Nr. 81 | November 2006
Novembre 2006
November 2006

# Focus:

# e-Mail

ISACA
Serving IT Governance Professionals
Switzerland Chapter

# Inhaltsverzeichnis


Editorial 4

e-Mail – Geschäftsunterlagen elektronisch archivieren – ein Überblick über die rechtlichen Anforderungen 5

e-Mail – Internet dans l'entreprise: mode d'emploi 10

e-Mail – Internet in der Unternehmung: Eine Gebrauchsanweisung 14

e-Mail – Konvergenz und Sicherheit im e-Mail Management 18

Outsourcing – A quoi sert un rapport SAS 70 et comment l'interpréter? 20

CISM – Neues CISM-Berufsbild – gültig für Prüfungen ab 2007 21

Express Line 23

The ISACA Crossword Puzzle 24

ISACA Switzerland 26

Veranstaltungen 30

Vereinsadressen 32



Impressum

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

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

Satz und Gestaltung:
WissensTransfer
Francesca Lüscher Baglioni
8235 Lohn SH



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



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

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

Erscheint 4 Mal jährlich
Auflage: 850 Exemplare

Nächste Ausgabe (Focus: Prüfungsplanung und integriertes Auditing): Februar 2007, Redaktionsschluss: 5. Januar 2007

# Editorial

## To archive or not to archive – Wie viele e-Mail Policies braucht eine Unternehmung?

Ich weiss nicht, wie es Ihnen geht, aber mir graut jeweils vor dem ersten Arbeitstag nach den Ferien: Es gilt, innerhalb kürzester Zeit aus ein paar hundert ungelesenen e-Mails die unwichtigen, wichtigen, dringenden und superdringenden Nachrichten herauszufiltern und entsprechend zu beantworten. Ca. sechs Wochen später steht jeweils eine weitere Entscheidung an: Welche e-Mails soll/muss ich archivieren und welche können getrost der Nachwelt vorenthalten bleiben.

Aber weshalb und vor allem welche e-Mails archivieren? Gemäss schweizerischem Recht müssen Geschäftsdokumente immer dann aufbewahrt werden, wenn sich damit Rechte und Pflichten feststellen lassen, die in der Unternehmensbuchhaltung Niederschlag finden. Während dies bei „normaler" Briefkorrespondenz noch einigermassen zu bewältigen ist, ist es bei e-Mails sehr viel schwieriger, diese entsprechend zu identifizieren. Manchmal ist man nur cc-Empfänger einer e-Mail, manchmal ist der wesentliche Inhalt einer e-Mail nicht im Text selbst, sondern in Anhängen in Word-, Excel- oder PDF-Format versteckt. Für internationale Firmen ist es zudem eine weitere Herausforderung, der jeweils lokalen Rechtsprechung Rechnung zu tragen. Da immer mehr Informatikdienste „outgesourced" und „offgeshored" sowie e-Mails zwischen verschiedenen Ländern und Rechenzentren dupliziert und repliziert werden, ist es für viele Unternehmen schwierig, überhaupt nachzuvollziehen, welche e-Mails wann, wo und wie lange verfügbar sind. Dies führt oftmals dazu, dass betriebsinterne e-Mail-Archivierungsvorschriften nicht eingehalten werden (können/dürfen).

Im Zusammenhang mit Gerichtsfällen werden e-Mails immer mehr als Beweise zugelassen. Themen wie e-Discovery, Litigation Support (Unterstützung der Rechtsabteilung bei Gerichtsfällen), Litigation Hold (Beweismittel dürfen während eines laufenden Gerichtsverfahrens in den USA nicht vernichtet werden) aber auch die Frage nach der Beweiskraft einer ungeschützt übermittelten und gespeicherten e•-Mail stehen deshalb zunehmend im Fokus der Unternehmen. In der Schweiz unterstehen e-Mails zudem dem Datenschutzrecht und Fernmeldegeheimnis, was bedeutet, dass die Einsichtnahme in private e-Mails sowie das systematische personenbezogene Überwachen von e-Mails eines Arbeitnehmers streng reglementiert ist. e-Mail-Systeme von Unternehmen mit Standort Schweiz müssen demnach die technischen und organisatorischen Anforderungen der Datenschutzverordnung erfüllen.

Experten empfehlen eine selektive Aufbewahrung von e-Mails. Aber wer bestimmt die Selektion und aufgrund welcher Fakten? Und wie werden diese Vorgaben im Unternehmen durchgesetzt? Ein scheinbar triviales technisches Problem entwickelt sich zu einer Art Quadratur des Zirkels. Das Wechselspiel zwischen Informatik und Recht, Technik und Organisation muss miteinander abgestimmt werden und entwickelt sich zunehmend zu einem Hochseilakt ohne Netz für die Unternehmen. Wir hoffen, in diesem ***NewsLetter*** einige Aspekte beleuchten zu können. Ich bin mir aber sicher, dass dieses Thema zunehmend an Bedeutung gewinnt und dies erst der Beginn einer langen Diskussion ist.

***Monika Josi***

## To archive or not to archive – Combien de directives sur la messagerie électronique sont-elles vraiment nécessaires dans une entreprise?

Je ne connais pas votre situation mais j'appréhende personnellement le retour des vacances. Comment identifier parmi plusieurs centaines de mails les mails urgents et importants et y répondre rapidement ? Environ 6 semaines plus tard se posera la seconde question : quels mails auront-ils l'honneur d'être archivés ?

Mais d'abord, pourquoi archiver des mails ? Selon le droit suisse, les entreprises doivent conserver la correspondance commerciale, dans la mesure où elle documente des droits ou des engagements qui se reflètent dans la comptabilité financière. Une interprétation relativement simple pour la correspondance « normale » mais qui se complique rapidement avec les mails. L'entreprise ne reçoit parfois un mail qu'en qualité de cc-destinataire, le contenu déterminant ne se trouve dans d'autres cas pas dans le mail mais dans les pièces qui y sont annexées en format Word, Excel ou pdf. La multitude des législations et des jurisprudences locales vient encore compliquer la situation des entreprises internatio-

nales qui doivent tenter de concilier des exigences parfois contradictoires. Le recours de plus en plus fréquent à l'outsourcing et à l'offshoring des services informatiques et la réplication ou la duplication des mails entre plusieurs localisations géographiques rendent souvent quasi-impossible l'identification exacte de tous les mails enregistrés. Comment assurer dans de telles conditions le respect de directives internes sur l'archivage ?

La jurisprudence nous montre que les mails jouent un rôle toujours plus important lorsqu'il s'agit de rechercher des preuves. Des thèmes comme : e-Discovery, Litigation Support (soutien IT pour la division juridique durant le procès), Litigation Hold (aux USA, les éventuels moyens de preuve ne peuvent être détruits avant la fin d'un procès) mais également la question du caractère probant d'un mail transmis ou archivé sans protection particulière deviennent des questions centrales pour une entreprise. En Suisse, la législation sur la protection des données et le secret postal protègent les mails, compliquant ainsi l'analyse ou la surveillance systématique des mails privés par les employeurs. Les systèmes de messagerie des entreprises actives en Suisse doivent ainsi répondre aux exigences techniques et organisationnelles de l'Ordonnance sur la protection des données.

Les experts recommandent un archivage sélectif des mails. Mais qui doit déterminer les critères ? Selon quelles bases légales ? Et surtout : comment assurer le respect de ces directives dans l'entreprise ? Un problème technique relativement trivial à l'origine tend à la quadrature du cercle. Le dossier passe des informaticiens aux juristes, des organisateurs aux techniciens, et l'entreprise demeure dans la position d'un funambule travaillant sans filet. Nous espérons vous donner dans ce numéro quelques éléments de réponse. Je suis cependant persuadée que l'importance de ce thème va encore croître dans le futur et que nous ne sommes qu'au début d'une longue discussion.

***Monika Josi***

# e-Mail

## Geschäftsunterlagen elektronisch archivieren – ein Überblick über die rechtlichen Anforderungen

Die Dokumentation der geschäftsrelevanten Vorgänge eines Unternehmens kann verschiedene Ziele verfolgen. So ist die rechtskonforme Aufbewahrung von Geschäftsunterlagen einerseits gesetzliche Pflicht und anderseits Teil des Risikomanagements eines Unternehmens. Darüber hinaus kann die Archivierung von Geschäftsdokumenten auch den Zweck verfolgen, die eigene Geschichte für sich und die Nachwelt nachvollziehbar aufzuzeichnen. Seit Inkrafttreten der neuen Buchführungsvorschriften können die gesetzlichen Aufbewahrungspflichten auch durch elektronische Archivierung erfüllt werden, was insbesondere bei e-Mail von Bedeutung ist.

### Die elektronische Archivierung – ein IT-Projekt?

Um es gleich vorwegzunehmen – es ist strikt davon abzuraten, die Umstellung vom Papierarchiv auf ein elektronisches Archiv ausschliesslich als IT-Projekt zu sehen. Eine solche Betrachtungsweise führt sehr leicht dazu, die Gesamtverantwortung nicht nur für das Projekt, sondern für die Archivierung insgesamt der IT-Abteilung zuzuschreiben. Die gesetzlichen Anforderungen an die ordnungsgemässe Führung und Aufbewahrung der Geschäftsunterlagen sind sehr viel komplexer und vielfältiger. Die Verantwortung für eine funktionierende IT-Infrastruktur ist nur ein Teil davon.

Bereits bei der Planung und der Realisierung des Projekts muss daher mit berücksichtigt werden, dass der rechtskonforme Umgang mit Geschäftsdokumenten eine Daueraufgabe des Unternehmens ist und in den Verantwortungsbereich der Geschäftsleitung fällt. Diese muss durch den Erlass von Weisungen und Policies die strategischen Ziele vorgeben, aus denen dann die konkreten Anforderungen und Pflichten abgeleitet werden können. IT-Governance ist dabei als Teil der Corporate-Governance zu betrachten und muss sicherstellen, dass die Informationstechnologie im Einklang mit den Zielen des Unternehmens eingesetzt wird. Das IT-Security-Konzept des Unternehmens muss somit auf das elektronische Archiv ausgedehnt werden. Zudem ist mittels einer Weisung über die aufbewahrungspflichtigen Dokumente dafür zu sorgen, dass die richtigen Dokumente archiviert werden. Ein Archivierungskonzept muss Vorgaben enthalten, wie die Archivierung zu erfolgen hat und dabei auch die Tatsache berücksichtigen, dass nicht mehr benötigte Dokumente zu löschen sind.

Sind diese Massnahmen getroffen, sind die Mitarbeitenden zu schulen und über die Folgen der Nichtbeachtung der Weisungen sowohl für das Unternehmen als auch für sich selbst aufzuklären. Die Einhaltung der Weisungen und Policies muss anschliessend im Sinn einer Daueraufgabe regelmässig kontrolliert werden.

### Die Identifikation der zu archivierenden Unterlagen

Die Frage, welche Dokumente wie lange zu archivieren sind, kann nicht in einer für alle Unternehmen gültigen Form beantwortet werden. Vielmehr muss jedes Unternehmen auf der Basis der für den eigenen Geschäftsbereich gültigen Normen und unter Berücksichtigung der individuellen Risiken für sich verbindlich festlegen, welche Dokumente wie lange zu archivieren sind.

Die Buchführungsvorschriften verpflichten die Unternehmen, alle Geschäftsdokumente aufzubewahren, welche zum Verständnis und zum Nachweis der Vermögenslage und des Geschäftsergebnisses eines Unternehmens erforderlich sind. Dabei kommt es in erster Linie auf den Inhalt der Dokumente und nicht auf ihre Form an. E-Mails sind deshalb gleich zu behandeln wie jede andere Geschäftskorrespondenz – ist der Inhalt buchungsrelevant, dann müssen sie aufbewahrt werden.

Aus Gründen der Beweissicherung kann es nötig sein, weitere Dokumente aufzubewahren oder die genannten Dokumente länger als gesetzlich vorgeschrieben aufzubewahren. Der Mangel an Beweisen kann im Streitfall zum Verlust einer Forderung oder dazu führen, dass das Unternehmen eine ungerechtfertigte Forderung nicht abwehren kann.

Darüber hinaus gibt es für einzelne Berufszweige und Branchen noch Sondervorschriften, welche ausdrücklich oder implizit die Aufbewahrung bestimmter Unterlagen verlangen. So müssen z.B. Unternehmen im Pharmabereich und in der Lebensmittelindustrie, im Bankenbereich oder im Energiesektor gemäss den für sie geltenden Sondervorschriften zusätzlich zu den auch für sie geltenden Buchführungsvorschriften ge-

wisse interne Abläufe dokumentieren und die daraus entstandene Dokumentation aufbewahren. Die Hersteller von Produkten nach Produktehaftpflichtgesetz können sich unter Umständen von ihrer Haftung befreien, wenn sie ihre Herstellungsprozesse nachweisbar dokumentieren und diese Dokumentationen archivieren.

Der Umfang und die Dauer der Aufbewahrungspflicht kann auch davon beeinflusst werden, ob ein Unternehmen nur national oder auch international tätig ist. An den US-Börsen kotierte Unternehmen und deren Tochtergesellschaften haben die Anforderungen des Sarbanes Oxley Act zu beachten. Bei wichtigen internationalen Geschäftsbeziehungen sollte generell abgeklärt werden, ob in elektronischer Form erstellte und archivierte Dokumente auch am Sitz des Geschäftspartners rechtsverbindlich sind.

## Der elektronische Lebenszyklus von Geschäftsdokumenten

Es gibt heute wohl noch kaum ein Unternehmen, welches seine Geschäftsdokumente nicht elektronisch erstellt und bearbeitet. Eine vollkommen medienbruchfreie elektronische Bearbeitung der Dokumente während ihres gesamten Lebenszyklus, einschliesslich Archivierung und Löschung der Dokumente, scheiterte bis zur Revision von Art. 957ff OR und dem Erlass der dazu gehörenden Geschäftsbücherverordnung (GeBüV) an den gesetzlichen Grundlagen. Heute müssen nur mehr die Bilanz und die Erfolgsrechnung schriftlich unterzeichnet im Original aufbewahrt werden. Für die Bücher, die Belege und die Geschäftskorrespondenz gilt diese Einschränkung nicht mehr – sie dürfen schriftlich, elektronisch oder in vergleichbarer Weise geführt und aufbewahrt werden.

Sind Geschäftsdokumente im Unternehmen in elektronischer Form vorhanden, dann können sie somit auch elektronisch aufbewahrt werden – und dies ohne dass sie zuvor ausgedruckt werden müssen. Eingehende Post liegt aber häufig noch in Papierform vor. Könnte diese nicht auch elektronisch archiviert werden, müssten Unternehmen weiterhin mehrere Archive führen – eines in elektronischer Form und eines in Papierform. Die Vorschriften über die elektronische Archivierung von Geschäftsdokumenten gelten deshalb nicht nur für elektronisch erstellte und elektronisch aufbewahrte Dokumente, sondern auch für solche, welche z.B. in Papierform vorhanden waren und dann erst eingescannt werden. Allerdings bleibt die Beweislast für die Übereinstimmung des Originals mit dem elektronischen Dokument beim aufbewahrungspflichtigen Unternehmen.

## Allgemeine Grundsätze der Aufbewahrung von Geschäftsdokumenten

Einige Vorschriften der GeBüV gelten allerdings unabhängig von der Aufbewahrungsform. So sind die sogenannten Grundsätze der ordnungsgemässen Buchführung zu beachten und die Dokumente sind sorgfältig, geordnet und vor schädlichen Einwirkungen von aussen sowie vor unberechtigtem Zugriff geschützt aufzubewahren. Zudem sind die Integrität und die Verfügbarkeit der Geschäftsdokumente während der gesamten Aufbewahrungsdauer sicherzustellen. Umfangreiche Dokumentationspflichten sollen sicherstellen, dass die archivierten Unterlagen während der gesamten Aufbewahrungsdauer verstanden werden können. Zu diesem Zweck müssen die Organisation, die Zuständigkeiten, die Abläufe und Verfahren sowie die Infrastruktur dokumentiert werden. Die Dokumentation muss ständig aktualisiert werden und ist gleich lang aufzubewahren, wie die Geschäftsbücher selbst.

Die Erfüllung einiger dieser gesetzlichen Vorgaben hängt natürlich von den verwendeten Aufbewahrungsmedien ab. Während die Integrität und die Verfügbarkeit von Papierdokumenten in erster Linie mit organisatorischen Massnahmen sicherzustellen sind, sind bei der elektronischen Archivierung zusätzlich die „Grundsätze der ordnungsgemässen Datenverarbeitung“ zu beachten. Im Unterschied zur herkömmlichen Archivierung in Papierform sind somit bei der elektronischen Variante die Besonderheiten der Informationstechnologie bei der Planung des Projekts und der Erfüllung der Aufgabe zu berücksichtigen.

Entschliesst sich ein Unternehmen, seiner Aufbewahrungspflicht durch die Archivierung in elektronischer Form nachzukommen, dann müssen im Bereich der Buchführungsvorschriften die spezifischen Voraussetzungen der GeBüV erfüllt werden, damit die elektronischen Dokumente die gleiche Beweiskraft haben wie Papierdokumente.

Wie diese Anforderungen genau zu erfüllen sind, überlässt der Gesetzgeber den „Vorgaben etablierter Standesorganisationen“. Er geht davon aus, dass z.B. die Treuhandkammer aus einem Bedürfnis ihrer Mitglieder heraus derartige Vorgaben machen wird. Zudem existieren insbesondere im Bereich Informationssicherheit bereits seit langem Normen, (z.B. CobiT, BSI Grundschutzhandbuch, etc.) welche auch im Bereich Archivierung anwendbar sind.

## Die Integrität der archivierten Dokumente

Um zu verhindern, dass der Beweiswert der archivierten Dokumente in Frage gestellt wird, muss deren Integrität während der gesamten Aufbewahrungsdauer sichergestellt werden. Da an die Integrität elektronisch archivierter Dokumente keine höheren Anforderungen gestellt werden als an die von Papierdokumenten, wird keine absolute Unabänderbarkeit der archivierten Daten verlangt. Voraussetzung ist aber, dass festgestellt werden kann, ob das Dokument nachträglich geändert wurde.

Art. 9 GeBüV erlaubt neben der Archivierung auf so genannten unveränderbaren Datenträgern ausdrücklich auch den Einsatz von veränderbaren Speichermedien. Allerdings muss im letzteren Fall durch zusätzliche technische Massnahmen sichergestellt werden, dass die Integrität der gespeicherten Daten erhalten bleibt. Als Beispiel für eine solche technische Massnahme nennt die GeBüV die elektronische Signatur. Es besteht aber kein gesetzlicher Zwang zu deren Einsatz. Es muss auch nicht die gemäss Art. 14 Abs. 2bis OR der Handunterschrift gleichgestellte qualifizierte elektronische Signatur verwendet werden, welche mit einem Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten verifiziert werden kann. Es steht einem Unternehmen somit frei, bei Verwendung von veränderbaren Speichermedien die technische Massnahme zur Integritätssicherung selbst zu wählen – solange sie ebenso sicher ist wie die elektronische Signatur.

Beim Einsatz der elektronischen Signatur in der Langzeitarchivierung sind einige zusätzliche Aspekte mitzuberücksichtigen, um die Beweiskraft der Dokumente zu erhalten. Eines der Probleme liegt darin begründet, dass die verwendeten kryptografischen Algorithmen nach einiger Zeit ihre Sicherheitseignung verlieren. Um die Integrität des Dokuments zu erhalten, muss die Signatur vor diesem Zeitpunkt erneuert werden. Zudem müssen die Komponenten zur Verifizierung und Visualisierung der elektronischen Signatur während des gesamten Aufbewahrungszeitraumes zur Verfügung stehen.

Werden veränderbare Speichermedien zur Archivierung verwendet, muss der Zeitpunkt der Speicherung nachgewiesen werden können. Hier sind neben dem Einsatz von Zeitstempeldiensten auch andere Massnahmen wie z.B. Protokollierungen zulässig, um diese Vorgabe zu erfüllen.

## Die Verfügbarkeit der Daten

Archivierte Dokumente müssen während der gesamten Aufbewahrungsdauer innerhalb einer angemessenen Frist verfügbar sein und sie müssen auf Verlangen einer Behörde auch in Papierform vorgelegt werden können. Die Verfügbarkeit impliziert nicht nur, dass die Daten gefunden werden, sondern auch, dass diese gelesen und verstanden werden können. Um diesen Vorgaben zu genügen, müssen Daten regelmässig auf ihre Lesbarkeit überprüft werden. Migrationskonzepte sowie die Dokumentation des Systems und der Abläufe stellen sicher, dass die Verfügbarkeit der Daten gegeben ist.

Die Forderung, dass die nötigen Hilfsmittel für die Einsicht und Prüfung während der gesamten Aufbewahrungsdauer zur Verfügung zu halten sind, impliziert die Vermutung, dass damit eine gesetzliche Pflicht zur Archivierung von Software begründet wurde. Das kann jedoch grundsätzlich verneint werden, solange mit Standardprogrammen gearbeitet wird. Entscheidet sich ein Unternehmen allerdings für den Einsatz hochspezialisierter Individuallösungen, dann kann die Verfügbarkeit unter Umständen tatsächlich nur durch die Aufbewahrung des verwendeten Programms sichergestellt werden. In diesem Fall sollte man sich wegen der grossen Abhängigkeit vom Anbieter der Archivierungslösung auch durch den Abschluss eines Escrow Agreements davor sichern, dass z.B. bei Konkurs des Anbieters das System nicht mehr gewartet und weiter entwickelt wird. Schliesslich ist die Verfügbarkeit der Daten auch durch regelmässige Sicherung der archivierten Daten sicherzustellen.

Art. 7 der GeBüV verlangt zudem, dass die archivierten Daten von den aktuellen Daten getrennt werden. Die Verantwortung für die archivierten Daten soll auf diese Weise genau festgelegt werden können. Zugriffe auf archivierte Daten sollen nur bestimmten Personen zu vordefinierten Zwecken vorbehalten bleiben und müssen aufgezeichnet werden. Auch aus datenschutzrechtlicher Sicht ist eine Trennung des Archivs von den aktuellen Daten wünschenswert.

Diesen gesetzlichen Anforderungen wird nicht nur durch eine physische Trennung Genüge getan. Die archivierten Daten können von den aktiven Daten auch getrennt werden, indem durch die Vergabe spezieller Zugriffsrechte ein „logisches Archiv“ geschaffen wird.

## Datenschutz und Archivierung – ein Widerspruch?

Vereinzelt wird die Auffassung vertreten, dass eine Persönlichkeitsverletzung gar nicht mehr möglich sei, wenn Daten bereits archiviert sind. Datenschutzrechtliche Aspekte

| ***Checkliste betreffend die Anforderungen an ein Archivsystem*** | |
|---|---|
| 1. Verwendung von standardisierten Datenformaten | Erleichtert die Migration von Daten.<br>Erhöht die Aussicht, dass die technischen Komponenten zur Visualisierung während des gesamten Aufbewahrungszeitraumes verfügbar sind.<br>Der Anwender ist dadurch weniger von einem Anbieter abhängig, was bei einer derart weitreichenden und langfristigen Investitionsentscheidung ausschlaggebend sein kann. |
| 2. Integrität | Das angewandte technische Verfahren muss sicherstellen, dass die Daten so aufbewahrt werden, dass nachträgliche Änderungen feststellbar sind.<br>Zulässig sind Signaturverfahren aber auch andere vergleichbare Verfahren. |
| 3. Unterstützung der Dokumentationspflichten | Die gesetzeskonforme elektronische Archivierung ist nur unter Einhaltung zahlreicher Dokumentationspflichten möglich. Das System sollte den Kunden bei der Erfüllung dieser Dokumentationspflichten durch die Integration entsprechender Tools unterstützen. |
| 4. Trennung zwischen Archivdaten und aktuellen Daten | Diese Trennung ist im Gesetz ausdrücklich vorgesehen und eine grundlegende Voraussetzung für die Regelung der Zuständigkeiten für archivierte Daten. |
| 5. Ausdruck in Papierform | Gerichte und Behörden können verlangen, dass die Dokumente in Papierform vorgelegt werden |
| 6. Berücksichtigung der datenschutzrechtlichen Anforderungen | Das Auskunftsrecht des Betroffenen muss gewährleistet werden.<br>Die Löschung und/oder Berichtigung einzelner Dokumente muss möglich sein, ohne dass die Beweiskraft der übrigen Dokumente schwindet. |
| 7. Sicherstellung der Wartung und Weiterentwicklung | Das Vertrauen in die Langlebigkeit des Systems und somit mittelbar auch in das langfristige Bestehen des Anbieters wird bei derart langfristigen Entscheidungen häufig eine ausschlaggebende Bedeutung haben. |

müssten somit nicht mehr berücksichtigt werden. Vertreter dieser Meinung verkennen, dass die datenschutzrechtlichen Grundsätze bei jeder Bearbeitung von Personendaten einzuhalten sind. Auch die Archivierung ist eine Bearbeitung von Daten im Sinn des Datenschutzgesetzes.

Grundsätzlich müssen datenschutzrechtliche Überlegungen aber bereits in die Erstellung der Weisung über die aufzubewahrenden Dokumente einfliessen. Nach den Grundsätzen der Verhältnismässigkeit und der Zweckmässigkeit dürfen nur die Daten archiviert werden, welche man unbedingt benötigt. Die anderen Personendaten sind zu löschen. Zudem muss das Archivsystem sicherstellen, dass das Unternehmen seiner Auskunftspflicht nach Datenschutzgesetz stets nachkommen kann. Eine Verletzung dieser Auskunftspflicht ist nach Art. 34 DSG mit Strafe bedroht. Die Archivierung von e-Mails stellt eine besondere datenschutzrechtliche Herausforderung für ein Unternehmen dar, welches alle e-Mails automatisch archivieren will. Um rechtskonform vorzugehen, sollte die private Nutzung unternehmensintern klar geregelt werden. Ist diese untersagt, dann gelten alle e-Mails als Geschäftskorrespondenz und dürfen auch archiviert werden. Dürfen die Mitarbeitenden auch privat mailen, dann ist eine automatische Archivierung aller e-Mails nur mit Zustimmung der Mitarbeitenden zulässig.

## Die Evaluation der geeigneten technischen Lösung

Unternehmen, welche einen Wechsel vom Papierarchiv auf die elektronische Variante planen, sollten bei der Suche nach der für sie geeigneten technischen Lösung die folgenden Empfehlungen berücksichtigen. Da die meisten Unternehmen dabei auf bereits vorhandenen Systemen aufbauen, können die Anforderungen allerdings von Projekt zu Projekt sehr unterschiedlich sein. Zudem sind die gesetzlichen Vorgaben sehr offen formuliert und ermöglichen, mit unterschiedlichen technischen Lösungen rechtskonform zu archivieren.

Die vorstehende Checkliste ist deshalb nur als Überblick zu verstehen und erhebt keinen Anspruch auf Vollständigkeit.

***Mag.iur. Maria Winkler***
***IT & Law Consulting GmbH***
***Zug***

## Résumé

Le passage d'un archivage papier à un archivage électronique est un projet qui doit être conduit par la ligne et non par l'informatique. La direction de l'entreprise doit fixer des objectifs clairs à un tel projet, en tenant en compte de la situation juridique (qui varie selon les branches) et en établissant les risques admissibles pour l'entreprise.

Les directives qui découleront de ce projet ne devront plus faire de distinction entre la correspondance papier et les mails. Elles devront en revanche maintenir une protection accrue des données personnelles archivées, ce qui peut poser certains problèmes dans le domaine des mails.

Le respect des exigences de l'Olico (RS 221.431) implique la mise en place de processus complexes, notamment pour le renouvellement périodique des mécanismes de chiffrage assurant la protection des données archivées.

# e-Mail

## Internet dans l'entreprise: mode d'emploi

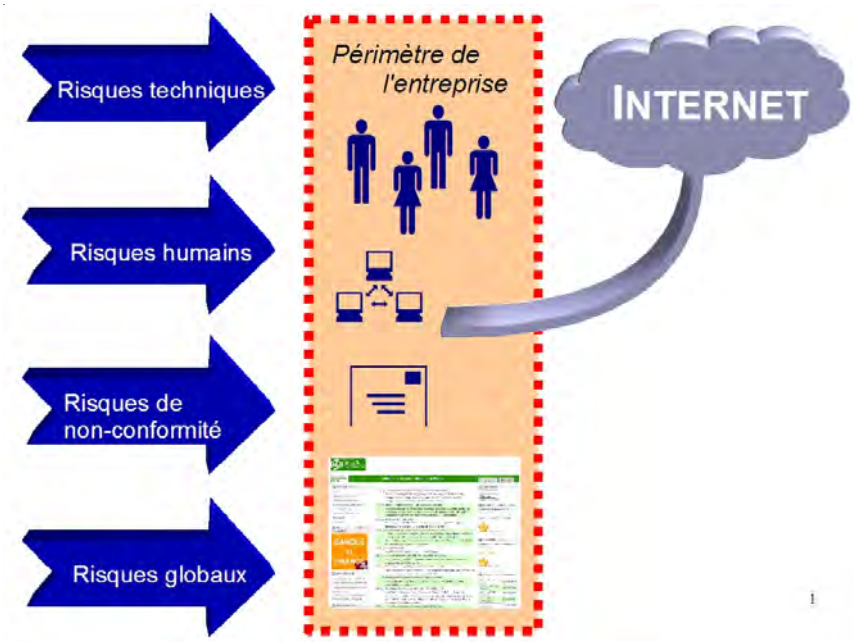
Dans quelles limites puis-je utiliser Internet et la messagerie électronique dans mon entreprise? Quelles données de ma messagerie électronique ou de ma session de surf mon employeur peut-il surveiller? Quelles sanctions peuvent m'être adressées lors d'une utilisation inadéquate de l'accès à Internet ou du courriel? ... Pouvoir répondre à de telles questions, c'est confirmer que des mesures de protection ont été établies, mises en place et communiquées dans l'entreprise.

Internet dans l'entreprise est un outil mis à disposition de l'employé par l'employeur. Il lui permet d'accéder à une base mondiale de connaissance et de bénéficier d'une plateforme de communication et d'échange d'informations. Mais cette interconnexion d'Internet au réseau de l'entreprise impose à chacun une prise de conscience face aux risques qui en découlent.

Pour la gestion et le contrôle de ces risques, la prévention doit prévaloir. Il s'agit donc, en particulier, d'assurer une surveillance proactive adaptée à l'utilisation d'Internet dans la société et ceci tout en respectant les données personnelles lors de l'observation des traces de surf et de messagerie.

### Une surveillance adaptée à la menace et en conformité avec les contraintes juridiques.

A la suite d'une motion parlementaire en 1984, le Conseil Fédéral a émis une ordonnance qui interdit la surveillance ciblée du comportement sur le lieu de travail. Le but découle d'une volonté de préserver la santé et la personnalité des employés lors de l'utilisation d'un système de surveillance.



En déclinant cette règle dans le cadre de l'utilisation d'Internet et de la messagerie électronique sur le lieu de travail, cela signifie qu'il n'est pas légal pour l'employeur d'effectuer une surveillance automatique d'un collaborateur de manière permanente. Il lui est possible, par contre, d'opérer une surveillance anonyme de manière continue et par sondage sur la base d'acronymes afin de s'assurer d'une utilisation conforme et licite d'Internet.

Une analyse nominative ne peut être réalisée par l'employeur que s'il a préalablement informé ses collaborateurs, constaté un abus ou soupçonné qu'un tel acte ait été commis.

En cas d'incident des installations techniques, l'employeur peut investiguer afin de déterminer l'origine du problème, comme par exemple une tentative d'intrusion, une infection par un virus ou un cheval de Troie. L'analyse des fichiers d'information liés à la connexion vers Internet pourra alors être effectuée afin de rechercher la cause de la panne, et éventuellement d'identifier un cas d'abus de la messagerie ou accasionné lors d'une session de surf.

En cas de soupçon d'abus, une analyse nominative peut alors être effectuée. S'il découle d'une erreur de détection, l'analyse des traces électroniques des activités Internet du collaborateur sera aussitôt interrompue. Si l'abus est avéré, l'employé encontrera des mesures disciplinaires telles que prévues dans le règlement d'utilisation d'Internet.

Reproduction autorisée du Préposé fédéral à la protection des données: « Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail ».

## Un courrier privé doit être remis à son destinataire sans être ouvert

A l'instar du courrier papier, la messagerie électronique privée bénéficie d'une protection totale. Un courrier privé doit être remis à son destinataire sans être ouvert ni traité (sauvegarde, transmission, ...). La difficulté essentielle provient de la capacité d'identifier la nature privée du message. Deux critères peuvent principalement permettre d'identifier des messages de cette nature: 1) la mention « privé » ou « en main propre »; 2) le type d'envoi: journal, magazine, caractéristiques graphiques (couleur, format, cartes postales électroniques,..). Par conséquent, il n'est pas possible d'associer du courrier professionnel uniquement à l'adresse nominative du type ***prénom.nom@entreprise.ch***. Pour une adresse de ce type, l'employeur peut, en cas d'absence du collaborateur, partir du principe qu'il s'agit d'un message professionnel si aucune mention ne spéficie explicitement le caractère privé de celui-ci. L'utilisation d'une adresse email liée à la fonction telle que ***marketing@entreprise.ch*** ou ***directeur.vente@entreprise.ch*** par exemple ou l'utilisation d'une adresse email personnelle accessible via le web (webmail) sont deux variantes qui peuvent permettre de dissocier plus efficacement le courrier professionnel du privé.

La surveillance de la messagerie électronique suit le même principe que pour le surf sur Internet, mais il est nécessaire de préciser que l'employeur ne peut lire un message privé qu'avec l'autorisation d'un juge dans le cadre d'une poursuite juridique.

## Une communication claire et formalisée grâce à une directive d'utilisation d'Internet

La directive ou le règlement d'utilisation d'Internet et de la messagerie électronique est une base de communication et de sensibilisation qui ne peut être négligée par l'employeur. Habituellement transmis par le biais du contrat de travail ou d'un avenant tel que le règlement du personnel par exemple, ce document réduit en effet les éventuelles mécompréhensions liées à l'utilisation autorisée des outils Internet dans le cadre de l'entreprise. Il précise en outre, pour l'employeur, les modalités de surveillance afin de respecter les conditions légales principalement liées à la protection des données personnelles.

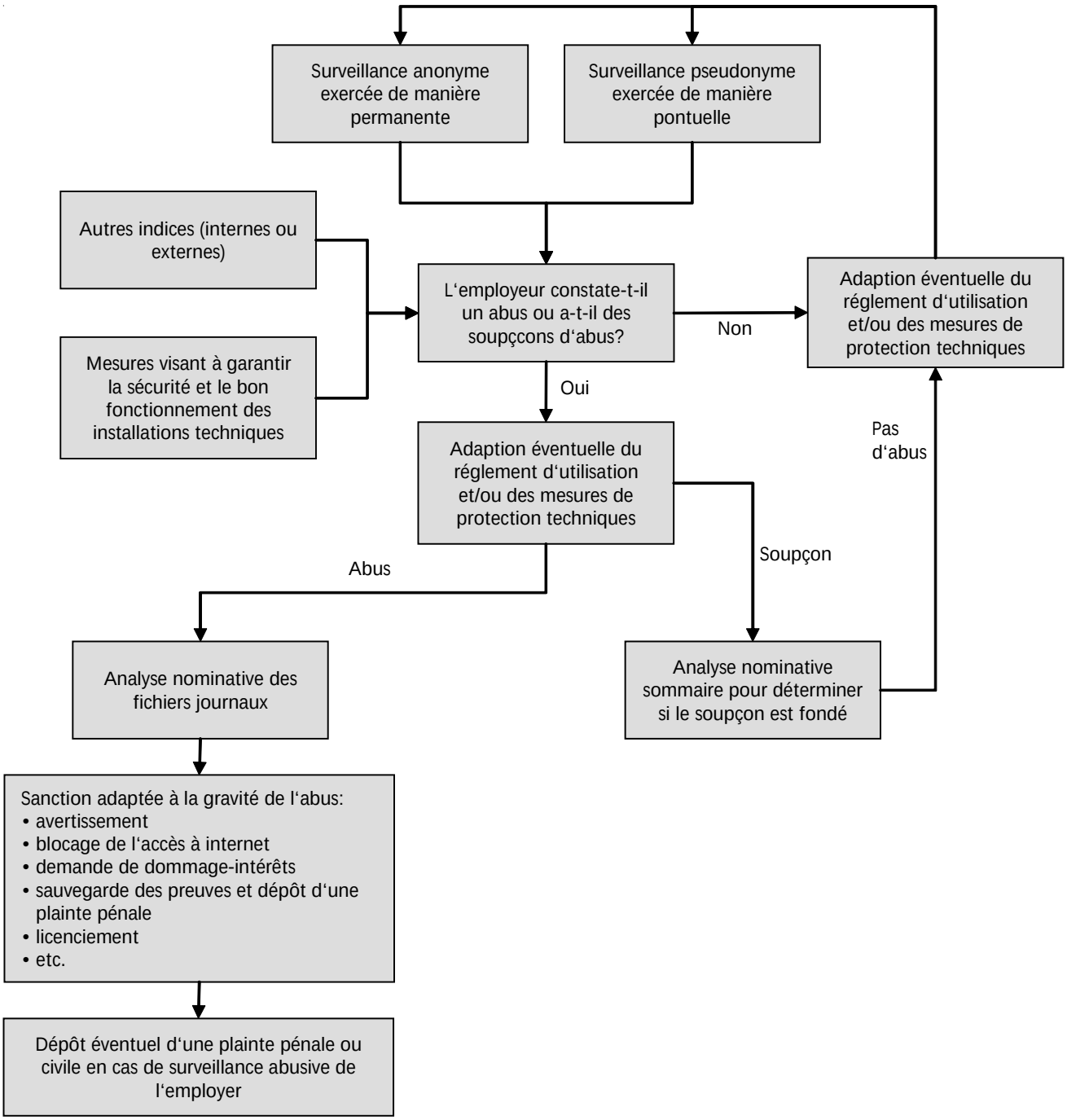
## Une seule réponse: la prévention.

En conclusion, la mise à disposition d'Internet dans l'entreprise doit être soumise à un principe de précaution afin de s'assurer que ses objectifs de développements stratégiques soient atteints. Employeur et employé ont alors des droits et des devoirs qu'ils ne peuvent ignorer et évitant des comportements inadaptés et risqués. Pour l'ensemble de ces cas, une seule réponse existe: la prévention.

***Marc Barbezat***
***b3b, La Tour-de-Peilz/VD***

***Membre du comité de l'ISACA pour la Suisse romande***

Référence utile:
Le site du préposé fédéral à la protection des données est incontournable:
http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html?lang=fr .




Vous y trouverez un document de référence pour approcher de manière adéquate cette problématique: « Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail »

## But et champ d'application

- *objectifs du règlement*
- *domaines applicables et limitations:*
  - *employés internes et externes*
  - *consultants, prestataires externes*
  - *...*
- *...*

## Présentation du contexte

- *Menaces et risques*
  - *codes malveillants: virus, cheval de Troie, vers, ...*
  - *installation « non officielle » de logiciels*
  - *...*
- *Les conséquences / impacts dûs à l'utilisation d'Internet*
  - *réputation, image*
  - *secret de fabrication ou commercial*
  - *...*
- *Outils mis à disposition*
- *...*

## Mesures de protection mise en oeuvre

- *Description des moyens de protection et prévention mis en oeuvre*
- *Structure de l'architecture de connexion (limite de périmètre: réseau interne, prestataire externe, Internet,...)*
- *Solution de cryptage*
- *Principe d'exploitation et de maintenance:*
  - *sauvegarde des messages*
  - *capacité de stockage*
  - *...*
- *Type de journalisations réalisée et objectifs relatifs*
- *...*

## Règlement d'utilisation

- Comportement attendu de l'employé
- Limite d'utilisation des outils Internet à des fins privées
- ...

## Règlement de surveillance

- Nature et fréquence de la surveillance anonyme et pseudonyme
- Description de la surveillance de l'infrastructure technique réalisée
- Organisation: nom de la ou des personnes chargées d'analyser de manière nominative les informations enregistrées
- ...

## Sanctions

- Conditions
- Liste des sanctions disciplinaires et modalités d'application
- ...

ISACA Serving IT Governance Professionals
Switzerland Chapter

# e-Mail

## Internet in der Unternehmung: Eine Gebrauchsanweisung

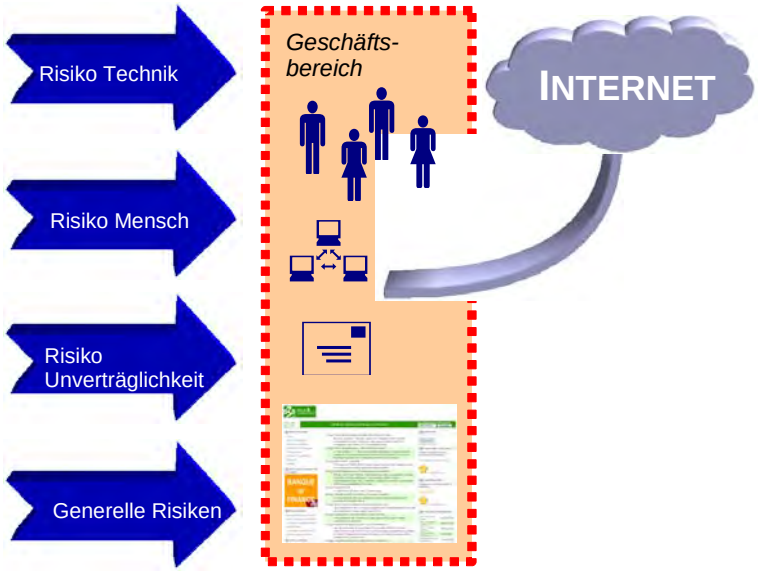
Mit welchen Beschränkungen darf ich Internet und die e-Mail-Möglichkeiten meines Arbeitgebers nützen? Welche meiner Internet- und e-Mail-Mitteilungsdaten darf mein Arbeitgeber einsehen? Mit welchen Konsequenzen muss ich rechnen, wenn ich die diesbezüglich gesetztenen Schranken überschreite? Der folgende Artikel tritt auf diese und ähnliche Fragen ein.

Internet in der Unternehmung ist ein Hilfsmittel, das heute viele Unternehmen ihren Mitarbeitern zur Verfügung stellen. Der Mitarbeiter kann damit von einer internationalen Informationsplattform und den Vorteilen der elektronischen Kommunikation profitieren. Allerdings ist die Anbindung des Internets an ein Unternehmensnetzwerk mit gewissen Risiken verbunden, die es zu beherrschen gilt.

Für die Identifikation und die Kontrolle dieser Risiken muss die Prävention vorherrschen. Es handelt sich demnach um eine proaktive Einstellung und Überwachung gegenüber dem Problem des Surfens und der Benützung der elektronischen Kommunikation. Dabei müssen allerdings die Bestimmungen des Datenschutzes hinreichend beachtet werden.

### Eine der Bedrohung angemessene Überwachung bei gleichzeitigem Einhalten der Rechtsgrundsätze.

In der Folge einer parlamentarischen Motion erliess der Bundesrat 1984 eine Verordnung, welche die stetige Überwachung des Personals am Arbeitsplatz verbot. Der Sinn war und ist, dem Gedanken des Persönlichkeitsschutzes Nachhaltung zu verschaffen. Eine dauernde Überwachung könnte die körperliche und geistige Gesundheit der Angestellten beeinträchtigen.




Umgesetzt auf die Thematik des Internet und des elektronischen Datenverkehrs heisst dies, dass es einem Arbeitgeber nicht gestattet ist, die entsprechenden Handlungen der Angestellten automatisch und dauernd zu überwachen und analysieren. Es ist ihm dagegen gestattet, in anonymer Weise von dem entsprechenden Verkehr Kenntnis zu nehmen oder bei begründetem Verdacht eines Missbrauchs eine direkte Überwachung anzuordnen.

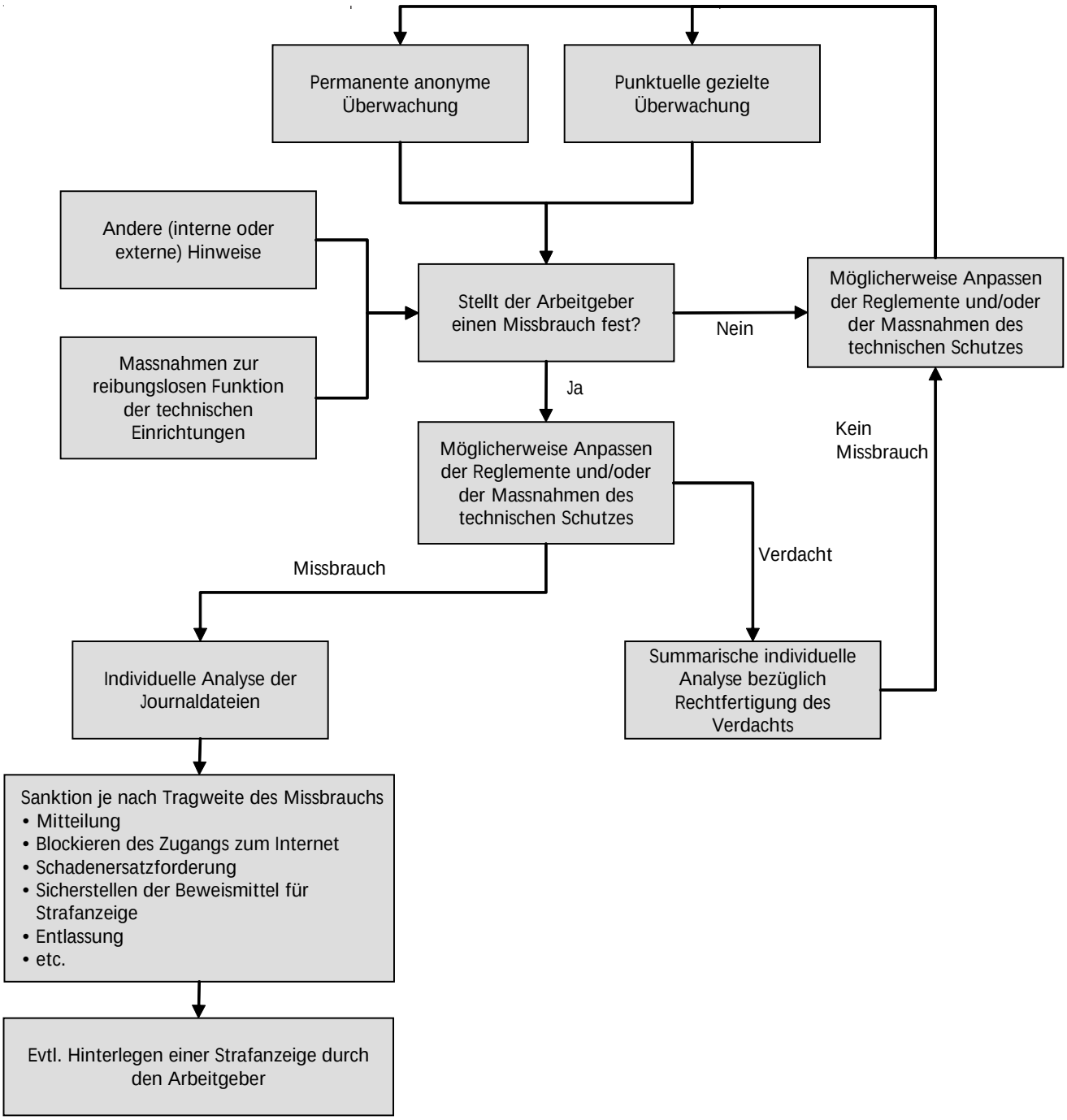
Eine individuelle Analyse kann nur stattfinden, wenn der Arbeitgeber die Angestellten vorher über eine allfällige Überwachung informiert hat, dass dies im Falle eines Verdachts auf Missbrauch erfolgen kann.

Bei ausserordentlichen Vorkommnissen, wie Hacking-Attacken, Virusinfektionen des Netzwerkes, Eindringen von Trojanischen Pferden, etc. hat der Arbeitgeber das Recht, Internetbenützungen und e-Mails von Angestellten zu untersuchen, um die Ursache des Angriffs zu eruieren.

Bei Verdacht des Missbrauchs kann auch eine personengerichtete Überwachung vorgenommen werden. Wird der Verdacht bestätigt, muss der Angestellte mit Sanktionen rechnen, wie sie in einem entsprechenden Reglement bezüglich Internetbenützung und elektronischer Kommunikation festgehalten sein sollten. Bei Nichtbestätigung des Verdachts sind die entsprechenden Daten zu löschen.

### Eine private Meldung muss an den Adressaten ungeöffnet weitergegeben werden

Das Postgeheimnis gilt analog dem schriftlichen Briefverkehr absolut auch im elektronischen Austausch von Mitteilungen. Eine private Mitteilung


Permanente anonyme Überwachung
Punktuelle gezielte Überwachung
Andere (interne oder externe) Hinweise
Massnahmen zur reibungslosen Funktion der technischen Einrichtungen
Stellt der Arbeitgeber einen Missbrauch fest?
Nein
Möglicherweise Anpassen der Reglemente und/oder der Massnahmen des technischen Schutzes
Ja
Kein Missbrauch
Möglicherweise Anpassen der Reglemente und/oder der Massnahmen des technischen Schutzes
Verdacht
Missbrauch
Individuelle Analyse der Journaldateien
Summarische individuelle Analyse bezüglich Rechtfertigung des Verdachts
Sanktion je nach Tragweite des Missbrauchs
• Mitteilung
• Blockieren des Zugangs zum Internet
• Schadenersatzforderung
• Sicherstellen der Beweismittel für Strafanzeige
• Entlassung
• etc.
Evtl. Hinterlegen einer Strafanzeige durch den Arbeitgeber

## Ziel und Umfang der Anwendung

- *Ziel des Reglementes*
- *Gültiger Bereich und Grenzen:*
  - *Interne und externe Angestellte*
  - *Berater, temporäre Angestellte, etc.*
  - *...*
- *...*

## Darstellung der Zusammenhänge

- *Gefahren und Risiken*
  - *Destruktive Programme wie Viren, Trojanische Pferde, etc.*
  - *Verbotene Installation von Software*
  - *...*
- *Auswirkungen der Internetbenützung*
  - *Image, Ruf der Firma*
  - *Fabrikations- und Berufsgeheimnisse*
  - *...*
- *Bereitgestellte Hilfsmittel*
- *...*

## Eingesetzte Schutzprogramme

- *Beschreibung der Schutzprogramme*
- *Architektur und Grenzen (internes Netzwerk, externe Berater, Internet…)*
- *Chiffrierungen*
- *Grundsätze des Betriebs und des Unterhalts*
  - *Sicherung der Meldungen*
  - *Speicherkapazität*
  - *...*
- *Journalisierung und deren Ziele*
- *...*

## Betriebsreglement

- Erwartetes Verhalten der Angestellten
- Grenzen der privaten Benützung
- ...

## Überwachnungsreglement

- Art und Häufigkeit der anonymen und persönlichen Überwachung
- Beschreibung der technisch realisierten Überwachung
- Organisation: Namen der zur Einsicht und Analyse Berechtigten
- ...

## Sanktionen

- Bedingungen
- Liste der Disziplinarmassnahmen und deren Anwendung
- ...

an einen Adressaten muss diesem ungeöffnet und ohne Verarbeitung (während der Übermittlung und Speicherung, etc.) übergeben werden. Unklar sind allerdings die Sachlage bei Routinehandlungen, wie Übermittlung und Datensicherung. Die hauptsächliche Schwierigkeit bezüglich des elektronischen Datenverkehrs liegt hier bei der Identifizierung einer persönlichen Mitteilung. Schlagwörter wie « privat » oder « vertraulich » etc. könnten zwar hilfreich sein, werden aber selten verwendet. Auch Formate und Bilderanhänge könnten einen Hinweis geben, sind aber nicht eindeutig. Es ist demnach unmöglich, eine Mitteilung als geschäftlich zu identifizieren nur weil eine Adresse des Typus' ***Vorname.Name@Unternehmung.ch*** verwendet wird. In diesem Fall darf der Arbeitgeber davon ausgehen, dass eine entsprechend adressierte ankommende Meldung für einen Angestellten geschäftlicher Natur ist. Es sei denn, es werde ausdrücklich auf die private Natur der Meldung hingewiesen. An die Funktion gebundene Adresstypen wie z.B. ***marketing@Unternehmung.ch*** oder ***Verkaufsdirektor@Unternehmung.ch*** oder das Verwenden einer persönlichen e-Mail-Adresse via Web (Webmail) sind zwei Varianten, um den Schwierigkeit der Identifizierung von privaten Meldungen zu begegnen.

Grundsätzlich sind Internet und e-Mail an die gleichen Überwachnungsprinzipien wie das Postgeheimnis gebunden. Es ist zu präzisieren, dass ein Arbeitgeber die private e-Mail eines Angestellten nur mit der Bewilligung bzw. Anordnung eines Richters im Rahmen einer Strafverfolgung vornehmen darf.

## Eine Weisung zur Benützung des Internet und der elektronischen Kommunikation schafft Klarheit

Eine Weisung oder ein Reglement zur Benützung des Internet und der elektronischen Post ist die Basis zur Sensibilisierung der Angestellten bezüglich der Risiken auf diesem Gebiet. Es sollte Teil des Arbeitsvertrags sein, der vom Arbeitgeber nicht vernachlässigt werden darf. Die Folgen einer Nichtbeachtung der Bestimmungen sind ebenso unmissverständlich herauszustreichen wie die Bedingungen, unter welchen die Mittel verwendet werden dürfen. Damit schafft sich der Arbeitgeber auch die rechtlich einwandfreien Grundlagen, damit er bei gegebener Notwendigkeit Einsicht in die Tätigkeit des Angestellten nehmen kann. Damit sind auch die Anforderungen des Datenschutzes respektiert.

## Einzige Antwort: Prävention

Zusammenfassend ist festzuhalten, dass die Benützung von Internet und elektronischer Kommunikation im Geschäftsleben dem Prinzip der Vorsicht unterliegen muss. Um Risiken richtig einzuschätzen, Gefahren vorzubeugen und strategische Geschäftsziele zu erreichen, müssen sowohl Arbeitgeber als auch Arbeitnehmer über ihre Rechte und Pflichten informiert sein. Ein nachträgliches Eingreifen erfolgt zu spät, weshalb nur die Prävention von Missbräuchen und Fehlern die richtige Antwort sein kann.

***Marc Barbezat,***
***b3b, La Tour-de-Peilz/VD***

Übersetzung durch die Redaktion

ISACA
Serving IT Governance Professionals
Switzerland Chapter

# e-Mail

## Konvergenz und Sicherheit im e-Mail Management

Verschiedene Technologien, Netze, Medien und Anwendungen wachsen zusammen. Eine Fotokamera, mit der man telefonieren und seine e-Mails lesen kann, ist heutzutage ein globales Hilfsmittel. Realisiert werden konnte das alles erst durch die Digitalisierung. Sie hat es ermöglicht, dass Daten, Fax, Musik und Videos sowohl über das Fest-, WLAN- oder Mobilfunknetz als auch über Satelliten transportiert werden können.

Konvergenz kommt vom lateinischen convergere (sich hinneigen) und bedeutet Annäherung. In der Kommunikation meint man damit, dass sich Angebote, wie Geräte, Netze und Dienste (Internet, mobile e-Mail etc.) einander annähern und miteinander verschmelzen. Konvergenz kommt heute auf allen Ebenen vor.

Mobilität ist heute selbstverständlich. Jeder ist überall erreichbar und kann jederzeit selbst von überall ein e-Mail senden und empfangen. Smartphone, Personal Digital Assistant (PDA) und Notebook haben längst auch dicke Terminkalender und Adressbücher ersetzt. Die Geräte machen e-Mail und Internet mobil. Zunehmend gibt es auch Business-Software, die man von unterwegs, also mobil, nutzen kann.

Wie aber steht es mit der Konvergenz hinsichtlich rechtlicher Anforderungen, Datenschutz und Sicherheit? Nach wie vor hinken diese Aspekte der Technik hinterher.

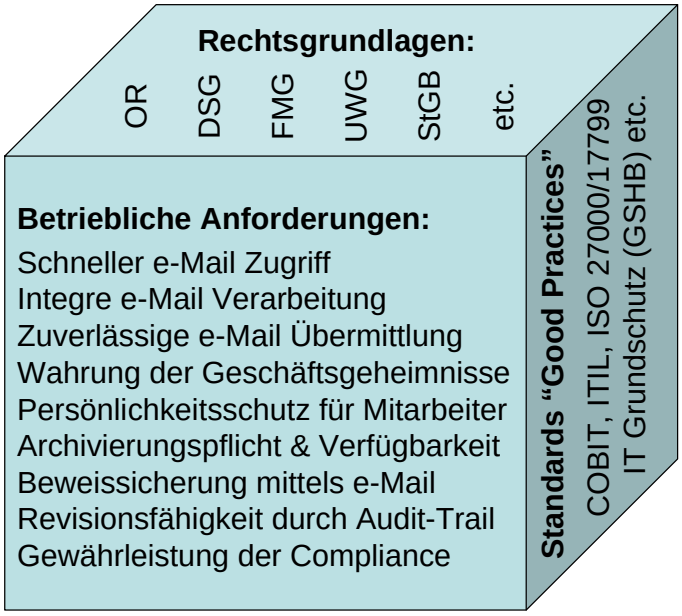
Ein Geschäftsmann möchte kein Fachmann für Kommunikation, Sicherheit und Kontrolle werden. Er möchte nur seine e-Mails lesen und beantworten können sowie alle seine Geschäftsdaten aktuell, richtig, vollständig und aufbewahrt zur Verfügung haben. Ihn interessieren auch die technischen Probleme nicht, die auftauchen, falls eine Verbindung mitten in der Übertragung zusammenbricht. Für den Kunden darf es kein Unterschied sein, ob der Geschäftspartner im Büro, unterwegs (auch in den Ferien) oder zu Hause arbeitet.

Die technischen Notwendigkeiten bei der sicheren Übertragung, Speicherung und Archivierung wichtiger Daten sind komplex und können nicht von jedem Geschäftsmann beherrscht werden. Die Anforderung, dass sensible Daten nur verschlüsselt transportiert, systematisch und sicher aufbewahrt werden, setzt hohe Kompetenz voraus. Das ist eine Herausforderung einerseits für die Anbieter von Telekommunikations- und Sicherheitslösungen und anderseits für die Professionals in den Bereichen Informatik-Recht und -Audit. Spezialisten sind sich einig, dass verschlüsselte und digital signierte e-Mails künftig vor Gericht eine wichtige Rolle spielen werden.

Je nach Unternehmensgrösse und Branche sind die nachstehenden Inhalte (Würfel) betrieblicher und rechtlicher Bedingungen dem e-Mail Management anzupassen. Dementsprechend sind adäquate Praktiken, Kontrollziele und Massnahmen darauf auszurichten. Die „Good Practices"-Standards sind sowohl für die Umsetzung als auch für die Überwachung (Monitoring) und die Prüfung (Audit) des e-Mail Managements hilfreich.

Integrierte e-Mail-Schutz- und -Aufbewahrungs-Lösungen sind teilweise noch in der Entwicklungsphase. Separate Dienstleistungspakete u.a. für Cleanmails, Filterfunktionen gegen Spam-, Phishing- und Viren-Attacken sowie Mechanismen für den sicheren e-Mail-Verkehr (Verschlüsselung,

e-Mail Management



Signatur, Zertifikat) stehen von Hard- und Softwareherstellern sowie von IT-Sicherheitsfirmen zur Verfügung. Zur Gewährleistung der Kompatibilität der verschiedenen Produkte müssen allerdings noch einige Anstrengungen unternommen werden.

Obwohl technische Möglichkeiten für die e-Mail-Archivierung vorhanden sind, fehlen meist die organisatorischen Regelungen und Klassifizierungs-Richtlinien (u.a. für geschäftlich relevante e-Mails gemäss Obligationenrecht mit einer Aufbewahrungspflicht von 10 Jahren). Oft sind auch Verantwortung und Kompetenzen für die Aufbewahrung von Geschäftsdokumenten und e-Mails unklar. Deutlich wird das insbesondere dann, wenn geschäftsrelevante Dokumente bei Rechtsstreitigkeiten innert angemessener Frist herangezogen werden müssen. Die elektronisch geführten und aufzubewahrenden Dokumente bzw. e-Mails haben nur dann Beweiskraft, wenn die Vorgaben der Geschäftsbücherverordnung (GeBüV, 2002) umgesetzt sind.

Eine Gartner Studie vom April 2005 kommt diesbezüglich zum Schluss, dass heute drei grundsätzlich unterschiedliche Vorgehensweisen der e-Mail-Speicherung und -Archivierung am häufigsten zum Einsatz gelangen:

1. Nichts speichern: Diese Variante steht allerdings im Widerspruch zu den meisten heute gültigen Vorschriften und ist daher nicht zu empfehlen.
2. Speichern von ausgewählten e-Mails: Wichtige Voraussetzung hierfür bildet die eindeutige Definition von verbindlichen Policies, bietet aber gleichzeitig die bestmögliche Kombination von Einhaltung gesetzlicher Vorschriften.
3. Alles speichern: Grundsätzlich ist man mit dieser Variante auf der sicheren Seite, aber die Nachteile liegen auf der Hand. Der Datenspeicher wächst ins Uferlose.

Nebst der Revisionssicherheit gilt es bei der Wahl des Archivsystems zu beachten, dass das Kosten-Nutzenverhältnis in vernünftiger Relation zur angestrebten Compliance steht.

Empfehlenswert ist daher eine Internet- und e-Mail-Policy, die nicht nur die erlaubte Nutzung regelt, sondern auch über die mit dem Internetgebrauch verbundenen Gefahren aufklärt. Denn oftmals sind sich die Benutzer über das Risikopotential und die vorhandenen e-Mail-Sicherheitsmechanismen nicht im Klaren. Hinweise über rechtliche Konsequenzen gibt auch der Leitfaden: Internet- und e-Mail-Überwachung am Arbeitsplatz (Version 2.0, 2003) des Eidgenössischen Datenschutzbeauftragten (EDSB).

Die Revision des Fernmeldegesetzes (FMG) verheisst den Mailboxen weniger unerwünschte Werbemails. Die meisten unerwünschten Massenmails, auch Spam genannt, stammen aber aus dem Ausland. Hier nützt das neue Gesetz wenig, solange keine internationalen Abkommen bestehen. Nach Ausarbeitung und Genehmigung der Verordnung vom Bundesamt für Kommunikation wird das FMG voraussichtlich 2007 in Kraft gesetzt. Im Gegensatz zur Schweiz besteht seit 2002 in der EU eine Datenschutzrichtlinie für elektronische Kommunikation, welche das Verbot unverlangter Werbemails regelt.

Laut Schätzungen des Marktforschungsinstitutes IDC werden im Jahr 2006 weltweit 83 Milliarden e-Mails verschickt. Davon sind 36 Mrd. Mails, die zwischen Personen ausgetauscht werden, 33 Mrd. Spam und 14 Mrd. automatische Benachrichtigungen. Eine Studie von SoftTrust bestätigt, dass rund jede dritte e-Mail für den Arbeitsalltag irrelevant ist! Um das e-Mail System nicht zu einer Informations-Schleuder verkommen zu lassen, ist der Umgang in Form eines e-Mail-Knigge im Rahmen einer e-Mail-Policy (siehe Hinweise) zu etablieren.

Wie intensiv mit den Möglichkeiten konvergenter Kommunikation und Sicherheit insgesamt umgegangen wird, variiert von Unternehmen zu Unternehmen. Das Ergebnis einer Studie von Arthur D. Little zeigt: Mitarbeiter von Unternehmen, die mobile Kommunikation intensiv nutzen, sind wesentlich flexibler. Gleichzeitig stieg die Zufriedenheit von Kunden und Mitarbeitern – und die Kosten sanken.

Generell setzt sich mehr und mehr beim Management durch: Wer auf die Effizienz professioneller Kommunikationslösungen künftig verzichtet, nimmt Wettbewerbsnachteile in Kauf. Das deckt sich auch mit den Erfahrungen der Mobilfunkanbieter in der Schweiz.

Daraus lässt sich ableiten, dass das e-Mail-Management für das Unternehmen bedeutend, von der Informatik-Revision als prioritäres Prüffeld zu betrachten und in die Jahresplanung einzubeziehen ist.

***Bruno Wiederkehr***
***ICT Consulting & Training***
***Erlenbach ZH***

Hinweise:
E-Mail Management Manual: Checkliste für eine E-Mail-Policy sowie deren Umsetzung unter www.mehrleisten.ch
Secure Mail: Sichere und diskrete Kommunikation mit dem Kundenberater unter www.credit-suisse.com/securemail
E-Mail und Recht: Empfehlenswerte Referatsnotizen und Präsentations-

folien gemäss Vortrag anlässlich ISACA GV 23.03.2006 unter www.isaca.ch/Downloads/AHS
E-Mail Audit Standards & Praktiken für sicheren E-Mail-Betrieb & -Unterhalt unter www.isaca.org
/IS Auditing Standards: z.B. G27 Mobile Computing, P2 Digital Signature
/K-Net: 10 Search Resultate, wie E-Mail-Policy, Security-Issues etc.
/Bookstore: Bücher, wie E-Mail Risk, Security, and Response etc.
/Journal: Schwerpunkt Thema Volume 4, 2006, Audit, Control and Security of Wireless Technologies.

# Outsourcing

## A quoi sert un rapport SAS 70 et comment l'interpréter?

Un thème qui parait très technique mais qui soulève des questions de principe passionnantes. Est-il possible pour un auditeur financier confronté à une situation d'outsourcing de ne se fier qu'à un rapport SAS 70 (***Statement on Auditing Standards No. 70, Service Organizations***) émanant de son confrère, auditeur du prestataire de service ?

Précisons-le d'emblée : la situation n'est pas fondamentalement différente qu'il s'agisse d'un rapport SAS 70 établit selon le standard de l'AICPA[1] ou d'un rapport correspondant à la NAS[2] 402. Le standard américain va certes plus dans les détails et constitue une plateforme très utile en pratique mais certaines questions de fond demeurent.

La première question est bien connue et tient au type de rapport. Comme la norme 402, le standard américain connaît un rapport de type I (correspondant à un rapport 402 de type A) qui se limite à une description et à une évaluation de la conception du système de contrôle interne, et un rapport de type II (402 B) qui va au-delà et contient une opinion sur l'efficacité opérationnelle des contrôles. ***Première recommandation : un rapport de type I devra être complété par des tests appropriés du système de contrôle interne pour pouvoir porter une opinion définitive sur le système de contrôle interne.***

La seconde question tient au périmètre couvert par les standards. Ils se concentrent en pratique aux contrôles généraux informatiques et ne couvrent pas automatiquement l'examen des contrôles applicatifs. Ils ne comprennent pas non plus l'examen du respect de certaines normes sectorielles, domaines bancaire ou pharmaceutique par exemple. ***Seconde recommandation : un rapport de type II doit être complété par des examens supplémentaires, en fonction de la branche d'activité du client – en particulier dans le domaine bancaire, voire également dans le domaine des contrôles applicatifs.***

La troisième question est temporelle. Tant la NAS 402 que le standard SAS 70 admettent qu'un rapport peut être délivré sur la base d'un examen ne portant que sur une période de 6 mois (de mars à septembre par exemple). La combinaison de cette norme avec l'exigence de la NAS 400 (chiffre 37) qui exige de l'auditeur de « ***déterminer si les contrôles internes ont été appliqués tout au long de la période*** » peut se révéler problématique. ***Troisième recommandation : un rapport de type II qui ne couvre pas tout l'exercice doit être complété par des examens supplémentaires, afin de déterminer si les contrôles internes ont été efficaces tout au long de la période.***

La quatrième question nous renvoie à l'éternel problème des interfaces. Difficile d'imaginer un outsourcing sans interface entre le client et le prestataire de service. Des données importantes doivent être transférées, parfois manuellement, mais dans la majorité des cas électroniquement. Les contrôles assurant la fiabilité de ces transferts impliquent aussi bien le prestataire de services que son client. L'audit de l'ensemble de ces

contrôles, qui sont implémentés dans les deux entreprises, n'est en pratique pas compris dans un rapport SAS 70. ***Quatrième recommandation : identifier les interfaces importantes entre le prestataire de service et son client et les auditer en collaboration avec l'auteur du rapport SAS 70.***

La cinquième (et provisoirement dernière) question concerne les relations entre les quatre acteurs de la constellation. Les deux auditeurs (l'auteur et le destinataire du rapport SAS 70) sont mandatés par leurs deux clients respectifs, qui ne souhaitent généralement pas que leurs auditeurs aient des relations directes. Le destinataire du rapport doit cependant s'assurer de l'indépendance et de la compétence de l'auteur du rapport. Il doit également avoir accès à une description détaillée des travaux effectués, afin de s'assurer que les contrôles importants selon sa propre analyse de risques ont tous été testés de manière appropriée. ***Cinquième recommandation : sans égard à l'avis de leurs clients respectifs, les deux auditeurs impliqués (l'auteur et le destinataire du rapport SAS 70) doivent entretenir des contacts directs réguliers[3].***

Ma conclusion personnelle, au terme du séminaire de la Chambre fiduciaire organisée en juin 2006 sur ce thème conjointement avec l'ISACA: Une standardisation des travaux d'audit peut concourir à une amélioration de la qualité. Le standard SAS 70 constitue à cet égard une base de discussion utile. Mais l'audit est une discipline complexe et il serait dangereux de croire – ou de faire croire à nos clients – qu'un rapport SAS 70 couvre de manière définitive et complète l'audit de l'outsourcing.

***Michel Huissoud, Jens/BE,***
***Vice-président ISACA Suisse***

Footnotes

[1] The American Institute of Certified Public Accountants

[2] Norme d'audit suisse

[3] Ce que prévoit expressément SAS 70 (chiffre 19) „If the user auditor believes that the service auditor's report may not be sufficient to meet his or her objectives, the user auditor may supplement his or her understanding of the service auditor's procedures and conclusions by discussing with the service auditor the scope and results of the service auditor's work.„

# CISM

## Neues CISM-Berufsbild – gültig für Prüfungen ab 2007

Im Normalfall etwa alle 4–5 Jahre wird das CISA-Berufsbild aktualisiert und an die veränderten Tätigkeiten des „typischen" CISA angepasst. Ich war daher sehr gespannt, ob wie erwartet auch das 2002 erstmals veröffentlichte CISM-Berufsbild in einem ähnlichen Rhythmus überarbeitet wird.

Da wir einen CISM-Vertiefungskurs anbieten, der bereits im Januar startet (mit einem Einführungs-Halbtag anfangs Dezember 2006), muss ich solche Veränderungen frühzeitig erfahren, um rechtzeitig alle notwendigen Anpassungen vornehmen zu können. Nach verschiedenen Mails mit ISACA hatte ich dann die klare Antwort: „Jawohl, auf 2007 erscheint das neue CISM-Berufsbild" und „Es gibt keine grösseren Änderungen gegenüber der alten Version".

Vor allem die zweite Information beruhigte mich – für die Anpassungen an das aktuelle CISA-Berufsbild (gültig für die Prüfung 2006) haben wir insgesamt fast 1000 Stunden aufgewendet: Für die Analyse der Veränderungen, die Planung und Durchführung des Umbaus des Kurses, die (neue) Zuordnung sämtlicher 1857 Multiple-Choice Fragen in unserer Datenbank zu den einzelnen „Task Statements" (den Aufgaben eines CISA), neue Auswertungen unserer Testprüfung und letztlich auch für die notwendigen zusätzlichen Unterrichtsinhalte.

Vor ein paar Tagen habe ich dann den Entwurf des CISM Candidates Guide erhalten – und war dann doch ein wenig schockiert. Zwar haben sich die fünf Areas des CISM nicht gross verändert:
Area 1: Governance der Informationssicherheit (23%)
Area 2: Informations-Risikomanagement (22%)
Area 3: Entwicklung des Programms für Informationssicherheit (17%)
Area 4: Management des Programms für Informationssicherheit (24%)
Area 5: Ereignis- und Reaktions-Management (14%)

Die Gewichtung der 5 Areas sowie ihre Titel wurden ganz leicht angepasst. Der Teufel steckt aber bekanntlich im Detail: Nur schon mengenmässig ist erkennbar, dass das neue CISM-Berufsbild wesentlich anders ist wie das alte. Anstelle der früher 36 Task Statements sind es nun deren 45 und anstelle der früher 74 Knowledge Statements immerhin neu deren 93. Bei genauerem Hinschauen habe ich dann noch festgestellt, dass es nicht einfach ein paar

zusätzliche Task- resp. Knowledge Statements gibt, sondern dass in einzelnen Areas diese praktisch vollständig ersetzt wurden.

## Was bedeutet das jetzt für uns alle?

***Für bereits zertifizierte CISM:***
Nichts; sie haben nach wie vor ihre laufende Weiterbildung zu beweisen. Das neue Berufsbild hat diesbezüglich keinen Einfluss.

***Für bereits geprüfte aber noch nicht zertifizierte CISM-Kandidaten:***
Voraussichtlich können sie ihre Berufserfahrung noch während einer gewissen Übergangsfrist nach dem alten CISM-Berufsbild belegen, wahrscheinlich ab Ende 2007 nur noch nach der neuen Aufteilung. Da aber die Areas im Prinzip unverändert erhalten blieben, dürfte das keine grossen Probleme bieten.

***Für zukünftige CISM-Anwärter (ab Prüfung 2007):***
Nichts; sie werden sowieso das neue CISM Review Manual verwenden und entsprechend nach dem neuen Candidates Guide lernen.

***Für andere CISM-Kursanbieter:***
Gemäss Aussagen von ISACA verfügt kein anderes Chapter auf der Welt über Kurse, wie wir sie bei uns in der Schweiz für CISA und CISM haben. In aller Regel bieten die ISACA Chapter einen 4–5 tägigen Kompaktkurs mit einer Foliensammlung von ISACA International an. Diese Foliensammlung wird von ISACA selbst aktualisiert werden.

***Für unseren CISM-Kurs in der Schweiz:***
Wenn wir unsere Erfolgsquote von 93% (Kurs 2006) auch nur annähernd beibehalten wollen, dürften grössere Anpassungen des Kurses zwingend sein. Wir werden also die neuen Task und Knowledge Statements wieder im Detail studieren, die Datenbank der Multiple-Choice Fragen anpassen und, und, und. Wir hoffen natürlich, dass wir 2007 eine entsprechend grosse Klasse führen werden, damit sich dieser riesige Aufwand auch einigermassen lohnt.

Wer sich selber ein Bild machen möchte: Auf der Einstiegsseite www.isaca.ch wird per Ende Oktober die „ISACA-Broschüre 06“ in einer aktualisierten Fassung vorliegen; dort drin ist das neue CISM-Berufbild mit allen Details in bewährter Manier zweispaltig Englisch und Deutsch gesetzt.

***Peter R. Bitterli, ITACS, Zürich***
***ISACA Switzerland Chapter***
***Ausbildungsverantwortlicher***

ISACA®
Serving IT Governance Professionals
Switzerland Chapter

www.isaca.ch

**Drei spannende Kurse**

**Risikoorientierte Jahresplanung der IT-Revision und Informationssicherheit**
1 Tag, ISACA-CH • 11. Dezember 2006 in Zürich

**Einführung in CobiT 4.0**
1 Tag, ISACA-CH • 12. Dezember 2006 in Zürich

**Introduction to CobiT 4.0**
1 Tag, ISACA-CH • 13. Dezember 2006 in Zürich

Weitere Informationen erhalten Sie in unserem Kurssekretariat:
**ISACA Switzerland Chapter**
c/o ITACS Training AG, Stampfenbachstr. 40
8006 Zürich, Schweiz, kurse@isaca.ch,
Tel. 044 444 11 01, Fax 044 444 11 02, www.isaca.ch

# Express Line

## A Word from the Chair

In the next few weeks, it will once again be renewal season at ISACA. All members will have the opportunity to easily renew their membership online by logging on to the ISACA web site.

As in previous years, all nonmembers who passed the December 2005 and June 2006 CISA or CISM examinations have been offered complimentary ISACA membership for the remainder of 2006.

***Steve Thorsted***
***Chair, Membership Board***

## December 2006 Exam

Registration for the 9 December 2006 CISA and CISM exams has now closed.

## Fraudulent Chinese Web Site

In May, a notice was posted regarding a web site (***www.cisaca.org***) originating out of China fraudulently claiming to be authorized by ISACA to register candidates for the CISA exam and to collect exam fees through its site. At that time, the site was inactivated; however, it has recently been reactivated. ISACA has also been informed that ***www.cisaca.com*** is a related site with similar claims.

Please be advised that neither of these web sites nor their owners are affiliated in any way with or endorsed by ISACA — nor have these web sites or their owners been authorized as registrars for the CISA exam or as distributors of any CISA study materials.

If there are any similar situations occurring in your geographic area, please contact the certification department at International Headquarters immediately. ters.

## Applications for Certification

Applications continue to arrive at International Headquarters. Processing can take eight weeks once the application is received.

Additionally, there are hundreds of exam passers from the 2001-2005 exams who have not submitted their applications. If they do not apply within five years of their exam date, their score is invalidated. Further application details are available at ***www.isaca.org/cisaapp*** or ***www.isaca.org/cismapp***.

## Assistance Sought in Identifying IP Violations

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

- IT Auditing: Irregular and Illegal Acts
- IT Auditing: An Adaptive Approach
- Profitable Sarbanes-Oxley Compliance
- Risk Management Approach to Business Continuity
- Winning as a CISO

Visit the ISACA web site at ***www.isaca.org/bookstore*** and take advantage of secure online ordering or see the ***Information Systems Control Journal®*** Bookstore insert for additional information.

## Italian Translation of CobiT Focus Newsletter Available

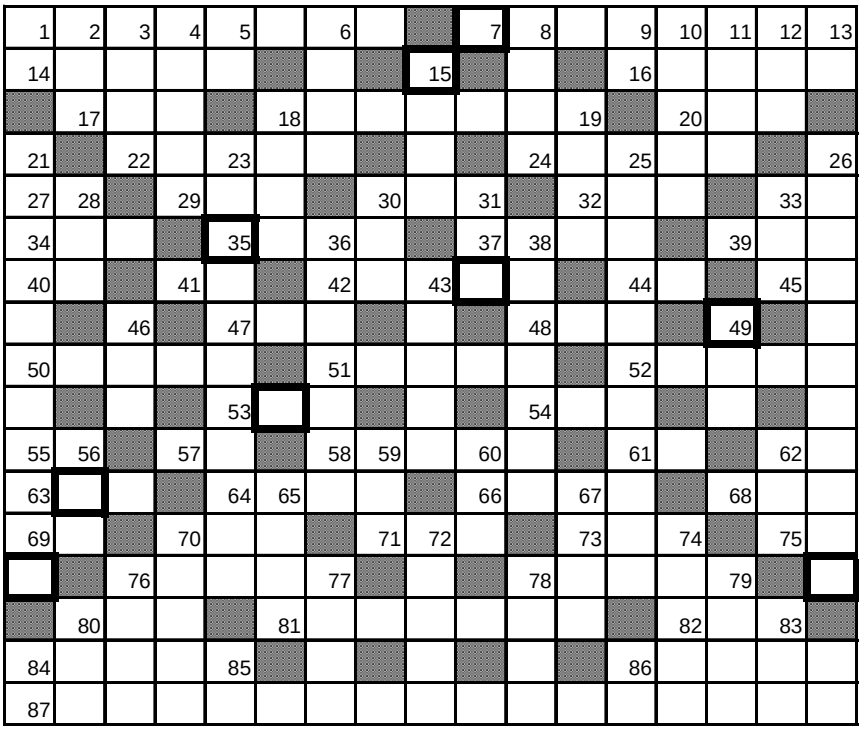
The ISACA Rome Chapter has completed the translation of all articles in ***CobiT Focus***, volume 1. The translated copy is available in PDF format at ***www.isacaroma.it/html/newsletter/node/199***.

If other chapters are interested in translating ***CobiT Focus*** or another ISACA/ITGI publication into the preferred language of its members, please contact Joann Skiba at ***jskiba@isaca.org***.

ISACA
Serving IT Governance Professionals
Switzerland Chapter

# The ISACA Crossword Puzzle 4/06

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



***Across***: 1 ***where some of them end up*** (pl); 7 ***illegal obtaining of passwords***; 14 distributions; 16 wild dog in Australia; 17 lacking moisture; 18 problem killers; 20 low card deal; 22 kinds; 24 type of bear that modelled for the Teddy; 27 French article; 29 astrological sign; 30 international standard organization; 32 frozen; 33 act; 34 question; 35 section; 37 ***most of it is***; 39 not near; 40 ***Swiss internet suffix***; 41 two equal vowels; 42 eat! (German); 44 negation; 45 two equal consonants; 47 French duke; 48 international labour organization; 50 language spoken in India; 51 ***?????***; 52 sea-living mammal; 53 Cassius Clay's taken name; 54 sick; 55 embossed on former French coins; 57 ***Austrian internet suffix***; 58 with the ***German internet suffix*** in front, a guarantee amount; 61 out (Latin); 62 railroad crossing in the US; 63 ocean; 64 preposition; 66 polar explorer in the nineteenthirties; 68 colour; 69 German pronoun; 70 French Noah; 71 first part of Brazilian metropolis 73 former Swiss Federal Councilor; 75 and (Latin); 76 monetary punishment (pl); 78 Negro sorcery; 80 anything but young; 81 small item (pl); 82 negation; 84 test; 86 title of Japanese emperor; 87 ***a nightmare for 51 across*** (two words).

***Down***: 1 anno domini; 2 colour; 3 automobiles; 4 this filmy wood got disturbed; 5 information system; 6 these (Spanish); 8 listen; 9 so dear; 10 mountainous; 11 former Peruvian noble; 12 soundless nogood; 13 walk; 15 number two (tried harder according to old advertisements); 18 ancient Greek philosophy school; 19 care (French); 21 unexpected winners (two words); 23 divorce – ***negatively used as e-mail NAK***; 25 ***the opposite of 23 down***; 26 ***passkeys*** (two words); 28 the fire leaves it; 30 possessive pronoun; 31 German exclamation of regret ; 33 kid's father; 36 ***proof of ACK***; 38 usefulness; 43 ***nuisance*** (pl); 46 conjunction; 49 rodent; 56 town (and hat) in North Africa; 59 brook near Baden-Baden; 60 negro tribe in Biafra; 62 where Salinger's catcher imagined himself to be; 65 be necessary; 67 take by force (third person sg); 70 town near Biel/Bienne; 72 famous fire fighter (Fred); 74 female first name (I=J); 76 French cop; 77 Connery's first name; 78 stinks in Latin; 79 … soit qui mal y pense; 80 gold (Spanish); 83 technical new offer; 84 touchdown; 85 local meal; 86 soundless ton.

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 5. Januar 2007.

Lösung Crossword Puzzle 3/06: COBITFOUR

***Across***: 1 JAL (Japan Air Lines); 4 Romano; 9 misbeseem; 16 Benares; 17 stem; 19 Onan; 21 MBA; 22 tirar; 25 DNA; 25 Oe; 27 cup; 29 no; 30 us; 31 overcoat; 34 lesson; 35 smug; 36 Ru; 39 opera; 41 ***approve***; 43 amber; 45 re; 46 sac; 47 Eve; 46 été; 49 Ma; 50 spear; 53 acro; 56 ***evidence***; 59 ***board***; 50 vor; 61 TI; 62 tons; 64 as; 65 Udo; 66 ante; 68 naïve; 71 Ste; 72 psi; 75 ***Waterfall***; 75 Leo; 77 ***ISO***; 79 ***clear***; 81 send; 82 QAV; 85 Ba; 84 spot; 86 IS; 87 olé; 88 taken; 90 oriental; 93 ever; 96 Delta; 97 er; 98 mit; 99 ils; 101 ora; 103 NY (new York); 105 stubs; 106 fleeces; 108 basso; 110 el; 111 rail; 112 estate; 114 ***accredit***; 117 LD; 118 Oz; 119 Ute; 120 AR; 121 PLO; 122 cieux; 125 uns; 126 Euro; 129 Hanro; 130 Dollars; 132 benchmark; 133 insure; 134 new.

***Down***: 2 abbé; 3 Lea; 4 Ragusa; 5 or; 6 men; 7 As; 8 ***OSI***; 9 ***measure***; 10 IMR; 11 SS; 12 EC; 13 eo; 14 Endo; 15 ***management***; 18 trump; 20 Nat; 21 motor; 22 to; 23 ivre; 24 ir; 27 Cerberus; 28 PS; 29 NN; 32 EU; 33 cement; 34 le; 35 ola; 36 spur; 37 ***governance***; 40 Pesos; 42 VEV; 43 Ate; 44 Ra; 46 SR (Swissair); 48 ediv (vide), 51 Pa; 52 addic(t); 54 ***controller***; 55 ***oversee***; 57 ***ITIL***; 58 ***COSO***; 59 basis; 62 Sedan; 66 AAA; 67 te; 69 ALD; 70 elate; 78 sportsclub; 80 lint; 83 beans; 85 timber; 89 k(nigh)t); 91 Eis; 92 ail; 94 viel; 95 RO; 95 da; 97 es; 100 sealink; 102 Ras; 104 yours; 106 flic; 107 cider; 108 battle; 109 SE; 110 Ed; 112 EZ; 113 tu; 114 ape; 1215 core; 116 ET; 118 ox; 120 anse; 122 car; 128 UOI (oui); 124 sou; 125 urn; 127 on; 126 CH; 129 ha; 130 DS; 131 LR.

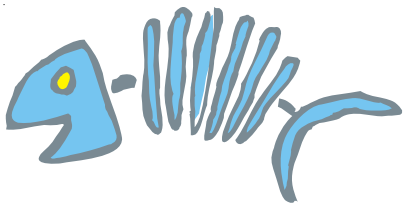
Watson: Blank crosses. Erroneous date (January) was unintentional.

Der Gewinner ist Massimo Magnini, complimenti! Er gewinnt damit $US 50 in Gutscheinen zum ISACA Bookstore. Herzliche Gratulation!

Der Watson wurde nicht entdeckt: Das Rätsel ist nicht punktsymmetrisch. Somit sind jetzt $US 150 im Jackpot.

There was an eager young audit assistant in search of a male
With qualities, such as muscles, a fortune of money and tail.
She looked in all kinds of possible directories,
And got tangled in many esoteric histories
All she could find were single addresses in the internet mail.

Eine Revisorin inspizierte zur Mannsuche zehntausend Fichen
Und kam in der Torschlusspanik schliesslich aufs Phishin'.
Doch keiner gab ihr das gesuchte „Pa-Wort",
Geschweige das von ihr gewünschte Ja-Wort.
Jetzt probiert sie's an Flüssen und Teichen mit schwimmenden Fischen.



# ISACA Switzerland

## Was denkt die SCHWEIGENDE MEHRHEIT?

Die Umfrage in der letzten Nummer des ***NewsLetters*** hat eine Resonanz ergeben, die unter fünf Prozent der Empfänger der Publikation liegt. Der Vorstand des ISACA Switzerland Chapters und die Redaktion sind erschüttert. Es ist klar, dass aufgrund dieser wenigen Meinungen keine vernünftigen Auswertungen entstehen können.

Sind die fehlenden Antworten als Einverständnis der bisherigen Erscheinungsweise zu interpretieren? Oder besteht gar kein Interesse am ***NewsLetter***?

Der Vorstand sieht sich den Tatsachen gegenüber, dass sich einerseits das Switzerland Chapter im Alleingang eine Erscheinungsweise von jährlich fünf Nummern (wie bisher) nicht leisten kann, andererseits ein totales Einstellen des Publikationsorgans derzeit nicht erwünscht ist. So wurde der Vorschlag, nur noch Fachartikel in einer einzigen Nummer erscheinen zu lassen im einen Extrem und jener, auf Fachartikel ganz zu verzichten im andern, verworfen.

Der Vorstand hat deshalb beschlossen, 2007 als „Probejahr“ zu deklarieren und einen Kompromiss einzugehen: Der ***NewsLetter*** wird 2007 in drei Auflagen in der bisherigen Form erscheinen: Anfangs Februar (damit die Einladung zur Vereinsversammlung beigelegt werden kann), Juni und Oktober.

Anlässlich der Vereinsversammlung 2008 soll endgültig über das Schicksal des ***NewsLetters*** entschieden werden.

Alle Mitglieder werden deshalb Ende nächsten Jahres aufgefordert, ihre Meinung bezüglich Fortbestand oder Einstellung des ***NewsLetters*** dem Vorstand mitzuteilen. Wir freuen uns zudem sehr über jeden Gedanken zu diesem Thema, welcher der Redaktion in der Zwischenzeit zugestellt wird. Besten Dank.

Focus der Februarnummer 2007 ist übrigens ***Prüfungsplanung und intergriertes Auditing***. Artikel sind willkommen.

***Daniela Gschwend und***
***Max F. Bretscher***

## Que pense la majorité silencieuse?

Vous n’êtes que 5% à avoir répondu à l’enquête contenue dans le dernier numéro de la ***NewsLetter***. Tant le comité de l’ISACA que l’équipe de rédaction sont déçus. Il est illusoire de procéder à une analyse sérieuse des résultats sur une telle base.

Comment interpréter ce faible taux de réponse : la majorité silencieuse est-elle satisfaite du statu quo ou se désintéresse-t-elle totalement de la ***NewsLetter***?

Pour le comité la situation est la suivante : sans le partenariat avec l’Allemagne et l’Autriche, ISACA Suisse n’a pas les moyens de poursuivre la publication annuelle de cinq ***NewsLetter***. Nous ne voulons d’autre part pas renoncer totalement à une ***NewsLetter***. Les discussions sur le contenu ne sont pas plus claires : elles vont d’un extrême (un exemplaire par année ne contenant que des articles techniques) à l’autre (une ***NewsLetter*** concentrée sur la vie de l’association et ne contenant aucun article technique).

Le comité a donc décidé de considérer l’année 2007 comme une année d’essai. Nous tenterons le compromis de trois ***NewsLetter***, la première en février (avec l’invitation à l’Assemblée générale 2007), puis en juin et octobre 2007.

La décision définitive sur le maintien ou la suppression de la ***NewsLetter*** sera prise lors de l’Assemblée générale de 2008. Tous les membres seront appelés à se prononcer sur cette question à la fin de l’année prochaine. Vos avis et commentaires sur cette question sont bien sûr toujours les bienvenus !

La prochaine ***NewsLetter*** paraîtra donc en février 2007 et sera consacrée à la ***planification de l’audit et à l’audit intégré (ou intégral)***. Vos contributions sur ce thème, en allemand, français ou anglais, sont également les bienvenues.

***Daniela Gschwend et***
***Max F. Bretscher***

# ISACA Switzerland

## AHS vom 29. August 2006

Nach den Sommerferien präsentierte uns Herr Urs Voigt der UBS einige „Facetten des Business Continuity Management (BCM)“. Das Thema war offensichtlich von grossem Interesse, so mussten diverse späte Anmeldungen wegen „ausgebuchtem Saal“ abgewiesen werden. Die Veranstalter bemühen sich, den (möglicherweise aufdatierten) Vortrag im nächsten Jahr wiederholen zu lassen.

Herr Voigt betonte, dass es sich bei den vorgestellten Elementen um das UBS-eigene Vorgehen handelt, und er davon absieht, die Sachverhalte umfassend darzustellen. Dennoch konnte es nicht vermieden werden, dass aufgrund der spannenden Darlegungen und der auflockernden Zwischenfragen der Teilnehmer die verfügbare Zeit überschritten wurde. Der anschliessende Apéro wird wohl einzelnen Teilnehmern die Möglichkeit geboten haben, individuelle Fragen zu stellen und hoffentlich befriedigende Antworten zu erhalten.

Obschon IT gerade für ein Finanzinstitut ein wesentliches Geschäftselement darstellt, ist es bei weitem nicht das einzige, welches bei einem BCM zu berücksichtigen ist. So sind System- und Prozessänderungen, Geschäftsunterbrüche jeder Art, Verlust von Personen und Gebäuden, Fehler, Abhängigkeiten von Dritten, externe Attacken, etc. bei den Vorkehren in Erwägung zu ziehen. Als Basis der einschlägigen Überlegungen der UBS stellte Herr Voigt einerseits die regulatorischen Vorschriften und andererseits die UBS-spezifische Gruppenpolitik vor. Darauf bauen sich stufenweise die Strategie, die Governanceprinzipien, die ***Terms of Reference***, etc. und letztlich das taktische Vorgehen mit Dokumentation, Tests, etc. auf. Treffend stellte Herr Voigt das „BCM-Gebäude“ mit LEGO-Klötzchen vor. Sie werden den Teilnehmern sicher wertvolle Gedankenanstösse liefern, wenn sie die Unterlagen zuhause nochmals Revue passieren lassen.

Was mich etwas irritiert hat, war die in der Einleitung angeführte ***Chinese Disaster Prediction***, die gemäss des Referenten weder risikobasiert, noch prozessorientiert, noch quantifiziert, noch detailliert sei. Der Rest der Präsentation lief nämlich genau auf das Gegenteil hinaus.

## AHS vom 26. September 2006

Kriminalfälle ziehen immer ein neugieriges Publikum an. Peter Steuri der Firma BDO aus Solothurn präsentierte interessierten Teilnehmern in vollem Saal Einzelheiten über den Fall KBV, der vor drei Jahren die Medien beschäftigte. Er selbst war mit der Aufklärung beschäftigt, weshalb er pikante Details näher erläutern konnte.

Der Fall war zwar als „konventionell“ (nicht-Informatik) angekündigt worden. Die Ausführungen zeigten aber doch, dass er mit Einsatz geeigneter Informatikmittel (erzwungene Funktionstrennung, Audit Software, Projektbegleitung, etc.) schon früher hätte aufgedeckt bzw. verhindert werden können.

Wer nun denkt, die Präsentation hätte dazu geführt, dass die anwesenden Revisions- und Sicherheitsleute Vorschläge zur Verhinderung derartiger Vorkommnisse vorgebracht hätten, sah sich überrascht. Die anschliessend rege benützte Diskussion brachte nämlich mehrheitlich zutage, dass sich viele Teilnehmer mit der Frage beschäftigten, wie eine Aufdeckung hätte verhindert werden können. Die Frage drängte sich am Schluss beinahe auf, ob die ISACA-Mitglieder die potentiell besseren Wirtschaftskriminellen sind!

***Max F. Bretscher***

## News aus den Interessengruppen

### IG Operational IT-Risk

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

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

Derzeit werden keine neuen Mitglieder aufgenommen. Wenn die Ergeb-

nisse vorliegen, wird die Interessengruppe darüber informieren.

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

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

Le groupe de travail qui rassemble les auditeurs informatiques des collectivités publiques a élaboré des recommandations à l'égard des responsables de projet informatique. Ce document d'une douzaine de pages est disponible en allemand, français et italien.

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

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

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

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

IG Computer Forensics

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

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

IG Einführung von IT-Governance

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

***Nächste Sitzung:*** November/Dezember 2006

Traktanden: Standortbestimmung der IG, Erweiterung der Aufgaben (CobiT 4.0, Schnittstelle zur Corporate Governance, Leitfaden), Abnahme Domäne „Auslieferung und Unterstützung“, Besprechung Entwurf zur Domäne „Planung and Organisation“.

IG Romandie

Marc Barbezat
b3b
Strasse
Ort
Telefon +41 79 56 55 666
Telefax +41
marc.barbezat@b3b.ch

## IG Outsourcing/Insourcing

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

Derzeit ruhend. Der Leiter sucht einen Nachfolger.

## IG MIS/EIS/DWH

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

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

- Wrap-Up/Standortbestimmung

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

- Weiteres Vorgehen

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

- Wahl des neuen IG Leiters

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

- Diverses

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

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

## IG SAP R/3

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

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

## IG (Self) Assessement mit CobiT 4.0

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

Nach anfänglichen Startschwierigkeiten besteht die IG CobiT nun bereits aus sechs Aktivmitgliedern. Zwei weitere Interessenten haben sich für die nächste Sitzung angekündigt und eine Person arbeitet wegen der grossen Distanz aus der Ferne als „unabhängige“ Review-Instanz mit.

Die bisherigen Diskussionen zur konkreten Ausgestaltung eines CobiT Self Assessment haben zu vielen, teilweise schwer zu konkretisierenden, Fragen geführt. Um eine Diskussionsbasis zu haben, hat Thomas Hediger einen kleinen Prototyp für eine der bisher diskutierten Vorgehensweisen erstellt. Die gewonnen Erkenntnisse werden bis zum nächsten Meeting am 31.10.2006 von weiteren IG-Mitgliedern wiederum mittels „Prototypen“ festgehalten und weiterentwickelt. Alle bisher gefassten Entscheide und Erkenntnisse werden neu in einem Dokument zusammengefasst und laufend nachgeführt.

Bis auf weiteres finden die IG-CobiT Sitzungen jeweils vor dem After-Hours Seminar (letzter Dienstag im Monat) von 14.00 –16.30 in der Nähe des Stampfenbachplatzes statt.

ISACA
Serving IT Governance Professionals
Switzerland Chapter

# Veranstaltungen

| | |
|---|---|
| BS 7799/ISO 27001 | 6.–10. November 2006<br>Zug, 5 Tage, Infoguard |
| Forensic Lab | 7.–9. November 2006<br>Karlsruhe, 3 Tage, Secorvo |
| Network Security | 11.–13. November 2006<br>Amsterdam, 3 Tage, ISACA |
| Information Security Management | 13.–15. November 2006<br>Amsterdam, 3 Tage, ISACA |
| ISO 20000 Consultant & Internal Auditor, inkl. int. Zertifizierung | 20.–22. November 2006<br>Zürich, 3 Tage, ISACA/Glenfis |
| After Hours Seminar: Spezialthema im Grenzbereich unseres Berufs: Risiko-Sport Gleitschirm-Fliegen | 28. November 2006<br>16:40-17:40, Zürich, ISACA CH |
| Content- und Mobile-Security Lab – Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung durch mobile Tech. und aktuelle Malware | 29. November – 1. Dezember 2006<br>Zürich, 3 Tage<br>ISACA CH/Compass |
| Swiss Infosec Special Event | 30. November – 1. Dezember 2006<br>Zürich, 2 Tage, Infosec |
| ITIL Foundation-Kurs mit Simulation (spielend lernen aber mit internationaler Zertifizierung abschliessen) | 6.–8. Dezember 2006<br>Zürich, 3 Tage, ISACA CH/Glenfis |
| ISO/IEC 27001 Lead Auditor-Lehrgang | 4.–8. Dezember 2006<br>Zürich, 5 Tage, Infosec |
| ISACA Erfahrungsaustausch: Risikoorientierte Jahresplanung | 11. Dezember 2006<br>Zürich, 1 Tage, ISACA CH |
| Risikoorientierte Jahresplanung der IT-Revision und Informationssicherheit | 11. Dezember 2006<br>Zürich, 1 Tag, ISACA-CH |
| Hacker, Spione und Datendiebe | 11. – 13. Dezember 2006<br>Zug, 3 Tage, Infoguard |
| Einführung in COBIT 4.0 | 12. Dezember 2006<br>Zürich, 1 Tag, ISACA-CH |
| Introduction to COBIT 4.0 | 13. Dezember 2006<br>Zürich, 1 Tag, ISACA-CH |
| CISM Vertiefungskurs 2007\|1 | 11. Januar 2007–22. Mai 2007<br>Zürich, 12 Tage, ISACA CH/ITACS |
| CISA Vertiefungskurs 2007\|1 | 15. Januar 2007–21. Mai 2007<br>Zürich, 14 Tage, ISACA CH/ITACS |
| CISM Prüfungsvorbereitungskurs 2007\|1 | 12. April 2007–22. Mai 2007<br>Zürich, 4 Tage, ISACA CH/ITACS |
| CISA Prüfungsvorbereitungskurs 2007\|1 | 16. April 2007–21. Mai 2007<br>Zürich, 5 Tage, ISACA CH/ITACS |

ISACA
Serving IT Governance Professionals
Switzerland Chapter

## Kontaktadressen Veranstalter

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

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

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

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

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

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

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

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

ISACA Switzerland Chapter
c/o ITACS Training AG
Stampfenbachstrasse 40
CH-8006 Zürich
Tel. + 41 44 444 11 01
Fax +41 44 444 11 02
info@isaca.ch
www.isaca.ch

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

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

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

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

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

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

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

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

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

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

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

ISACA
Serving IT Governance Professionals
Switzerland Chapter

# Vereinsadressen

## Austria Chapter

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

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

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

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

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

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

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

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

www.isaca.at

## Switzerland Chapter

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

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

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

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

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

***Sekretär***
c/o Präsidentin

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

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

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

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

www.isaca.ch