Information Systems Audit and Control Association

News Letter

Nr. 61, November 2002

Thema Ausbildung

Switzerland Chapter
Germany Chapter
Austria Chapter

© 19.11.2002

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o Monika Josi
PricewaterhouseCoopers AG
Nordstrasse 15
8035 Zürich

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

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

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

Abo-Preis:
Mitglieder gratis
Abonnemente und Einzelnummern auf Anfrage

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

Erscheint 5 Mal jährlich
Auflage: 1000 Exemplare

Nächste Ausgabe (Thema: Datenschutz):
Februar 2003, Redaktionsschluss:
17. Januar 2003

Inhaltsverzeichnis

Editorial 4

Ausbildung – Identifier les besoins en formation : intuition ou système ? 5

Ausbildung – Computer und Web Based Training 7

Ausbildung – IT Security Awareness Programm 9

Ausbildung – Lernen ist lernbar, welche Ausbildung ist heute notwendig? 13

Ausbildung – Blended-Learning-Konzept (BLK) 16

Projektleitung und projektleitende Revision von Softwareentwicklungsprojekten 18

Risikomonitoring mit CAAT 20

The ISACA Crossword Puzzle 22

News aus den Interessengruppen 24

DACH-News 26

Veranstaltungen 28

Express Line 30

Germany Chapter 31

Austria Chapter 32

Switzerland Chapter 33

Editorial

„Es gibt nichts Teureres als Aus- und Weiterbildung.“ Ein Zitat von einem kostengestressten Lehrmeister, den ich als Ausbildungsberater vor über zwanzig Jahren aufsuchte. Ich nahm die Aussage als Vorwurf entgegen, senkte den Kopf und zuckte mit den Achseln. Auch ich hatte meine Kostengrenzen.

Als ich aufblickte, sah ich das Augenzwinkern meines Gegenübers, als er fortfuhr: „…ausser *keine* Aus- und Weiterbildung.“ Ich habe diesen Gag inzwischen in verschiedenen Varianten immer wieder gehört und gelesen. Vielleicht trifft er sogar zu.

Im Umfeld der sich seit Jahrzehnten rasant weiter entwickelnden Informatik ist die Aussage wohl sehr richtig. Jemand, der sich nicht laufend weiterbildet, ist schnell weg vom Fenster, verpasst Aufstiegschancen und wird letztlich arbeitslos. Zusätzlich verbreiterte sich diese Disziplin derart, dass ein „Auf-der-Höhe-Bleiben“ flächendeckend gar nicht (mehr) möglich ist: Eine Spezialisierung ist nicht nur gefragt, sondern ein Muss. Demnach ist auch die Aus- und Weiterbildung spezialisiert.

Nur: Es gibt verschiedene Arten und Qualitäten von Aus- und Weiterbildung. Die logische Fortsetzung des Spruchs meines eingangs erwähnten Gesprächspartners wäre demnach: „…am Teuersten ist wahrscheinlich eine falsche und schlechte Aus- und Weiterbildung.“

Viele Ansätze, wie die richtige Aus- und Weiterbildung anzubieten und auszuwählen ist, sind zu beobachten. Die vorliegende Ausgabe des *News-Letters* illustriert in mehreren Beiträgen, wie die Autoren die Herausforderung angehen.

Ich wünsche Ihnen, liebe Leserin, lieber Leser, in diesem Sinne eine allseits „lehrreiche“ Lektüre und für die kommenden Festtage viel Schönes und Gutes.

Max F. Bretscher, Redaktor

« Il n’existe rien de plus coûteux que le perfectionnement professionnel. ». Cette citation vient d’un conseiller en formation que j’avais consulté il y a une vingtaine d’années. Je l’ai reçu comme un reproche, j’ai rentré la tête dans les épaules et je m’apprêtais à repartir penaud. Je devais finalement également respecter mon budget.

Avant de le quitter, j’ai relevé les yeux et j’ai vu qu’il rigolait. Il poursuivi sa citation : « … sauf pas de perfectionnement professionnel du tout ! ». J’ai entendu depuis ce gag dans plusieurs variantes et peut-être qu’il contient même un fond de vérité.

Cette citation est certainement encore plus juste dans le domaine informatique. Le développement frénétique auquel nous assistons oblige à un perfectionnement professionnel permanent. A défaut, ce sont des opportunités de carrière qui peuvent disparaître puis finalement le chômage qui pourrait menacer. Le développement de cette discipline rend d’autre part impossible de rester à la hauteur sur toute la palette des technologies de l’information. Une spécialisation devient incontournable et le perfectionnement professionnel doit s’aligner sur cette tendance.

Bien. Mais on constate également différentes qualités d’offres de perfectionnement. Une variante de la citation de tout à l’heure pourrait être : « le gaspillage le plus important réside dans une mauvaise formation ou une formation inappropriée. »

Il existe beaucoup d’avis et de démarches sur les pièges à éviter et la manière dont une bonne formation doit être organisée. Ce numéro de votre *NewsLetter* illustre quelques points de vue sur ce thème.

Je vous souhaite, chers lecteurs, une lecture très « instructive » de ces articles et je vous adresse mes vœux les meilleurs pour les jours de fête qui déjà approchent à grands pas.

Max F. Bretscher, rédacteur en chef

Ausbildung

Identifier les besoins en formation : intuition ou système ?

La demi-vie de la formation : ne vaudrait-il pas mieux privilégier le développement de la personnalité plutôt que l'acquisition de savoir ?

La science médicale connaît la notion de demi-vie. Il s'agit de la durée nécessaire à une substance thérapeutique pour perdre la moitié de son efficacité. Un bon médicament doit généralement présenter une longue demi-vie. C'est ce que nous souhaitons tous dans le domaine de la formation. Suivre un séminaire qui nous sera encore utile dans dix ans. Donner un cours qui marquera de nombreuses années les étudiants.

L'offre de formation peut viser à développer les connaissances, le savoir-faire ou la personnalité des étudiants. Dans le domaine professionnel de l'expertise comptable, le savoir et le savoir-faire ont traditionnellement bonne presse. Le responsable d'un service d'audit donnera plus facilement son feu vert à un séminaire sur les dernières normes comptables qu'à un cours sur les techniques d'interviews. Si l'on se place sous l'angle de la demi-vie, force est de constater que cette attitude n'est pas automatiquement la meilleure. La situation dans le domaine de l'audit informatique est extrême. Les connaissances acquises risquent de se révéler caduques après quelques mois, dépassées par l'avancée technologique. Il est donc essentiel de ne pas l'oublier lors de l'établissement d'un programme de formation. Une revue des objectifs d'enseignement devrait permettre de substituer aux classiques objectifs « l'étudiant a été informé de … » des objectifs plus prometteurs de type « l'étudiant est capable de … », voire « le comportement de l'étudiant a été modifié de la manière suivante : … ».

Le recours systématique à des études de cas, des travaux de groupe ou à des jeux de rôle pour dispenser du savoir constitue à cet égard un compromis efficace, qui permet de joindre à l'acquisition de notions – peut-être rapidement dépassées – des méthodes d'apprentissage qui peuvent laisser des traces plus durables sur le plan humain.

Programmer une formation professionnelle ne doit pas relever du hasard

La formation s'inscrit dans un cycle plus général qui est comparable à celui du Knowledge-Management. Un tel cycle comprend traditionnellement huit étapes, allant de la définition des objectifs stratégiques à l'évaluation de l'efficacité de la formation en passant par l'organisation concrète des cours (voir figure 1).

La définition des objectifs constitue pour une école ou une association professionnelle l'étape essentielle de ce processus. Qui doit identifier les besoins futurs ? Et avec quels moyens ? Nous sous-estimons probablement aujourd'hui l'apport des associations professionnelles. Entre la pratique professionnelle quotidienne et les hautes sphères universitaires, des associations comme la Chambre fiduciaire ou l'ISACA ont un rôle essentiel à jouer. Les membres de leurs différentes commissions, groupes d'intérêts ou de travail et autres comités devraient être en mesure de relayer les besoins de la base afin de permettre aux écoles

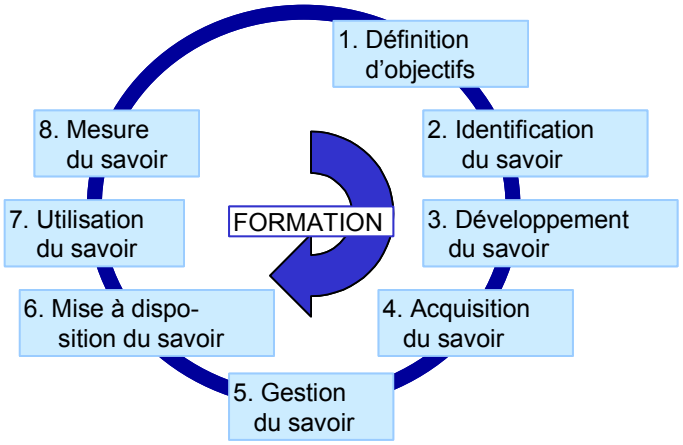


Figure 1: une formation ne se limite pas au point 6 « Mise à disposition du savoir » mais doit s'inscrire dans un cycle

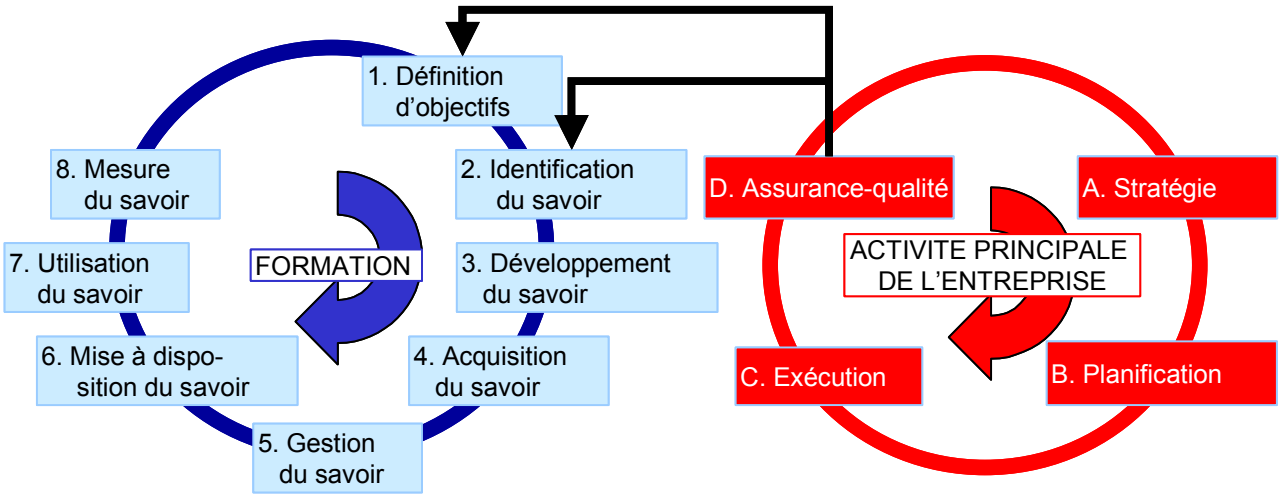


Figure 2: l'assurance-qualité de l'entreprise constitue un input essentiel pour la formation

professionnelles de mettre sur pied les offres de formation correspondantes. Encore faudrait-il que ces écoles recherchent activement et de manière supra-disciplinaire ces informations et disposent du réseau nécessaire. Certainement un point susceptible d'être amélioré dans le futur.

Le lien avec les systèmes d'assurance-qualité des entreprises – abordé ci-après – constitue un autre instrument qui mériterait d'être renforcé.

L'évaluation de l'efficacité de la formation professionnelle (point 8. « Mesure du savoir ») est un autre point important et souvent négligé de ce cycle. On se rend compte que considérées sous cet angle, les méthodes d'évaluation mises actuellement en place dans des institutions comme l'Académie suisse d'expertise comptable ou l'ISACA sont insuffisantes. Les informations collectées par questionnaires à la fin d'un séminaire permettent tout au plus d'identifier les problèmes les plus grossiers mais ne sauraient donner une information sur l'efficacité de la formation. Celle-ci devrait être mesurée au poste de travail et au terme du laps de temps nécessaire à la mise en œuvre des objectifs de formation. Les filières de formation professionnelles qui mettront en place un tel système intégré bénéficieront dans le futur d'un réel avantage concurrentiel.

L'apport essentiel de l'assurance-qualité

Les entreprises investissent à juste titre d'importantes ressources dans des systèmes d'assurance-qualité. La grande vague des certifications ISO est probablement terminée mais elle a laissé de traces qui mériteraient d'être considérées par les personnes actives dans le domaine de la formation professionnelle.

Au sein des entreprises déjà, un audit de la fonction « formation » devrait vérifier que la communication fonctionne de manière satisfaisante. Ce n'est pas le cas si le responsable de la formation réimprime année après année le même programme de formation interne sans réaliser que les responsables de l'assurance-qualité se plaignent de devoir toujours corriger les mêmes erreurs. Un programme de formation interne devrait systématiquement intégrer les expériences vécues, y compris les éventuelles critiques exprimées par les auditeurs internes ou externes, avant que l'entreprise puisse prétendre qu'elle est une « lernende Organisation » qui tient compte des « lessons learned » (voir figure 2).

Cette réflexion à l'échelon des entreprises vaut également à l'échelon des écoles professionnelles. Quitte à court-circuiter les responsables des ressources humaines des différents partenaires, les écoles devraient identifier les acteurs de l'assurance-qualité au sein de la branche, afin d'identifier à la source et de comprendre les besoins des employeurs.

La prochaine mise en place d'une institution suisse de surveillance des activités d'audit externe constitue à cet égard une chance à saisir pour l'Académie suisse d'expertise-comp-

table et pour tous les autres organismes offrant des offres de formation professionnelle dans ce domaine.

Encore faudra-t-il que cette nouvelle institution accepte de communiquer de manière transparente les erreurs constatées dans la branche. Un thème relativement tabou jusqu'à l'affaire Enron…

Zusammenfassung

Der Autor stellt sich die Frage, wie die Erfordernisse an die Ausbildung festgestellt werden sollen. Er orientiert sich an der Halbwertszeit des Wissens und fordert, dass die Bewertung diesen Umstand berücksichtigt. Die Qualität der Ausbildung kann eigentlich erst nach einiger Zeit beurteilt werden. Deshalb ist eine Systematik notwendig, welche sich in zwei Regelkreise aufteilt. Der erste beinhaltet die Ausbildung an sich, der über

- Zieldefinition,
- Identifikation,
- Entwicklung,
- Aneignung,
- Verwaltung,
- Bereithalten und
- Benützen zum
- Messen

des Wissens führt.

Der zweite Regelkreis, welcher jede Institution bzw. Firma selbst betreiben sollte, beinhaltet die Stufen

- Strategie
- Planung
- Ausführung und
- Qualitätskontrolle

Die aus Qualitätssicherung und -kontrolle gewonnenen Erkenntnisse fliessen sodann korrigierend und bereichernd in die Zieldefinition und die Identifikation des Wissens des ersten Regelkreises ein.

Michel Huissoud,
vice-président ISACA (Suisse)

Ausbildung

Computer und Web Based Training

Computer und Web Based Trainings, kurz CBT und WBT genannt, sind Lernprogramme für das Selbststudium mit dem Computer. Computer Based Trainings werden auf dem PC installiert, Web Based Trainings sind über das Intra- oder Internet zugänglich. Diese Form des Lernens ist nur *relativ* neu, sie hat jedoch mit dem Internet eine weitere Dimension erhalten. Der Zugang zu den Lernprogrammen über das Internet ist einfacher und weniger aufwändig als das Installieren des Lernprogrammes auf den PC und die Programmierung der Lernprogramme ist durch neue Programmiertools einfacher und effizienter geworden. So kommen wir als Lernende und Ausbildende immer häufiger in Kontakt mit diesen Lernformen am PC.

Finanzielle Überlegungen

CBT/WBT ist teuer, hört man oft, und wird aus diesem Grund ohne genaues Nachrechnen und Vergleichen mit konventioneller Ausbildung als Idee rasch verworfen. Es lohnt sich jedoch, die Ausbildungssituation zu analysieren und alle Vor- und Nachteile der konventionellen Ausbildung mit CBT/WBT zu vergleichen und erst dann zu entscheiden.

Ab 200 Lernenden beginnt sich CBT/WBT zu lohnen. Bei 1000 Lernenden ist CBT/WBT häufig günstiger als konventionelle Ausbildung. Wenn man eine Offerte für das Erstellen von CBT/WBTs einholt, sind die Kosten auf den ersten Blick hoch. Rechnet man jedoch nach, wie viele Kursleitende eingesetzt werden müssten, um 1000 Personen zu schulen, was die Organisation dieser Schulungen und die Räume kosten, erkennt man rasch, dass CBT/WBT sich auszahlt. Es lohnt sich übrigens auch, mehrere Offerten einzuholen, die Preise varieren stark.

Einsatz von CBT/WBTs

Lernprogramme eignen sich nicht für jede Lernsituation und für jeden Lerninhalt. Wie und wo ist der Einsatz von CBT/WBT sinnvoll? CBT/WBTs sind ideal für die Erarbeitung von theoretischem Wissen. Zum Beispiel als Vorbereitung für einen Lehrgang. Ebenso kommen Lernprogramme für die Prüfungsvorbereitung zum Einsatz. Diese beiden Anwendungsmöglichkeiten eignen sich vor allem für Schulen und Institute, wo viele Lernende denselben Stoff beherrschen müssen.

Ein weiterer Einsatzbereich ist in grossen Unternehmen, wenn sehr viele Mitarbeitende in kurzer Zeit geschult werden müssen. Häufig kann in einer solchen Situation das Unternehmen nicht genügend Ausbildende zur Verfügung stellen oder hat nicht genügend Räumlichkeiten, um die Mitarbeitenden in Kursen zu schulen. Manche Unternehmen können es sich zudem nicht leisten, dass ein grosser Teil der Mitarbeitenden am Arbeitsplatz fehlt, um einen Kurs zu besuchen. Man denke zum Beispiel an ein Call-Center. Mit CBT/WBT können die Mitarbeitenden stundenweise am Arbeitsplatz lernen und sind nie einen ganzen Tag abwesend.

Ein weiterer wichtiger Gedanke zum Einsatz von CBT/WBTs ist, dass diese nie ohne begleitende Massnahmen eingesetzt werden sollten. Diese Massnahmen können sehr unterschiedlich sein. Bei einem WBT, das zur Erarbeitung von theoretischem Wissen eingesetzt wird, kann eine Anleitung für die Lernenden zum Umgang mit dem WBT genügen. Wenn in einer grossen Unternehmung 2000 Personen in mehreren Schulungsphasen umfangreichen Stoff erlernen, kann es sinnvoll sein, eine dieser Phasen als konventionelle Schulung zu gestalten, damit die Lernenden die Möglichkeit zum Kontakt mit Ausbildenden haben. Ohne diese begleitenden Massnahmen besteht die Gefahr, dass sich der Lernende isoliert fühlt, niemanden hat, an den er Fragen richten kann und niemand kontrolliert, ob die Lernziele erreicht wurden.

Aufbau eines CBT/WBTs

Ein sinnvoller Aufbau des CBT/WBTs ist sehr wichtig. Mit den heutigen technischen Möglichkeiten ist es relativ einfach, ein attraktives CBT/WBT zu gestalten mit der Gefahr, dass zu viele Animationen und optische Effekte eingebaut werden, welche zwar für das Auge attraktiv sind, aber keine didaktische Funktion erfüllen. Diese Animationen und Effekte haben zudem ihren Preis.

Eine Möglichkeit, ein CBT/WBT didaktisch sinnvoll aufzubauen, ist, die Gliederung in drei grundlegende Teile: Lernen, Üben, Test. Im Teil Lernen wird erklärt und vorgemacht. Der Lernende ist relativ passiv, schaut und hört zu. Beim Üben macht der Lernende nach, was ihm vorgezeigt wurde, löst Aufgaben, die prüfen, ob er die Ausführungen im Teil Lernen verstanden hat. In diesem Übungsteil bietet das Lernprogramm Hilfe an, wenn der Lernende nicht mehr weiter weiss. Der letzte Teil Test ist ähnlich aufgebaut wie der Teil Üben, es fehlt jedoch die Hilfefunktion. Der Lernende kann sich selbst prüfen und in der Testauswertung feststellen, wie viel Wissen er sich schon angeeignet hat. Bei diesen Tests ist es wichtig, dass die Aufgaben bei jedem Durchgang neu gemischt werden und nicht immer die gleichen Aufgaben gestellt werden. So kann der Lernende den Test so oft absolvieren, bis er die Lernziele erreicht hat.

Produktion eines CBT/WBTs

Die Produktion eines CBT/WBTs ist grob in zwei Kompetenzbereiche gegliedert: Den Bereich der Ausbildung und den Bereich der Programmierung. Die Ausbildungsfachleute sind verantwortlich für alle Lerninhalte und die Einbindung des CBT/WBTs ins gesamte Ausbildungskonzept der Institution oder des Unternehmens. Es muss ein Konzept für das CBT/WBT erstellt werden, welches den didaktischen Aufbau beschreibt, die Lernziele und groben den Lerninhalt definiert und das grafische Konzept enthält. Im Falle eines WBTs müssen auch die Einbindung ins Intra- oder Internet und die Zugriffe der Lernenden und allfälliger Betreuungspersonen geregelt werden. Nach der Erarbeitung des Konzeptes wird ein Drehbuch geschrieben. Das Drehbuch enthält die Lerninhalte, beschreibt den didaktischen Aufbau, die Navigation und alle Regieanweisungen für die Programmierer. Nun folgt die Programmierung, mehrere Tests durch Programmierer und Anwender und danach wird das CBT auf CD gebrannt und das WBT aufs Netz geschaltet.

Die beiden Arbeitsschritte Konzept und Drehbuch sind relativ heikel, weil sie eigentlich von beiden Parteien, den Ausbildern und den Programmierern ausgeführt werden sollten, dies aber in der Praxis oft nicht geschieht. Wenn man sich als Institut oder Unternehmen für ein CBT oder WBT entschieden hat, sucht man eine Firma, die es produziert. Man erwartet, dass man dieser Firma die Lerninhalte übergeben kann und diese das CBT/WBT produziert. Manche dieser Firmen beschäftigen jedoch keine Ausbildungsfachleute und so besteht die Gefahr, dass der didaktische Aufbau von Informatikern bestimmt wird, was nicht in allen Fällen gute Resultate bringt und manchmal durch teure Animationen kompensiert wird. Man sollte sich als Auftraggeber immer absichern, ob die Firma, welche das CBT/WBT produziert, Ausbildungsfachleute in die Arbeit einbezieht. Ansonsten sollte man dies selber tun.

Schlussgedanken

Ein didaktisches Konzept ist die Basis des CBT/WBTs. Es bestimmt alle wichtigen Faktoren aus Sicht der Ausbildung. Die Programmierung arbeitet im Auftrag der Ausbildung. Das heisst, es wird nicht programmiert, was die neuste Technik an Spezialeffekten darzustellen fähig ist, sondern was die Ausbildung bestimmt, um den Lernenden ein didaktisch sinnvolles Lernprogramm zu bieten.

Francesca Lüscher Baglioni, WissensTransfer, Lohn

Ausbildung

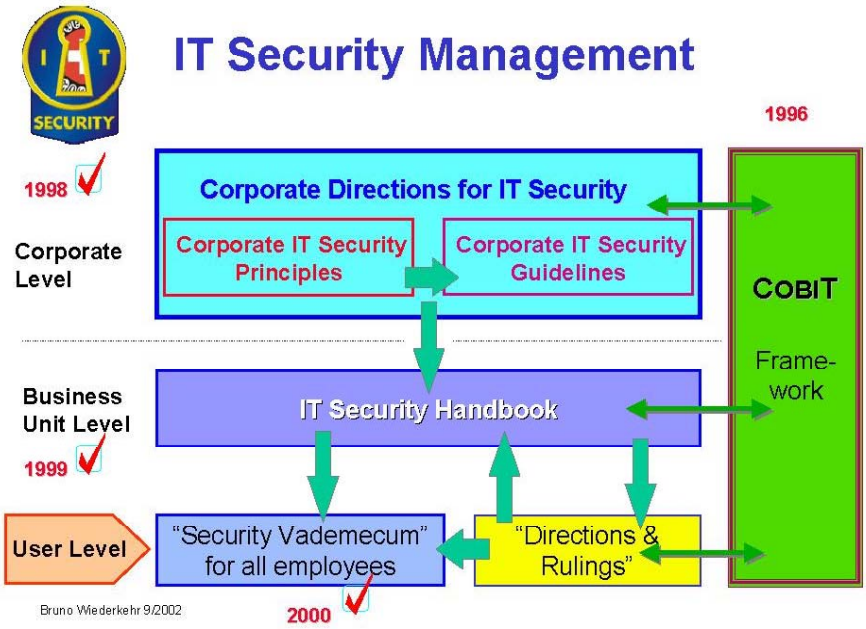
IT Security Awareness Programm

In den meisten Fällen bestehen Grundlagen für ein IT Security Awareness Programm; häufig hingegen lässt die konsequente Umsetzung zu wünschen übrig. Dazu ein bekanntes Zitat: Theoretisches Wissen ist gut, unternehmerisches Denken und Handeln sind besser.

Impulse zur Sensibilisierung

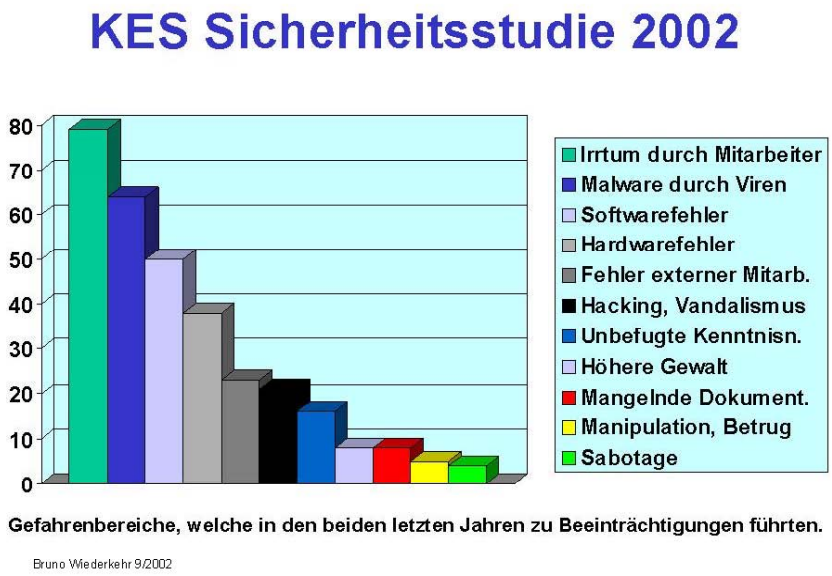
Angesichts des beachtlichen Nutzens und der Arbeitserleichterung, welche ein sinnvoller Einsatz der IT (Informations-Technologie) bewirken kann, dürfen anderseits die Gefahren nicht aus dem Auge verloren gehen. Ein allzu sorgloser oder gar fahrlässiger Umgang mit dieser Technologie kann gravierende Konsequenzen nach sich ziehen. Eine der wichtigsten Aufgaben des Awareness Programmes sollte daher in der Sensibilisierung der Mitarbeitenden für das Thema IT-Sicherheit sein und u.a. die folgenden Punkte beinhalten:

- IT-Sicherheitspolitik und -Management der RA/SL-Gruppe (siehe Abbildung)
- Ziele und Inhalt des IT-Sicherheitskonzeptes
- Verpflichtung der IT-Benutzer und Aufgabenverantwortlichen
- Erläuterung der Grundprinzipien der CIA: „Confidentiality, Integrity, Availability“
- Risiken und Gefährdungen durch den IT-Einsatz
- Sicheres Umgehen mit IT-Geräten, Software und Daten
- Gewährleistung der IT-Sicherheit durch Sensibilisierung und Kontrolle



Die Erfahrungen haben gezeigt, dass die Gewährleistung von IT-Sicherheit in Projekten und im laufenden Betrieb zu wenig berücksichtigt ist oder den IT-Benutzern selbst überlassen wird.

Die Planung, die Realisierung und die Kontrolle der Sensibilisierung ist eine ständige Managementaufgabe. Die Gewährleistung der Sicherheit im laufenden Betrieb ist die Pflicht eines jeden Mitarbeitenden.



Probleme und Gefahren

Während einerseits mit der Vernetzung vielfältige Informationen für einen breiten Benutzerkreis zur Verfügung stehen, bereitet anderseits der Schutz von vertraulichen Daten vor unberechtigter Kenntnisnahme oder vor unbefugter Manipulation Probleme.

Die Komplexität der Probleme und Gefahren (Quelle: Studie 2002 KES: Kommunikation und EDV-Sicherheit) erfordert jedoch komplexe Sicherheitslösungen, deren Stärke vom schwächsten Glied der Kette abhängig ist.

An Bedeutung zugenommen haben gemäss Studie die Gefahrenbereiche, wie Hacking, unbefugte Kenntnisnahme und Informationsdiebstahl.

Eine ordnungsgemässe Aufgabenerfüllung verlangt von allen Verantwortlichen für den notwendigen Schutz vorausschauend Sorge zu tragen. IT-Sicherheit wird nicht automatisch produziert, sie ist nur im Zusammenwirken zwischen technischen und organisatorischen Massnahmen durch alle Mitarbeitenden erreichbar.

Untersuchungen zur IT-Sicherheit belegen immer wieder, dass fehlendes Bewusstsein über die Auswirkungen von Schäden und Beeinträchtigungen beim Management und bei den Mitarbeitenden zu den Haupthindernissen bei der Verbesserung der IT-Sicherheit zählen.

Auch wird häufig ein Zielkonflikt zwischen originärer Aufgabe und IT-Sicherheitserfordernissen empfunden, obwohl sich die täglichen Aufgaben nur unter Berücksichtigung von Sicherheitsaspekten auf die Dauer ordnungsgemäss erfüllen lassen. Im Weiteren ist die Nutzung der IT zur Aufgabenerfüllung für zahlreiche Mitarbeitende unverzichtbar.

Bereitschaft zur Umsetzung

Wie aus der ersten Abbildung hervorgeht, haben wir uns seit längerem auf strategischer und operativer Ebene mit dem IT-Sicherheits-Management befasst. Es gibt bereits eine Fülle von Informationen im Online-Zugriff zu diesem Thema. Aber Hand aufs Herz, wer hat das Vademecum IT-Sicherheit von A–Z gelesen und auch wirklich verstanden?

Der Schlüssel zum Erfolg und die Bereitschaft zur konkreten Umsetzung liegt darin, dass allen verständlich ist, was das Unternehmen erreichen will (Vision), wozu die Mitarbeitenden berufen sind (Mission) und welche Leistung hinsichtlich IT Security Awareness erwartet wird.

Auf einer verständlichen Grundlage können konkrete Pflichten und Aufgaben ermittelt und abgestimmt werden, um anschliessend mit Motivation und guter Leistung das Ziel zu erreichen. Für die Entwicklung und Ausbildung stehen nach didaktischen Grundsätzen verschiedene Modelle, Werkzeuge und Verfahren für die Sensibilisierung von Datenschutz und Datensicherheit zur Verfügung, wie z.B.:

- Lernprogramm SAVE und Test Informatiksicherheit, SmartForce Prokoda Schweiz GmbH, Wallisellen für RA/SL

■ Die goldenen Regeln zur Informatik-Sicherheit, Acadia, Stäfa für Swiss Re
■ Datenschutz „Data Protection“, HSE, Dublin für Swiss Life (UK) Schulung von allen Mitarbeitenden im Jahre 2001
■ Sensibilisierung IT Sicherheit (Lehrbrief, Tipps, Informations-Börse etc.), www.bsi.bund.de

Neue und bestehende Ansatzpunkte

Bei der Weiterentwicklung sind die Erfahrungen aus der Vergangenheit und der Gegenwart sowie die Möglichkeiten der Zukunft zu betrachten und wo möglich miteinander zu verbinden und zu nutzen, wie z.B.:
■ Verbreitung der ersten Datenschutz- und Datensichenheits-Richtlinien bei allen Organisationseinheiten (Hauptsitz, Niederlassungen, Tochtergesellschaften) unterstützt durch eine Präsentation und eine Tonbildshow „Daten sicher wie Gold“
■ Einführung von VLIC (Virtual Learning and Information Center) sowie Nutzung des bestehenden Intranets (ZIS: Zentrales Informations-System) als Informations- und Lernplattform
■ Erstellung, Speicherung und Verbreitung der Corporate Directions for IT Security, des IT Security Handbooks sowie das Vademecum IT Sicherheit für alle IT Benutzer
■ Laufende Inkraftsetzung von diversen Regulativen, welche sich auf den Datenschutz- und die Datensicherheit beziehen
■ Bereitstellung von Lernprogrammen (WBT: Web-Based Training), welche eine unabhängige (zeitlich/örtlich) Awareness Schulung bzw. Benutzung des Sensibilisierungs-Programmes erlauben

Für das gute Gelingen hinsichtlich der Entwicklung und Durchführung des Programmes ist die Entscheidung und das Commitment der obersten Geschäftsleitung eine Voraussetzung.

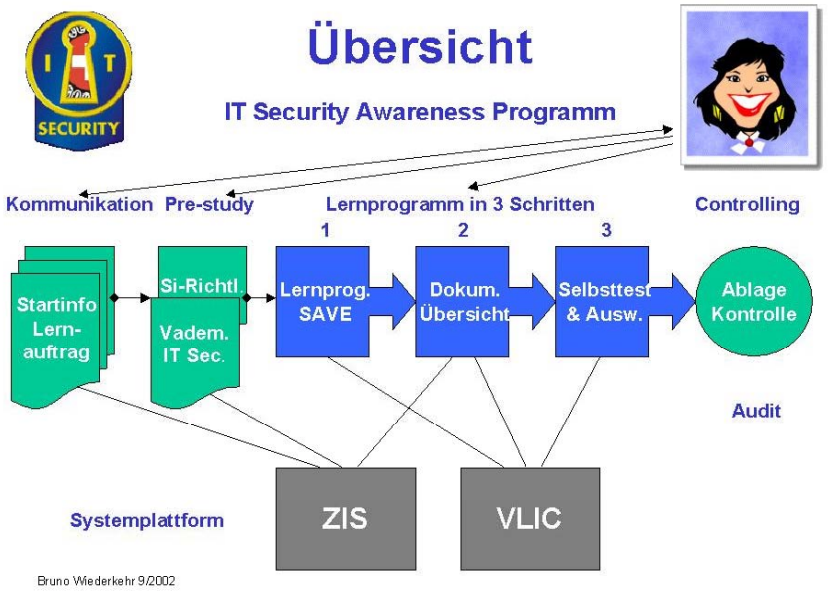
Für Neueintretende und bestehende Mitarbeitende der RA/SL Schweiz ist die Durchführung des Online-Schulungprogrammes für die IT Security ab Beginn des Jahres 2003 vorgesehen.

Vom Konzept zur Umsetzung

Beim Aufbau eines IT Security Awareness Programmes muss darauf geachtet werden, dass sich die vielschichtigen Informationen und deren Links generisch auf das Lernziel beziehen. Dabei stellt sich die zentrale Frage: „Was muss der IT-Benutzer zum Zeitpunkt der Schulung und bei der täglichen Arbeit wissen und einhalten?“

Diese Hauptanforderung wurde bei der Auswahl und dem Aufbau (siehe Übersicht) der einzelnen Schulungselemente immer wieder hinterfragt. Gleichzeitig wurde berücksichtigt, dass die betroffenen Informationen, welche in Abhängigkeit zueinander stehen, klar abgestimmt und referenziert wurden, wie z.B. Inhalte der Datenschutz- und Datensicherheits-Richtlinie, Erläuterungen im Vademecum IT-Sicherheit, Beschreibungen des SAVE-Lernprogrammes und der Präsentation mit den entsprechenden Links sowie die Fragen im Cybertest.

Bei der Implementierung des IT Security Awareness Programmes ist zu erwähnen, dass der Einbettung in die Aufbau- und Ablauforganisation, der Regelung der Zuständigkeit sowie der Kommunikation und der internen Kontrolle eine besondere Bedeutung zukommt.



Zur Gewährleistung der obligatorischen Durchführung des Awareness Programmes ist der Aufruf an alle Mitarbeitenden durch den Präsidenten der Konzernleitung eminent wichtig. Ebenso ist die vorherige Orientierung des Managements und die funktionstüchtige Bereitstellung des Lernprogrammes in der jeweiligen Landessprache D/F/I/E von Bedeutung.

COBIT	Beurteilung der IT Prozesse
PO4.6	Verantwortung für logische und physische Sicherheit
PO6.11	Kommunikation des IT-Sicherheitsbewusstseins
AU7.3	Schulung von Sicherheitsprinzipien und Sicherheitsbewusstsein
M2.4	Betriebliche Sicherheit und Sicherstellung der internen Kontrolle
M3.5	Unabhängige Bestätigung der Einhaltung von externen und internen Vorschriften
M3.7	Proaktiver Einbezug der Revision

Für Mitarbeitende, welche mit der Materie IT-Sicherheit vertraut sind, sollte der Aufwand pro Lernschritt nicht mehr als 30 Minuten betragen; total 1 1/2 Stunden ohne vorhergehendes Studium (Pre-study) des Vademecum IT-Sicherheit und der RA/SL-Grundsatzrichtlinie. Zur Erleichterung des Einstieges in das Lernprogramm wird mit einer Startinformation auf einen klar strukturierten Lernauftrag hingewiesen.

Mit dem Controlling wird der Rücklauf der Tests, das Mahnwesen und die Ablage der Dokumente in den Personaldossiers sichergestellt.

Vorteilhaft ist, wenn das Konzernrevisorat einerseits bei der Konzeption projektbegleitend einbezogen wird und anderseits die IT Security Awareness in die jeweiligen Prüfungsprogramme aufnimmt.

Die entsprechenden Kontrollziele können für die Planung und Durchführung der Audits aus dem COBIT-Framework entnommen werden. Im Vordergrund steht die IT Ressource „Personal“. Wesentliche IT Prozesse sind:

Erst wenn die Aktualität des IT Security Awareness Programmes durch ein adäquates „Change Management“ sichergestellt ist, kann die notwendige Sicherheit, Effizienz und Effektivität gewährleistet werden.

Sowohl die Zuständigkeiten als auch die wesentlichen Aufgaben hinsichtlich der Gewährleistung der internen Kontrolle (u.a. Führungskontrollen) sind im Konzept festzulegen.

Lessons learned

Es ist von Bedeutung, dass Feststellungen und Empfehlungen, welche durch das Management, die Revision, aber auch durch die Mitarbeitenden, aufgedeckt wurden, ernst genommen werden.

Damit besteht die Chance, neue Gefährdungen und Risiken zu lokalisieren, zu analysieren sowie ein Feedback bezüglich den zu treffenden Massnahmen an die Sicherheits-Verantwortlichen weiterzuleiten.

Aufgrund ungenügender oder nicht getroffener Datenschutz- und Datensicherheits-Massnahmen könnte die Motivation und die Sensibilisierung bei den Mitarbeitenden abnehmen.

Ausblick

Dank der neuen Strategie, deren Struktur und der transformationellen Führung der Rentenanstalt/Swiss Life kann ein Projekt wie das IT Security Awareness Programm einfacher, schneller und mit weniger Aufwand erfolgreich abgeschlossen werden.

Mit dieser Erkenntnis und dem Verständnis für Effizienz und Effektivität kann einerseits das Vertrauen der über 13 000 Mitarbeitenden und die Stabilität im aktiven Veränderungsprozess in der ganzen Gruppe vorangetrieben werden. Ein weiterer Vorteil liegt darin, dass mit der laufenden Vereinheitlichung der internationalen, europäischen und nationalen Qualitäts- und Sicherheits-Standards das IT Security Awareness Programm adäquat angepasst werden kann.

Es ist besonders darauf zu achten, dass die Ressource „Personal“ gegenüber den übrigen IT-Ressourcen im Vordergrund steht und entsprechend berücksichtigt wird. Nur so können bei Abweichungen die Sicherheits-Indikatoren im Rahmen eines Frühwarnsystems zum Tragen kommen. Durch ungenügende Kom-

munikation und Motivation könnte die Sensibilisierung und die Leistung der Mitarbeitenden eingeschränkt werden.

Wenn es gelingt, mit dem IT Security Awareness Programm einen weiteren Beitrag zur Verbesserung der IT-Sicherheit in der ganzen RA/SL-Gruppe zu erzielen, sind wir der Corporate- und IT-Governance wieder ein Stück näher gekommen.

Motto: Vertrauen ist gut, Governance ist besser !

Bruno Wiederkehr,
Rentenanstalt/Swiss Life, Zürich

Ausbildung

Lernen ist lernbar – welche Ausbildung ist heute notwendig ?

Warum ISACA-CH 20% Ausbildungsrabatt für Arbeitslose gibt

Die schlechten Nachrichten jagen sich. Externe Informatik-Dienstleister (Beratungsunternehmen, Revisionsgesellschaften) bauen ihre Personalbestände dramatisch ab. Die grossen Häuser entlassen gleich Hundertschaften, die kleineren stellen den Betrieb ein oder gehen in Konkurs. Dies hat natürlich auch im Berufsumfeld, in dem wir uns bewegen, teils dramatische Auswirkungen.

In den letzten Monaten habe ich praktisch jede Woche solche Hiobsbotschaften vernommen. Nachdem auch Banken und Versicherungen damit begonnen haben, Mitarbeiter im Informatikbereich sowie im Backoffice abzubauen, spitzt sich die Lage langsam zu. Richtig bewusst wurde mir das aber erst als Folge verschiedener Erreignisse: Auf ein Stellenangebot (40 %) zur Unterstützung vor allem im Ausbildungsbereich (Bereitstellung von Unterlagen, Versand von Kursausschreibungen usw.) meldeten sich fast 300 Bewerberinnen! Auf der anderen Seite habe ich in den letzten Wochen mit mehreren RAV (Regionale Arbeitslosenvermittlungs-Zentren) Gespräche geführt über den Stellenwert des vom ISACA-Switzerland Chapter angebotenen Vertiefungskurses Informatik-Revision/Sicherheit CISA-Kurs). Mindestens vier der diesjährigen Kursteilnehmer sind arbeitslos – und die RAV fragen sich zu Recht, ob sie einen in ihren Augen teuren Kurs überhaupt unterstützen sollen.

Anforderungen an die Ausbildung von Mitarbeitern

Was sind denn eigentlich die Anforderungen an einen kompetenten Mitarbeiter in unserem Berufsumfeld? Ich habe mir im Zusammenhang mit einer (unveröffentlichten) Stellenanzeige überlegt, welche Voraussetzungen ein Bewerber heute erfüllen muss. Von diesen möchte ich einige aus einer persönlichen Warte vorstellen und kommentieren.

Kommunikative Fähigkeiten, Verhandlungsgeschick, hohe Sozialkompetenz

In jeder Ausprägung unseres Berufsbildes – sei es als Revisor, Sicherheitsverantwortlicher oder als Unternehmensberater – ist eine klare Kommunikation, welche auch auf die Bedürfnisse des Gesprächspartners eingeht, von zentraler Bedeutung. Traurig ist aber, dass ein grosser Teil der sich in diesem Umfeld tummelnden Personen nie gelernt hat, wirklich mit Kunden, Partnern

oder Berufskollegen zu kommunizieren.

Ich mag mich noch gut an meinen ersten Kurs in diesem Bereich erinnern: „Gesprächsführung für Revisoren“ (oder so ähnlich) hiess er. Mein damaliger Arbeitgeber, das Inspektorat der SKA, hatte diesen Kurs speziell für alle Informatikrevisoren organisiert. Bei vielen der Übungen waren wir Teilnehmer manchmal sehr skeptisch über den Nutzen für unsere Praxis – nach weiteren Kursen in diesem Bereich bin ich heute klar der Ansicht, dass damals ein ganz wichtiger Grundstein gelegt wurde für meine Kommunikation mit Kunden, Geschäftspartner, Freunden und Bekannten. In den letzten Wochen habe ich mit verschiedenen Berufskollegen auch über ihre Ausbildung gesprochen; kein Einziger hat einen Kurs in diesem Bereich auch nur erwähnt.

Analytisches, kritisches und unternehmerisches Denkvermögen

Die Durchführung von Revisionen, Reviews, Sicherheitsanalysen, aber auch die Erstellung von (Sicherheits-) Stategien und Konzepten bedingen neben einem ausgeprägt sorgfältigen und systematischen Vorgehen einen hohen Grad an analytischem Denkvermögen. Klein ist wahrscheinlich die Zahl derjenigen Personen, welche sich solche Fähigkeiten im Verlaufe ihrer primären Berufsausbildung oder in einem Studium erwerben konnten. Am besten lernt man das wahrscheinlich „on the job“. Damit verstehe ich aber ausdrücklich nicht, dass man einfach auf die internen oder externen Kunden losgelassen wird und dann so nebenbei das Handwerk erlernen kann. „On the job“ heisst für mich, während den ersten Jahren der Berufslaufbahn durch beispielhaftes Verhalten der Arbeitskollegen, der verantwortlichen Mandatsleiter oder Vorgesetzten immer wieder auf die verschiedenen Fragestellungen aufmerksam gemacht wird und – noch viel wichtiger – die Antworten darauf sachlich einwandfrei argumentieren muss. Persönlich habe ich bis zur Aufnahme der selbstständigen Erwerbstätigkeit von allen Vorgesetzten in dieser Hinsicht immer wieder profitiert; diese gaben sich selten mit billigen Antworten zufrieden. Eine solche Ausbildung „on the job“ ist aber wahrscheinlich eher selten.

Gutes Verständnis für ganzheitliche, praxisbezogene Lösungen im Schnittpunkt von Organisation, Informatik und Sicherheit

Sicherheit, Controlling, Interne Kontrolle, IT-Governance, usw. sind Themen, welche meines Erachtens immer ganzheitlich betrachtet werden müssen. In Einzelbereichen, so z.B. bezüglich Sicherheit und auch Controlling bestehen zahlreiche Ausbildungsmöglichkeiten. Ausbildungen zum Thema IKS gibt es vor allem an der Schweizerischen Akademie für Wirtschaftsprüfung (früher: Kammerschule). Jedoch ist trotz dieser an sich fundierten Ausbildung leider sogar unter Wirtschaftsprüfern oft nur ein rudimentäres Verständnis für Interne Kontrolle vorhanden – vor allem im Bereich der anwendungsbezogenen (applikationsabhängigen) Kontrollen. Bezüglich IT-Governance gibt es praktisch gar keine Ausbildung – ganz im Gegensatz zu Corporate Governance, wo bald jedes Ausbildungsinstitut aus naheliegenden Gründen eine Ausbildung anbietet. Alle mir bekannten Ausbildungsmöglichkeiten fördern jedoch kaum das vernetzte Denken, das für praxisbezogene Lösungen unabdingbar ist. Auch hier bin ich überzeugt, dass man nur durch jahrelanges Coaching durch erfahrenere Berufskollegen ein wirklich gutes Verständnis erwerben kann.

Breites und fundiertes Wissen der Informationstechnologie

Seit dem Informatik-Ausbildungsdebakel vor ca. zehn Jahren hat die Schweiz in diesem Bereich massiv Terrain gutgemacht. Nach der Softwareschule Schweiz sprossen zahlreiche Informatikschulen aus dem Boden; so mauserte sich z.B. die SBG-interne Schule zu einem der grössten Anbieter in der Schweiz, dem Institut für Informatikausbildung (IFA). Auch wenn in den letzten Monaten das Pflaster deutlich härter geworden ist, kann sowohl auf der Stufe der Berufsprüfung als auch der Diplomprüfung an verschiedenen Schulen eine hervorragende Ausbildung erworben werden. Neben der klassischen Ausbildung zum Wirtschaftsinformatiker sind in den letzten Jahren verschiedene Ausbildungsrichtungen hinzugekommen, so z.B. die Ausbildung zum Web-Assistenten, zum Webmaster oder zum Web Project Manager – um nur einige zu nennen. Es ist jedoch kaum erstaunlich, dass mit der Flaute im

Bereich von e-commerce und e-business und generell im gesamten Informatikbereich einige der Schulen Mühe bekunden oder sich sogar in die Arme einer Konkurrenz flüchten mussten. Der Druck vom Markt (weniger Kursteilnehmer) wird auch gnadenlos weitergereicht, z.B. auf die Dozenten, welche (angesichts des erheblichen Vorbereitungsaufwands) mancherorts auf einen Teil der ohnehin niedrigen Stundenentschädigungen verzichten müssen. Das Defizit in diesem Ausbildungssegment liegt vor allem im Bereich von Umschulungen – es werden immer noch zu wenige Ausbildungen angeboten, welche auf bestehenden aber teilweise vielleicht veralteten Berufskenntnissen aufsetzen.

Breites und fundiertes Wissen in Bezug auf IT-Sicherheit und IT-Revision

Es ist selbstverständlich, dass ein Spezialist für IT-Sicherheit oder IT-Revision in diesen Bereichen über eine solide Ausbildung verfügen soll. In den letzten Boomjahren wurde das manchmal verpasst; und oft wurde ein solcher Kurs ohne konkreten Bezug zum persönlichen Ausbildungsbedarf konsumiert. Wir sind aber in der glücklichen Situation, dass es in der Schweiz neben einigen nationalen und internationalen Kongressen unterdessen auch zahlreiche Anbieter gibt, welche im Themenbereich der IT-Sicherheit in erster Linie eigentliche Spezialistenkurse anbieten. Dazu müssen (dürfen!) wir auch das ISACA Switzerland Chapter rechnen: Wir organisieren gegenwärtig pro Jahr zwischen 10 und 15 Kurse. Daneben bieten wenige private Anbieter Kompaktkurse an, in denen in etwa einer Woche eine solide Grundlage für die Berufstätigkeit gelegt werden soll.

Seit Jahren besteht in Luzern mit dem Nachdiplomkurs Datenschutz und Informationssicherheit sowie dem darauf aufbauenden Nachdiplomstudium Informationssicherheit eine fundierte Grundausbildung, welche aber trotz einiger allgemeinen Themen (z.B. relativ viele Stunden „Recht“) eher techniklastig ist.

Unser eigener Vertiefungskurs Informatik-Revison/Sicherheit (CISA-Kurs) liegt im Bereich zwischen den sehr kurzen Kompaktkursen und einem mehrjährigen Nachdiplomstudium (4–5 Semester). Mit den 17 Ausbildungstagen in den sechs Monaten zwischen Dezember und Mai ist die zeitliche Belastung überschaubar – auch wenn ein Kursteilnehmer zur persönlichen Vorbereitung auf den Unterricht noch mit sicher 30–50 zusätzlichen Tagen Aufwand rechnen muss. Ganz offensichtlich besteht ein Bedürfnis des Marktes: Seit zwei Jahren muss der Kurs doppelt geführt werden; und dieses Jahr könnten wir sogar drei kleine Klassen führen, da die beiden Klassen ausgebucht sind.

Interessant ist, dass die RAV die ISACA-Kurse als zielstrebige, nutzbringende Ausbildung anerkennen, welche die Vermittlungsfähigkeit von arbeitslosen Spezialisten verbessern soll. Obwohl unser Vertiefungskurs vom Preis-/Leistungsverhältnis als sehr günstig beurteilt werden kann, liegen die Kosten über den von den RAV üblicherweise unterstützten Ausbildungen. Ganz offensichtlich sind sowohl die regionalen Vermittlungszentren als auch die zentrale Stelle, welche derartige Kurse bewilligen muss, davon überzeugt, dass ein Nutzen klar ersichtlich ist. Vermittelt werden ja für eine extrem breite Palette von Themen jeweils die folgenden Inhalte: Was verbirgt sich hinter diesem Begriff? Welche Risiken und welche Sicherheitsanforderungen (Kontrollziele) bestehen dabei? Mit welchen Massnahmen können diese Sicherheitsanforderungen abgedeckt werden, so dass das jeweilige Risiko beherrscht ist? Wie kann man das jetzt auch noch überprüfen?

Nach Ansicht der RAV sind Absolventen eher in der Lage, in vielen Bereichen der Informatik eingesetzt zu werden, auch ausserhalb des eigentlichen Gebietes von Sicherheit und Revision. Schliesslich lernt man, wie man die Informatik „in den Griff“ bekommt (IT-Governance!).

Also – planen Sie Ihre Ausbildung sorgfältig! Denken Sie aber daran, dass neben IT- und Kontrollwissen auch andere Fertigkeiten gefragt sind. Wir halten Sie auf unserer Homepage www.isaca.ch auf dem Laufenden.

Peter R. Bitterli,
Bitterli Consulting AG, Zürich

Ausbildung

Blended-Learning-Konzept (BLK)

e-learning-Tool in Ausbildungsmodul Wirtschaftsprüfung integriert

Die Schweizerische Akademie für Wirtschaftsprüfung bereitet Studierende mit einem Lehrgang auf die Höhere Fachprüfung dipl. Wirtschaftsprüfer vor. Im Sommer 2002 wurde im Lehrgangsmodul Wirtschaftsprüfung erstmals das Blended-Learning-Konzept getestet. Die Ergebnisse dieses Pilotprojektes sind vielversprechend.

Blended-Learning

In der Erwachsenenbildung ist die Ausbildungszeit, gemessen an der Anzahl Seminarlektionen, ein äusserst knappes Gut. Nachgefragt werden ganzheitliche Qualifizierungslösungen, welche ein effizientes Lernen ermöglichen. In einem Gesamtmodell bzw. in einem Curriculum werden die Elemente des Lernens zusammengeführt und aufeinander abgestimmt. Flexibles, zeit- und ortsunabhängiges Studieren im Selbststudium wird mit Präsenzstudium kombiniert. Das Methodenspektrum reicht vom Selbstlernen mittels Standardliteratur über e-learning bis zum klassischen Präsenztraining.

In den Boom-Jahren der New Economy wurde e-learning als effizientes und kostengünstiges Instrument propagiert. Wie auch in anderen Gebieten der New Economy konnten die Versprechen nur teilweise eingelöst werden. Ein wesentlicher Grund für diese Tatsache liegt darin, dass e-learning-Ansätze nicht in ein ganzheitliches Konzept eingebunden werden, welches neben computergestützten Elementen auch „klassische“ Lehr- und Lernformen wie beispielweise Vorlesungen oder Workshops umfasst. Ganzheitliche Lernsysteme werden auch „blended“ (engl. „Blender“ = Mixer) genannt, woraus sich der Begriff „Blended Learning“ abgeleitet hat.

Blended Learning im Modul Wirtschaftsprüfung

In der Ausbildung zum dipl. Wirtschaftsprüfer testete die Schweizerische Akademie für Wirtschaftsprüfung im Sommer 2002 das Blended-Learning-Konzept (BLK). Im Modul Wirtschaftsprüfung wird das Handbuch für Wirtschaftsprüfung (HWP) als Basisliteratur verwendet. Mit Hilfe eines Arbeitsplanes wird der Lernprozess gesteuert. Der Arbeitsplan definiert die Vor- und Nachbereitungsarbeiten der Studierenden. Diese stehen in einem direkten Kontext zu entsprechenden Vorlesungen bzw. zu entsprechenden Seminaren. Im Rahmen der Vorbereitungsarbeiten wurde im Sommer 2002 erstmals und auf freiwilliger Basis ein e-learning-Tool eingesetzt (vgl. Abbildung 1).

Die Modulleitung definiert im Arbeitsplan die Kapitel des HWP, welche die Studierenden vor dem Besuch der Modulvorlesungen bzw. Modulseminare studieren müssen. Im Lerntool Wirtschaftsprüfung formulierte die Modulleitung Wissens- und Verständnisfragen zum entsprechenden Kapitel des HWP (vgl. Abbildung 2). Dadurch hatten die Studierenden die Möglichkeit, den „Lernstoff“ online zu trainieren. Das

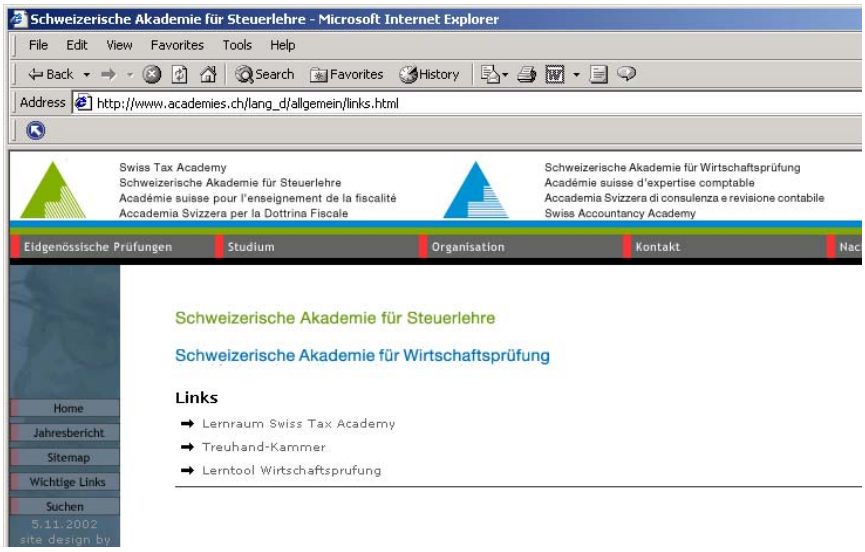


Abbildung 1: Einstieg in das Lerntool Wirtschaftsprüfung

Lerntool Wirtschaftsprüfung ermöglicht auch die Durchführung einer Online-Prüfung. Bei der Vorbereitung der Seminare können die Dozentinnen und Dozenten die Ergebnisse der Online-Prüfung berücksichtigen.

Erste Erfahrungen

Von den Studierenden haben 28 % das Lerntool Wirtschaftsprüfung genutzt. Im Betrieb wurden keine technischen Schwierigkeiten festgestellt. Die Resultate der Lehrgangsevaluation 2002 für das Modul Wirtschaftsprüfung zeigen, dass das Lerntool aus Sicht der Studierenden gut in das Curriculum eingebaut werden konnte. Die Akademie beabsichtigt, das Lerntool auszubauen und auch im nächsten Durchgang wieder einzusetzen.

Link

Blended-Learning-Konzept:
www.athemia.com

Thomas Suter,
Geschäftsführer des Kompetenzzentrums Aus- und Weiterbildung der Treuhand-Kammer, Zürich

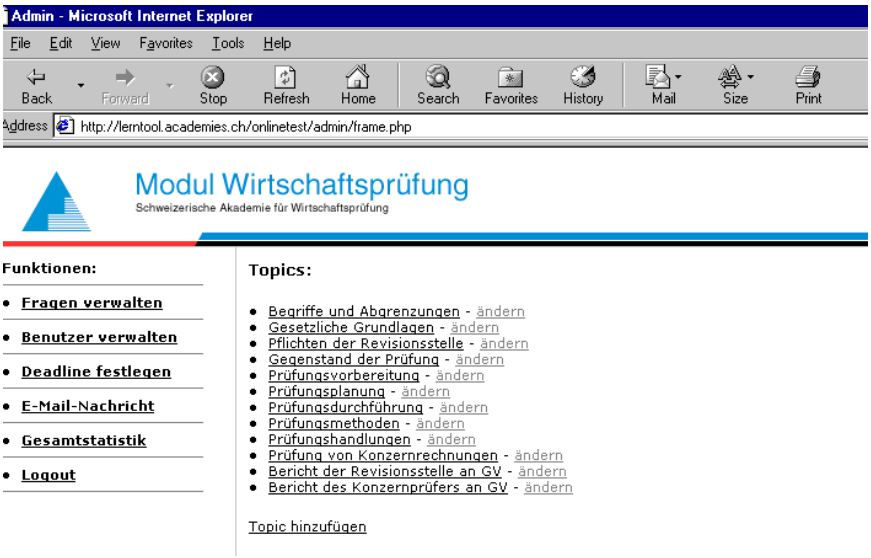


Abbildung 2: Administratoren-Tool für die Modulleitung

Projektbegleitung und projektbegleitende Revision von Softwareentwicklungsprojekten

Einführung

Dieser Artikel diskutiert wesentliche Aspekte der projektbegleitenden Revision bzw. des Projektmanagements von IT-Entwicklungsprojekten. Zielgruppe sind interne und externe Auditoren, Führungskräfte im IT-Bereich, aber auch Projektleiter von IT-Projekten.

Die Vorteile der projektbegleitenden Revision dürften den Lesern dieses Magazins bekannt sein: Anstelle des retrospektiven Ansatzes begleitet der Revisor das Projekt von Anfang an und kann bei auftretenden Risiken gegensteuern. Das bedeutet für den Project Owner eine höhere Erfolgswahrscheinlichkeit des Projektes, für den Projektleiter zusätzliche Unterstützung bei der erfolgreichen Bewältigung des Projektes und für den Revisor erhöhte Einflussmöglichkeiten.

Beachte die üblichen Eckpfeiler des Projektmanagements

Die Eckpfeiler des Projektmanagements sind, wie der erfahrene Auditor beziehungsweise Projektleiter weiß, methodengetriebenes Know-how und somit unabhängig von dem Bereich, in welchem das zu betrachtende Projekt durchgeführt wird. Sie sollen hier nur kurz namentlich erwähnt werden:

- Saubere Projektplanung vor dem Start des Projektes unter Berücksichtung der Faktoren Zeit, Kosten und Qualität, unter anderem anhand eines Projektnetzplans, einem Plan für das Ressourcenmanagement, einer Kosten/Nutzen-Rechnung auf der Basis üblicher Investitionsrechnung, klar definierter Projektrollen für alle „Stakeholders“ (all diejenigen Personen und Gremien, die das Projekt positiv oder negativ beeinflussen können) und einer Risikoanalyse:
- Motivation der Mitarbeiter
- Regelmäßige Prüfung des Projektfortschritts
- Aktualisierung der Projektpläne („Tracking & Tracing“)
- Kontakthaltung zum Abnehmer/ Anwender
- Angemessene Dokumentation des Projektes
- Übergabe der Project Deliverables

Weitere Schritte können abhängig vom jeweiligen Einzelfall notwendig sein.

Detailliertes Fachkonzept vor Beginn der IT-Konzeption

Ein in enger Zusammenarbeit mit dem zuständigen Fachbereich erstelltes Fachkonzept sollte vor dem Beginn der IT-Konzeption (bei größeren Projekten im Rahmen einer Vorstudie) finalisiert und abgestimmt vorliegen. Dies schützt zwar nicht vor Änderungen während des Projektes, stellt aber sicher, daß die generelle Marschrichtung fixiert und akzeptiert ist. Dieses Fachkonzept sollte so detailliert wie möglich sein (bei der Definition von grafischen Benutzerschnittstellen beispielsweise bis hinab zu einzelnen Bildschirmmasken), ohne jedoch Annahmen zur technischen Realisierung zu treffen – dies ist Aufgabe des DV-Konzeptes.

IT-Konzept vor Beginn der Implementierungsphase; iterativer Entwicklungsansatz

Das grobe IT-Konzept sollte vor dem Beginn der Implementierungsphase vollständig und abgestimmt vorliegen. Ein bis ins letzte Detail vorausgeplantes IT-Feinkonzept kann sich bei komplexen Projekten jedoch als Nachteil erweisen, da dies in der Regel Ausdruck des traditionellen Wasserfall-Entwicklungskonzeptes ist, welches zunehmend kritisch bewertet wird. Im Falle komplexer IT-Architekturen, die heute bei vielen Projekten anzutreffen sind, empfiehlt sich ein iterativer Entwicklungsansatz; es sollte dann zu Beginn der Implementierungsphase das IT-Feinkonzept für den ersten Iterationsschritt fertig gestellt sein.

Beachte technische Nebenbedingungen („Technical Constraint Analysis“)

Die Definition von Strategie und Fachkonzept wirft bei den meisten

IT-Entwicklungsprojekten die vergleichsweise geringfügigsten Schwierigkeiten auf. Häufig treten jedoch mit Beginn der IT-Konzeptionierungsphase Probleme auf, weil dem Projektmanager das tief greifende technische Verständnis bestimmter Sachverhalte fehlt und er sich nicht in hinreichendem Maße der fachlichen Expertise von internen oder externen IT-Architekten bedient. Die Friktion zwischen Plan und Wirklichkeit wird stärker und nimmt mit fortschreitender Implementierung mehr und mehr zu.

Die Empfehlung kann hier nur lauten, im Zweifelsfall immer Rücksprache mit einem entsprechend qualifizierten Experten zu halten, um keine falschen Annahmen bezüglich Aufwand oder Durchführbarkeit zu treffen. Nicht nur eine zu niedrige Aufwandsschätzung kann kritisch sein; auch eine zu hohe Schätzung kann ein Projekt gefährden. Eine falsche Einschätzung von technischen Nebenbedingungen oder der technischen Durchführbarkeit generell kann fatale Folgen haben.

Change Management

Gerade bei IT-Projekten, und insbesondere bei der Softwareentwicklung und dem Customizing von Standardsoftware, können Änderungen – zum Beispiel in der Zielarchitektur, aber auch bei den zugrunde liegenden Geschäftsprozessen und Unternehmensstrukturen – Projekte gefährden, ja sogar zum Scheitern verurteilen. Ein angemessener Change Management Prozeß wird auch dieses Risiko nicht ausschliessen, aber minimieren können. Es sollte eine Aufgabe sowohl des projektbegleitenden Revisors als auch des Projektleiters sein, den Kunden proaktiv auf mögliche Risiken hinzuweisen und bei der Entwicklung von Lösungsstrategien zu unterstützen. Hierbei sollten auch Kommunikationskultur und Kommunikationsstrukturen des Kunden Beachtung finden.

Noch ein Hinweis der die Notwendigkeit eines guten Change Management Prozesses dokumentiert: Nach Statistiken der US Food & Drug Administration (FDA) waren von allen Softwarefehlern, die in den vergangenen Jahren den Rückruf eines von der FDA regulierten Produktes verursachten, nur 21 Prozent bereits beim Markteintritt des Produktes vorhanden; 79 Prozent hingegen wurden nach Markteinführung durch ein Update der Software nachträglich eingebaut. Dies führt uns zum nächsten Punkt:

Angemessenes Testkonzept (“don't just click to test”)

Ein angemessenes Testkonzept kann den Unterschied zwischen Erfolg und Mißerfolg eines Projektes ausmachen. Leider wird viel zu häufig unter dem scheinbar übermächtigen Zeitdruck des Projektes die Implementierung eines solchen Testkonzeptes unterlassen. Dies führt dann häufig zu Problemen bei der Endabnahme oder gar beim Betrieb.

Die Empfehlung kann hier nur lauten, die Entwickler zumindest auf ein angemessenes White-Box- und Black-Box-Testing sowie auf Integrationstests zu verpflichten, diese Tests nachvollziehbar zu dokumentieren und bei jeder Programmänderung aufs Neue angemessene Tests durchzuführen. Bei Software für kritische Bereiche[1] ist dieses Vorgehen längst Pflicht. Es steht zu hoffen, daß sich diese Anforderungen zumindest in Ansätzen allgemein durchsetzen werden.

In praktisch jedem Projekt macht sich der Mehraufwand für ein zumindest halbautomatisches Testverfahren sehr schnell bezahlt.

Dokumentation

Ein Projekt ist zwar nicht „nur so gut wie seine Dokumentation“, aber in bestimmten Fällen kann ein Projekt dieser Situation nahe kommen – eine komplexe Software zum Beispiel ist ohne angemessene Dokumentation tatsächlich praktisch nutzlos. Leider kann es durchaus vorkommen, daß der Kunde für etwaigen Mehraufwand zur Dokumentation nur wenig Verständnis hat. Hier ist dann das Überzeugungsvermögen des Auditors bzw. Beraters gefragt. Der Kunde muß dann davon überzeugt werden, daß der Mehrnutzen den Mehraufwand überwiegt und eine Nachvollziehbarkeit der Ergebnisse in seinem ureigenen Interesse liegt. Eine mögliche Argumentationsstrategie könnte das Software Lifecycle Model sein (20-80-Regel: 20% des Gesamtaufwands für eine Applikation fällt zur Entwicklungszeit an, 80% im laufenden Betrieb für Wartung und Pflege).

Projektabschluß

Zum Abschluß eines Projektes ist es wesentlich, daß die Perzeption des Kunden dahin geht, daß das Projekt ein Erfolg und der Auditor oder Projektleiter sein Geld wert war. Denn nur dadurch kann sichergestellt werden, daß der Kunde beim nächsten Projekt wiederkommt. Dies ist meistens genau dann der Fall, wenn zu keinem Zeitpunkt des Projektes beim Kunden ein Bruch zwischen der Erwartungshaltung und der wahrgenommenen Leistung eintritt.

Die eigene Perzeption bezüglich des Projekterfolgs hingegen ist absolut sekundär. Der projektbegleitende Auditor oder Berater schuldet in der Regel nicht den Projekterfolg, sondern „Due Professional Care“ und – „that the customer feels it’s his own success.“

Über den Autor

Ulrich H. Benzing, CISA, ist Vorstand der German Technologies AG, welche als Unternehmensberatung Kunden in den Bereichen IT Management, IT Security und Softwareentwicklung unterstützt.
uhb@german-technologies.com

Endnote

1 Beispielsweise FDA “General Principles of Software Validation”, 11.01.2002

Risikomonitoring mit CAAT

Der Bedarf für ein Früherkennungssystem für IT-Risiken ergibt sich für viele Unternehmen nicht nur aus gesetzlichen Anforderungen, sondern auch aus rein ökonomischen Überlegungen. Die „klassischen“ IT-Risiken, wie fehlende Systemverfügbarkeit oder fehlender Datenschutz, können mit den üblichen Methoden der Risikoprävention, wie z.B. Notfallplanungen oder ausgefeilten Berechtigungskonzepten, im wesentlichen unter Kontrolle gehalten werden. Eine schwerwiegende Risikolücke ergibt sich im Bereich der Anwendungssysteme. Kein Softwaresystem ist fehlerfrei (man hat sogar schon von Fehlern im SAP-Umfeld gehört). Dies ist nicht nur eine theoretische Wahrheit, sondern kostet in der Praxis die Unternehmen weltweit zum Teil erhebliche Summen bis hin zur Bestandsgefährdung.

Das am schwierigsten zu handhabende IT-Fehlerrisiko ist dabei nicht der Super-GAU, der Anwendungssysteme lahm legt, Datenbanken in Datenmüllhalden verwandelt und in jedem systemgenerierten Reporting leicht zu erkennen ist, sondern der versteckte kleine Fehler, der nur bei bestimmten Datenkonstellationen zum Tragen kommt. Ein falscher Steuerschlüssel oder eine falsche Währungsumrechnung kann langfristig mehr Schaden anrichten, als ein abgestürztes Anwendungssystem.

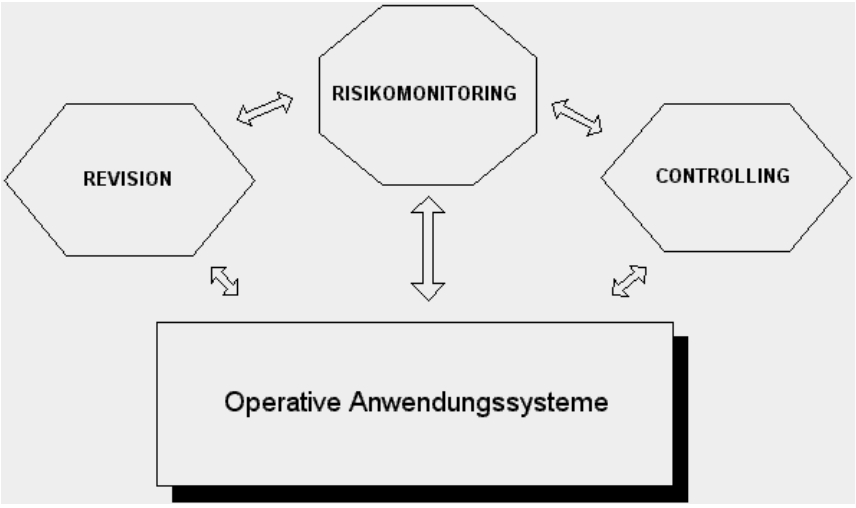
Zwei Ansätze liegen zur Schließung der Risikolücke auf der Hand. Zum einen müssen Systeme so fehlerfrei wie möglich implementiert werden, d.h. hohe Standards in Entwicklung und Qualitätssicherung sind unbedingte Voraussetzung zur Verringerung des Risikos. Zum anderen müssen Anwendungssysteme und Prozesse überwacht werden. Was liegt hier näher als ein Softwaresystem zur Überwachung von Anwendungen einzusetzen?!

Systeme, die Systeme überwachen, in technischen Anwendungsbereichen, wie z.B. in Fertigungsstraßen oder in Netzwerken, sehr verbreitet, in betriebswirtschaftlichen Prozessen aber noch Neuland.

Grundsätzlich bietet sich bei kaufmännischen Anwendungssystemen eine Überwachung der kaufmännischen Daten an. IT-Risikomonitoring bedient sich der Daten von Anwendungssystemen, kann aber auch auf bereits vorhandene verdichtete Datenbestände, z.B. für Controlling- oder Revisionszwecke, zugreifen. Wesentlich für die Brauchbarkeit solcher Daten ist allerdings die Fehlerfreiheit des Verdichtungsprozesses, hier ist im Zweifel die Überwachung der Rohdaten vorzuziehen.

Der Monitoringprozess gestaltet sich in seiner Struktur relativ einfach. Anhand von festgelegten Grenzwerten werden Datenobjekte und ihre Beziehungen untereinander zyklisch überwacht.

Ein Beispiel: Im Rahmen des Risikomonitorings werden wöchentlich alle Ausgangsrechnungen eines Unter-



nehmens überprüft. Sinkt die Summe der Rechnungsbeträge unter einen festgelegten Schwellenwert, weichen einzelne Rechnungsbeträge von festgelegten Durchschnittswerten erheblich ab, sind negative Rechnungssummen dabei, oder ist der Debitor gesperrt, werden die betroffenen Einzelfälle zur Überprüfung durch einen „Risikocontroller“ protokolliert.

Das Beispiel zeigt die enge Verwandtschaft zwischen den Ansätzen für Risikomonitoring, Controlling und Revision. Prinzipiell ist ein Überwachungssystem zum Zwecke des Risikomonitorings ebenso für Controlling und Revision („Continuous Auditing“) geeignet. Dies erleichtert zudem die Auswahl geeigneter Softwarewerkzeuge. Steht ein Data-Warehouse für das Controlling zur Verfügung, kann dies relativ einfach genutzt werden.

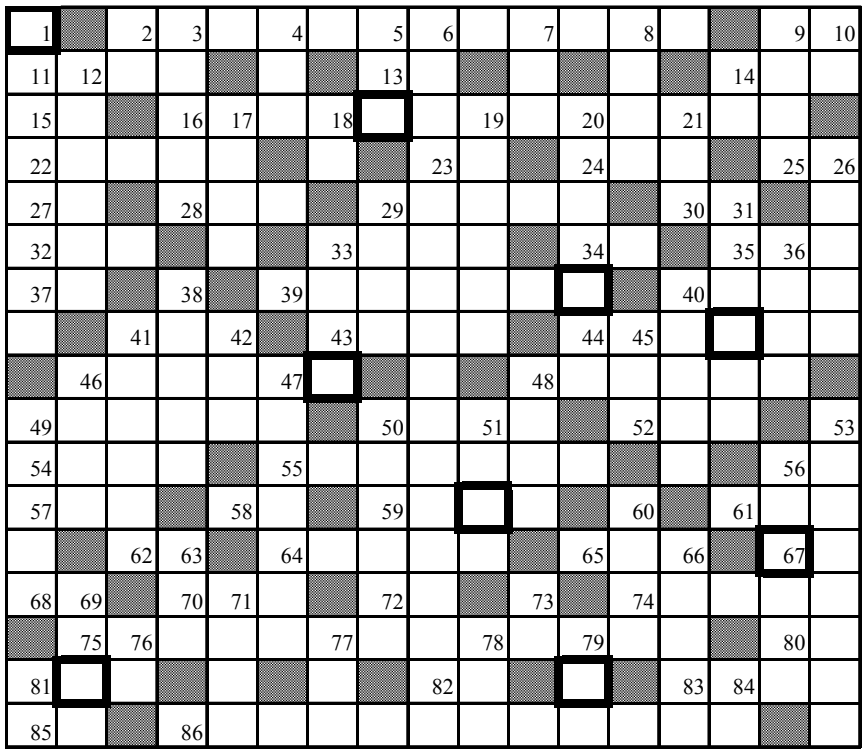
Preiswerter als ein Data-Warehouse und in Teilbereichen flexibler sind Softwarelösungen aus der Revision (CAAT). Die beiden wesentlichen Produkte für die Datenprüfung (ACL und WinIDEA) bieten sich hier aus Gründen der Flexibilität und Performance an.

Die einfache Struktur und die bereits vorhandenen Softwarelösungen sollten aber nicht täuschen. Die eigentliche Kunst des Risikomonitorings, nach den hier vorgestellten Prinzipien liegt in der Festlegung welche Datenobjekte, nach welchen Verfahren und mit welchen Grenzwertparametern zu überwachen sind. Hier ist viel Arbeit zu leisten. Ein funktionierendes Risikomonitoring-System kann aber erhebliche Schäden durch Softwarefehler abwenden und zudem wertvolle Daten für Controlling und Revision liefern.

Holger Klindtworth, CISA
Susat & Partner.

The ISACA Crossword Puzzle 5/02

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: 2 Babysachen zum Kuscheln (Mz); 9 technischer Boxausdruck; 11 Schlaufe; 13 Dehnlaut; 14 Angsttraum; 15 dem lateinischen König fehlt das „e"; 16 Angriff in einer Debatte; 22 Ausdruck der Zuneigung; 23 tiefster Offiziersgrad (Abk); 24 drei gleiche Buchstaben; 25 Einheitsbahn (Abk); 27 „heilige" Abkürzung; 28 Maschinenteil; 29 Homers Ilium; 30 französische Insel; 32 nordische Totengöttin; 33 gegenseitige Wechselbürgschaft; 34 Nahrungsmittel; 35 windabgewandte Seite; 37 pers Fürwort (frz); **39 Ausbildungsstätte (Mz);** 40 Textilart; 41 Ausdruck des Staunens; 43 heim (engl); **44 ist nicht nur für die Anrechnung zu 86 waagrecht hilfreich;** 46 beachteter Überrest; **48 moderner Ersatz zu 6 senkrecht;** 49 umstrittene Provinz Jugoslawiens; 50 so hätte „DRS1" früher heissen können; 52 kaputt; 54 nordisches Göttergeschlecht; 55 Antrieb (Mz); 56 pers Fürwort; 57 engl Zahlwort; 58 Doppelkonsonant (z.B. für Prokura); 59 angelehnt (engl); 61 Tante (span); 62 hier; 64 Fischerrute; 65 diese (frz); 67 Finanzinstitut (Abk); 68 zweite Stufe der it Tonleiter; 70 frz Artikel; 72 Eisernes Kreuz (Abk); 74 einfache Behausung (Mz); **75 ohne dieses geht es kaum;** 80 wäre auf französisch ja gelacht; 81 Mass der Fadenstärke; 82 Umlaut; 83 erwachsener Knabe; 85 span Artikel; **86 studieren nach dem Abschluss.**

Senkrecht: **1 Schulungsform hands-on;** 2 was einem nach Briefschluss noch eingefallen ist; 3 Hebel (engl); 4 Ohr (engl); **6 wenn er kaputt ist, sind die schönsten Folien nutzlos;** 5 amerik Geheimdienst (Abk); 7 Bestand; 8 Hinterteil (engl); 9 Futterpflanze; 10 russischer Strom; 12 Fremdländische (Mz); 14 Aktienkapital (Abk); 17 biblischer Riesenvater; 18 weibliches Bekleidungsstück (Abk); 19 Koralleninsel (Mz); 20 Wasserstelle für Tiere; 21 Schrei (frz); 26 geschnittenes Holz; 29 Television hinter Ort (Abk); 31 Backform; 33 Zahlwort; 36 arab Fürstentitel; 38 chem Grundstoff; 40 Nachkomme des ersten Sohns von Noah; 41 so ist das Wild bei der Nahrungsaufnahme; 42 keine positive Nachricht, wenn positiv; 45 Querstange beim Segelschiff; 46 Blume; 47 Orientierungshilfe; 48 alkoholisches Getränk; 49 männliches Haustier; **50 temporäre Aufenthalte zur Ausbildung (engl);** 51 legendäre Wunderschale; **53 Form der Ausbildung;** 56 der Fan tut es; 60 afrikanische Wildart; 63 Weltraum; 66 Additionstotal; 69 Grautier; 71 eine der Gezeiten; 73 zu (lat); 76 Fluss in Graubünden (Landessprache); 77 Vollbrachtes; 78 Aufforderung zum Training; 79 Fluss im Elsass; 81 frz Adelsprädikat; 84 Präposition.

Die Lösung liegt in den markierten Feldern. Dieses Wort ist auf einer Postkarte zu senden an M.F. Bretscher, Oberrenggstrasse 8, CH-8135 Langnau a/A bis 15. Januar 2002. Lösungen werden auch entgegengenommen unter der Adresse mbretscher@kpmg.com.

Lösungswort Kreuzworträtsel 4/02: *Kunterbunt*

Versteckte Einzelheit: Die Nummer 70 fehlt im Kreuzworträtsel.

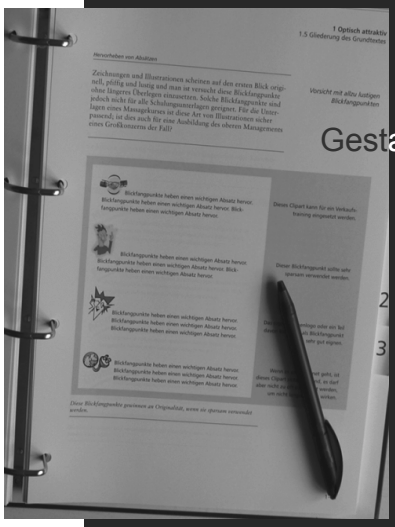
Das Lösungswort wurde richtig von mehr als fünf Teilnehmerinnen und Teilnehmern eingesandt, weshalb wieder einmal ein Gewinner ausgelost werden konnte. Es ist Jakob Kaufmann. Herzliche Gratulation!

Die versteckte Einzelheit wurde einmal mehr nicht entdeckt. Somit befinden sich weiterhin $ 100 im „Watson“-Jackpot.

Waagrecht: 1 Taste; 5 SA; 7 Po; 9 solid; 14 alto; 15 *Mosaike*; 18 Riri; 19 TI; 20 TuS; 21 Io; 22 Knie; 25 Spitals; 28 Mehl; 30 alle; 32 Wasa; 33 GI; 34 Albis; 36 anbei; 38 LR; 40 Eva; 42 aes!; 44 toi; 45 Abo(rigine); 46 *Bilderraetsel*; 51 Ibis; 52 Aer; 53 Hase; 54 *Durcheinander*; 59 Che; 61 Ike; 62 MII; 63 mit; 65 hu; 66 antik; 67 Oskar; 69 SE; 71 Hang; 74 Zorn; 76 Andy; 77 Geselle; 81 Toys; 83 ad; 84 Ogi; 85 lo; 86 Eber; 89 *Eintopf*; 92 Leda; 94 rerun; 96 IG; 96 ni; 97 banal.

Senkrecht: 1 Tank; 2 al; 3 steil; 4 to; 5 so; 6 Asti; 7 Pisa; 8 OK; 10 or; 11 Limes; 12 ir; 13 Dill; 15 MIS; 16 Auto; 17 Eis; 23 naiv; 24 Ela; 26 Prise; 27 Lunte; 28 Mai; 29 halb; 31 ELAL; 32 weis'; 33 *Gemisch*; 35 *bedeckt*; 38 Botanik; 39 *Rosette*; 41 abide; 43 Preis; 45 Alarm; 47 ISU; 48 RAE; 49 Arn; 50 Ehe; 55 Ring; 56 Heime; 57 Amsel; 58 Diaz; 60 Huhn; 64 Isny; 66 any; 68 rot; 72 Adler; 73 fegt; 75 Rosen; 76 Aber; 77 Gde; 78 Song; 79 lion; 80 Elf; 82 Saal; 87 BE; 88 Ru; 90 II; 91 Pi; 92 la; 93 da.

Wissens so bringen Sie's rüber Transfer



Gestaltung von
Schulungsunterlagen
und Präsentationsfolien

www. wissenstransfer.ch

Francesca Lüscher Baglioni
Eidg. dipl. Betriebsausbilderin
Ausserdorf 22, 8235 Lohn
Tel. 052 640 09 47

News aus den Interessengruppen

Neue Interessengruppen

Wir planen, neue Interessengruppen zu gründen. Als mögliche Themen sind vorgeschlagen:

- IG Continuous Auditing
- IG e-security (z.B. Attack and Penetration, e-defense, e-security Architecture)
- IG Archivierung (Aktualisierung der Arbeiten der ehemaligen IG Aufbewahrung)
- IG ??? Anregungen für weitere IGs nimmt Rolf Merz gerne entgegen.

IG e-business

Leitung a.i.:
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@eycom.ch

Nächste Sitzung: Dezember 2002/ Januar 2003 (genauer Termin wird mit den Teilnehmern noch vereinbart), E&Y, Zürich
Traktanden:

- Entwurf Management Präsentation
- Entwurf Business Case
- Präsentation/Besprechung der Business Cases

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 Anwendung von COBIT

Leitung a.i.
Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 6679
Fax. +41 58 286 6827
rolf.merz@eycom.ch

Die IG soll reaktiviert werden. Dazu werde ich die bisherigen IG-Mitglieder anschreiben. Weitere Interessenten melden sich bitte bei Rolf Merz.

IG Outsourcing/ Insourcing

Jean-Pierre Brenn
Ernst & Young
Postfach 5272
8022 Zürich
Tel. +41 1 286 32 79
Fax. +41 1 286 42 33
Jean-pierre.brenn@eycom.ch

Letzte Sitzung: Aus Termingründen musste die auf den 28. Oktober 2002 angesetzte Sitzung ausfallen.

Nächste Sitzung: Offen

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@eycom.ch

Letzte Sitzung: 2. Oktober 2002, EY Zürich
Traktanden:

- Organisatorisches
- Referenzmodell und Metadaten
- Kontrollziele / Risk Matrix
- Diverses

Nächste Sitzung: Ende November/ Anfang Dezember 2002. Interessenten melden sich bitte bei Daniel Oser.

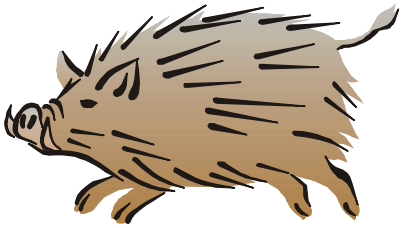
IG SAP R/3

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

Letzte Sitzung: Donnerstag, 14. November 2002, Bei PWC, Zürich
Traktanden:

- ACL/Berechtigungen wie prüfen (Hr. Appl., SNB)
- Qualitätsprüfungskonzept im SAP (Hr. B. Bolli, CCSAP BAIT)
- Im SAP das Risk assessment tool RAT einsetzen (Hr. A. Hilsbos, PWC)
- Neues vom Jahresmeeting SAP-AK's (H.J. Stritter, EDV-Audit-Consult)
- Übertragung von SAP Walldorf (M. Galli)
- SAP und AIS AUDITool News, Erfahrungen und Tips (alle)

Nächste Sitzung: Termin noch offen. Interessenten melden Sich bitte bei der IG Leiterin.



Eine Bache fand ihre Familie grossartig und cool:
Die Frischlinge wälzten sich grunzend im Pfuhl,
Der Keiler vertrat sich gerade die Beine,
Und Jagdsaison war ohnehin keine:
Die Jäger mussten zum Nachsitzen gerade zur Schul.

Shaw's Higgins taught Liza thoroughly where it is raining:
On the plain there in Spain, he was insisting and claiming.
It was sunshine when I was in Córdoba
The same held true when in Málaga.
I guess Higgins himself needs a few lessons and training.

Un réviseur de Paris cherchait partout l'amour et la passion.
Il n'était pas content avec la moitié, une portion ou une ration.
Il demandait tout à Lausanne et à Genève
Mais toutes les filles là étaient courtes et brèves:
« Il nous semble qu'il te faut du comment et de la formation. »

DACH-News

D: Aktivitäten des German Chapter

Am 7. Juni und 25. Oktober 2002 hat sich der Vorstand des ISACA German Chapter jeweils zu seinem vierteljährlichen Vorstandsmeeting in Hamburg bzw. Frankfurt am Main getroffen, um persönlich zu besprechen, was in den letzten Monaten passiert ist und wie wir die Zukunft des Vereins kurz-, mittel- und auch langfristig gestalten wollen. Dazwischen haben wir regelmäßige Telefonkonferenzen eingeführt, um möglichst zeitnah Planungen und Umsetzungen besprechen sowie weitere Entscheidungen treffen zu können.

Zentrale Themen der letzten Treffen waren die Nachschau der CISA-Kurse in Frankfurt und Hamburg, weitere Verbesserungen unseres prämierten Internetauftritts, die Zukunft von Arbeitskreisen, die IT-Security-Conference in München, die Präsenz des ISACA auf dem IT-Management Forum 2002 in Mainz, die Rückschau unserer Präsenz auf der Systems in München, zukünftige Präsenz auf weiteren Messen, die Zukunft des Berufsbildes des IT-Revisors bzw. des CISA in der Öffentlichkeit sowie die bevorstehende Einführung des CISM-Examens.

Im Verlauf der Treffen traf der Vorstand einige Entscheidungen, von denen hier die wichtigsten kurz zusammengefasst dargestellt werden sollen:

- Auch im kommenden Jahr soll im Rahmen des CISA-Kurses wieder ein Testexamen angeboten werden. Die Vorbereitungsunterlagen für den Kurs sollen kontinuierlich weiterentwickelt, verbessert und vereinheitlicht werden.
- Diverse Verbesserungen unserer Website sowohl in der Erscheinung als auch inhaltlich, beginnend mit unserer bereits produktiven dynamischen Navigationsleiste, werden von uns zukünftig umgesetzt.
- Wir wollen auf Veranstaltungen innerhalb des ISACA sowie auch anderen Fachveranstaltungen zukünftig präsenter sein als in der Vergangenheit.
- Weitere Kooperationen sind angestrebt und werden daher von uns gesucht und geprüft.
- Eine Präsenz auf der CEBIT in Hannover in 2003 wird geplant.
- Das CISM-Examen soll von uns entsprechend in Deutschland angeboten werden.

Besonders gefreut haben wir uns natürlich noch über die Bestehensquote der Deutschen CISA-Kandidaten, die wieder einmal besser war als die weltweite. Wir möchten hiermit allen bestandenen CISAs die herzlichen Glückwünsche des Vorstands aussprechen und hoffen auf ein entsprechendes Abschneiden auch im Jahr 2003.

Nachdem einige besonders engagierte Teilnehmer des diesjährigen CISA-Kurses das CISA Review Manual in einem ersten Anlauf übersetzt haben, wird nun vom German Chapter ein Projekt zur offiziellen Übersetzung des Manuals 2003 gestartet. Alle an einer Mitarbeit an diesem Projekt interessierten Mitglieder mögen sich bitte bei unserem für das CISA-Examen zuständigen Vorstandsmitglied Michael Schneider (Handy: 0163-7569124, e-mail: michaelschneider@deloitte.de;) melden, der weitere Informationen hierzu geben kann.

Dies sind natürlich nicht alle Themen, die besprochen wurden, aber sie sollen einen kleinen Einblick in die Arbeit des Vorstands ermöglichen. Natürlich hoffen wir mit den bereits ergriffenen sowie den für die Zukunft geplanten Aktionen, den Nutzen des Vereins für die einzelnen Mitglieder weiter steigern und den Bekanntheitsgrad des ISACA sowie auch des CISA-Examens in Deutschland zu erhöhen. Mit der Einführung des CISM-Examens hoffen wir, auch im Bereich des IT-Security-Managements eine adäquate Berufsqualifikation etablieren zu können.

Ingo Struckmeyer

CH:

20 % Rabatt für Arbeitslose bei allen ISACA-Kursen

Der Vorstand des ISACA-Switzerland Chapter hat entschieden, zur Unterstützung unserer Berufsgruppe bis auf weiteres sämtliche Kurse für Arbeitslose um 20 % zu vergünstigen (Rabatt auf dem Nicht-Mitgliederpreis; jedoch nicht auf den

auswärtigen Übernachtungs-/Verpflegungskosten). Wir möchten damit gerade in der heutigen Arbeitsmarktsituation ein Zeichen setzen! Selbstverständlich können auch andere Personen von unseren Kursen profitieren – wir werden auf das Frühjahr verschiedene neue Kompaktkurse ausschreiben, bei denen der Fokus eher in der Breite liegt. Als Ausbildungsverantwortlicher des ISACA-Switzerland Chapter liegt mir natürlich daran, dass möglichst viele unserer Mitglieder, aber auch unserer Berufskollegen von solchen Möglichkeiten profitieren!

Peter R. Bitterli

Voranzeige: EUROCACS 2004 in der Schweiz

Entgegen unserer Erwartungen und entsprechenden Kommunikation an der letzten Generalversammlung wurde Zürich als Ort der Durchführung für die EUROCACS 2004 gewählt. Das freut uns natürlich riesig! Aufgrund unserer Erfahrungen aus der Konferenz 1999 wissen wir, dass es einiges zu organisieren und abzuklären gibt. Freiwillige Helferinnen und Helfer sind deshalb gesucht! Meldungen nimmt vorläufig die Redaktion entgegen. Derzeit prüfen wir übrigens Alternativen für den Durchführungsort. Datum der Konferenz: ca. Ende März 2004.

German Technologies AG
- IT-Beratung
- IT-Projektmanagement
- IT-Entwicklung

Universität des Saarlandes ◪ Gebäude 34 ◪ 66123 Saarbrücken ◪ contact@german-technologies.com

Veranstaltungen

Network Security	18.–20. November 2002 München, 3 Tage, ISACA
Controlling & Securing Windows 2000	26.–29. November 2002 London, 4 Tage, MIS
Intensivlehrgang für Informations- und IT-Sicherheitsbeauftragte	1.–5. Dezember 2002 Brunnen, 5 Tage, Infosec
Vertiefungskurs Informatik-Sicherheit & Informatik-Revision CISA-Kurs 2003	6. Dezember 2002–19. Mai 2003 Zürich, 17 Tage, ISACA CH
Advanced Certified Security Revisor	9.–13. Dezember 2002 Heilbronn, 5 Tage, Integralis
Fraud Week	20.–21. Januar 2003 London, 2 Tage, MIS
Internet Security Lab	29.–31. Januar 2003 Zürich, 3 Tage, ISACA CH
SES-Fachtagung Sicherheit im Wandel	30. Januar 2003 Zürich, 1 Tag, SES
Application Security Lab	5.–7. Februar 2003 Zürich, 3 Tage, ISACA CH
Neuigkeiten in der Überwachung von Zahlungs- und Effektenabwicklungssystemen	18. Juni 2003 Bern, 1 Tag, ISACA/Kammerseminar
EuroCacs	23.–26. März 2003 Amsterdam, 4 Tage, ISACA

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

Datenschutzbeauftragter des Kantons Zürich
IT-Sicherheitsberatung und -Revision
Andrea Carlo Mazzocco, CISA
Kurvenstrasse 31
CH-8090 Zürich
Tel. +49 1 259 46 08
Fax. +49 1 259 51 38
andreacarlo.mazzocco@dsb.zh.ch
www.datenschutz.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

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

ISACA CH
Kurssekretariat
c/o. Bitterli Consulting AG
Konradstr. 1
8005 Zürich
Tel. +41 1 440 33 60
Fax. +41 1 440 33 61
kurse@isaca.ch

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

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

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

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

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

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

Express Line

A Word from the Chair

The membership renewal invoices for 2003 are currently being printed and will be sent shortly to all current members.

As you may be aware, it is easier to retain current members than to attract new members. Retention normally can be correlated directly to membership and chapter satisfaction. I encourage each chapter to do its best in increasing its membership retention over 2002.

Howard Nicholson
Chair, Membership Board

New CISM(r) Credential

The Certified Information Security Manager (CISM) certification is now available. This management-level certification was initiated more than two years ago after a membership survey and board-appointed task force indicated a need for such a program. CISM addresses the proliferation of global information security concerns by providing executive management with assurance that information security professionals, specifically those managing an information security system, have the required experience and knowledge to provide effective information security management and consulting services.

The first exam (English only) will be offered in June 2003. The exam is intended to be available in every worldwide location in which the CISA exam is conducted, which consists of 200 test sites in more than 75 countries.

Information has been posted to the ISACA web site at www.isaca.org/cism. Each chapter will soon receive an inventory of a general CISM information brochure along with CISM grandfathering applications.

CISA Update

2003 CISA study materials are now available through the ISACA bookstore. The 2003 CISA Review Manual, 2003 CISA Questions, Answers and Explanations Manual (500 study questions) and 2003 CISA Questions, Answers and Explanations Manual Supplement (100 questions) are excellent sources for candidate preparation for the 2003 CISA exam. The CISA Questions, Answers and Explanations CD-ROM (600 questions) and the CISA Study Course (currently under development) will be available in December for chapter download and use.

Standards Update

Newly Issued Guidance

The Standards Board recently issued an IS Auditing Guideline on Reporting, effective 1 January 2003 to replace guideline 070.010.010. There also are six exposure documents, posted to the ISACA web site, including four guidelines – Review of System Development Life Cycle, Review of Business to Consumer E-commerce, Review of Enterprise Resource Planning Systems and Internet Banking – and two procedures – Intrusion Detection System Review and Malicious Logic. The exposure period ends 30 November 2002.

A comprehensive standards PDF document containing all the standards, guidelines and procedures has been posted on the ISACA web site at www.isaca.org/standard/stdownload.htm.

Germany Chapter

Vereinsadressen

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

Präsidentin
Karin Thelemann
Arthur Andersen WPG StB GmbH
Mergenthaler Allee 10-12
D-65760 Eschborn
Tel. +49 619 699 6488
Fax. +49 619 699 6449
karin.oberle@de.arthurandersen.com

Konferenzen
Georgios Safaridis
D-Hamburg
georgios_safaridis@web.de

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

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

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

Publikationen
Ingo Struckmeyer
comdirect bank AG
Internal Audit
Pascalkehre 15
25451 Quickborn
Tel. +49 4106 704 1233
Fax. +49 4106 704 1990
ingo.struckmeyer@comdirect.de

CISA-Koordinator
Michael M. Schneider
Arthur Andersen WPG StB GmbH
Arnulfstrasse 126
D-80636 München
Tel. +49 89 1269 7176
Fax. +49 89 1269 7180
michael.m.schneider@
de.arthurandersen.com

Austria Chapter

Vereinsadressen

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

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

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

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

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

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

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

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

Switzerland Chapter

Vereinsadressen

Präsidentin
Daniela S. Wüst
Swiss Re
Mythenquai 50/60
8022 Zürich
Tel. +41 1 285 69 36
Fax. +41 1 285 33 69
daniela_wuest@swissre.com

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

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

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

CISA-Koordinator
Thomas Bucher
Ernst & Young Ltd
Badenerstrasse 47
8022 Zürich
Tel. +41 58 286 42 90
Fax. +41 58 286 36 88
thomas.bucher@eycom.ch

Sekretär
c/o Präsidentin

Information & Kommunikation
Monika Josi
PricewaterhouseCoopers
Nordstr. 15
8035 Zürich
Tel. +41 1 630 27 82
Fax. +41 1 630 27 55
monika.josi@ch.pwcglobal.com
Adressmutationen bitte hier melden.

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

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

Marketing
Bruno Wiederkehr
Rentenanstalt/Swiss Life
General Guisan-Quai 40
Postfach 4338
8022 Zürich
Tel. +41 1 284 31 07
Fax. +41 1 284 47 33
bruno.wiederkehr@swisslife.ch

Homepage ISACA Switzerland Chapter: www.isaca.ch