -ausfälle von Zulieferanten von Informationen (Kreditkartenfirmen, Clearingstellen, Bankdebitoren und -kreditoren, usw.). Daneben sind aber immer wieder die neusten Entwicklungen zu berücksichtigen, zu denen ich neben den politischen Gegebenheiten und dem daraus erwachsenden Personen- und Handelsschrankenabbau auch Klimaveränderungen und andere Naturereignisse zähle.

Ich bezweifle ernsthaft, ob sich die Bankverwaltungsräte mit diesen Dingen je befassen. Vielmehr lassen sie sich von ihren Fachkräften in den Schlaf der Gerechten einlullen. Vielleicht braucht es hin und wieder ein Jahr-2000-Gespenst. Wartet es hinter der nächsten Ecke?

Prinzip 2

Der Verwaltungsrat muss sich darüber vergewissern, dass die Interne Revision wirksam und umfassend prüft und sich auf einem hohen Stand der Ausbildung bewegt.

Verschiedene Institutionen (und dazu zählt auch die ISACA) verlangen von ihren Mitgliedern, dass sie sich nach Erhalten eines Diploms weiterbilden. Die Institutionen halten in ihren Regelwerken fest, wie die Angemessenheit der Fortbildung zu erfolgen hat. Die notwendigen ***Contact Hours*** oder ***Credits*** können auf verschiedene Art erworben und nachgewiesen werden; etliche davon beruhen auf einer Selbsteinschätzung der betroffenen Personen (z.B. Selbststudium von Literatur).

Frage: Verlangen die Bankverwaltungsräte je Auskunft über den Stand

der IT-Qualität der Internen Revision? Wie sind sie allenfalls in der Lage, eine entsprechende Auskunft zu werten? Fordert Basel II hier nicht Erfüllbares?

Prinzip 3

Die oberste Geschäftleitung hat das ***operational risk management framework*** konsistent umzusetzen und die entsprechende Politik, die Prozesse und die Verfahren zu entwickeln.

Ich stosse mich ein bisschen am Ausdruck „konsistent". Leider weiss ich nicht, womit ich diesen Ausdruck mit der Umsetzung in Zusammenhang bringen soll. Ich nehme einmal an, dass dieses Rahmenwerk in allen flankierenden Dokumenten, wie Mitarbeiterhandbüchern, Führungsmanuals, Stellenbeschreibungen, ja sogar Budgetrichtlinien, Geschäftsberichten, VR-Protokollen, usw. verankert werden bzw. Erwähnung finden müsste.

Bei den zu entwickelnden Prozessen und Verfahren stellt sich mir die Frage, ob damit Tagungen gemeint sind, in welchen eine entsprechende Schulung betrieben wird. Die blosse Ernennung eines ***Compliance Officers*** kann ja auch nicht die Antwort sein. Seine einschlägigen Aktivitäten müssen beschrieben werden, damit sie selbst auch kontrollierbar sind. Bisher habe ich vergeblich bei betroffenen Firmen gezielte, systematische und konkrete „Prozesse und Verfahren" zur Risikoverminderung, geschweige denn zur Verhinderung von Betrug gefunden.

Tun die heutigen Verwaltungsräte alles dies? Vorschläge sind wohl gefordert.

Max F. Bretscher, CISA, CISM

Forensic

IT-Unterschlagungsprüfung

1. Einführung

Die Anzahl wirtschaftskrimineller Handlungen steigt seit Jahren sowohl im Empfinden der Unternehmensmanager als auch nach aktuellen Studien an, wobei die subjektive Steigerungsempfindung, die sich in aktuellen Studien widerspiegelt, erheblich über der tatsächlichen Steigerung liegt. Aus diesem neuen Fokus auf dolose Handlungen und ihren Folgen lassen sich Fragen für die Unternehmen ableiten, die geklärt werden müssen, um eine wirksame und ökonomisch angemessene Reaktion zu entwickeln:

- Wer sind die Täter, welche Taten werden verübt und wie werden diese Taten aufgedeckt?
- Wie können dolose Handlungen bereits im Vorwege verhindert werden?
- Welche Ermittlungsmethoden bieten sich bei Verdacht an und was muss bedacht werden?

2. Die Täter

Einheitlich zeigen alle aktuellen Berichte zur Wirtschaftskriminalität eine überwiegende Mehrheit interner Täter. Externe Täter spielen, obwohl es je nach Deliktform natürlich Unterschiede gibt, auch in Komplizenschaft mit internen Mitarbeitern nur eine eher untergeordnete Rolle.

Der interne Täter kann dabei aus jeder Schicht der Unternehmenshierarchie kommen. Obwohl von absoluten Zahlen her das Thema Management-Fraud eine geringe Rolle spielt, wandelt sich das Bild, wenn man die mögliche bzw. tatsächliche Schadenshöhe betrachtet, die „durch Manager" entstehen kann.

Unabhängig von der hierarchischen Position geht die einschlägige Literatur von einer Dreiteilung der Menschen unter ethischen Aspekten aus. Ein Viertel der Mitarbeiter eines Unternehmens sind dabei unbedingt vertrauenswürdig und unter keinen Umständen bereit, eine kriminelle Handlung zu begehen.

Die Hälfte der Menschen ist im Normalfall vertrauenswürdig.

Eine sehr gute Gelegenheit in Verbindung mit besonderen Situationen – z.B. Ärger mit dem Vorgesetzten – kann diese Personengruppe allerdings in Versuchung und damit auch schlussendlich zu kriminellen Handlungen führen.

Das letzte Viertel benötigt nur eine gute Gelegenheit, um kriminell zu werden.

3. Deliktformen

Wirtschaftskriminelle Handlungen prägen sich in verschiedenen Deliktformen aus. Eine große Menge der Vorfälle gliedert sich in die Delikte:

- Betrug
- Untreue
- Unterschlagung und
- Diebstahl

Die genaue Abgrenzung der Delikte ergibt sich aus den strafrechtlichen Definitionen, wobei es in diesen Fällen um tatsächliche Verluste für das

Unternehmen oder entgangene Gewinne geht.

Beispiele sind hier z.B.:
- die Zahlung von Geldsummen an den Täter über fiktive Kreditoren im Rahmen eines fiktiven Geschäftes, abgewickelt durch den Täter;
- Absprachen mit dem Lieferanten zum Nachteil des Unternehmens oder
- schlichter Diebstahl von Vermögensgegenständen aus Lager oder Büro.

Häufig unterschätzt und zum Teil schwer abzugrenzen ist der Diebstahl geistigen Eigentums. Dies beinhaltet nicht nur die Verletzung des Patentrechts, sondern auch den Diebstahl von Ideen bei der Behauptung im Markt, z.B. im Marketing.

Zunehmend im Blickpunkt (allein schon aufgrund der Schadenhöhe) sind die Delikte des „Cybercrime", wie z.B. Hackerangriffe oder Virusinfektionen, aber auch die verbotene Nutzung von IT-Funktionen, wie eMail oder Internet zu privaten Zwecken.

Weitere Deliktformen (zum Teil auch in Mischformen) in der Wirtschaftskriminalität sind:
- Bestechung/Begünstigung
- Wirtschaftsspionage
- Sabotage
- Erpressung
- Geldwäsche

und die durch spektakuläre Fälle in den Blickpunkt gerückte
- Bilanzfälschung.

Ein besonderer Trend, der sich besonders in konjunkturell schwierigen Zeiten häuft, ist die kriminelle Handlung „für" das Unternehmen, wie z.B. der Betrug am Kunden, um den Arbeitsplatz bzw. das Unternehmen zu „retten". Dies geschieht zum Teil mit Wissen bzw. auf Veranlassung der Unternehmensleitung bzw. ist auf verfehlte Eigeninitiative der beteiligten Mitarbeiter zurückzuführen.

4. Aufdeckung bzw. Verhinderung der Straftaten

Es zeigt sich, dass ein wirksames internes Kontrollsystem der beste Schutz vor kriminellen Handlungen ist. Dies gilt sowohl für die Prävention als auch für die Aufdeckung durch entsprechende Kontrollen.

Der zweite überaus erfolgreiche Kommissar ist der Zufall, der besonders bei wiederholten bzw. lang laufenden Verbrechen zuschlägt. Interne und externe Hinweise, anonym oder auch nicht, sind eine weitere Säule der Tatfeststellung.

Die Prüfung von Sachverhalten durch die interne bzw. externe Revision im Rahmen von Routineprüfungen oder bei konkreten Verdachtsmomenten spielt ebenfalls eine bedeutende Rolle.

5. Prävention

Wie können kriminelle Handlungen im Vorhinein verhindert werden?

In jedem Fall durch eine Mischung der Methoden und nicht durch eine einzelne Maßnahme.

Gefährdungsanalyse

Diese beinhaltet
- Durchführung einer regelmäßigen Analyse gefährdeter Bereiche.
- Bewertung der Risiken und
- Feststellung von Angriffspunkten für externe und interne Täter.

IKS – Internes Kontrollsystem

Schaffung eines internen Kontrollsystems mit Komponenten der Fraud-Prävention und -Aufdeckung.

Richtlinien

Schaffung von ethischen Richtlinien im Unternehmen. Diese sollten praktische Anweisungen beinhalten für den Umgang mit unethischem Verhalten, z.B. die Reaktion auf versuchte Bestechung oder Meldewege bei der Aufdeckung von kriminellen Handlungen.

Einrichtung von Meldewegen

Festlegung einer „Fraud-Hotline" und Festlegung klarer Ansprechpartner für das Melden von kriminellen Handlungen. Eine klare und kommunizierte Struktur senkt die Hemmschwelle, die gerade historisch in Deutschland besonders hoch ist, unethisches Verhalten zu kommunizieren. Erfahrungen aus dem Ausland, z.B. aus den USA, wo Fraud-Hotlines stark verbreitet sind, zeigen, dass sie bei einer deutlichen Verbesserung der Aufklärungsrate zu keiner Verschlechterung des Betriebsklimas führen.

Schulung/Sensibilisierung

Neben Richtlinien und klar definierten Meldewegen müssen Schulungen durchgeführt und Mitarbeiter sensibilisiert werden. Dies führt insgesamt zu einer deutlichen Verbesserung der Situation.

Externe/Interne Prüfungen

Nicht nur im Verdachtsfall, sondern auch zur Abschreckung sollten regelmäßig im Unternehmen Prüfungen durchgeführt werden. Dies gilt besonders auch für Bereiche, in denen Herrschaftswissen angehäuft wurde, z.B. in der Informationstechnik oder beim Produktmanagement, wo Abhängigkeiten und mangelnde Kontrollmöglichkeiten den Einsatz von externen Spezialisten erfordern.

6. Ermittlungsmethoden

Im Rahmen einer Untersuchung von kriminellen Handlungen kommen verschiedene Ermittlungsmethoden zum Einsatz. Im Folgenden werden einige dieser Methoden vorgestellt. In jedem Fall sollten solche Methoden aber juristisch einwandfrei durchführt und vollständig, ggf. in Form eines Untersuchungstagesbuches zeitgenau und zeitnah protokolliert werden.

Eine der wesentlichen Ermittlungsmethoden ist die Befragung von Beteiligten. Diese Methode sollte ***immer*** im Beisein von Personen geschehen, die als Zeugen in Frage kommen. Sie ist aber für verdeckte Ermittlungen natürlich nur bedingt geeignet. Es ist dringend darauf zu achten, dass nicht in Folge einer Befragung Beweismittel vernichtet werden oder die eigene juristische Position in Frage gestellt wird.

Oft genannt, aber in einem komplexen IT-Umfeld oft überschätzt, ist die Beobachtung. Beobachtung ist in der Regel verbunden mit der Überwachung von Personen durch Personen. In einschlägigen medialen Darstellungen werden Beobachter dabei meist mit Trenchcoat und Schlapphut dargestellt. Dies macht auch gleich die Problematik in Verbindung mit der Überwachung deutlich: Eine Überwachung, ohne dass der Verdächtige sie bemerkt, ist zumindest aufwendig.

Für den Revisor eine der wesentlichsten Möglichkeiten Beweise zu erlangen, ist natürlich die Analyse von (finanziellen) Daten und die Sichtung und Sammlung von Dokumenten.

7. ERP-Systeme (SAP R/3) – Entdecke die Möglichkeiten

Durch die durchgängige Datenbasis und den hohen Integrationsgrad des Systems, wird die Ermittlung in einem Verdachtsfall beim Einsatz von ERP-Systemen, wie SAP R/3 signifikant erleichtert.

- SAP bietet umfangreiche Möglichkeiten der Online- bzw. Offline-Überwachung von Benutzern und Prozessen;
- SAP bietet die Möglichkeit, Daten zu exportieren und mit Revisionssoftware zu analysieren.

Zur Verdeutlichung der Möglichkeiten hier u. a. Beispiele der Ermittlung mit Datenanalyse auf Basis von SAP-Daten in den einzelnen SAP-Modulen:

Basissystem

Benutzerüberwachung
Über das Systemmonitoring bietet SAP die Möglichkeit einer sehr detaillierten Prozessüberwachung. User und Transaktionen können Online überwacht werden. Damit kann eine Beobachtung von Verdächtigen ohne direkten physischen Kontakt und damit der Gefahr der Entdeckung realisiert werden.

Tabellenprotokollierung
Über die aktivierte Tabellenprotokollierung und die Auswertungen der Systemprotokolle können über die Stammdatenänderungsbelege hinaus Anhaltspunkte für dolose Handlungen ermittelt werden, z.B. durch die Änderung von Zahlungsbedingungen.

User mit kritischen Berechtigungen
User mit kritischen Berechtigungen (SAP_ALL, SAP_NEW etc.) können identifiziert werden.

Benutzer
Benutzer, die obwohl längst aus dem Unternehmen ausgeschieden, noch aktiv sind, können identifiziert werden.

Änderungsbelege Benutzer
Benutzer, die temporär mit Super-User-Rechten ausgestattet wurden oder Benutzer, die insgesamt nur kurzfristig eingerichtet wurden, können identifiziert werden.

Programmentwicklung
Über eine Stichprobe (oder eine Volltextsuche) kann in eigenentwickelten SAP-Programmen nach einer Umgehung der Berechtigungsprüfung gesucht werden.

Hauptbuch

Belegkopf (Tabelle BKPF)
Der Belegkopf des SAP-Systems ist ein kleiner Schatz für den Ermittler. Im Belegkopf werden verschiedene wertvolle Informationen zur Belegerfassung vermerkt, z.B. finden wir hier:

- den Erfasser der Transaktion
- Erfassungsdatum und Uhrzeit
- Belegdatum
- Transaktionsname und die
- Belegart als Kennzeichen für den Geschäftsvorfall

Fragestellungen, die mit diesen Daten beantwortet werden können, sind vielfältig:

- Häufungen von Geschäftsvorfällen (z.B. Gutschriften) pro Benutzer;
- Erfasser, die nicht im Netzwerk angemeldet sind (in Verbindung mit Protokolldaten);
- Buchungen an Feiertagen und zu ungewöhnlichen Uhrzeiten (z.B. nach 23:00 Uhr);
- Große Abstände zwischen Erfassungs- und Belegdatum;
- etc.

Kreditorendaten

Kreditorendaten sind in vielen Unternehmen entscheidend für den Abfluss wesentlicher liquider Mittel. Als Basis für viele Auswertungen kann eine Kombination aus Stamm-, Bewegungs- und Änderungsdaten genutzt werden, wie z.B. das Kreditorenverzeichnis (Report RFKKVZ00), die Kreditoreneinzelpostenliste (Report

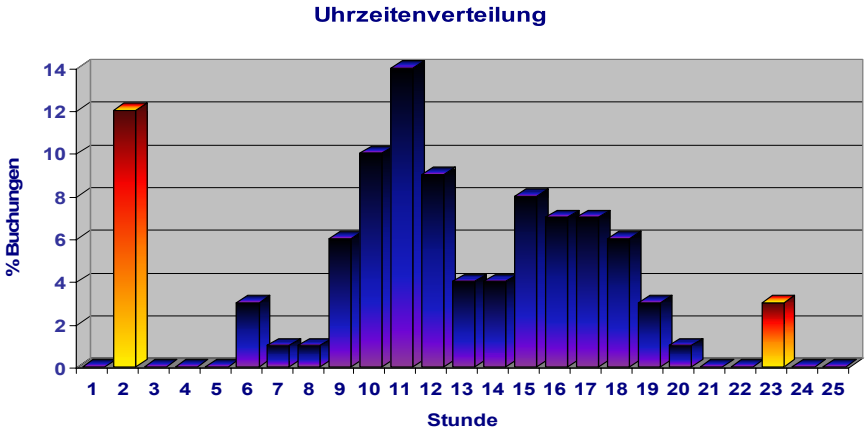


Abb: Verteilung des Buchungsstoffes über die Stunden am Tag (Erfassungsstunde)

RFKEPL00) und die Änderungsbelege für Kreditorenstammdaten (Report RFKABL00).

Fragestellungen:

- Häufige Stammdatenänderungen
- Änderungen der Bankverbindung
- Kreditorenbankverbindung = Mitarbeiterbankverbindung (z.B. aus SAP HR)
- Häufungen von Zahlungen unter einem Zahlungslimit
- Abwicklung über CPD-Konten

Debitoren

Debitorendaten sind, besonders wenn es z.B. um Gutschriften und andere „besondere" Geschäftsvorfälle geht, ein lohnendes Untersuchungsziel. Hierzu bietet sich besonders die Debitoreneinzelpostenliste an (Report RFDEPL00).

Fragestellungen:

- Kreditorische Debitoren
- Anleger ist einzig Buchender
- Hohe Anzahl von Gutschriften/Retouren pro Vertriebsmitarbeiter
- Änderung von Zahlungsbedingungen

8. Geschnappt… und dann ?

Verhärtet sich der Verdacht durch Beweise, sind entsprechende Maßnahmen einzuleiten. Wesentlich ist dabei, vorbereitet zu sein!

In jedem Fall sollte ein vorbereiteter Maßnahmenkatalog existieren, der im Falle einer kriminellen Handlung angewandt wird. Der Zeitfaktor ist in Hinsicht auf Beweismittelsicherung und mögliche Regressforderungen ein wesentlicher Faktor. Checklisten bzw. Maßnahmenkataloge müssen dabei nicht neu erfunden werden, sondern finden sich in der einschlägigen Literatur oder im Internet.

Erster Schritt im Fall einer identifizierten dolosen Handlung sollte die Einberufung eines interdisziplinären „Fraud"-Teams sein. Das „Fraud"-Team besteht aus Ermittlungsspezialisten, Juristen, Mitarbeitern betroffener Fachbereiche – soweit Prozesskenntnisse von Nöten sind – und Mitgliedern der Geschäftsleitung.

Eine erste Ausmaßabschätzung sollte in Verbindung mit der Beweismittelsicherung und ersten Befragungen erfolgen. Das Thema einer möglichen Verleumdungsklage sollte dabei stets bedacht sein.

Betroffene verdächtige Mitarbeiter sollten sofort freigestellt werden. Jegliche Zugangsmöglichkeiten sowohl zu Systemen als auch zu Räumlichkeiten sind sofort zu unterbinden. Arbeitsrechtliche Maßnahmen sind in der Folge einzuleiten, speziell bei fristlosen Kündigungen ist auf ein formal richtiges Verfahren zu achten, z.B. ob die Person, die die Kündigung ausspricht, auch dazu berechtigt ist!

Ist die kriminelle Handlung vom Unternehmen bewältigt, in welcher Form auch immer, sollte sich die Organisation als lernend erweisen und das IKS entsprechend verbessern, um zukünftige Vorfälle zu vermeiden.

9. Fazit

Dolose Handlungen sind ein Problem mit Zukunft! Auch in den nächsten Jahren werden kriminelle Handlungen zunehmend von starker Bedeutung für die Unternehmen sein.

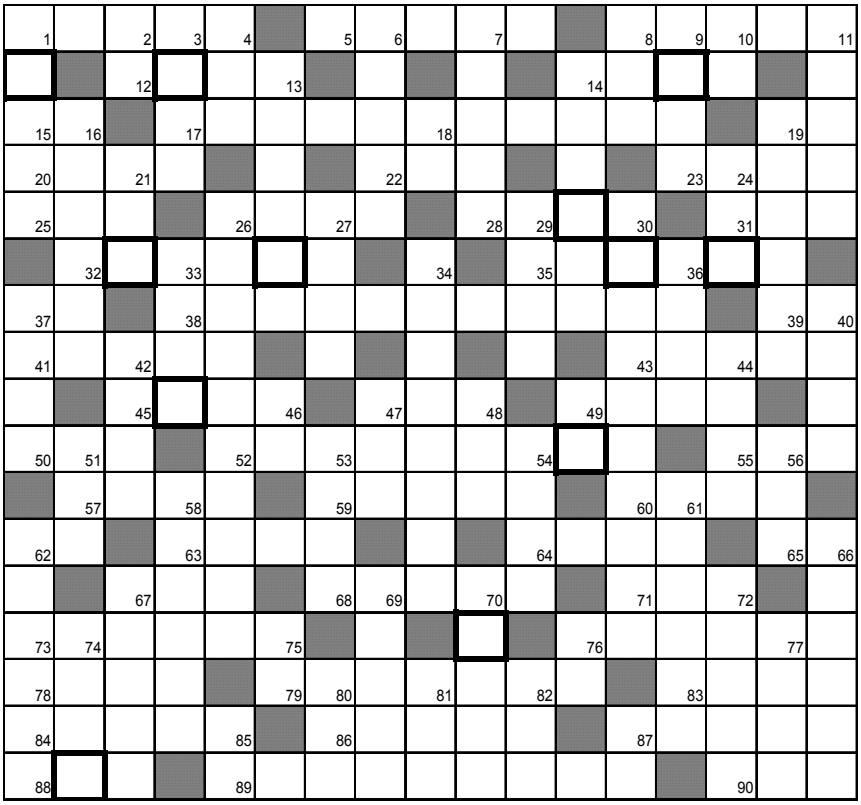
Dies führt zu einem Handlungsbedarf, speziell auch in den Bereichen der Prävention von Delikten und der rechtzeitigen Vorbereitung durch Maßnahmenkataloge und Notfallpläne.

Um im Falle eines Verdachts erfolgreich Ermittlungen durchzuführen, können moderne ERP-Systeme wesentlich zu Ermittlungserfolgen beitragen. Hier zahlt sich die funktionale und datentechnische Integration für den Ermittler aus.

Holger Klindtworth
CISA CIA CISM Dipl.-Inf.
Susat & Partner oHG
h.klindtworth@susat.de

The ISACA Crossword Puzzle 1/05

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 Fiel einst vom Himmel; 5 Eskimoapostel; 8 Tageszeit; 12 verloren (engl); 14 Verschwörung (engl); 15 Tuberkulose; ***17 abmachen***; 19 frz AG; 20 Blasinstrument; 22 Gewässer; 23 der Balkanfluss ist nicht draussen; 25 Kosewort der Artillerie; 26 Temperaturbezeichnung; 25 Futterstelle; 31 typisches Engländergetränk; 32 Militärplatz im Tessin; 35 Spezialarzt; 37 babyl Erdgott; ***38 mehrfach beteiligt*** (engl); 39 Einzelzimmer; 41 Ritze; 43 Gestalt aus Schillers Don Carlos; 45 eben nicht nostro; 47 Klostervorsteher; 49 Westeuropäer (Mz); 50 Mündungsarm des Rheins; ***52 damit befassen sich die Vorschriften***; 55 metallisches Element; 57 Honig (frz); 59 Kapitalertrag; 60 Flächenmass (Mz); 62 multiple Sklerose; 63 Schwermetall; 64 Werk von Emile Zola; 65 trägt Fridolin im Wappen; 67 der Unionsgeneral hat sich dem Wind abgekehrt; 68 eingedeutschte Sauce; 71 Common Task Test; 73 Bandbreite; 76 Geldsumme; 78 Zeitbegriff (Mz); ***79 mit diesen 26 senkrecht befassen sich die Vorschriften***; 83 Nadelbaum; 84 Not; 86 griech Buchstabe; 87 der ehemalige Autorennfahrer Al ist im christlichen Gebet im Zusammenhang mit Vater zu vernehmen; 88 noch (engl); 89 verzieren; 90 Transaktionsnummer.

Senkrecht: 1 Bundesrat im zweiten Weltkrieg; 2 AZ aus Westeuropa; 3 entstehende Sonne; 4 nordische Gottheit; 6 Gotthelf brachte ihn mit Geld in Verbindung; 7 Soll; 8 engl Biersorte; 9 der bekannteste ist wohl James; 10 und (lat); 11 röm Göttin; 13 engl Schwänzer; 14 mit a zum vornhinein; 16 grobe Sackleinwand (engl); 18 AZ aus der Westschweiz; 19 Verschlussart; 21 „lebende“ Vorsilbe; 24 rote Teamorganisation; ***26 zentrales Element der Vorschriften***; 27 inhaltslos; 29 Peitsche; ***30 Beherrschung***; 33 grosses Lager; ***34 eben nicht Oxley***; 36 Aufforderung zur Auferstehung; 37 Grautier; 40 Garnitur; 42 umgangssprachlicher Trinker; 44 das span Zahlwort fährt auch Velo; 46 kurzes Werk; 47 Flächenmass in der Schweiz; 48 drei gleiche Konsonanten; 49 eine der Geliebten des Göttervaters; 51 Ort bei Chur; 53 säte in der Antike Zwietracht; 54 nicht diese (i=j); 56 schmal im Durchlass; 58 Flächen; 61 Nagetier (Mz); 62 Stangen; 66 sich temporär niederlassen; 67 Vorrat; 69 anpeilen; 70 Art (Mz); 72 traurig; 74 Stange (span); 75 Nahrungsmittel; 76 AZ aus der Hauptstadt; 77 Einwand; 80 Norddeutscher Rundfunk; 81 Erzieher Samuels im AT; 82 Bezeichnung einer Walart; 85 lautloser englischer Hund; 97 frz Zahlwort.

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 14. März 2005.

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 Crossword Puzzle 5/04:
Bonn am Rhein

Across: 1 archangels; 9 has; 10 ore; 11 Ru; 12 ***Pankow***; 14 abash; 16 Erin; 17 TNT; 19 ave; 20 ***Munich***; 22 saves; 24 USS; 25 hem; 27 can; 28 mariner; 31 pie; 33 AO; 34 III; 36 ***Saxons***; 38 stand; 40 cis; 41 red; 42 ce; 43 chil(e); 45 ***d.h.***; 46 emir; 48 hot; 49 ***Main***; 51 at; 52 ***OBerliner***; 55 EB; 57 lo; 58 serin; 60 itsi (bitsi, teeny weeny); 62 votes; 64 GBN; 66 beret; 67 II; 68 yachts; 69 SSSSS.

Down: 1 ax(e); 2 chains; 3 Hanni; 4 ask; 5 gown; 6 er; 7 Lea; 8 Bushes; 11 raven; 12 ***Prussia***; 13 other; 15 ***Bavaria***; 16 emu; 18 TS; 21 chains; 23 ace; 16 Mia; 29 nose; 30 Eider; 31 psychology; 32 excite; 34 IA; 35 incite; 37 oil; 39 TDE; 41 ***Rhine***; 44 hobo; 45 daisy; 47 ma; 49 ML; 50 nerves; 53 rat; 54 riots; 56 basis; 59 NT, 61 SBT; 63 ***Eis***; 65 Ba.

English crossword puzzles seem to have it not very easy: Not more than five answers…

Watson: Maybe it was too obvious, maybe it was too confusing, maybe it was too difficult: The shaded squares form the shape of today's Germany. Anyway, nobody saw it. Jackpot increased to $US 200.00! Just for the hell of it: Here is another crossword puzzle that shows the contours of Germany again, this time is the crossword puzzle in German, too. Both crossword puzzles have the chance of winning.

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

Alle Kurse mit hohem Labor-Anteil

Drei spannende Kurse!

Application Security Lab
Workshop für Sicherheit von Web-Anwendungen
15. - 17. März 2005 in Zürich

Internet Security Lab
Angriffszenarien und Abwehrmassnahmen
20. - 22. April 2005 in Zürich

Evidence Lab
Workshop über die Spurensuche in Computersystemen
11. - 13. Mai 2005 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. 044 440 33 64, Fax 044 440 33 61

Waagrecht: ***1 AZ Karlsruhe***; 3 Einschaltknopf; 4 Behältnis; 7 kurze Grossstadt; 10 Hinterhältigkeit; 11 Fallwind in Dalmatien; 12 39 senkrecht ist eine; 15 die Stadt in Finnland ist auch „down under" anzutreffen; ***16 Gegenspieler Luthers im mittelalterlichen Deutschland;*** 18 tonloses Rohr; 19 kurzer Lebenslauf; 20 ist süss, sagt man; 22 anhänglich; 23 bei geheimer Abstimmung unerlässlich; 25 Gliedmassen; 26 gr Buchstabe; 27 kurze frz Heilige; 29 CZ Zinn; 30 frz Negationsteil; 32 arab Artikel; 33 Laubengang; 36 kurzes Segment; 38 Prunkwagen; 41 alles andere als schwach; ***44 wo man den Ausdruck „Saupreuss, damischer" hören kann***; ***46 deutscher Ostseehafen***; 47 Raummeter; 48 engl Ohr; 49 kurze Ehrenfahne; 50 gr Luft; ***51 mit 53 waagrecht zusammen ein deutscher Hansestadtstaat***; ***53 siehe 51 waagrecht***; 54 Hindernis; 56 Kunstgips; 59 Engelsbezeichnung (ph = f); 61 frz Windrichtung; 62 Schicksal; 64 ägypt Sonnengott; ***65 fränkische Flurbezeichnung***; 66 Tells Geschoss; 69 Leichathletikclub; 70 junges Schwein; 73 der Tierteil kann sich beim unsorgfältigen Umblättern ergeben; 76 Sage; ***77 zeitweise auch in 1 senkrecht zu hören***; 78 AZ Schweiz; 79 aus (lat); 81 kurzer Krafttrank; 82 böse Fehler; 86 Europameisterschaft; 88 drei gleiche Vokale; 89 es (engl); 90 jap Ureinwohner; 92 ehemaliges Schweizer Ski-As (Philippe); 93 mit angehängtem TE ein Kartenspiel; 95 zwei gleiche Vokale; 97 Berg bei Lugano; ***98 beim Regierungswechsel ein politisches Schlagwort in Deutschland***; 100 Prüfer; ***103 der Befehl zu 98 waagrecht***; 105 der Businessboss; 106 engl Zahlwort; 107 reell; 110 lange Leine; 111 sollte man eigentlich nie sagen; 112 Rudergemeinschaft; 113 kurz: Die Grande Nation.

Senkrecht: ***1 Deutsche Grossstadt***; 2 Werk von Sophokles; 5 benützen (engl); 6 unser Studiengebiet; 7 griechisch (frz); ***8 deutsche Gegend,*** möglicherweise Ursprungsland antiker Briten; ***9 Süssspeise, JFK behauptete, einer zu sein***; 11 poetische Quelle; 13 Gemeinschaften; 14 Nachlassempfänger (Mz); ***15 ehemalige Autorennstrecke der 9 senkrecht***; ***17 AZ Kempten***; 21 was das Wild häufig tut: es ...; 22 Eimer; ***24 ehem. Rundfunksender aus der Hauptstadt***; 26 mit vorgesetztem 79 waagrecht der Entdecker im Genitiv; 28 Preistabellen; 31 nicht nur seit Sarbanes-Oxley ein wichtiges Studienobjekt; 32 Langschwanzpapagei; 34 Was der Gott bei der Erschaffung der Kreatur wohl befiehlt; 35 Fehler (engl, Mz); 37 was der schnelle Fahrer gemacht hat; 39 gr Göttin der Zwietracht; ***40 der Hanseat muss von 46 waagrecht nach 51 waagrecht auf dem Seeweg dort durch***; 41 ***ein Arminia-Bundesligaklub ist dort daheim***; 42 relativ langer Zeitabschnitt; 43 tonloses nimmt; 45 Obstfrucht (Mz); 46 die Schlange im Dschungelbuch; 51 sehr kurzes Lachen; 52 rülpsen (engl); 54 ihre (frz); 55 nordisches Nutz- und Wildtier; 57 Postwertzeichen (Mz); ***58 „out of Rosenheim";*** 60 Flugkörper (Mz); 63 AZ Finnland; 67 Bruder Jakobs im AT; ***68 AZ Landsberg***; 69 Flamme; 71 Ernst Meier; 72 pers Fürwort; 74 auf Neudeutsch: „look"; 75 Heiland; 80 CZ Xenon; 83 der mit dem roten Büchlein; 84 schrieb der Römer für eins und eins; ***85 mit angehängtem b ein Fluss in Deutschland; 87 die geheime südliche Hauptstadt***; 91 sagenhafter Ritter; 94 Verlies; 96 ***Witzfigur aus der Hauptstadt***; 97 Aufforderung zum Apport; 99 Ersatzordnung; 100 Laut; 101 Tennissatz; 102 Kahn; 104 span Artikel; 108 Rekrutenschule; 109 dort (it).

Bitterli Consulting

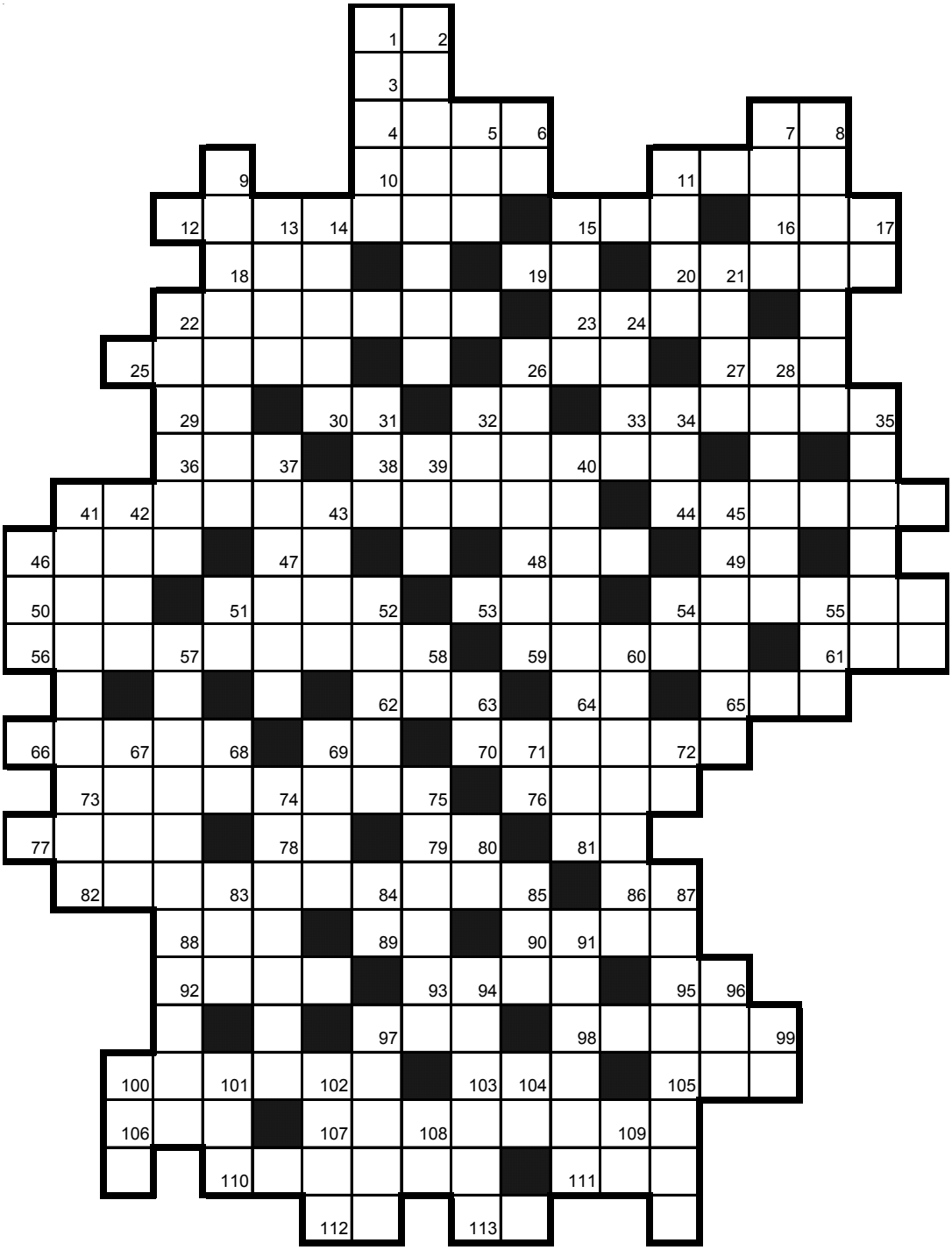
Zu vermieten direkt beim HB

Ab 1. April
Büroräumlichkeiten
Konradstrasse 1, 8005 Zürich
(neben Hauptbahnhof, Gleis 18)
3 Räume, 83m², Telefonanlage, ISDN- und Computer-Netzwerk, Einbruchmeldeanlage

Bei Fragen und für Besichtigungstermine kontaktieren Sie bitte:

Bitterli Consulting AG
Konradstrasse 1, 8005 Zürich
Stampfenbachstrasse 40, 8006 Zürich (ab 1. April)
Tel +41 (0)44 440 33 60,
Fax +41 (0)44 440 33 61

Übersichtsplan:
www.bitterli-consulting.ch/deutsch/pagesnav/KO.htm



Express Line

A Word from the Chair

Greetings and Happy New Year! As a reminder, please be advised that second invoices will be sent to members in late January. As was the case last year, members can also choose to renew online.

Sunil Bakshi
Chair, Membership Board

Certification Update

The audit for documentation of 2003 continuing professional education activities has recently begun. A randomly selected group of Certified Information Systems AuditorTM (CISA) holders has been sent an audit letter requesting written support documentation for 2003 continuing professional education hours. If any of your chapter members have questions about the 2003 audit request, please have them contact the certification department at certification@isaca.org or +1.847.253.1545, ext. 471, 403 or 474.

CISA and CISM® Pins

New this year, all chapters were sent CISA and Certified Information Security Manager® (CISM) pins for distribution to ISACA members who were newly certified from 1 January 2003 through 30 November 2004. These pins and a list of the newly certified members were shipped to all chapter presidents in December. All individuals who are not members of the association were contacted via e-mail and advised to contact the local chapter if they wish to receive recognition of their certification and a pin. Please contact the certification department at certification@isaca.org or +1.847.253.1545, ext. 403, 474 or 471, with any questions concerning the pins.

2005 Bulletins of Information

Please advise potential CISA and CISM candidates that a copy of the 2005 Bulletin of Information for each certification can be downloaded from ISACA's web site (www.isaca.org) or requested from the certification department at certification@isaca.org.

2005 Exam Registration

Exam registration forms for the 2005 CISA and CISM exams are now being received. Please remind candidates to submit their registration forms quickly and encourage them to save US $35 by registering online. Registration deadlines for the 2005 exams are:
Early: 2 February 2005
Final: 30 March 2005

CISA Job Analysis

The CISA job analysis project was recently completed and the results reported to ISACA's CISA Certification Board in November. Through a series of meetings, focus groups, interviews and surveys, a current view of the tasks performed by CISA holders and the knowledge required to perform these tasks was determined and validated. The results will help ensure that the CISA exam continues to meet the highest standards for professional certification and is representative of the work and knowledge required of CISA holders in practice. The results will be posted to the ISACA web site in June 2005 and will serve as the basis for the 2006 CISA exam.

New CISM Job Practice Analysis Begins

ISACA has begun a CISM job practice analysis study to update the criteria used to certify and examine CISM candidates. As part of this process, a series of task force meetings and focus panels has been scheduled to gather information from experienced practitioners. The initial task force meeting is scheduled for January 2005, and work should be complete by the end of 2005. Results will be implemented beginning with the 2007 exam.

2005 CISA and CISM Exam Reference Materials

CISA Review Manual 2005, CISA Review Questions, Answers & Explanations Manual 2005 (550 questions), CISA Review Questions, Answers & Explanations Manual 2005 Supplement (100 questions) and CISM Review Questions, Answers & Explanations Manual 2004 are also available in English. For information about availability in other languages, please see www.isaca.org/cisabooks.

Forum

... and you think SOX is tough!

On November 17, 2004 the last „after-hour-seminar“ of the ISACA Switzerland chapter took place at the familiar and „historic“ ***Landesmuseum*** in Zurich. Dr. Hans-Beat Jenni of ***Swissmedic*** presented the nature and characteristics of „Computerized System Validation in the Pharmaceutical Environment“.

The term Computerized Systems encompasses hardware, software, environment, users, interfaces, documentation and, last but not least, validation. I suspect that a parallel could be drawn if auditors had to express their opinion not only on internal controls (as in SOX or Basel II, expressing their opinion on the exactitude of managements' statements in this connection), but also on the quality of internal audit.

The audience was more or less stunned to get an insight into the severity with which controls have to be implemented and quality assured in this industry. It dawned on many a participant that pharmaceutical products are not necessarily expensive because of their intrinsic value, but because of the immense development and process maintenance cost. Dr. Jenni cited examples where investments of millions of dollars had to be ditched because a lack of control or quality assurance had been discovered and could not be repaired.

It probably was clear for everyone that the hospital and pharmaceutical branches need special care and supervision because not only health and wellbeing, but life itself is at stake. One would expect that government supervision bodies would take an active role and send legions of auditors to the production plants and hospitals. Not so. A series of „Good Practices“ (laboratory, manufacturing, distribution and clinical ones), hereafter GxP, form the basis of the „code of ethics“ of the industry. The principles have been approved by the OECD as well as countries around the world. As new developments are occurring all the time it was agreed that amendments or appendices to the basic protocol would be added in order to avoid tiresome and onerous procedures in legal battles through parliaments around the globe.

What impressed me the most was the statement by Dr. Jenni that the inspection (by ***Swissmedic***) focuses on the person(s) charged with the Quality Assurance rather than e.g. the mechanics of production themselves. Moreover, a global view and approach of the system is preferred against detail verifications. The inspector is trained to find deviations rather than approve systems as such.

As the enterprises in this industry need a license to produce, sell and/or operate, they strive to adhere to the GxP. The development evolves further all the time, and compliance with rules of all countries into which products are exported have to be adhered to. Wow. In just a short time Dr. Jenni succeeded in making his mark: SOX is just regarding financial facts and figures, the GxP addresses „everything“.

I am looking forward to the interesting topics of the after hour seminars in 2005!

Max F. Bretscher

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

Achtung wichtig!

Das ISACA-Kurssekretariat ist ab 14. März 2005 unter der folgenden Adresse erreichbar:

ISACA Switzerland Chapter
Kurssekretariat
c/o ITACS Training AG
Stampfenbachstrasse 40
CH - 8006 Zürich
Tel +41 (0)44 444 11 01
Fax +41 (0)44 444 11 02

DACH-News

D: Aktivitäten des German Chapters

Ein weiteres Jahr der Vorstandsarbeit ist nun beinahe vorüber und in Kürze steht wieder die Mitgliederversammlung des ISACA German Chapters an. Diese wird am 11. März 2005 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 weiter aktiv den Verein vorantreiben.

Zum ***NewsLetter*** 4/2004 möchte ich eine fälschliche Angabe zum Autoren des Artikels „Die Linux Audit Group – ein Erfahrungsbericht" richtig stellen. Der Artikel wurde natürlich nicht von mir geschrieben, sondern von Herrn Neuy, der mit großem Einsatz das Thema im Rahmen des ISACA vorangetrieben hat und ohne den sowohl das Ergebnis wie auch dieser Artikel nie zustande gekommen wäre. Herr Neuy, vielen Dank noch einmal von dieser Seite.

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 ***NewsLetter*** und lassen Sie andere auch ein wenig an Ihren Praxiserfahrungen oder dem erworbenem Wissen teilhaben. Wenn Sie Fragen dazu haben sollten, können Sie das Vorstandsmitglied Ingo Struckmeyer 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 möchten wir an dieser Stelle nochmals für ihre wirklich gelungenen Artikel danken. Insbesondere möchte ich all denjenigen danken, die am ersten ***NewsLetter*** des German Chapter mitgewirkt haben.

Ingo Struckmeyer
Vorstand German Chapter

CH

100. Vorstandssitzung des ISACA Switzerland Chapter

Am 14. Dez. 2004 hat die Präsidentin zur 100. Vorstandssitzung eingeladen. Zwischen der ordentlichen Sitzung und dem köstlichen Mittagessen versammelten sich der Vorstand und das Redaktionsteam zum Fototermin im Lichthof der SwissRe.

Im 15. Jubiläumsjahr des ISACA Switzerland Chapter war der Vorstand mit der Durchführung der EuroCacs 2004 in der Schweiz besonders gefordert. Weiterhin beschäftigten uns auch das Ausbildungsangebot und unsere „Kundeninterfaces": vor allem der Webauftritt hat sich im 2004 markant

Vordere Reihe v.l.n.r.: Max Bretscher & Francesca Lüscher Baglioni (Redaktionsteam), Pierre Ecoeur, Daniela Gschwend (Präsidentin), Bruno Wiederkehr
Hintere Reihe v.l.n.r.: Thomas Bucher, Michel Huissoud, Rolf Merz, Peter Bitterli

verbessert und die Auflage des ***News-Letters*** wurde wiederum gesteigert. Sie halten nun die Nummer 72 vom ***News-Letter*** in den Händen, die mittlerweile an rund 1100 Mitglieder der ISACA Chapter CH, D und A verteilt wird.

Das End-Jahres Meeting diente zugleich dazu, die Ziele, Termine, Themen, Beiträge, Ausbildungen und Veranstaltungen für das kommende Jahr festzulegen. Auch die ISACA als Non-Profitorganisation muss die Kosten sowie die Qualität im Auge behalten. Nichts Neues werden Sie sagen, klar. Wir haben uns neben den Ausbildungs- und Marketingthemen vor allem mit der Balance zwischen Attraktivität des ***Newsletters*** versus zusätzliche Gestaltungskosten befasst. Das Resultat werden Sie demnächst sehen.

Wir haben uns vorgenommen, dass wir alle Bilanz ziehen über die Qualität, mit der wir unsere Mitglieder bedient und unsere Interessenten erreicht haben. Und da die Jahreswende normalerweise nicht nur „Bilanz ziehen", sondern auch „gute Vorsätze fassen" bedeutet, fragen wir uns, wie wir unsere Beziehungen zu unseren Mitgliedern und Interessenten verbessern können. Mit der Teilnahme an unserer GV in Biel bietet sich eine gute Gelegenheit, mehr darüber zu erfahren. Reservieren Sie sich schon heute das Datum des 17. März 2005.

Der Vorstand und das Redaktionsteam wünscht Ihnen ein erfolgreiches Neues Jahr. Wir freuen uns, Ihnen im 2005 erneut relevante, aufschlussreiche und anregende Beiträge sowie professionelle Ausbildungsveranstaltungen anbieten zu können. Um dieses Ziel zu erreichen sind wir selbstverständlich weiterhin auf Ihr freiwilliges Mitwirken und kritischen Feedback angewiesen.

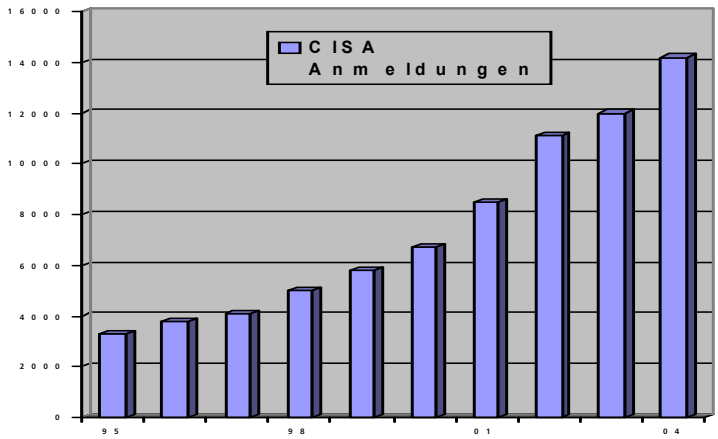
Bruno Wiederkehr

Neue Horizonte in der ICT Ausbildung

Die Information Systems Audit and Control Association (ISACA) ist eine weltweite Vereinigung von Fachleuten, die sich mit Governance, Sicherheit, Kontrolle, Revision und Management der Informations- und Kommunikationstechnologie (ICT) befasst. Die ISACA besteht aus über 40'000 Mitgliedern in mehr als 100 Ländern.

reichte Qualität der vom ISACA Switzerland Chapter gemeinsam mit ITACS Training angebotenen Zertifikatskurse.

Ein CISA muss in sieben verschiedenen Schwerpunktbereichen seine Kenntnisse nachweisen: Neben der Informatik-Revision sind dies u.a. Führung, Entwicklung sowie Unterhalt der Informatik, Informations- und Kommunikationstechnologie, Sicherheit, Kontrolle, Geschäftskontinuität usw.



Quelle: CISA Exam Bulletin of Information 2005

Rund 12'700 Kandidaten haben weltweit an den CISA- und CISM-Examen vom 13. Juni 2004 teilgenommen. Davon haben 53 %, d.h. rund 6'700 Kandidaten, die CISA-Prüfung („Certified Information System Auditor") bestanden; bei der neuen CISM-Prüfung („Certified Information Security Manager") waren es rund 73% (also gut 500) der rund 600 Kandidaten.

Hervorragend hingegen sind die Zahlen in der Schweiz: die Erfolgsquote von 95% der am Schweizer CISA-Kurs teilnehmenden Kandidaten ist ausgezeichnet und hat den Landesdurchschnitt auf immerhin rund 80% hochgedrückt; beim CISM-Kurs waren es immer noch respektable 85%. Dies zeigt einerseits das hohe Niveau der fachspezifischen Berufskenntnisse in der Schweiz und andererseits die er-

Ein CISA setzt sich im gesamten Informatikumfeld sehr intensiv mit den jeweiligen Risiken, Sicherheitsanforderungen und möglichen Massnahmen auseinander. Dabei befasst er sich insbesondere mit der Frage, ob die Risiken durch angemessen Vorkehrungen abgedeckt sind, um die Geschäftsziele effektiv und effizient zu erreichen.

Die Tendenz der weltweit an der Prüfung registrierten CISA's ist weiterhin steigend.
Beim relativ neuen CISM-Berufsbild liegt der Focus beim Management der Informationssicherheit, beim Risikomanagement und beim Responsemanagement, wobei eher die organisatorischen als technischen Fragen im Vordergrund stehen.

Das Interesse an den beiden Zertifikatskursen und die hohe Erfolgsquote ist

ein Indiz dafür, dass sich die Schweiz auf die steigenden Anforderungen im Bereich Revision und Sicherheit vorbereitet. Die Ausbildung im ISACA-Kurs erfolgt in einer idealen Mischung aus Präsenzunterricht, Selbststudium und zu lösenden Aufgaben („Blended Learning"). Der 17tägige CISA-Kurs (CISM-Kurs: 13 Tage) ermöglicht somit einen effizienten und zielorientierten Wissensgewinn. Die Vorbereitungskurse haben bereits begonnen. Weltweit finden die Examen einmal im Jahr jeweils Mitte Juni statt. Anmelden kann man sich bis 30. März 2005 unter www.isaca.org.

Die ISACA selbst verfügt über eine enorme Wissenssammlung, welche weltweit den Mitgliedern für die praktische Umsetzung zur Verfügung steht. Dies betrifft zum Beispiel die Einführung neuer Regulative, wie Basel II, Sarbanes-Oxley-Act, welche unweigerlich zu Zusatzaufwänden in der ICT führen. Daneben gibt es unzählige Dokumente zur Beherrschung der technologie-bedingten Risiken (Viren, Spam und Phishing-Attacken usw.).

Das ISACA Switzerland Chapter hat gegenwärtig 600 Mitglieder. Mit der letztjährigen Zunahme von annähernd 20% und als anerkannter Leader in IT Governance hat die ISACA die Nase vorn. Weitere Informationen zu unseren Veranstaltungen werden laufend auf dem Web unter www.isaca.ch (national) und www.isaca.org (international) publiziert.

Bruno Wiederkehr
ISACA Switzerland Chapter
www.isaca.ch

2005 Jahr der Technik

CISA/CISM: Wir gratulieren nochmals!

Folgende Kandidaten haben die Prüfung im 2004 erfolgreich bestanden (aufgeführt sind nur die Kandidaten, welche das Einverständnis zur Freigabe ihres Resultats gegeben haben):

CISA-Prüfung:
Jürg Altmeier
Attila Banko
Dan Basile
Olivier Battaglia
Otte Bertschi
Hans Beumer
Franz Bruhin
Urs Burkart
Thierry Cesne
Michele Corletto
John Dempsey*
Martin Falconer
Jürgen Flaig
Markus Frei
Daniel Fuchs
Achilles Haering
Martin Hauser*
Falk Hennig
Götz Hoffmann*
Alex Hofmann
Tina Hostettler
Philipp Husi
Mafaz Ishaq
Michael Kupferschmid
Nathalie Lacambra
Alexandre Malotchko
Isaac Mendelberg
Marcel Meyer
Thomas Moll
Jürgen Müller
Dana Nicoara
Cayhan Oezguerol
Yvan Reymond
Didier Schmassmann
Preethi Subramanian
Ralph Theiler
Albert Thompson
Chandrasekar Varahan
Matthias von Wartburg
Jean-Claude Wicki
Antonie Wüthrich
Ling Yun

CISM-Prüfung:
Johannes Buck*
Thomas Leuthard*
Luc Pelfini
Urs Schmid
Francois Sordet*

* Top Scorers! Die ersten drei CISA/CISM, bezogen auf den Prüfungsort Zürich. Im zweiten und dritten Rang gab es jeweils mehrere Kandidaten mit gleicher Punktzahl.

CISA/CISM Coordinator,
ISACA Switzerland Chapter
Thomas Bucher

CISA/CISM Club besucht die SF DRS Fernsehstudios in Zürich

Als CISA/CISM-Club-Anlass hat am Donnerstag, 4. November 2004 die Führung in den SF DRS Fernsehstudios in Zürich stattgefunden. Einige der vielen Bilder von den Studios und den 16 Teilnehmern (nebenstehend).

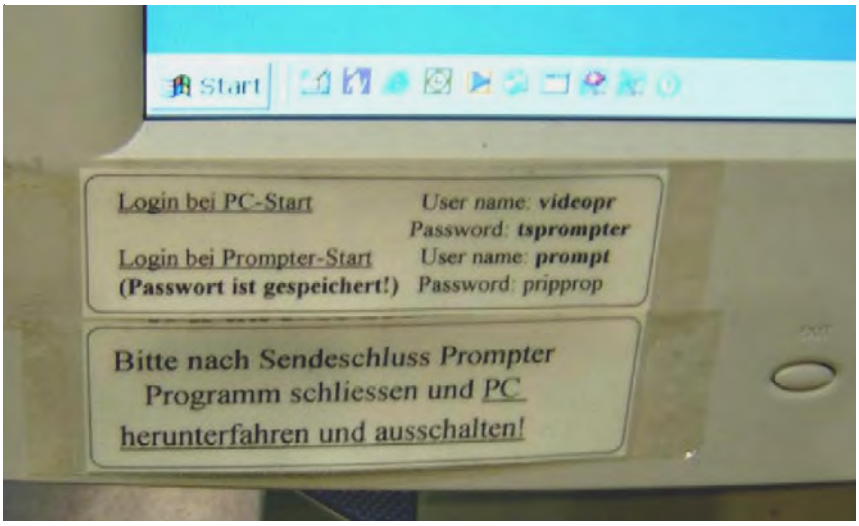
CISA/CISM Coordinator, ISACA Switzerland Chapter
Thomas Bucher

Michel Huissoud berichtet:

Die beiden Gesetze DNA-Profil-Gesetz und Bundesgesetz über die elektronische Signatur und die dazugehörenden Verordnungen wurden unter der Systematischen Rechtssammlung (SR) des Bundes publiziert.

DNA-Profil-Gesetz:
<http://www.bk.admin.ch/ch/d/sr/c363.html>

DNA-Profil-Verordnung:
<http://www.bk.admin.ch/ch/d/sr/c363_1.html>
Bundesgesetz über die elektronische Signatur (ZertES):



<http://www.bk.admin.ch/ch/d/sr/c943_03.html>
Verordnung über die elektronische Signatur (VZertES):
<http://www.bk.admin.ch/ch/d/sr/c943_032.html>

Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur:
<http://www.bk.admin.ch/ch/d/sr/c943_032_1.html>

Der Text der technischen und administrativen Vorschriften des BAKOM sind in den amtlichen (AS) und systematischen Rechtssammlungen (SR) des Bundes nicht publiziert. Sie können beim BAKOM unter dem folgenden Link bezogen werden:
<http://www.bakom.ch/imperia/md/content/deutsch/telecomdienste/internet/digitalesignatur/ptad.pdf>

News aus den Interessengruppen

IG Operational IT-Risk

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

Die Interessensgruppe „Operational IT-Risk“ hat sich in den vergangenen Monaten intensiv mit der Frage beschäftigt, welche (IT-) Sicherheitsanforderungen in den verschiedenen Gesetzen und Verordnungen (Basel II, EBK-Richtlinien, HIPAA, CFR 11, EU Datenschutzgesetz, DSG und VDSG usw.) vorkommen. Die Arbeit hat zu ein paar interessanten Erkenntnissen aber wenig direkt in die Praxis umsetzbaren Ergebnissen geführt.

Die Interessengruppe „Operational IT Risk“ plant in der jetzigen Phase eine Kochbuch-ähnliche Anleitung für das Management von IT-Risiken, welche vor allem für KMU, für Unternehmen ohne grosse Sicherheitsanforderungen an die IT oder für die ersten Schritte in ein umfassenderes IT-Risikomanagement (analog CobiT Quickstart) gedacht ist. Für diese zweite Phase werden noch zwei bis drei neue Mitglieder gesucht; arbeitswillige Personen mit genügend Zeit sollen sich bitte (erneut) an den IG-Leiter wenden.

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

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

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 juri-diques 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

Leider musst die für den 14.12.2004 geplante Sitzung verschoben werden. Ein neuer Termin wird voraussichtlich für März 2005 festgelegt.Weitere Interessenten können sich bei Rolf Merz anmelden.

Traktanden:
1. Präsentation der beiden Pilotprozesse PO1 und PO10
2. Festlegen Weiteres Vorgehen
Themen, Ziele und Organisation der nächsten Sitzung

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: Mittwoch, 30. März 2005, 09.30 bei Ernst & Young AG, Bleicherweg 21, Zürich
Traktanden:
- Wrap-Up/Standortbestimmung
- Weiteres Vorgehen
- Wahl des neuen IG-Leiters

■ Diverses
ev. gemeinsames Mittagessen

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

Aus dem Protokoll der IG-SAP vom 13. Mai 2004:
Herr Bolli (Bundesamt für Informatik und Telekommunikation, CCSAP Entwicklung und Qualitätssicherung) zeigte die Veränderungen auf, die durch den Einsatz von WEB-Applikations-Server und damit der Programmiersprache Java auf uns zukommen.

Der Input ins SAP-System kommt vom SAPGUI und vom Internet zum Verbindungsserver und von da in beiden Formaten zur Datenbank. Der SAP WEB Dispatcher entscheidet auf welche Queue (Instanz) der Input geht.

In Java wird weniger programmiert, sondern vielmehr modelliert. Das Change Management System macht eine Versionen-Verteilung-Comp.

Wichtige Erkenntnisse:
■ Java sollte nie direkt auf das SAP-System zugreifen, sondern über API (Application Programming Interface) auf die Datenbanken zugreifen oder über UME-API (User Management Engine Application Programming Interface).
■ Im Portal im UME muss angegeben werden, auf welche Daten der Zugriff erlaubt ist.
■ Die Java-Entwicklung sollte in einem EU-Umfeld (Entwicklungsunit) gemacht werden.
■ Java ist schwierig zu prüfen, eigentlich fast unmöglich.
■ Man kann aber die Rückmeldung (XE) prüfen; dazu ist ein Prüfverfahren einzurichten.
■ Man sollte die Schnittstellen von SAP (Web AS) verwenden.
Wegen Sicherheitsrisiken ist es besser erst ab Web AS 6.40 und XE Java zu verwenden.
■ Zur weiteren Sicherheit empfiehlt es sich, eine SSL-Zertifizierung zu machen.

Wie sieht voraussichtlich die Zukunft aus?
■ ABAP wird mindestens noch fünf Jahre zur Entwicklung verwendet, nur neue Features und Portale usw. verwenden heute schon Java.
■ Web AS 6.40 wird mit ABAP verwendet und ist im Enterprise 4.7 Release.

Herr Kowalski (Bundesamt für Informatik und Telekommunikation, CCSAP Entwicklung) stellt uns CRM Internet Sales vor. Um die Regel des BIT „von aussen keinen Zugriff auf innen“ zu beachten, wurde folgende Lösung angewandt: Kunde gibt Daten vom Internet (aussen) und SAP ***holt sie ab*** (innen).

Um den Ausgleich im FI-Bereich flüssig zu gestalten wird das Clearing der Kreditkarten mit der Software „Match-box“ gemacht.

Das heisst: Aufwand verbucht = Erlösminderung verbucht. „Match-box“ mit Referenznummer kann beim Input oder beim Clearing installiert sein. Jedes Kreditinstitut hat ein eigenes Format.

Frau Galli stellt kurz die Präsentation „Stand der Sicherheit der in der Schweiz eingesetzten SAP-Systeme“ von Herrn Altmeier, dem Leiter der Arbeitsgruppe SAP der FGSec, vor. Herr Altmeier hat diese Präsentation beim Anlass der FGSec vom April 2004 vorgestellt. Einige der Anwesenden waren an dieser Veranstaltung.

Erfahrungsaustausch
■ Die Liste der neuen Aktivitäten im System unter Enterprise wird nochmals versandt werden.
■ Der Link zu Herrn Schiweks AIS-Präsentation zu den Änderungen mit Enterprise 4.7 wird nochmals versandt werden.
■ Eine Liste der neueren SAP-Hinweise im Zusammenhang mit Security im SAP wird versandt werden.
■ Eine IBS-News-SAP über die Zukunft mit SAP wird versandt werden.

Interessenten können sich bei Monika Galli, Leiterin IG-SAP melden.

Veranstaltungen

Application Security Lab – Workshop zum Thema Sicherheit von Web-Anwendungen	15.–17. März 2005 Zürich, 3 Tage, ISACA CH/Compass
Informations- und Know-How-Schutz im Unternehmen	16. März 2005 Zürich, 1 Tag, SSI/MediaSec
BS7799 Überblick über die Normen	21. März 2005 Zürich, 1 Tag, Infosec
How to Audit SAP R/3 Basis	4.–7. April 2005 Genf, 4 Tage, MIS
CobiT User Convention	11.–12. April 2005 TBA (Europa), 2 Tage, ISACA USA
Internet Security Lab – Workshop mit Angriffsszenarien und Abwehrmassnahmen	20.–22. April 2005 Zürich, 3 Tage, ISACA CH/Compass
Service Management - ITIL Foundation Training – Auf der Basis de facto-Standards ITIL mit Links zur BS 15000 Zertifizierung	2.–4. Mai 2005 Zürich, 3 Tage ISACA CH/glenfis
Evidence Lab – Workshop über die Spurensuche in Computersystemen	11.–13. Mai 2005 Zürich, 3 Tage, ISACA CH/Compass
Audit & Control of Information Technology & Systems	17./18. Mai 2005 London, 2 Tage, MIS
Wireless-LAN-Sicherheit	20. Mai 2005 Zürich, 1 Tag, Infoguard
Fraud Bootcamp	23.–27. Mai 2005 Genf, 5 Tage, MIS
ITIL Business Continuity and IT Service Continuity – Von Business Continuity zur IT Disaster Recovery auf der Basis des de facto-Standards ITIL	26.–27. Mai 2005 Zürich, 2 Tage, ISACA CH/glenfis
2nd Annual CISO Executive Summit	16./17. Juni 2005 Genf, 2 Tage, MIS
International Conference	19.–22. Juni 2005 Oslo, 4 Tage ISACA
Wirtschaftsspionage – Cyber Crime and Best Defence	24. Juni 2005 Zürich, 1 Tag, Infoguard
Prüfung von Schnittstellen/Audit des Interfaces	30. Juni 2005 Bern, 1 Tag, ISACA/Kammer

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.ch

There once was an old audit fellow named Box
Who had the nerve to wear all colours of socks.
Some of them red, others yellow and blue
He referred to Basel as his number two,
And Sarbanes he called for short only SOX.

SOX

Ein Revisor hielt im Keller als Reserve zehn kastrierte Rinder,
Zum Nachschütten, wenn die Qualität des Weines sei minder.
Er verwechselte Ochsen mit Oechsle,
Und zusätzlich Sarbanes mit Oxley.
Jetzt lachen alle Familienglieder, besonders die Kinder.

Vergessen Sie das Backup !

Das smarte, revolutionäre und vollautomatische Datensicherheits-system aus der Schweiz

ab Sfr/Monat 480,-

Detaillierte Informationen bestellen Sie über www.swissvault.ch

SWISSVAULT®
the backup butler by SIAG

- ☑ automatisches Backup
- ☑ 448 Bit Verschlüsselung
- ☑ automatische Datenaus-lagerung in Swiss Fort Knox
- ☑ ultraschneller Restore
- ☑ globaler Einsatz
- ☑ automatisches Datenarchiv inkl. Versionsmanagement
- ☑ von 250 GB bis 4250 GB
- ☑ SATA Raid 5 Disk-Array's
- ☑ Desktops, Laptops, Servers
- ☑ Live-Database-Backup
- ☑ Open File Management
- ☑ zentrales Management
- ☑ modular & wartungsfrei
- ☑ höchste Sicherheit

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
Michael M. Schneider
Tel. +49-69 75606 121
michaelschneider@deloitte.de

Austria Chapter

Vorsitzender (Präsident)
Ing. Mag. Dr. Michael Schirmbrand
Tel: +43 1 211 70-2831
michael.schirmbrand@at.eyi.com

Stellvertretender Vorsitzender I (Vizepräsident I)
Dipl.-Ing. Maria-Theresia Stadler,
Tel: +43 1 531 27-857
maria-theresia.stadler@oekb.co.at

Stellvertretender Vorsitzender II (Vizepräsident II)
Mag. Josef Renner, StB
Tel: +43 1 50188-0

Sekretär
Mag. Gunther Reimoser, CISA
Tel: +43 1 21170-4113
gunther.reimoser@at.eyi.com

Kassier
Mag. Helmut Zodl
Tel: +43 1 21145-0
helmut_zodl@at.ibm.com

CISA-Koordinator
Mag. Maria Rieder
Tel: +43 1 71715-0
maria.rieder@aon.at

Public Relations/Newsletter-Koordination
Rolf von Rössing
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

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 1 440 33 60
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@ah.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 1 910 96 33
bru.wiederkehr@bluewin.ch

Homepage ISACA Switzerland Chapter: www.isaca.ch