Nr. 76 | September 2005

Schwerpunkt-Thema:

Schnittstellen-Prüfung

Inhaltsverzeichnis

Editorial 4

Schnittstellen-Prüfung – Kammer-Seminar Nr. 928 vom 30. Juni 2005, ein Erfahrungsbericht 5

Schnittstellen-Prüfung– Swissdec: Lohnstandard-CH 7

Schnittstellen-Prüfung– Swissdec: Norme suisse en matière de salaire 10

Schnittstellen-Prüfung– Exemples pratiques d'erreurs dues aux interfaces 12

Schnittstellen-Prüfung – Schnittstellenfehler in der Praxis 13

Schnittstellen-Prüfung – Das Input-Output-Bild 14

Schnittstellen-Prüfung – Projets XBRL – La transformation du Reporting d'Affaire 16

Schnittstellen-Prüfung – Projekte XBRL – Die Transformation der Finanz-Berichterstattung 17

Biometrie – Leveraging the Use of Biometrics 18

Aus der Praxis – Revenue Assurance – A first cut 23

Express Line 25

The ISACA Crossword Puzzle 26

Standards – CobiT goes EU 28

DACH-News 29

Veranstaltungen 33

Vereinsadressen 35

Impressum

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

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

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

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

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

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

Erscheint 5 Mal jährlich
Auflage: 1350 Exemplare

Nächste Ausgabe (Thema: Prüfungsstandards): November 2005, Redaktionsschluss: 24. Oktober 2005

Editorial

Les interfaces, un risque trop souvent négligé !

Comment punir un programmeur ? Confiez-lui le développement d'un interface entre deux applications ! Et si vous voulez être vraiment méchant, choisissez deux applications situées dans deux entreprises différentes et deux pays différents… Lorsqu'il aura identifié les responsables de ces deux applications, leurs besoins, la technologie à mettre en place, les modèles de données et les contrôles à mettre en place, il pourra attaquer le morceau de choix : élaborer une convention fixant la manière dont cet interface évoluera dans le futur. S'il lui reste un peu de courage, il pourra se pencher sur la redoutable question des tests : comment organiser des tests d'acceptation impliquant deux environnements ? Le dernier séminaire conjoint de la Chambre et de l'ISACA a été l'occasion de découvrir les très nombreuses erreurs que génèrent en pratique les interfaces. Ces exemples édifiants, très souvent liés à des tests insuffisants, montrent l'importance de ce thème pour un auditeur. Les interfaces augmentent significativement tant les risques inhérents que les risques de contrôle. Si l'interface relie deux entreprises se pose de surcroît la question du risque de non-détection puisque deux équipes d'audit devront coordonner leurs travaux pour vérifier la fiabilité de cette passerelle.

Ce séminaire a également été l'occasion de découvrir le projet d'interface standard reliant les applications de gestion des salaires avec les caisses de compensation, la SUVA et les administrations fiscales cantonales. Une description de ce projet innovateur vous en dira plus.

Découvrez également dans ce numéro de la NewsLetter :

- la première publication du comité informatique de la Chambre fiduciaire (Fachstab für Informatik) qui a traduit en allemand le fameux Guide de la CNCC et l'offre en download gratuit.
- Les « recommandations à l'égard des responsable de projet IT », un produit élaboré par le IG IT Government Audit de l'ISACA et que vous pouvez également télécharger gratuitement.

Bonne lecture !

Michel Huissoud
Vice-président
ISACA Switzerland Chapter

Schnittstellen, ein zu oft vernachlässigtes Risiko!

Wollen sie einen Programmierer bestrafen?! Einfach: Beauftragen Sie ihn eine Schnittstelle zwischen zwei Anwendungen zu programmieren. Wenn Sie noch ein bisschen bösartiger sein wollen, siedeln Sie die Anwendungen in zwei verschiedenen Unternehmungen in zwei verschiedenen Ländern an. Bis er die richtigen Verantwortlichen für die Anwendungen und die zutreffenden Regeln und Gesetze der Länder gefunden hat, hat er sich wohl längst gewünscht, es existierten Standards für solche Koordinationsfragen. Wenn ihm noch ein Rest Mut geblieben ist, macht er sich hinter die notwendigen Tests, die zwischen den Stellen auszuführen sind. Das durch ISACA und die Schweizerische Treuhandkammer gemeinsam durchgeführte Seminar vom 30. Juni 2005 beleuchtete diese Problematik. Die Veranstaltung deckte viele Fehlermöglichkeiten auf, die oft erst sehr spät entdeckt wurden. Wichtige Erkenntnisse waren, dass für den Informationsaustausch zwischen Unternehmungen und Ländern mit unterschiedlichen Gepflogenheiten gemeinsame Regeln zu schaffen sind, falls sie nicht bereits existieren. Damit kann viel Ärger vermieden werden.

Das Seminar beleuchtete ebenfalls die von der SUVA erarbeiteten Standards im Lohn- und Gehaltswesen der Schweiz und informierte über internationale Bestrebungen in der Standardisierung von Finanzinformationen.

Finden Sie weiter in dieser Ausgabe des NewsLetters:

- Die Publikation des vom Fachstab für Informatik aus dem Französischen übersetzten Leitfadens der CNCC und die Einladung zum gratis Herunterladen dieses Werkes.
- Die Empfehlungen für die IT-Projektleiter, das durch die Interessengruppe Government Audit der ISACA erarbeitet wurde und ebenfalls gratis heruntergeladen werden kann.

Ich wünsche Ihnen eine angenehme Lektüre!

Michel Huissoud
Vizepräsident
ISACA Switzerland Chapter

Schnittstellen-Prüfung

Kammer-Seminar vom 30. Juni 2005, ein Erfahrungsbericht

Das diesjährige Kammer-Seminar vom 30. Juni 2005 in Bern hatte das Thema „Schnittstellen-Prüfung“ zum Inhalt und richtete sich an Wirtschafts- und Informatikprüfer, welche Anwendungen und ihre Schnittstellen prüfen. MitarbeiterInnen der Abteilung Infomation Risk Management (IRM) von KPMG stellten sich zur Verfügung, diesen Erfahrungsbericht zu verfassen.

Morgens um 8:30 traf man sich zum Begrüssungskaffe im Hotel Bellevue Palace***** in Bern. Um 9.00 ging es pünktlich los mit einer kurzen Begrüssung durch Michel Huissoud. Danach folgten fünf Vorträge auf dessen Inhalt wir im Folgenden kurz eingehen.

1. Zertifizierung Standardschnittstelle-CH

Lohnabrechnungen mussten bisher mit hohem administrativen Aufwand individuell für die einzelnen Lohndatenempfänger (UVG, AHV, Steuerbehörden…) aufbereitet werden. Durch den Lohnstandard CH wird die Lohndeklaration für den Deklarationspflichtigen einfacher, schneller, günstiger und qualitativ besser. Die hohe Qualität wird dadurch erreicht, dass Daten über eine Standardschnittstelle aufbereitet und sicher übermittelt werden. Es wurde aufgezeigt, worauf bei der Implementierung in die verschiedenen Zulieferersysteme zu achten ist. Im Rahmen des Abnahmeprozesses stellt eine Zertifizierung sicher, dass die Anforderungen an Inhalt und Umfang der Daten erfüllt werden.

2. Risikoorientierte Prüfungsansätze für Schnittstellen

Die fehlende Transparenz über Schnittstellen innerhalb eines Unternehmens ist vielfach auf nicht vorhandene Dokumentationen zurückzuführen. Auch die Auswirkungen eines Softwareupdates auf die Schnittstellenfunktionalität sind oftmals schwer abzuschätzen.

Aufgrund der fehlenden Transparenz über die Schnittstelle sowie der hohen Anzahl Schnittstellen ist ein risikoorientierter Ansatz zur Prüfung von Schnittstellen unumgänglich. Dabei geht es darum, den Kernprozess unterstützende Schnittellen zusammen mit den Prozessverantwortlichen zu identifizieren, anhand Szenarien die Risiken zu bewerten und geeignete Massnahmen zu ermitteln. Dabei sind die nicht standardisierten Schnittstellen von besonderer Bedeutung.

3. Prüfung bei ausgelagerten Rechnungsprozessen

Das Outsourcing von Prozessschritten führt zwangsweise zu verschiedenen organisations- und systemseitigen Schnittstellen. Am Beispiel eines outgesourcten Billingprozesses wurde die Möglichkeit einer gesamtheitlichen und prozessorientierten Prüfung von Schnittstellen aufgezeigt. Dabei werden Prozesse klar definiert (Input, Output, Zweck und Owner der Prozesse) und die beteiligten Systeme identifiziert und in denjenigen Aspekten der Prozesskette ermittelt, in welchen die inhärent grössten Risiken beinhaltet sind. Anhand der identifizierten Risiken werden diejenigen Prüfgebiete bestimmt, welche den grössten Nutzen generieren, wodurch eine effiziente und effektive Schnittstellenprüfung erfolgen kann.

4. XBRL – Empfehlungen für XBRL Prozesse

XBRL steht für Extensible Business Reporting Language. Bei XBRL handelt es sich um eine Erweiterung des Formats XML (eXtensible Markup Language) und ist für Finanzinformationen bestimmt. Dabei ist die Datenstruktur systematisch den Normen der Rechnungslegung, Finanzen oder branchenspezifischen Kontenplänen angepasst. XBRL ist aus der Motivation entstanden, einen Standard zu entwickeln, um den Ansprüchen der finanziellen Berichterstattung hinsichtlich Vollständigkeit, Korrektheit und Unabhängigkeit von Kommunikationsnetzwerken gerecht zu werden. XBRL unterstützt einen automatisierten und transparenten Berichterstattungsprozess und soll manuelle Kontrollen reduzieren. XBRL wird durch ein internationales Konsortium geregelt. Zurzeit laufen weltweit diverse Projekte und wird sind gespannt, ob sich dieser Standard durchsetzen wird.

5. Schnittstellenfehler in der Praxis

Viele Informationsbedürfnisse, oft ungenügend geregelter Informationsaustausch, gleichzeitige Verschwendung und Mangel an Informationen sind Beispiele der heutigen Integrationssituation. Bei einem Vergleich zwischen der Infrastruktur des Menschen und der einer Firma wird ersichtlich, dass der Mensch gut organisiert ist und Firmen aufgrund der Komplexität viele Schnittstellenfehler aufweisen.

Lessons learned

Verantwortlichkeiten an den Systemgrenzen sind schwer definierbar; diesbezüglich nehmen wir die Erkenntnis mit, dass neben Applikations- und Datenowner auch Schnittstellenowner bestimmt werden sollten und die Verantwortlichkeiten für Dokumentation und Unterhalt der Schnittstellen genau definiert werden müssen.

Nicht nur bei Computerschnittstellen, sondern auch bei Schnittstellen zwischen Mensch und Maschine, typischerweise übers Grafical User Interface (GUI), besteht ein grosses Fehlerpotential. Diesbezüglich ist es wichtig, bei der Prüfung von Schnittstellen auch den Faktor Mensch zu berücksichtigen.

Eine Standardisierung der Schnittstellen innerhalb der Firma kann wesentlich zur Reduktion der Komplexität führen und die Risiken aufgrund fehlender Transparenz verringert werden. Eine Zertifizierung standardisierter Schnittstellen gibt zusätzliche Sicherheit.

Unsere Motivation

Die Prüfung von Schnittstellen ist einer der Prüfbereiche, in den wir als KPMG IT-Prüfer in der externen Revision oft involviert werden. Um die Richtigkeit und Vollständigkeit der ausgewiesenen Zahlen des Hauptbuches zu überprüfen, müssen zwangsläufig auch die Zulieferersysteme berücksichtig werden. Als hohes Risiko werden dabei die Übertragungsstrecken (Schnittstellen) zwischen Zulieferersystem (Nebenbuch) und Empfangssystem (Hauptbuch) eingestuft.

Unser Vorgehen bei der Prüfung der Schnittstellen besteht grob gesagt darin, automatische, halbautomatische und manuelle Kontrollen in einem ersten Schritt zu identifizieren, welche die Vollständigkeit und Korrektheit der übermittelten Daten sicherstellen. Weiter wird die Effektivität dieser Kontrollen geprüft. Dabei müssen auch der Umgang und die Behandlung von Warnungs- und Fehlermeldungen überprüft werden.

Die Komplexität die bei der Überprüfung von Schnittstellen zu berücksichtigen ist, hat uns motiviert, an diesem Kammer-Seminar teilzunehmen, mit dem Ziel, mehr über die Prüfung von Schnittstellen zu erfahren.

Melanie Boehi, Birgitta Ljunggren, Andrea Stanek und Elias Schibli
KPMG Zürich

Une contribution spontanée supplémentaire pendant une pause du séminaire.

Eté à Berne

Les interfaces sont comme les vagues de la mer, elles viennent, s'en vont et sont infinies.

Il faut une bonne méthodologie pour les inventorier, les classifier, les attribuer à un responsable.

Une standardisation des interfaces, des systèmes et logiciels aide l'entreprise à prévoire au lieu de guérir et n'oublions pas „d'arroser le tout d'une bonne documentation!" et de télécharger les bonnes pratiques de la CNCC sur www.isaca.ch.

JS

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

Die Vertiefungskurse für 2006 – jetzt anmelden!

Zwei spannende Kurse!

CISA
IT-Audit, IT-Security und IT-Governance
14 Tage, berufsbegleitend
16.1.2006 - 15.5.2006
Zürich/Schweiz
96,4% Erfolgsrate an Prüfung 2005

CISM
Management der Informationssicherheit
12 Tage, berufsbegleitend
12.1.2006 - 16.5.2006
Zürich/Schweiz
Neuer Kurs!

Informationsveranstaltung: 28. Nov. 2005, 16.45 -18.45

Weitere Informationen erhalten Sie in unserem Kurssekretariat:
ISACA Switzerland Chapter
c/o ITACS Training AG, Stampfenbachstrasse 40
8006 Zürich, Schweiz, kurse@isaca.ch
Tel. +41 (0)44 444 11 01, Fax +41 (0)44 444 11 02

Schnittstellen-Prüfung

Swissdec: Lohnstandard-CH

Ein wichtiger Schritt in Richtung effizienter und wirtschaftlicher Kommunikation zwischen Unternehmen und Behörden

Wirkungsorientierte Verwaltungsführung?

Die Begriffe „New Public Management“ und „wirkungsorientierte Verwaltungsführung“ prägen seit einigen Jahren die Diskussionen um nötige Reformen in der öffentlichen Verwaltung. Die Verwaltungsbehörden sollen in ihrem Handeln nicht nur rechtmässig vorgehen, sondern auch effizient und wirtschaftlich. Der Bürger wird als Kunde der Verwaltungsbehörden betrachtet, welcher von dieser eine Dienstleistung bezieht. Bürgern und Unternehmen soll die Möglichkeit geboten werden, auf einfache und effiziente Art mit den Behörden zu kommunizieren und dadurch Zeit und Kosten zu sparen. Soweit die Theorie.

In der Praxis wendet heute gemäss dem Bericht des Bundesrates „Massnahmen des Bundes zur administrativen Entlastung in den Unternehmen“ vom 16. Juni 2003 ein durchschnittliches kleineres oder mittleres Unternehmen (KMU) im Monat rund 55 Stunden für den Papierkrieg mit den Behörden auf. Der Verkehr mit den Sozialversicherungen und der Aufwand für den Verkehr mit den Steuerbehörden machen dabei rund 50 % des gesamten Administrativaufwandes aus.

Die Übermittlung von Lohndaten

So müssen Unternehmen beispielsweise die Lohndaten der Arbeitnehmer sowohl der Kantonalen Ausgleichskasse als auch der Unfallversicherung und den Steuerbehörden mitteilen. Allerdings müssen die Lohndaten wegen unterschiedlicher Anforderungen jeweils separat aufbereitet werden, was den rund 300 000 Unternehmen in der Schweiz Zeit und Geld kostet. Die Gründe für diese verschiedenen Lohndeklarationen liegen auf der Hand – eine Vielfalt von Organisationsformen im Sozialversicherungsbereich und die dezentrale Organisation der staatlichen Verwaltung führen zu zahlreichen unterschiedlichen Vorschriften betreffend der Durchführung der Lohndeklaration. Die massgeblichen Bundesgesetze (ATSG, AHVG, UVG, usw.) überlassen es den einzelnen Durchführungsorganen, verbindlich festzulegen, wie die Lohndeklaration erfolgen muss.

Die bereits erwähnte dezentrale Organisationsstruktur hat zudem in den letzten Jahren eine Vielzahl von unterschiedlichen IT-Lösungen hervorgebracht, mit welchen die einzelnen Ausgleichskassen, Steuerbehörden und Versicherungsträger ihre Aufgaben erfüllen. Häufig wurden grosse Summen in die Entwicklung von speziell auf die Bedürfnisse des Versicherungsträgers oder der Steuerbehörde angepassten Individuallösungen investiert. Diese Investitionen gilt es zu schützen. 80 % der schweizerischen Unternehmen erledigen ihre administrativen Aufgaben mit Hilfe von zeitgemässen IT-Lösungen und verfügen über Internetzugang. 90 % aller für die Lohndeklarationen nötigen Daten sind deshalb in den Unternehmen bereits heute in elektronischer Form vorhanden. Warum wird dieses Potenzial nicht für eine effiziente automatische Verarbeitung genutzt?

Das Einheitliche Format ELM/Salary Declaration

Auf der Basis dieser für alle Beteiligten unbefriedigenden Situation haben die Suva und die AHV-Ausgleichskassen im Jahr 2003 die Initiative „Einheitliches Lohnmeldeverfahren ELM/Salary Declaration“ gestartet. Ziel ist es, die Abläufe zu vereinfachen und zu vereinheitlichen. Unternehmen sollen die Lohndaten nur mehr einmal aufbereiten müssen, um sie anschliessend per Mausklick via Internet an die Sozialversicherungsträger und Steuerbehörden zu übermitteln. Dass dieses Ziel nicht einfach zu erreichen ist, liegt auf der Hand. Der Schlüssel zum Erfolg liegt in der Standardisierung von Abläufen und Verfahren.

Die Suva und die AHV-Ausgleichskassen, welche sich extra zu diesem Zweck in einem neuen Verein eAHV/IV organisiert haben, haben sich entschlossen, ein einheitliches Datenformat (ELM/Salary Declaration), auf der Basis des XML-Formats für die elektronische Übermittlung von Lohnmeldungen zu entwickeln. Das sogenannte XML-Format oder Extensible Markup Language ist ein offener Standard, der von w3c (World Wide Web Consortium), der unabhängigen Standardisierungsinstitution des WWW definiert und publiziert wurde. XML ist ein textbasiertes Format und deshalb auch von blossem Auge lesbar. Zudem

ist XML unabhängig von Plattformen und Lieferanten.

Die Suva erstellte bereits im Jahr 1974 die erste Richtlinie „Lohnprogramme" für den Lohnstandard-CH, welcher den Lohnbuchhaltungssystem-Herstellern als Grundlage für die Berechnung der beitragspflichtigen Löhne für die UV, die AHV/IV/EO und die ALV dient und welcher neu um das Modul Steuern (Lohnausweis) erweitert wurde. Die auf der Basis des Lohnstandard-CH erstellte Lohnmeldung soll nun in einem einheitlichen XML-Schema übermittelt werden. Sämtliche Hersteller von Lohnbuchhaltungssystemen müssen somit nur mehr eine Schnittstelle programmieren und unterhalten.

In Zukunft können somit sowohl die Unternehmen als auch die Sozialversicherungsunternehmen, die Steuerbehörden und eventuell weitere Interessierte zwischen mehreren Lohnbuchhaltungssystemen wählen, welche diese Standards erfüllen. Die Standardisierung hat zudem den Vorteil, dass eine gesetzliche Änderung mit zertifizierten Lohnbuchhaltungssystemen wesentlich einfacher und effizienter umgesetzt werden kann.

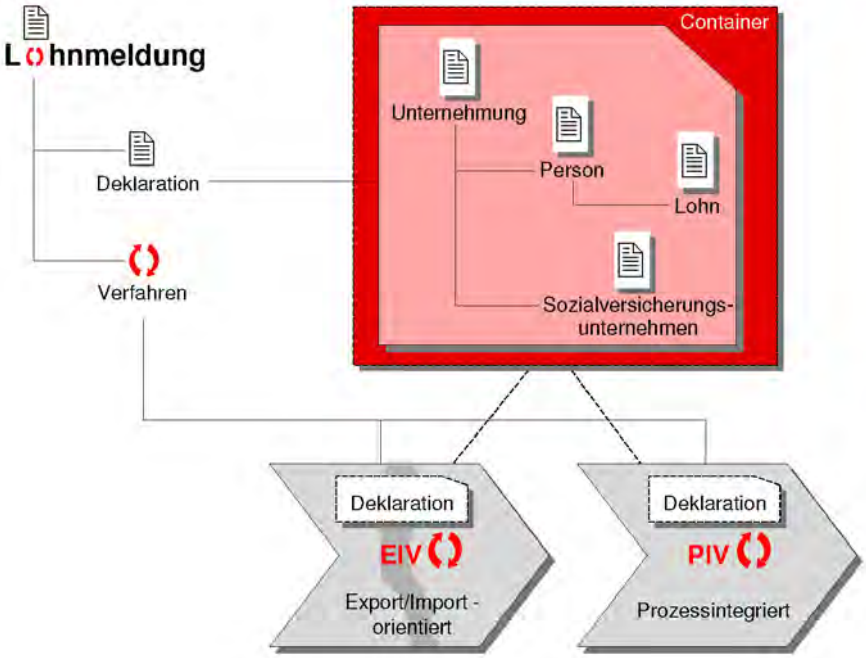
Neben diesen neuen, auf XML basierenden, Richtlinien für die Lohnbuchhaltung und deren Revision wird die Suva in diesem Zusammenhang noch weitere Dienstleistungen für die Unternehmen, Sozialversicherungsträger und weitere Interessierte erbringen. Dazu gehören die Zertifizierung von Lohnbuchhaltungssystemen, die Pflege des XML-Schemas und Stylesheets sowie die Bereitstellung von Referenzinstallationen und Testdaten (www.swissdec.ch).

Das Verfahren

Die Definition eines einheitlichen Datenformats bei der Lohnmeldung ist aber nur ein erster Schritt in Richtung Optimierung der Wertschöpfungsprozesse bei der Übermittlung von Lohndaten. Ein logischer weiterer Schritt ist die Vereinheitlichung des Übermittlungsverfahrens. Es stehen die beiden Varianten der Übermittlung über das Export/Import-Verfahren (EIV) und das Prozessintegrierte Verfahren (PIV) zur Verfügung. Während im ersten Fall die Daten via Austausch von Datenträgern oder als elektronische Datei via Internet übermittelt werden, erfolgt im Prozessintegrierten Verfahren (PIV) eine Übermittlung webbasiert und die dahinter liegenden Geschäftsprozesse sind vollkommen integriert, so dass eine Übermittlung und Weiterbearbeitung (Unternehmen, Sozialversicherung) ohne Medienbrüche erfolgen kann. Die Suva und mehrere weitere Verwaltungsbehörden bevorzugen das PIV und werden dieses Ziel in der Zukunft gemeinsam verfolgen.

übermittelt und die eingegangene Rückmeldung verarbeitet wird. Im Fehlerfall muss für jede Übermittlung eine separate Korrektur vorgenommen werden. Zudem müssen die Daten für die kantonalen Steuerverwaltungen nach Kantonen gesondert sowie die Pakete einzeln verschickt werden. Bei einer Übermittlung der Daten an das Bundesamt für Statistik, das ebenfalls an einer Beteiligung an der Entwicklung des Lohnstandard-CH interessiert ist, müssten die Daten anonymisiert werden.

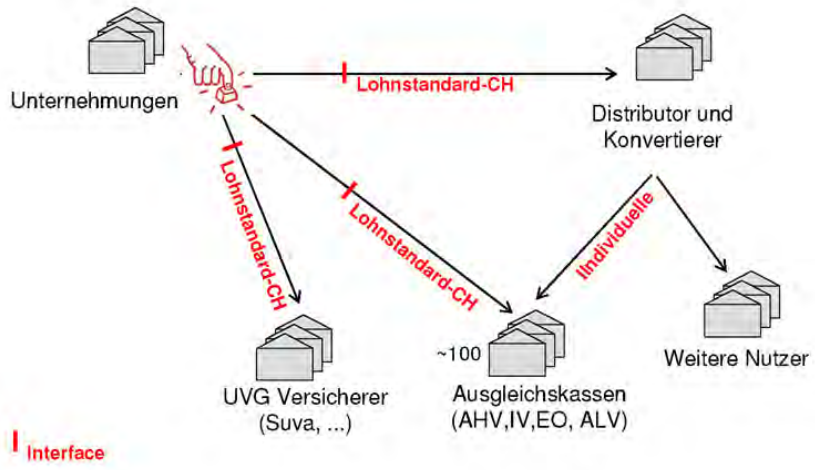
Um diesen Anforderungen gerecht zu werden, und das Verfahren für die Unternehmen zu vereinfachen, bietet sich die Integration eines sogenannten „Distributors" an, welcher für die Verteilung und eventuelle Transformation der Daten zuständig ist. Der Distributor ist somit der einzige Empfänger der Daten aus der Lohnbuch-

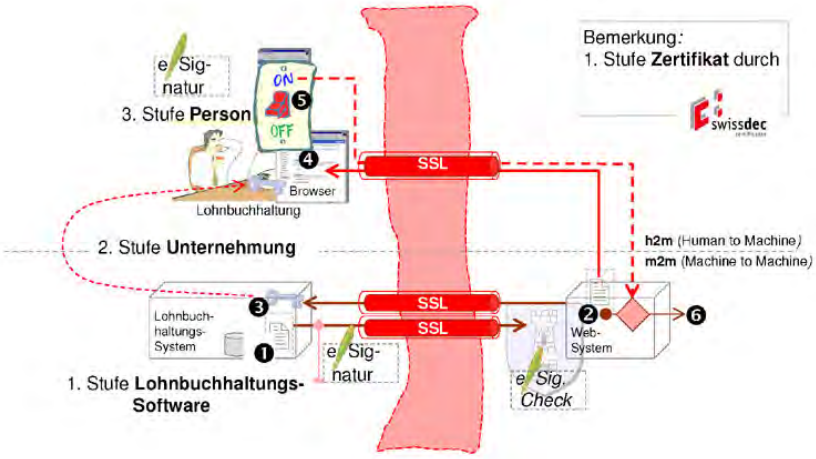


Distributor

Die aufbereiteten Daten aus den Lohnbuchhaltungssystemen sollen somit in Zukunft mittels einer Transaktion an mehrere Empfänger übermittelt werden, wobei jeweils die Empfängeradresse gesucht, die Daten

haltung, welcher Validität, Plausibilität und Benutzer-Authentifizierung überprüft und die Lohndaten an die Empfänger weiterleitet. Die Antworten der einzelnen Empfänger werden gespeichert, gesammelt und an den Sender zurückgegeben. Der wirtschaftliche Nutzen des Distributors liegt in der ein-





facheren Handhabung für den Endnutzer in einem Unternehmen, in einer höheren Qualität der so übermittelten Daten und im einmaligen Aufbau der Sicherheitslösung.

Sicherheit

Eine webbasierte Übermittlung von Personendaten bedingt selbstverständlich ein erhöhtes Augenmerk auf die Sicherheit der Bearbeitung und Übermittlung der Daten. Die Lohndaten werden vor der Übermittung mit einer digitalen Signatur versehen und die Übermittlung erfolgt SSL-verschlüsselt.

Der neue Lohnstandard-CH

In Zukunft wird der Lohnstandard-CH aus den beiden Teilen Lohndeklaration und Verfahren bestehen. Die Suva wird die Hersteller von Lohnbuchhaltungssystemen im Hinblick auf die Einhaltung der entsprechenden Vorgaben beraten und den Lohnbuchhaltungssystemen, welche die Anforderungen erfüllen, das Label „swissdec-certificated“ erteilen.

Standardisierung bedingt Zusammenarbeit

Das Erreichen dieser Ziele hängt aber wesentlich vom Willen aller Stakeholder ab, auf Lösungen, welche ausschliesslich auf die eigenen Bedürfnisse ausgerichtet sind zu verzichten und das gemeinsame Ziel einer einheitlichen Übermittlung von Lohnmeldungen in den Vordergrund zu stellen. Die Wirtschaft fordert diese Standardisierung und wird es den beteiligten Verwaltungsbehörden danken.

Ernst Stalder und Enrico Roncaglioni, SUVA Luzern

Schnittstellen-Prüfung

Swissdec: Norme suisse en matière de salaire

Un pas important vers une communication efficace et économique entre les entreprises et les autorités

Nouvelle gestion publique?

Les notions de „new public management“ et de „nouvelle gestion publique“ réapparaissent régulièrement depuis quelques années dans les discussions autour des réformes nécessaires dans l'administration publique. Les actes des autorités administratives doivent être non seulement conformes au droit mais encore efficaces et économiques. Le citoyen est considéré comme le client des autorités administratives, dont il bénéficie des prestations. Les citoyens et les entreprises doivent avoir la possibilité de communiquer de manière simple et directe avec les autorités, sans gaspiller leur temps ni leur argent. Voilà pour la théorie.

Dans la pratique et selon le rapport du Conseil fédéral du 16 juin 2003 sur les „Mesures d'allègement administratif de la Confédération pour les entreprises“, une PME de taille moyenne consacre environ 55 heures par mois à traiter la paperasserie destinée aux autorités. Les échanges avec les assurances sociales et les autorités fiscales représentent près de 50 % des charges administratives.

Transmission de données salariales

Les entreprises doivent par exemple communiquer les données salariales de leurs employés à la caisse cantonale de compensation, à l'assurance-accidents et aux autorités fiscales. Cependant, pour répondre aux exigences des unes et des autres, ces données doivent être préparées séparément, ce qui représente une perte de temps et d'argent pour 300 000 entreprises en Suisse. La raison de ces différences s'explique aisément: la diversité des structures du domaine des assurances sociales et la décentralisation des administrations impliquent tout autant de prescriptions sur l'établissement des déclarations de salaires, car les lois fédérales déterminantes en la matière (LPGA, LAVS, LAA, etc.) laissent à chaque organe d'exécution le soin de fixer lui-même ses propres modalités.

Ces dernières années, ce phénomène de décentralisation a par ailleurs favorisé l'apparition des différentes solutions IT utilisées par les caisses de compensation, les autorités fiscales et les assureurs. De grosses sommes ont souvent été investies dans le développement de solutions individuelles spécialement adaptées aux besoins des assureurs ou des autorités fiscales. Ces investissements doivent être valorisés. 80 %des entreprises suisses liquident leurs travaux administratifs en employant des solutions IT et disposent d'un accès à Internet. 90 % des données nécessaires pour les déclarations de salaires sont d'ores et déjà disponibles sous forme électronique dans les entreprises. Pourquoi ce potentiel n'est-il pas exploité pour automatiser le traitement?

Format unifié de communication des salaires PUCS

Ayant constaté les insuffisances de la situation pour l'ensemble des intéressés, la Suva et les caisses de compensation AVS ont lancé en 2003 l'initiative „Procédure unifiée de communication des salaires PUCS“. Son but: simplifier et harmoniser les démarches administratives. Grâce à elle, les entreprises prépareront une seule fois les données salariales qu'elles transmettront ensuite en un clic de souris via Internet aux assureurs et aux autorités fiscales. Il est évident que cet objectif n'est pas facile à atteindre. La clef du succès réside dans la normalisation des processus et des procédures applicables.

La Suva et les caisses de compensation AVS, qui ont spécialement créé une nouvelle association eAVS/AI dans ce but, ont décidé de développer un format de données unifié (PUCS/ Salary Declaration) sur la base du format XML pour la transmission électronique des déclarations de salaires. Le format XML ou eXtensible Markup Language est un format standard ouvert, défini et publié par w3c (World Wide Web Consortium), l'institution de normalisation indépendante de la toile. XML est un format basé sur du texte et, partant, facilement lisible. D'autre part, XML fonctionne indépendamment des plates-formes et des fournisseurs.

En 1974, la Suva avait déjà élaboré une première directive „programmes salaires“ pour la norme suisse en matière de salaire utilisée par les concepteurs de logiciels pour le calcul des salaires soumis aux cotisations de l'assurance-accidents, de l'AVS/AI/APG et de l'AC, et qui a été récemment

complétée par un module impôts (certificat de salaire). Les déclarations établies selon la norme suisse en matière de salaire seront désormais transmises sous forme de documents XML (schéma unifié). De cette manière, les concepteurs de logiciels n'auront plus qu'une seule interface à programmer et à mettre à jour.

A l'avenir, les entreprises, les assurances sociales, les autorités fiscales et les autres intéressés auront le choix entre plusieurs systèmes de comptabilité des salaires conformes aux critères de la norme. Autre avantage de la normalisation: la certification des systèmes de comptabilité des salaires, qui simplifiera l'application des futures modifications légales.

Outre ces nouvelles directives de comptabilité des salaires basées sur le schéma XML et leur mise à jour, la Suva fournira également des prestations de services complémentaires aux entreprises, aux assureurs et aux autres intéressés: certification des systèmes de comptabilité des salaires, gestion du schéma XML et des feuilles de style, fourniture d'installations de référence et de données de test (www.swissdec.ch).

Procédure

La définition d'un format de données unifié pour la déclaration de salaires n'est qu'un premier pas vers l'optimisation des processus de valorisation en matière de transmission de données salariales. L'unification de la procédure de transmission constitue un second pas en avant. Il existe deux options au choix: la procédure orientée exportation/importation (EIV) et la procédure intégrée dans un processus (PIV). Dans le premier cas, les données sont transmises par échange de supports de données ou de fichiers électroniques via Internet. Dans le cas de la PIV, la transmission s'effectue en revanche par le biais d'un serveur Web: les processus sous-jacents étant parfaitement intégrés, la transmission et le traitement ultérieur des données (entreprise, assurance sociale) se déroulent sans rupture de média. La Suva et plusieurs autres autorités administratives, qui privilégient la formule PIV, sont décidées à poursuivre cet objectif ensemble.

Répartiteur

A l'avenir, il suffira donc d'une seule transaction pour communiquer à plusieurs destinataires les données extraites d'un système de comptabilité des salaires, autrement dit rechercher leurs adresses, leur transmettre les données et traiter la réponse. En cas d'erreur, les rectifications sont effectuées séparément pour chaque transmission. Par ailleurs, les données destinées aux autorités fiscales cantonales sont envoyées séparément pour chaque canton. En cas d'échanges avec l'Office fédéral de la statistique, qui envisage également une participation au développement de la norme suisse en matière de salaire, les données devront être transmises dans des conditions garantissant l'anonymat le plus complet.

Pour satisfaire à ces exigences et simplifier la procédure pour les entreprises, il est possible d'intégrer un „répartiteur" chargé de la ventilation et de la transformation éventuelle des données. Dans ce cas, le répartiteur est le seul récepteur des données extraites de la comptabilité des salaires, dont il contrôle la validité, la plausibilité et l'authenticité des utilisateurs, avant de les transmettre aux différents destinataires. Les réponses de chacun sont enregistrées, regroupées puis retournées à l'émetteur. L'utilité économique du répartiteur réside dans la simplification des démarches de l'utilisateur final au sein de l'entreprise, la meilleure qualité des données transmises et la mise en place d'une seule solution de sécurité.

Sécurité

La transmission de données personnelles avec un système Web implique forcément une prise en compte particulière du facteur sécurité: avant la transaction proprement dite, les données salariales sont toujours pourvues d'une signature digitale et sécurisées par chiffrement SSL.

Nouvelle norme suisse en matière de salaire

A l'avenir, la norme suisse en matière de salaire comprendra deux parties, à savoir la déclaration de salaires et la procédure de transmission. La Suva conseillera les concepteurs de logiciels de comptabilité des salaires concernant les prescriptions à respecter et attribuera le label „swissdec-certificated" aux systèmes qui remplissent les exigences.

La normalisation: un travail d'équipe

La réalisation des objectifs fixés dépend toutefois de la volonté des parties prenantes à renoncer à des solutions exclusivement axées sur leurs propres besoins pour privilégier un objectif commun visant à unifier les procédures de transmission de données salariales. L'économie exige cette normalisation et saura se montrer reconnaissante envers les autorités administratives impliquées.

Ernst Stalder et Enrico Roncaglioni, SUVA Luzern

Schnittstellen-Prüfung

Exemples pratiques d'erreurs dues aux interfaces

Cas 1: oubli de lecture d'un incrément

Les données du système A (administration publique, importantes informations relatives à la propriété foncière) sont distribuées chaque semiane à une dizaine d'autres systèmes par le biais d'une plateforme d'échange. Les données incrémentées durant une semaine n'ont par erreur pas été lues. L'erreur n'a été découverte que 4 mois plus tard. Durant ce laps de temps, tous les travaux ont été effectués avec des données inconsistantes.

Cas 2: différences sémantiques

Des dysfonctionnements importants son apparus dans des moteurs destinés à des ascenseurs et à des chaînes de montage. Ils proviennent de différences d'interprétation ou de calcul de certains champs de l'interface entre les fournisseurs et le fabricant. En moyenne 4 moteurs ont dus être remplacés dans une centaines d'unités rappellées dans l'entreprise.

Cas 3: Erreurs de calcul dans une consolidation

Une erreur dans la lecture du décompte des prestations d'un système d'information clinique a été la source de plusieurs erreurs de facturation. Lors de la prise en compte de la prestation, le système n'a pas tenu compte du champ « nombre » et n'a donc pas procédé à la multiplication nécessaire. Une constatation trop fréquente.

Cas 4: Les limites des logiciels standards

Lors d'une période de surcharge, le système de gestion des commandes d'une entreprise de commerce a eu un comportement chaotique. Les clients ont reçu des articles ne correspondant pas à leur commande. La cause de ces erreurs résidait dans le nombre d'input entrant parallèlement dans le système. Au-delà de 400 la surcharge a provoqué le déclenchement d'un mécanisme de blocage automatique dans la base de données sous-jacente (problème de la coordination entre applicatif, système d'exploitation et base de données).

Cas 5: Erreur « irréversible »

Une personne est chargée de saisir et de muter les données d'état-civil dans un système central qui alimente plusieurs autres systèmes. Lors de la saisie des données de deux époux, il choisit le faux Hans Müller. Quelques jours plus tard, l'erreur est découverte et corrigée dans le système central. C'est oublié qu'entretemps l'information erronée a été transmise à d'autres administrations, dont la'dministration fiscale qui entame sur cette base une procédure de taxation intermédiaire pour le faux Hans Müller. Une procédure d'extourne n'avait pas été prévue entre les deux systèmes.

Thomas Marko, lic. oec., Winterthur

Schnittstellen-Prüfung

Schnittstellenfehler in der Praxis

Fall 1: Inkrement einlesen vergessen

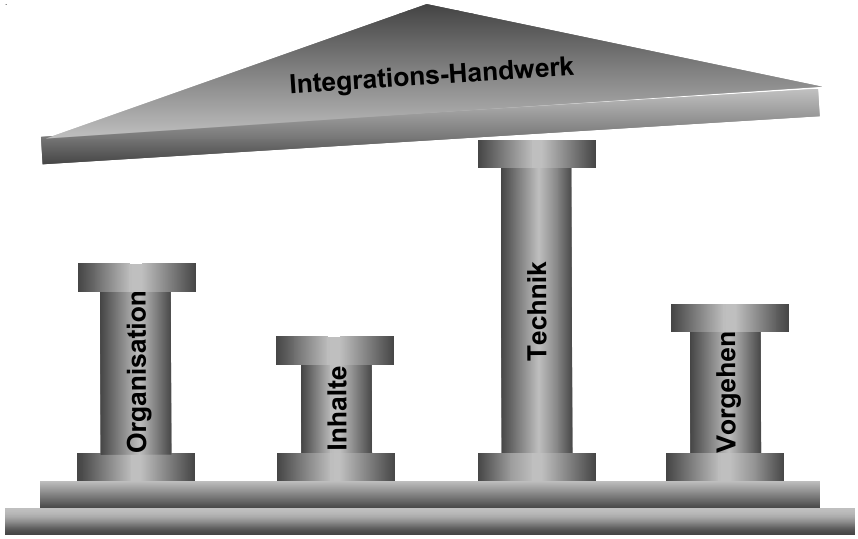
Die Daten des Systems A (öffentliche Verwaltung, wichtige Informationen zu Grundbesitz und Eigentümern) werden über eine „Datendrehscheibe" ein Mal pro Woche an ca. 10 Empfängersysteme verteilt. Ein Wochen-Inkrement wurde versehentlich nicht eingelesen. Man hat es erst 4 Monate später entdeckt und bis dahin mit inkonsistenten Daten gearbeitet.

Fall 2: Semantik-Differenzen

Die für Lifte und Förderbänder in einer länderübergreifenden Kooperation produzierten Motoren erbrachten im produktiven Einsatz die erwartete Leistung nicht, weil man sich beim Datenaustausch nicht auf die exakt gleichen Berechnungs-Modelle abstützte. In ca. 100 „Spezial-Fahrzeugen" mussten in einer Rückrufaktion durchschnittlich vier Motoren ersetzt werden.

Fall 3: Berechnungsfehler bei Summierung

In der Leistungsabrechnungs-Schnittstelle eines Kliniksystems wurde bei der Zusammenfassung der Buchungen falsch summiert. Jede Leistung wurde nur einmal gezählt, auch wenn unter „Anzahl" z.B. 3 drinstand.



Fall 4: Grenzen der Basis-Software

Bei hoher Last kamen in einem Transaktionssystem im Handel Bestellungen durcheinander. Besteller erhielten falsche Artikel geliefert. Ursache war, dass bei hoher Belastung (ab 400 parallelen Input-Strömen) der Sperrmechanismus der Basis-Software (Kombination Betriebssystem/Integrationssoftware/Datenbank) versagte.

Fall 5: „Irreversibler" Fehler

In einem System, wo Zivilstands-Änderungen sofort an diverse Amtsstellen weitergemeldet werden, wählt der Zivilstandsbeamte für die Erstellung des Ehescheins beim Erfassen der Personalien versehentlich den falschen Hans Müller als Ehemann aus. Dieser merkt es zum Glück noch vor dem Unterschreiben; der Zivilstandsbeamte korrigiert in seinem System auf den richtigen Hans Müller und das Ehepaar erhält den korrekten Eheschein. Inzwischen wurde die Meldung aber ans Steueramt gesendet. Dort wurde automatisch eine Zwischentaxation veranlasst und zwei Steuererklärungen zusammengelegt. Ein „Undo" ist nicht möglich.

Thomas Marko, lic. oec., Winterthur

Schnittstellen-Prüfung

Das Input-Output-Bild

Eine altbewährte – und technologieunabhängige – Methode zur Schnittstellen-Identifikation, der -Kontrolle und -Prüfung.

Die Methode beruht auf der Beobachtung, dass die meisten Informationen dahin tendieren, die Systeme „U-förmig“ zu durchlaufen. Abbildung 1 zeigt ein solches Bild bei der Stammlistenerfassung bei der Zahlung von Kreditoren durch eine Bank: Der Teilnehmer sendet die ausgefüllte Stammliste mit den zu zahlenden Beträgen seiner Bank (-filiale). Diese tippt oder scannt sie ein und übermittelt via Intranet die Aufträge an ihre Zentrale. Dort werden die Aufträge durch ein Subsystem „Stammlistenverarbeitung“ behandelt und verbucht. Der Teilnehmer erhält einen Belastungsbeleg der ausgeführten Transaktionen mit einer neuen Blanko-Stammliste für die nächste Verarbeitung zugesandt. Das damit abgebildete „U“ ist unschwer zu erkennen.

Zugegeben: Nicht alle Stellen in jedem System können mit Leichtigkeit in eine Reihenfolge gebracht werden, dass die „U“ zwangsweise entstehen. Dies wird einem geübten Anwender besser gelingen, als einem Anfänger, der wohl mehr Radiergummi als Bleistift in seinen ersten Gehversuchen verbraucht. Immerhin: Praktisch alle Systeme (nicht nur organisatorische, wie in den Abbildungen angedeutet – auch Computerprogramme bezüglich ihrer Module und Befehlslinien!) lassen sich in einem solchen Bild darstellen.

Die Theorie des Input-Output-Bildes behauptet nun, dass für ein vollständig bezüglich Schnittstellen kontrolliertes Diagramm auf jeder Trennlinie eine Kontrolle bezüglich Vollständigkeit, Richtigkeit und allenfalls Tagfertigkeit aufweisen muss. Dabei unterscheidet man sogenannte „Weitergabekontrollen“ (Kleinbuchstaben) und kompensierende Kontrollen (Grossbuchstaben). Abbildung 2 illustriert diese Situation, wobei eine ganze Reihe neuer „U“ entstehen können.

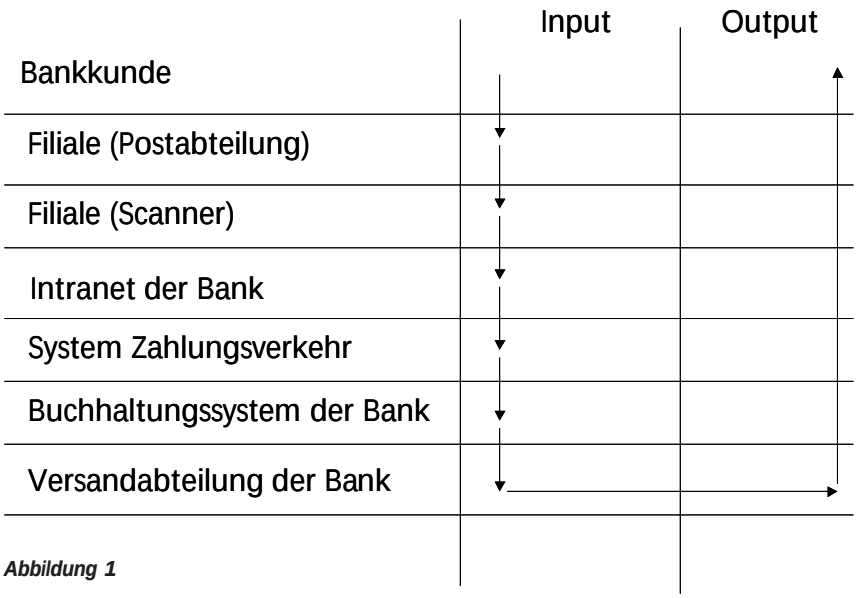


Abbildung 1

Eine rechtzeitig ausgeführte kompensierende Kontrolle macht alle ihr „unterliegenden“ Kontrollen überflüssig. Somit können mit dem Input-Output-Bild auch überflüssige Kontrollen identifiziert (und eliminiert) werden! Rechtzeitig deshalb, weil in gewissen Systemen (gerade im Zahlungsverkehr!) Kontrollen mit Zeitverzögerung möglicherweise zu spät greifen, um „Unglücke“ zu verhindern.

Die Ausgestaltung der Kontrollen kann unterschiedlich erfolgen:

a Der Bankkunde lässt sich von der Filiale die Abgabe der Stammliste bestätigen

b Die Postabteilung nummeriert automatisch die erhaltenen Stammlisten

c Der Scanner erstellt ein Hash-Total der gelesenen und übermittelten Stammlisten

d Ein datiertes Kontrolltotal zwischen Netzwerk und ZV-System bestätigt die Übernahme

e Wie d) vorstehend

f Das Buchungssystem erstellt ein Begleitbordereau zu den zu versendenden Auszügen

A Der Kunde vergleicht die Belastung mit der Kopie der abgegebenen Stammliste: Da extern, eine starke Kontrolle, aber gerade deshalb nicht im Einflussbereich des Unternehmens

B Die Filiale bestätigt den Empfang der Stammliste

C Die Postabteilung erhält eine Bestätigung des Scanners über die erfolgreiche Erfassung

D Das Intranet bestätigt der Scannerabteilung die erfolgreiche Übermittlung

E Das ZV-System bestätigt dem Internet die erfolgreiche Verarbeitung

F Das Buchungssystem bestätigt dem ZV-System die Verbuchung

G Kontoauszug an den Bankkunden

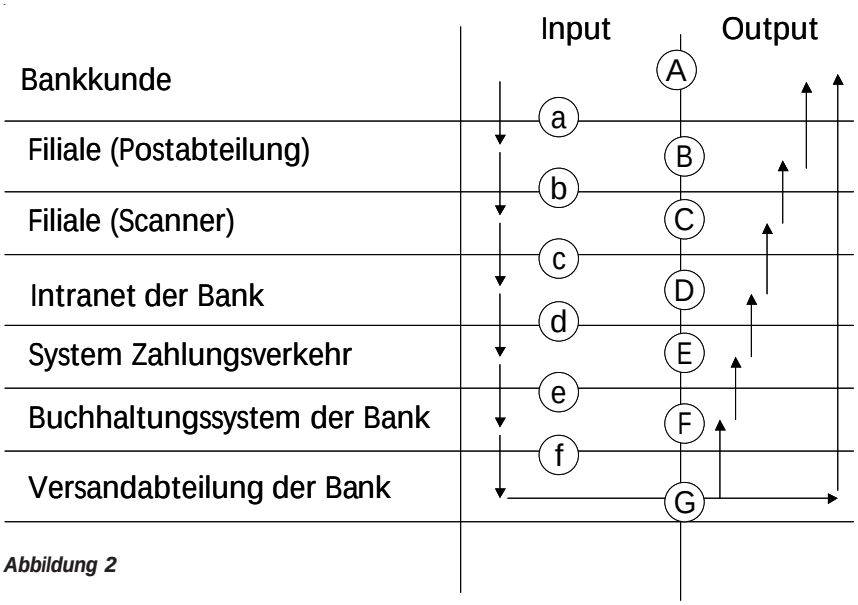


Abbildung 2

Es ist zulässig, die Frage nach dem Sinn aller dieser Kontrollen zu stellen. Unter Umständen sind die Kontrollen A und G hinreichend! Einige Präsentatoren an der Veranstaltung vom 30. Juni 2005 in Bern erweckten bei mir diesen Eindruck, indem sie festhielten, dass isolierte Schnittstellenkontrollen praktisch unwichtig seien. Wichtig sei die Kontrolle über das gesamte System.

Möglich. Aber: Eine Bank mit einem guten Qualitätsniveau wird wahrscheinlich auf die Kontrollen b), c), d) und f) nicht verzichten wollen.

Und noch eine letzte Bemerkung: Es kann vorkommen, dass bei allen Bemühungen an gewissen Stellen kein „U“ konstruiert werden kann. Ein typisches Beispiel dafür ist die Ablage bzw. Archivierung. In diesen Fällen sollte die entsprechende Weitergabekontrolle besonders stark sein (z.B. visierte Protokollierung) und mittels Einhalteprüfungen getestet werden.

Max F. Bretscher, CISA, CISM,
Langnau am Albis

Schnittstellen-Prüfung

Projets XBRL – La transformation du Reporting d'Affaire

Les systèmes actuels sont marqués par un certain nombre de carences comme la rupture dans la chaîne logistique du reporting financier ou encore la grande difficulté à transmettre les informations d'un logiciel à l'autre, d'un standard d'échange à l'autre, d'un réseau à l'autre.

Les fonctionnalités souhaitées et souvent exprimées sur le reporting financier sont toujours de disposer d'une information complète, fiable et transparente, qui s'affranchisse des ressaisies, et des réseaux de communication et de formats informatiques propriétaires, et donc de disposer d'un format d'échange d'information, (soit donc XBRL – Extensible Business Reporting Language).

Au-delà des standards d'échanges propriétaires, largement utilisés et basés directement sur des logiciels, EDI avait percé il y a quelques années dans le domaine transactionnel sous l'égide des travaux UN/CEFACT, mais EDI en plus d'être rigide dans sa structure s'appuie sur des réseaux propriétaires de type X400 ou X25, ou autres avec des translateurs pour le rendre compatible Web, d'où un coût souvent élevé.

Puis avec l'émergence de l'Internet est apparu le format XML qui est à la base de XBRL. XML (eXtensible Markup Language) (dit méta-langage), distingue la forme (l'enrobage – les schémas), du contenu (les données), grâce à des balises. Mais XML n'est pas suffisant, c'est juste du texte entre des balises qu'il faut „réinventer" à chaque fois et donc réinventer les schémas. XBRL est une version enrichie d'XML dédiée aux données financières dont les schémas sont des structures spécifiques appelées Taxonomies permettant structuration des données en suivant systématiquement des Normes comptables, financières, ou prudentielles voire de sociétés.

L'émergence d'XBRL dans le Monde est régie par un consortium international -– XBRL International, dont le siége est au Etats-Unis ayant des juridictions dans chaque pays qui le souhaite. Des projets XBRL existent de par le monde et nous citerons en exemple le projet de mise en place d'XBRL dans la société Wacoal au Japon.

Enfin dernier point pour le contrôle et la certification des comptes, aujourd'hui sans XBRL on assiste souvent à un processus manuel qui reste périodique et opaque avec des informations enfouies dans les processus organisationnels. Nul doute que demain en XBRL on assistera à un processus automatisé et transparent de reporting, mais les questions de la certification devront évoluer avec l'émergence du standard.

Gilles Maguet, XBRL Paris

Schnittstellen-Prüfung

Projekte XBRL – Die Transformation der Finanz-Berichterstattung

Die aktuellen Systeme sind gekennzeichnet durch eine gewisse Anzahl Schwachstellen, wie der Bruch in der logistischen Kette der finanziellen Berichterstattung, der schwierigen Übertragung von einem Rechner auf einen anderen, von einem Standard zum anderen, von einer Datenbank zu anderen.

Die gewünschten Funktionalitäten der finanziellen Berichterstattung sind immer die Lieferung einer vollständigen Information, wahr und transparent, frei von wiederholten manuellen Doppelerfassungen, unabhängig von Kommunikationsnetzwerken und der proprietären Kommunikationsprotokolle. Diese Erwartungen haben zum Austauschformat XBRL – Extensible Business Reporting Language geführt.

Neben den proprietären Austauschstandards hat sich vor einigen Jahren vor allem EDI im Bereich der Transaktionsverarbeitung unter der Führung der Arbeiten von UN/CEFACT durchgesetzt; aber EDI ist – zusätzlich zu seiner eher rigiden, auf den proprietären Kommunikationsprotokollen X400 oder X25 aufbauenden Struktur – oft viel zu teuer wegen der• für das Internet notwendigen Übersetzungskomponenten.

Dann ist mit der Ausbreitung des Internet das Format XML erschienen, das die Basis darstellt für XBRL. XML (eXtensible Markup Language – eine Meta-Sprache), unterscheidet mit Hilfe von Containern zwischen der Form (den Schemata), und dem Inhalt (den Daten). XML ist aber nicht ausreichend, sondern besteht nur aus Text zwischen Marken, welche man immer wieder „neu erfinden“ muss; und damit auch die Schemata. XBRL ist eine angereicherte Version von XML, welche für finanzielle Informationen bestimmt ist, wo die spezifischen Strukturen (Taxonomien genannt) es erlauben, die Daten zu strukturieren und somit systematisch den Normen der Rechnungslegung, Finanzen oder branchenspezifischen Kontenplänen zu folgen.

Das Erscheinen von XBRL wird durch ein internationales Konsortium (XBRL International) geregelt. XBRL-Projekte bestehen auf der ganzen Welt.

Ein letzter Punkt im Zusammenhang mit der Kontrolle und Zertifizierung der Konten: Ohne XBRL muss man sich heute oft mit manuellen Kontrollen behelfen, welche periodisch und oft mit in den organisatorischen Prozessen versteckten Informationen undurchsichtig bleiben. Es bestehen keine Zweifel darin, dass XBRL einen automatisierten und transparenten Berichterstattungsprozess unterstützt; aber die Fragen der Zertifizierung müssen sich noch zusammen mit der Etablierung eines Standards entwickeln.

Gilles Maguet, XBRL Paris

Information Systems Audit and Control Association®

www.isaca.ch

Vier spannende Kurse!

Application Security Lab
Dreitägiger Workshop zum Thema Sicherheit von Web-Anwendungen mit praktischen Beispielen zu HTTP/S; J2EE, Web-Services und Datenbanken
14. - 16. September 2005 in Zürich

Internet Security Lab
Dreitägiger Workshop mit Angriffsszenarien und Abwehrmassnahmen, illustriert mit „Hands-On“-Praxisbeispielen
16. - 18. November 2005 in Zürich

Wirtschaftskriminalität
Unser praktischer Kompaktkurs vermittelt Ihnen die notwendigen Theorie- und Praxisgrundlagen für das Krisenmanagement sowie die Aufdeckung und Analyse von Wirtschaftsdelikten
19. - 20. September 2005 in Zürich

ITIL Foundation Training
Service Management auf der Basis des de-facto Standards ITIL, mit übersichtlichem Prozessmapping ITIL – CobiT und Links zur BS 15000-Zertifizierung
28. - 30. September 2005 in Zürich

Weitere Informationen erhalten Sie in unserem Kurssekretariat

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

Biometrie

Leveraging the Use of Biometrics

Introduction

Concrete evidences for the growth in biometrics are starting to emerge. According to market research group Frost & Sullivan, the biometrics market will reach a phenomenal $2.05 billion by 2006. Such figures are backed up by three primary reasons as to why a business should adopt biometrics:

- to improve an organisation's security by providing positive identification of individuals accessing their premises and networks
- to save large sums of money by significantly easing user provisioning and password management
- to increase usability and convenience to staff.

The following article points out some basics about how biometric systems work, what kind of issues they face and what are actual research topics in this area which are currently on the way of being used on a wide scale.

Short Introduction to Biometrics

Explained simply, biometrics is the statistical analysis and measurement of human traits or characteristics. Once these measurements have been taken, they may then be used to authenticate an individual user. This is done by comparing the sampled geometric against a template taken earlier.

In general, biometric methods can be segregated into two main categories:

- Phenotypic or Behavioural – Phenotypic traits are one that we develop or acquire over time through our own individual experiences, such as pronunciation or handwriting which are used in techniques as voice recognition or signature verification.
- Genotypic (genetic) of Physical – Genotypic identification is the use of individual genetic traits to identify a person. This would include such things as fingerprint analysis or facial recognition.

For the use of identifying users, basically both biometric methods can be used. However, there can be differences in implementing them for different applications as we will see below.

The Use of Biometrics for Authentication

An essential aspect of security is the concept of authentication – the ability to prove that someone or something is what it claims to be. In the systems' security area there are three commonly accepted types of user authentication:

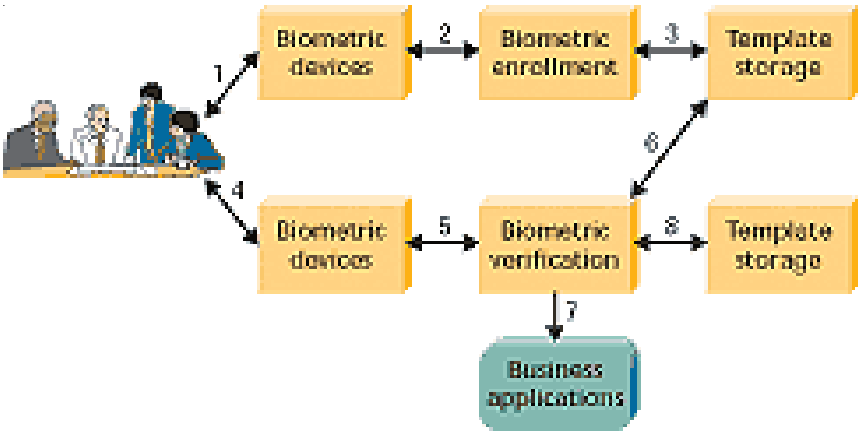
- Something you have – keys, tokens, smart cards or digital certificates
- Something you know – passwords, personal identification numbers (PIN) or other personal information such as your pet's name or mother's maiden name
- Something you are – a biological trait (a biometric)

At first glance, biometrics appears to be the most secure and appealing of the three options. It is nearly impossible to steal or falsify one's genetic traits.

In addition, they cannot be lent to another user and they cannot be forgotten. In most cases, they are not intrusive and are convenient to the end user. Nevertheless, some issues remain, like we will se further on in the text.

How a Biometrics System Works

The following picture from „A Practical Guide to Biometrics Security Technology" [2], depicts the way, a biometric system works:



(1) Capture the chosen biometric; (2) process the biometric and extract and enroll the biometric template; (3) store the template in a local repository, a central repository, or a portable token

such as a smart card; (4) live-scan the chosen biometric; (5) process the biometric and extract the biometric template; (6) match the scanned biometric against stored templates; (7) provide a matching score to business applications; (8) record a secure audit trail with respect to system use.

The problem that all biometric security access procedures and devices still have in common, is the necessity of establishing fault tolerance limits of the matching process: When the fault tolerance limits of the matching algorithm are set very narrowly, the system's security is increased on the one hand, but on the other hand, user-friendliness of the system is likely to decline in proportion (False Rejection Rate – FRR). Are on the other hand parameters set in a way that the matching algorithm permits considerable deviation, then this will make it easy to use the system, but greatly diminish its protective value (False Acceptance Rate – FAR). It is a subtle task, however, to find the proper balance between the right „amount" of FRR and FAR.

Identification versus Verification

However, before discussion the use of biometrics for authentication, it is important to point out the difference between Identification and Verification:

Verification (1:1)
The main characteristics of a verification technique are that the live-scanned biometric credentials are compared with data of the pre-stored biometric template (one-to-one match). Most devices use the verification method for authentication, where usually a PIN or Pass phrase is needed to unlock the biometric template. It's very appropriate to use phenotypic (behaviour) biometrics for verification purposes.

Identification (1:n)
The identification process on the other hand is much more complex, because the scanned or presented live samples are compared with all biometric templates stored in a database (one-to-many mach). The biometric system therefore keeps checking until it finds a match and is able to declare that it has „identified" you. Depending how „strong" the parameters of the biometric system are, there can be more than one successful match.

In most cases, the identification method is much more resource and time consuming, making it hard, especially for lager organisations with a large size of the database or watch-list, to successfully implement a biometric identification system. In addition, there are some technical security constraints to overcome such as database storage of the pre-stored biometric templates, access control and integrity of these templates as well as transmission issues for either the live sample to the data or the biometric template.

Why should Biometric Systems be Applied

As shortly outlined in the introduction, there are some good reasons for applying biometric systems, where also a business case can be set up. In addition,

- „What's the point of spending a huge amount of money in securing your application, network and perimeter defence if you don't know the users who are assessing them? Obvious little, but this is exactly what most companies are currently doing with using UID's and passwords which can be easily guessed or hacked.
- The UID/password combination is not only relatively insecure; it is also inconvenient for staff and financially inefficient for companies to manage. As everybody knows, passwords are forgotten, lost or compromised on a daily basis, which results in the IT department being bothered for a new code. The cost of maintaining passwords is costly and with this in mind, the ROI on biometrics is commonly realised in a few months' time.

Thus, by leveraging biometrics, convenience for the users could be significantly increased and less money wasted.

Design Considerations in Applying Biometrics for Authentication

For a system that authenticates the identity of an individual by measuring some characteristics of that person and comparing it against a previous stored measurement, there are three possible „locations" for performing this „match":

Match-on-Client
To perform the match on the client is potentially the most unsafe place to match. Beside the fact, that there is a tendency to be always on / always connected, the pre-stored biometric template is probably most prone to attacks via malicious software like viruses, worms of phishing attacks.

Match-on-Server
Where the „match-on-server" solution significantly increases the security of the centralized store of pre-recorded biometric templates and provides improved functionality for recording audit trails, there remains other issues in the area of communication security and responsiveness of the system (usually the data of the live-samples have to be transmitted to the server and the computed response goes back to the client).

Match-on-Token

It is likely the most secure place to match live samples and the biometric templates on a token. This requires storage space and computing power on the token (smart card) used, which could lead to some performance/ quality issues. Nevertheless, privacy issues are greatly enhanced.

Match-on-Token can be seen as the favourable technique to be used in state of the art environments.

Available Biometric Security Access Tools for PCs

The range of biometric security access tools for PCs meanwhile extends from mice and keyboards with integrated fingerprint scanners to webcam solutions whose software is able to recognize the facial features of registered persons to scanners that make use of the distinct iris patters of humans for identifying individuals. When the PC is booted the security software that goes with the tool writes itself into the log-on routine expanding the latter to include biometric authentication. In many instances the screen saver is integrated into the routine thus allowing for biometric authentication after breaks from work while the PC is still running. Sophisticated solutions, moreover, permit biometrically-based security protection of specific programs and/or documents.

One example are IBM's actual ThinkPad notebooks (T42 and higher models), which have a fully integrated fingerprint reader on the keyboard.

A single swipe of the finger allows a sensor to take an image of the fingerprint for biometric identification. A biometric sensor, which is integrated on the keyboard, takes sequential „snapshots" of your finger as it slides over the service. It then „stitches" those snapshots together to form a fingerprint image (combination of a behaviour and genetic imprint). In order to overcome the issues of the „match-on-client" solution listed above, the ThinkPad comes with an Embedded Security Subsystem (ESS) which provides additional functionality like: support for fingerprint reader (securely storing biometric templates), support for wireless security credentials, enhanced security for digital certificate-enabled applications as well as a password manager and multifactor identification.

Selected Research Activities Ready for Being Used

IBM's researchers are working in many areas in the Security and Privacy area, out of which the following two examples of assets have been chosen, which address some challenges faced with biometrics:

- „Sign & Go" – Increase security of signature verification with a dynamic signature verification approach
- Conversational Biometrics – increase reliability of voice prints

Sign & Go – Dynamic Signature Verification

The dramatic rise in identity theft and the growing use of multi-function signature captures devices in the retail sector provides favourable conditions for the deployment of dynamic signature verification (DSV) in retail settings. Reliable authentication and authorization are increasingly becoming necessary for many commonplace activities such as boarding an aircraft, crossing international borders, entering a secure physical location, and performing financial transactions.

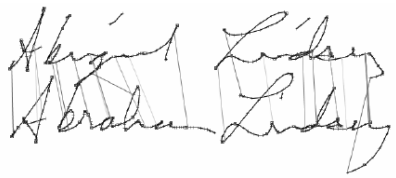
Credit card transactions, however, have used signatures for „authentication" at retail establishment for years, using surprisingly weak security. Each time a customer makes a purchase at a retail store, the cashier may or may not visually compare the offered signature against the reference on the back of the card.

When a subject signs on paper, they leave a static image of their signature. Forgers, who want to falsify a signature, practice the art of reproducing the image (or shape) of a signature, with little regard to the motions that caused the image. Pen motions are ephemeral and are therefore not captured on the paper.

But when signing, the hand can operate in a regime known as ballistic motion, where the muscles are not controlled by sensory feedback. Walking and playing piano are examples of ballistic motions, where the actions are based on prior repeated experience (training), rather than closed loop feedback. Thus, when signing, the hand often moves faster than an individual could volitionally control through hand-eye coordination. This is the area, where dynamic signature verification sets in.
Ballistic motions are generally rapid, practiced motions whose repeatability

increases with speed. When a signature is captured with a digitizer, the pen motions (dynamics) can be recorded such as velocity, acceleration and other dynamic features. This would allow detecting abrupt changes in signature dynamics and resulting in indicating potential fraud.

However, the challenge to a Dynamic Signature Verification system can be stated as follows; given a small set of reference signatures, determine the probability that a new signature submitted for testing is authentic. From this probability a binary (Yes/No) verdict results typically by applying an acceptance threshold to a match probability. Setting the acceptance is a delicate balance of not annoying too many customers with False Rejects, while maintaining enough security to reject all but the most skilled, practiced, or lucky forgers.



Dynamic Time Warping (DTW) is a technique which compensates for minor signature speed variations, normalizing the time duration of signatures, to provide correspondence between points in offered signatures and points in reference signature. The algorithm identifies the best monotonic map between points in the test signature and points in the reference signature, based on some „cost function“. The result may be interpreted as a monotonic curve in a coordinate system in which one axis is the index of the points in the reference, and the other axis is the index of points in the test signature. The process also results in a cost value, which reflects the quality of the alignment and the similarity between corresponding portions of the signature.

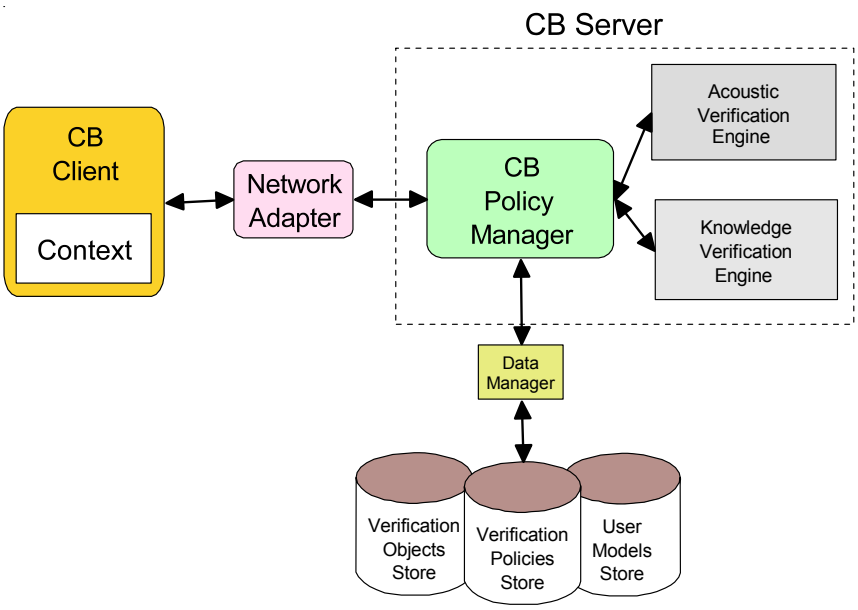
IBM Researchers have developed a dynamic signature verification system and proved that it is possible to reach an Equal Error Rate (ERR) on skilled forgeries and authentic signature of 1.5% to 4% using commercial point-of sales hardware and the DTM algorithm mentioned above [4].

Speaker Recognition with Conversational Biometrics

Conversational Biometrics (CB, see also [5]) combines powerful and accurate acoustic text independent speaker recognition with additional verification sources such as spleen knowledge to create more flexible and robust user verification and detection solution. Therefore, a system that uses CB does not necessarily accept a user solely on the basis of single identity evidence, but may prompt the user to provide multiple and additional source of identity evidence until the rules mandating the security policy be satisfied. By prescribing a tighter policy, the user's identity can be verified to a very high degree of certainty. On the other hand, for low risk transactions, user verification can be performed in an efficient and cost effective manner.

When user verification is performed by a conversational system such as an automated voice response unit, the rich information present in the user's voice should be used for user verification. A user's voice conveys both knowledge (content) and a biometric indication of the user's identity. CB uses the same speech signal to verify both the user's knowledge and the user's voice. Every user utterance is shipped to a text independent speaker recognition engine for automatic voiceprint analysis, as well as a speech recognition engine that extracts the spoken text.

Based on the security policy, a CB Policy Manager (CBPM) decides at any point of interaction with the user whether to elicit more speech from the user, accept the user, or reject. Every new utterance is analyzed both for content (spoken text) and for speaker characteristics (biometrics). The CBPM



can be used to combine acoustic verification with knowledge verification. However, it actually provides a much broader framework that allows to dynamically combining any multiple verification sources, such as possession-based verification (e.g. key, caller-ID) and other types of biometrics (e.g. fingerprint, iris).

The CBPM is a framework that allows dynamic generation of verification challenges on the fly, such that the verification session will obey a predefined security policy. It has access to a pool of possible verification challenges, or Verification Objects (VOs). Examples of a VO include knowledge topics (mother's maiden name, favourite colour, application – specific topic), possession – based VOs (caller-id or key), and different biometrics (fingerprint, keyboard stroke, retina). A security policy is a Finite State Machine (FSM) that at each state includes either a specific VO or a list from which a VO will be randomly chosen at run time. The FSM always ends in either acceptance or rejection of the user.

Conversational Biometrics may be used for user verification and fraud prevention. It can also be used together with existing rule -based and neural network transaction analysis fraud detection systems. For example, the acoustic speaker recognition engine can be used to determine the user identity in non-repudiation cases. It can also efficiently analyze large amounts of recorded audio to detect „familiar" voices from previously detected fraud cases.

Conclusion

There is always a trade-off between security and convenience. An unlocked car with the keys in the ignition is very convenient to use, but also easy to steal. Banks who issue credit cards want their customers to use their cards frequently, while minimizing their exposure to fraud.

The use of biometrics obeys the same rule, making it necessary to well balance risks and investment costs. Where this article has shown that there are biometric technologies ready for use, there is still much to clarify form an operational perspective. Learning of experiences made with the roll-out of other technologies in the past, such as Public Key Infrastructure (PKI), clearly shows that too much attention being given at device level and not enough to the broader operational perspective will result in missing the targets and therefore successful implementation of biometric system will fail. End-user psychology must be investigated seriously and human factors have to be taken fully into considerations. Biometric is an emerging technology, don't spoil successful implementation by looking slanted towards technology only.

Christoph A. Burkhardt,
IBM Schweiz

References:
[1] „Biometrics: An In Depth Examination", Kyle Cherry, SANS Institute 2004, Information Security Reading Room
[2] A Practical Guide to Biometric Security Technology, Simon Liu and Mark Silverman, http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm
[3] „e-Passports – Part 1", Biometrics Technology Today, June 2004
[4] Retail Applications of Signature Verification, Thomas G. Zimmerman, Gregory F. Russel, Andre Heilper, Barton A. Schmith, Jianying Hu, Dmitry Markman, Jon E. Graham, Clemens Drewer, SPIE Defense and Security Symposium 2004, Orlando, Florida, April 15, 2004
[5] A PROGRAMMABLE POLICY MANAGER FOR CONVERSATIONAL BIOMETRICS, Ganesh N. Ramaswamy Ran D. Zilca Oleg Alecksandrovich, Eurospeech 2003, Geneva

Aus der Praxis

Revenue Assurance – A first cut

Zusammenfassung

Inhalt des Artikels ist die kurze Darstellung eines Revenue Assurance Projektes zur ersten Aufnahme von Schwachstellen. Ausgehend davon sind inhaltliche Abgrenzung, Projekt Management, Vorgehensmethode sowie Anhaltspunkte für die Potentialanalyse skizziert.

Wesentliche Erkenntnis ist, dass ein derartiges Projekt direkt vom CFO gesponsert wird, thematisch abgegrenzt ist, ein interdisziplinäres Team aufgestellt ist, die Ausgangsrisiken definiert sind und Klarheit über die Bewertung der Leakages herrscht.

Scope

Revenue Assurance Projekte definieren sich durch Randbedingungen wie technisches Umfeld, wirtschaftliche Situation, involvierte Standorte, Länder, Sprach- und Zeitzonen, „Fertigungstiefe“, Komplexität der Produkte/Produktionsanlagen usw., beinahe obligatorisch erscheinen da die Forderungen nach der thematischen Abgrenzung, dem klarem Auftrag und den erwarteten Ergebnissen.

Die unter Revenue Assurance verstandenen Inhalte sind zudem nicht fest und variieren je nach Situation, Hersteller, Berater und Rolle im Unternehmen. Allgemeine Themen sind zum Beispiel Product definition, Good Standing, Rating, Billing, Reconciliation, Dunning, Fraud, Subscription, Lost orders, Customer satisfaction, Tool selection etc.

Der Projektauftrag sollte klar formuliert sein, zum Beispiel die Feststellung, ob alle erbrachten Dienste leistungs- und vertragsgemäß bezahlt wurden/werden.

Ergebnisse sind in jedem Falle die kalkulierten Verluste, Schwachstellen in der Kontrollumgebung und daraus resultierende Empfehlungen für organisatorische Anpassungen. Ebenfalls sollte vorab die „Kalkulation“ der Verluste definiert werden. Je nach Sichtweise und Interpretation ergeben sich erfahrungsgemäß sehr differenzierte Blickwinkel auf die Verluste.

Parallel zur Abgrenzung des Projektes ist es ratsam, alle wesentlichen Ansprechpartner vorab durch das C-Level (CEO, CFO, CIO, etc.) Management zu instruieren. Außerdem muss sichergestellt sein, dass Ansprechpartner mit Fachkenntnissen (IT, Produkte, Prozesse) real verfügbar sind.

Erfahrungswerte zeigen, dass trotz der oben empfohlenen thematischen Eingrenzung von komplexen Systemumgebungen und Prozessen auszugehen ist. Einer der Kernpunkte ist die angemessene Kommunikation. Mehr als in anderen Projekten (Systemeinführungen, etc.) hängt der Erfolg davon ab, in welchem Maße es gelingt, Fragestellungen angemessen zu kommunizieren und sich auf die unterschiedlichen Gegebenheiten in den Unternehmensbereichen einzustellen. Empfehlenswert ist ein multidisziplinäres Team, welches gleichermaßen durch Interne und Externe besetzt ist. Der CFO sollte als Sponsor die Notwendigkeit des Projektes unterstreichen.

Die permanente Unterstützung durch das C-Level Management in jeder Phase des Projektes sowie ein angemessenes Risiko Management sind ebenfalls kritische Erfolgsfaktoren. Insbesondere bei der Bewertung einzelner Sachverhalte/Leakages kommt es auf Unterstützung an. In regelmäßigen Steering Committees müssen die „wesentlichen Revenue Streams“ durch geeignete Personen vertreten sein.

Methode

Vereinfacht dargestellt sind folgende wesentliche Schritte notwendig, um Revenue Leakages aufzuspüren:

- Risiken abgrenzen/ermitteln,
- Risiken bewerten/Maßnahmen ableiten, und
- Verluste kommunizieren.

Für die Identifikation von Schwachstellen gibt es keinen Königsweg. Üblich sind Risikoanalysen deren „Startpunkt“ sich aus der jeweiligen speziellen Situation vor Ort ergibt. Grundsätzlich lassen sich zum Beispiel neue Produkte, wichtige Bilanzpositionen, IT-Architektur, Best Practise, etc. als Ausgangspunkte festhalten. Bewährt haben sich dabei industriespezifische Risikolisten. Darin sind die häufigsten in der Branche festgestellten/vermuteten Schwachpunkte beschrieben.

Große Beratungs- und Wirtschaftsprüfungsgesellschaften und Spezialisten verfügen im allgemeinen über branchenspezifische Risikolisten. Allerdings liegt dabei nicht immer der Fokus auf Revenue Assurance. Daher ist es der Sache dienlich, diese Listen vorab kritisch durch das Projekt Team prüfen zu lassen.

Wenn keine Erfahrungswerte vorliegen und nicht mit externer Unterstützung gearbeitet wird, dann ist es notwendig, die Risiken in Workshops zu entwickeln. Es ist in jedem Fall empfehlenswert, vorab sicherzustellen,

dass die gewonnen Erkenntnisse in einen geregelten Management-Kreislauf fließen und für Folgeuntersuchungen zur Verfügung stehen.

Bei den Analysen hat es sich bewährt, vermutete Schwachstellen „längs“ der Wertschöpfungskette zu evaluieren. Bei dieser umfangreichen Untersuchung werden die Risiken Schritt für Schritt durch nahezu alle Applikationen, Interfaces, Billing Prozesse (Registration, Good Standing, Rating, Collection, Dunning, Termination, etc.), Netzwerke und Departments überprüft. So lassen sich die wesentlichen Revenue Streams identifizieren, kritisch die entscheidenden Prozessgrößen hinterfragen („What could go wrong?“) und dokumentieren. Für die Kommunikation der Ergebnisse ist es sehr empfehlenswert, Risiken durch Stichproben zu erhärten (run to run samples), beziehungsweise konkrete Beispiele aufzuzeigen.

Die einzelnen Risiken lassen sich inhaltlich beziehungsweise Stream bezogen gruppiert in einem Risiko Portfolio zusammenfassen um so das „big picture“ aufzustellen.

Zeit ist bei den meisten Projekten limitiert, erfahrungsgemäß bewirkt die enorme Komplexität ein hohes Maß an Disziplin, enge Abstimmung und Projekt Controlling. Für die Feststellung, Diskussion und Kommunikation der Risiken sollten vorab angemessene Zeiten und Teilnehmerkreise eingeplant werden.

Es ist empfehlenswert und notwendig, binnen kürzester Zeit reaktive Maßnahmen zu implementieren, um akute Verluste zu verhindern. Gleichzeitig sollte die Umsetzung zukunftsorientierter Maßnahmen in Betracht gezogen werden.

Dies sollte jedoch im Gegensatz zu den reaktiven Maßnahmen zeitversetzt erfolgen, denn die Organisation ist zunächst mit der Umsetzung der reaktiven Maßnahmen beschäftigt. In der Regel lassen sich die Fachabteilungen nach erfolgreicher Umsetzung besser für proaktive Aktivitäten „gewinnen“.

Potential

Generell gilt ein Schätzwert von circa 5% für den Verlust vom Gesamtumsatz. Hersteller von Tools und Anbieter von Dienstleistungen stellen teilweise bis zu 15% Verlustpotential in Aussicht. Eine so hohe Verlustrate ist in Einzelfällen möglich. Generell hat sich jedoch gezeigt, dass der tatsächlich nachweisbare Verlust bei circa 3% liegt. Hohe Revenue Assurance Potentiale gehen oft einher mit schwachen Kontrollumgebungen. Daher lassen sich die oben genannten „Erfahrungswerte“ anhand des eigenen Kontrollsystems „abschätzen“. Oft sind die Unternehmen besser als bei Projektstart zunächst angenommen.

Andere typische Merkmale für die Potentialanalyse sind Massendaten, die Anzahl der Produkte, Kundenstruktur, Preismodelle/Tarife, zeitliche Abfolge neuer Produkte, Technologiewandel, Time to Market, Legacy Systems/Zugriff auf deren Daten, verteilte Systemwelten, Datenkonsistenz, Anzahl der Schnittstellen Abfolge der Verarbeitung und Menge der transportierten Daten.

Grundsätzlich lässt sich Revenue Assurance wie eine gewöhnliche Investition betrachten. Bei circa 3% bis 5% Potential vom Umsatz und den oben genannten Parametern ergeben sich ausreichend Ansatzpunkte für eine „Investition“.

Revenue Assurance hat sich in der Vergangenheit aus den Gegebenheiten der Telcos und der ISPs entwickelt. Dennoch nimmt das Bewusstsein für die Thematik zu. Es gibt viele vergleichbare Zusammenhänge in anderen Wirtschaftsbereichen. Dies sind zum Beispiel Versorger (Gas, Strom, Öl, Wasser), Retailer, Logistics, Supply Chain Management, Banken, Autovermietungen, Behörden und Credit Card Provider.

Marc Weber, CISA
AOL Deutschland GmbH & Co. KG

Express Line

A Word from the Chair

As the incoming chair of the Membership Board, I welcome all new chapter officers Registration for the December Certified Information Systems Auditor™ (CISA®) and Certified Information Security Manager® (CISM®) exams will close on 30 September 2005.

To keep all members on the same schedule, ISACA has determined that nonmember exam passers will receive notification in August that they have been granted a free trial membership for the remainder of the calendar year. For example, June 2005 exam passers are receiving a free trial membership beginning this month, and December 2005 and June 2006 exam passers will receive a free trial membership beginning in August 2006.

Steve Thorsted
Chair, Membership Board

CobiT Foundation Course Launched

The IT Governance Institute® (ITGI) and ISACA recently released the CobiT® Foundation Course, a self-paced, electronic tutorial developed by ITpreneurs, a leading provider of training solutions in the area of IT management and control best practices, to help IT professionals become skilled at using Control Objectives for Information and related Technology (CobiT®) within their organizations.

The CobiT Foundation Course features case studies; real-world examples; an overview of CobiT's control objectives, control practices, management guidelines and audit guidelines; and 40 sample questions that help prepare users for the CobiT Foundation exam. Additional information is available at www.isaca.org/cobitcampus.

Practical Steps

Visit www.isaca.org/bookstore and take advantage of our secure online ordering, or see the Information Systems Control Journal® Bookstore insert for additional information. Contact the Bookstore at bookstore@isaca.org or +1.847.253.1545, ext. 401 or 478, with any questions.

News Briefs

Damianides Featured in Sarbanes-Oxley Webcast

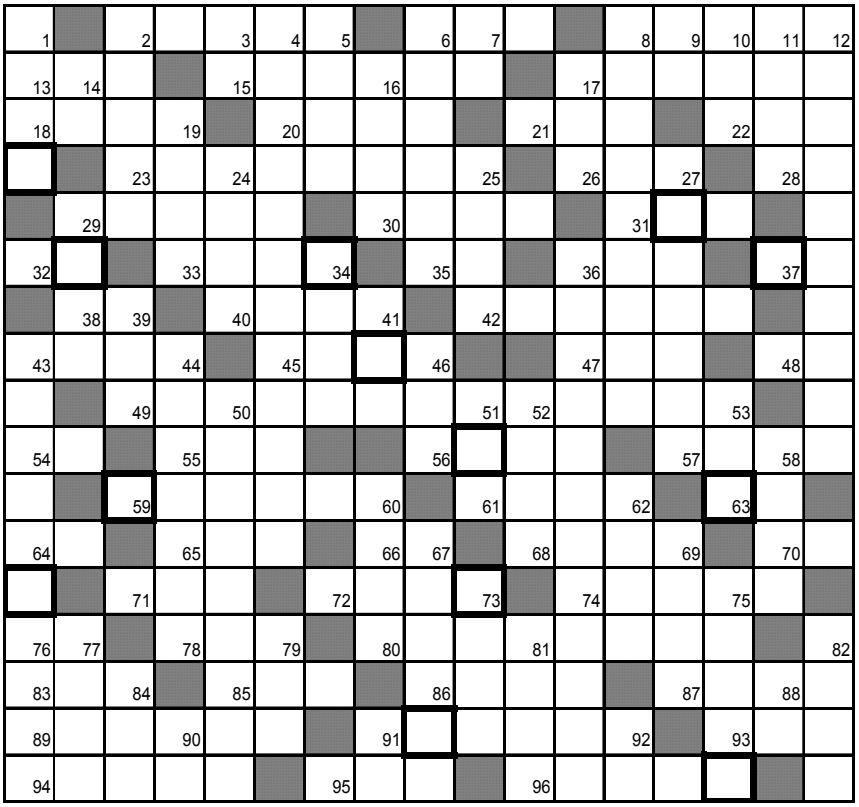
Marios Damianides, CISA, CISM, CPA, CA, 2004-05 international president of ISACA, was recently featured as a panelist in an InformationWeek webcast titled „The Road Ahead: Living With Sarbanes-Oxley…Forever." The webcast is available for viewing until 12 November 2005 at https://www.cmpnetseminars.com/BTG/default.asp?K=3IK6A&Q=244. The panelists discussed how companies performed in year one of Sarbanes-Oxley, additional reporting requirements, techniques for improving compliance, how to justify budgets for ongoing compliance and looking to the future.

There was an eager young audit assistant named Grace
Investigating fraudulent books, arsenic and very old lace.
She encountered a bloody mess,
As anyone could easily guess,
And used to call it a stupid old problem of interface.

Eine Revisorin mit dem hübschen Namen Belle
Suchte und fand die Fehler meistens an deren Quelle
Manchmal aber – ein wirklicher Hit –
Traf sie auf einen gewaltigen Schnitt
Anstelle der Quelle, aber doch eine verwundbare Stelle.

The ISACA Crossword Puzzle 4/05

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



Waagrecht: 2 Deckel; 6 der Bruder von Jaffet kommt auch beim englischen Frühstück vor; 8 manche mögen es so; 13 amerikanischer Geheimdienst (Abk); 15 Glied (engl); 17 Gewässer in Bayern; 18 englischer Hase; 20 irischer Männername; 21 der Musiker würde dem frz Fürwort wahrscheinlich B sagen; 22 kurzer engl Vorname; ***23 sollte die 49 waagrecht überwachen;*** 26 engl Bejahung; 28 launischer Ausruf; 29 neuseeländischer Ureinwohner; 30 inhaltslos; 31 neue Partei Deutschlands; 32 spanisches aromatisches Getränk; 33 männliches Nutztier; 35 Rekrutenschule; 36 United Federal Internet; 37 oft im österreichischen Internet anzutreffen; 38 frz Artikel; 40 dem Heidekraut fehlt das K; 42 Wurfkörper (Mz); 43 Wintersportgeräte; 45 legendärer lettischer Eishockey-Torhüter; 47 leeres Gerede; 48 pers Fürwort; ***49 Schwerpunktthema***; 54 die deutsche Vorsilbe ist auch im Welschland anzutreffen; 55 chinesische Dynastie; 56 da; 57 nordischer Hirsch; 59 Dozent und Student können es gleichsam sein; 61 immer lautlos; 63 herzloses Ego; 64 hohe Spielkarte; 65 lautloser Strom vom Gotthard zur Nordsee; 66 Vorwort; 68 schwäbischer Flur; 70 der Kanton ist auch eine Gesellschaftsform; 71 Düsenflugzeug; 72 griech Philosophenschule; 74 vietnamesisches Zentralland; 76 ultraviolett; 78 Elend; ***80 von da weg sollte 49 waagrecht kontrolliert sein;*** 83 kurzer release; 85 Lebensende; 86 so schreibt sich wohl der langjährige Präsident Indiens neu; 87 Windrichtung; 89 Hauptstadt Armeniens; 91 klein; 93 Maschinenteil; 94 wird sprichwörtlich im Heuhaufen gesucht; 95 deutsches Adelsprädikat; 96 alte Wiese.

Senkrecht: 1 Widerhall; 2 normalerweise schreibt der Spanier das Saiteninstrument ohne H; 3 Konjunktion; 4 Damen aus Westeuroopa; 5 arabischer Fürst; 6 Bremse; 7 Flächenmass; 8 Kleid von Meister Lampe; 9 Europameisterschaft; 10 Bestand; 11 Hilfszeitwort; ***12 so entstehen Missverständnisse;*** 14 im Auftrag; 16 vorderasiatischer Gott; 17 spanischer König; 19 Held (it); 24 Ort im Waadtland; 25 Chaos (engl); 27 gewundene Form; 29 Stift an der Donau; 34 Produkt aus Mendrisio; ***36 Vorgang, bei dem 49 waagrecht eine wichtige Rolle spielt;*** 39 Aggregatzustand des Wassers; 41 Klostervorsteher; ***43 elektronische solche können 49 waagrecht absichern;*** 44 Schneidewerkzeuge; 46 Zürichs MIT; ***50 auch dies kann 49 waagrecht absichern,*** 51 kurze englische Schwester; 52 Truppenspitze; 53 Erzieher Samuels; 58 Ort am Zugersee; ***60 dies fliesst über 49 waagrecht (engl);*** 62 Wallensteins Berater; 67 Klosterfrauen; 69 vier gleiche Buchstaben; 73 Einspruch; 75 unbewegt (zwei Wörter); 77 die Wahre; 79 Laut; 81 Stadt und See in Nordamerika; 82 nordische Sagensammlung; 84 Augendeckel: 88 ägypt Sonnengott; 90 engl pers Fürwort; 91 jap Brettspiel; 92 Generalagentur.

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 24. Oktober 2005.

Solution 3/05: RULE OF THUMB (also some kind of fingerprint…)

Across: 1 ***vulnerable***; 10 kerb; 13 OTP; 14 mace; 15 ***retina***; 18 i.e.; 19BU; 20 etc; 22 bandy; 24 XL; 25 es; 26 bobbin; 29 RS; 30 Ei; 32 inn; 35 us; 36 bi; 37 monogram; 41 IS, 42 pale; 44 card, 45 linear; 47 pills; 48 HGO; 49 LA; 50 its; 51 mind; 52 (s)u(r)e; 53 ***fingerprint***; 54 ah; 55 ***hand***; 56 rye; 57 re; 58 olé; 59 black; 61 soccer; 63 anew; 64 Yale; 65 Ho(hoho); 66 stronger; 68 SF; 69 Ea; 71 rua; 72 TS, 74 (Aloha) Oe; 75 admire; 78 SS; 79 IQ; 80 grand; 82 Goa; 84 an; 85 zu; 86 enable; 89 Amur; 91 bel; 92 rare; 93 ***fortresses***.

Down: 1 ***voice***; 2 Ute; 3 LP; 4 emu; 5 Ra; 6 aces; 7 bet; 8 er; 9 ET; 10 Knan; 11 EAN; 12 boys; 16 ebb; 17 ibis; 19 ***blind***; 21 CB; 23 drill; 25 England; 27 Ob; 28 bus; 31 ***image***; 33 no; 34 paniero; 36 bald; 38 oro; 39 ri; 40 ***metrics***; 41 ir; 42 pint; 43 eschew; 49 link; 51 mirrors; 53 face; 54 alert; 55 half; 58 one; 60 ***laser***; 61 so; 62 ER; 63 again; 65 ham; 67 nu; 69 Edda; 70 FR; 73 ***souls***; 73 oger; 75 Anne; 76 ill; 77 e.g.; 78 Samt; 81 aer; 83 oar; 84 are; 85 zee; 87 BC; 88 EF; 90 Ur; 91 BS.

Watson: Of the entire alphabet, the letter J is the only one not contained in the crossword puzzle.

There were not enough solutions. The Jackpot is $US 100.00.

General Motors Corporation

General Motors Audit Services provides independent internal controls assessment services for GM's global operations, including all majority-owned subsidiary companies. To strengthen our team we are looking for a self-motivated individual for the position of

SENIOR INFORMATION TECHNOLOGY AUDITOR

The qualified candidate will perform a wide variety of IT reviews, covering infrastructure, systems development, e-business, application and ERP systems; as well as support integrated business process audits in the automotive and financial services area. The position would be based at the Opel Headquarters in Rüsselsheim, Germany, reporting to the IT Audit Manager.

Required experience and qualifications include three to five years of information systems audit experience and/or other related control and security experience, preferably in a large multinational organization; knowledge of generally accepted IT audit and IT security standards and control practices; strong communication (both verbal and written) and interpersonal skills; and the ability to travel up to 80 %.

Interested candidates should send applications with a detailed CV to Vicki Keen, Executive Assistant, GM Audit Services, Victoria.Keen@gmacio.com.

Standards

CobiT goes EU

Die EU-Kommission hat die Control Objectives for Information and related Technology (CobiT) als einen von drei akzeptierten Standards zur IT-Sicherheit festgelegt.

Im Zuge der Änderung von Durchführungsbestimmungen beim Rechnungsabschlussverfahren des Europäischen Ausrichtungs- und Garantiefonds für die Landwirtschaft (EAGFL) hat die EU-Kommission im März die Anforderungen an die Vertraulichkeit, Vollständigkeit und Verfügbarkeit von Computerdaten konkretisiert. Statt einer allgemeinen Forderung „angemessener Verfahren“ muss sich die Sicherheit von Informationssystemen nun „auf die Kriterien … eines der folgenen internationen Standards“ stützen: ISO 17799/BS7799 „Code of pratice for Information Security Management“, das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder die ***Control Objectives for Information and Related Technology (CobiT) der Information Systems Audit and Control Association (ISACA)***.

IT Governance Institute

„Diese Verordnung ist ein grosser Schritt nach vorne, um Informationssysteme in der ganzen EU in höherem Masse schützen zu können“, erklärte hierzu Georges Ataya, Leitungsmitglied des IT Governance Institute (ITGI, www.itgi.org). Diese Einrichtung wurde 1998 gegründet, um das Bewusstsein von Unternehmen im Hinblick auf die Kontrolle der Informationstechnik zu schärfen und die Entwicklung internationaler Standards in diesem Bereich voranzutreiben. ITGI bietet Symposien, Grundlagenforschung und Fallstudien an, um den Führungskräften und den Vorständen von Unternehmen bei der Verantwortung für die Sicherheit ihrer Informationsysteme zu helfen.

Gutes Beispiel

Ataya, der auch Professor an der Solvay Business School in Brüssel ist, führte weiter aus: „Alle Unternehmen und Organisationen sollten schon zum Schutz ihrer Kunden, Auftraggeber und Angestellten internationale Systemsicherheitsstandards berücksichtigen – unabhängig davon, ob öffentliche Einrichtungen oder Privatunternehmen.“ Die Institutionen der Europäischen Union gehen nun mit gutem Beispiel voran. Vor allem die Dienststellen des EAGFL, die für die Auszahlung der Subventionen im Agrarsektor zuständig sind, wurden angewiesen, rückwirkend zum 16. Oktober 2004 einen der drei genannten Standards zu erfüllen.

Die Generaldirektion Landwirtschaft und ländliche Entwicklung der Europäischen Union, die im Jahre 2004 mit 98 Milliarden Euro rund die Hälfte des gesamten EU-Budgets verwaltete, hatte die Wichtigeit eines umfassenden IT-Sicherheitsmanagements bereits frühzeitig erkannt und sich schon 2001 für CobiT entschieden. Seitdem arbeitet das IT Governance Institute eng mit der Generaldirektion Landwirtschaft und ländliche Entwicklung zusammen und führt für die Auditoren regelmässig Schulungen durch.

Die neue EU-Verordnung Nr. 465/2005 legt nun fest, dass Auditoren ab dem Haushaltsjahr 2008 einen Nachweis über die Sicherheitsmassnahmen auf der Grundlage der jeweils angewendeten Standards zu erbringen haben. Während der Haushaltsjahre 2004 bis 2007 müssen die Prüfungsberichte eine Bewertungsziffer für jeden Bereich des gewählten Standards auf der Grundlage des Maturity Modells enthalten, das direkt aus dem CobiT „Generic Proces Maturity Model“ entwickelt wurde.

Die Verordnung steht in den 19 offiziellen EU-Sprachen auf Seite 6 des Amtsblatts der Europäischen Union unter http://europa.eu.int/eur-lex/lex/JOHtml.do?uri=OJ:L:2005:077:SOM:DE:HTML oder (auf Deutsch) direkt via http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32005R0465:DE:HTML zur Verfügung.

CobiT liegt mittlerweile in Release 3.2 vor, besteht aus gängigen generell akzeptierten Praktiken (Best Practices) und dient der Steuerung und Überwachung der Sicherheit von Informationstechnik. Materialien zu CobiT liegen auf www.isaca.org/cobit/ zum freien Download bereit.

Karin Thelemann,
Präsidentin ISACA Germany Chapter

DACH-News

D: Aktivitäten des German Chapters

In den letzten Monaten wurde im Hintergrund intensiv von unserem Vorstandsmitglied Heinrich Geis an dem neuen Webauftritt des ISACA German Chapter gearbeitet. Nun ist es soweit und unsere neue Homepage ist online. Die Adresse hat sich nicht geändert, die Seite ist weiterhin unter www.isaca.de zu finden. In der nahen Zukunft wird es noch weitere Neuerungen inhaltlicher Art auf unserer Seite geben, aber wir wollen natürlich nicht zu viel vorwegnehmen – schauen Sie einfach ab und an einmal vorbei.

Da CobiT im letzten und diesen Jahr immer mehr an Popularität gewonnen hat, haben wir zwei wirklich interessante Angebote mit professionellen Seminarveranstaltern zum Thema CobiT ausgehandelt. Die beiden Veranstalter sind Management Circle sowie Serview mit einem ein- bzw. zweitägigen Seminar. Auch für weitere Seminare des Anbieters Serview haben wir entsprechende Rabatte ausgehandelt. Weitere Informationen hierzu finden Sie auf unserer Website.

Unsere CISA-Kurse sind auch dieses Jahr wieder erfolgreich in Frankfurt und Mannheim gelaufen. Erstmalig wurde das Testexamen neben Frankfurt auch in Hamburg angeboten. Allen CISA-Kandidaten drücken wir für die bevorstehende Prüfung die Daumen und hoffen, dass die Ergebnisse unserer Teilnehmer so erfolgreich wie in den Vorjahren sein werden.

Ingo Struckmeyer,
Vorstand ISACA Germany Chapter

CH:

Gratulation

Einmal mehr haben wir allen Grund, auf unser Mitglied Urs Fischer stolz zu sein. Er schreibt uns:

Lieber ISACA Vorstand

For your information. Gruss Urs

P.S. Als erstes nicht US-amerikanisches Mitglied des Audit Committee in der Geschichte der ISACA und des IT Gov. Institutes.

Und dies aufgrund folgender Mitteilung, die seine Mailbox erreichte:

Greetings,
As a membership-based organization, ISACA is dependent on the contributions made by its many volunteers. In preparation for each new administrative year, members are invited to submit their applications to serve on ISACA/ITGI key boards and committees. Based on these applications, and recommendations from the Boards of Directors/Trustees, key board chairs and appropriate chapter presidents, the composition of each key board or committee is finalized, with a balance sought between continuity of membership and the need for new views, including expertise in strategic areas.

It is with great pleasure that Everett Johnson, 2005-06 International President, invites you to serve on the ***Audit Committee*** for the upcoming administrative year. In order for us to formalize your appointment, please signify your willingness to serve by replying to this e-mail. Kevin Weston has agreed to chair the 2005-06 committee. You will soon be receiving various orientation materials from the staff liaison assigned to this committee. Included will be goals for the upcoming year, meeting/conference call schedules, minutes from previous meetings, and various other materials to assist you throughout your 2005-06 year of service.

Best regards, Bill Lewis, Executive Assistant, Information Systems Audit and Control Association,
IT Governance Institute

Urs Fischer hat (natürlich) akzeptiert.

Schon wieder ein Kompliment!

On behalf of the Membership Board, I am pleased to extend congratulations to the Switzerland Chapter for achieving recognition for your web site. Your chapter has been awarded a Silver level award. You should be proud of the work your chapter has put forth in the design, content and management of your chapter web site in order to earn this recognition.

Each year the ISACA International membership board reviews all of the chapter web sites that link from the ISACA web site. The criteria used when selecting the winners is available on the awards page of the chapter leader area of the ISACA web site. We encourage you to review the criteria periodically to assist in your chapter's web site development and to strive for the gold level award next year.

Please accept our congratulations on a job very well done by you and your chapter board.

Sincerely, Megan (Maynard) Moritz
Chapter Relations Coordinator

Fachstab für Informatik der Treuhand-Kammer

Die Mitglieder des Fachstabes für Informatik der Schweizerischen Treuhandkammer erachteten den Leitfaden der CNCC als wertvoll und übersetzten ihn. Er ist besonders hilfreich bei der Umsetzung des Prüfungsstandards 401.

Les membres du Fachstab ont estimé que le Guide élaboré par le Compagnie nationale (française) des commissaires aux comptes (CNCC) constitue un excellent ouvrage de vulgarisation, facilitant l'intégration de la dimension informatique dans l'audit des comptes annuels. Ce document contribue à l'application pratique des Normes d'audit suisses, en particulier de la norme 401.

Der Leitfaden kann unter folgender Adresse heruntergeladen werden:

http://www.treuhand-kammer.ch/pix/files/Guide%20CNCC%20D%20V21.pdf

La version française peut être commandée sous forme papier auprès de la CNCC (www.cncc.fr)

Einladung CISA/CISM

CISA bzw. CISM Prüfung im 2005 in Zürich absolviert und ***erfolgreich*** bestanden?

Ich lade Sie herzlich zu unserem CISA/CISM-Essen ein.

Wann: 1. Dezember 2005
Ort: Au Premier im 1. Stock des Hauptbahnhofs in Zürich
Zeit: Ab 18.30 Apéro und ab 19.30 Abendessen (Ende um ca. 23.00)

Bitte teilen Sie mir bis am 15. November 2005 via Email mit, wenn Sie am Abendessen teilnehmen möchten (die Platzanzahl ist beschränkt) und informieren Sie mich bitte gleichzeitig ob ein vegetarisches Menu bevorzugen.

Alle anderen CISA und CISM's sind auch herzlichen zum Abendessen eingeladen, müssen das Essen/Trinken aber selbst bezahlen.

CISA/CISM-Koordinator
Thomas Bucher
tbucher@deloitte.com

CISA-Prüfung

Bei Redaktionsschluss eingetroffen: 96% der CISA-Kandidaten aus der Schweiz haben die Prüfung 2005 bestanden. Gratulation! Details im nächsten Newsletter.

News aus den Interessengruppen

IG Operational IT-Risk

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

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

Derzeit werden keine neuen Mitglieder aufgenommen. Wenn die Ergebnisse vorliegen, wird die Interessengruppe darüber informieren.

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

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

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

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

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

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

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

IG Computer Forensics

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

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

informatiques, tous les intéressés de tout niveau de connaissance sont les bienvenus.

IG Einführung von IT-Governance

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

Letzte Sitzung: 4. Juli 2005 bei E&Y, Zürich
Beschluss zum weiteren Vorgehen:
Aus dem IT Governance Implementation Guide werden die Tabelle 14, Seite 24 und das Raster der Pilotprozesse genutzt, um folgende Informationen zu erarbeiten:
1. Auf Stufe Domäne werden a) die Zielsetzungen, b) die Risiken und c) die Chancen in betrieblich verständlicher Form bestimmt.
2. Für die 15 auf Seite 24 aufgeführten Schlüsselfragen werden je 3 bis 8 praxisorientierte Unterfragen definiert, anhand derer die Schlüsselfragen im konkreten Falle beantwortet werden können. Für jede Unterfrage wird – sofern möglich – die Messgrösse/Kontrolle und das Instrument/Hilfsmittel kurz beschrieben.

Bis 28.10.2005 werden die Domänen in Arbeitsgruppen bearbeitet und anschliessen in der IG verteilt.

Nächste Sitzung: 7. November 2005 bei EFK, Bern, 08.30 – 12.30 Uhr
Traktanden:
1. Besprechung und Genehmigung der Arbeitsergebnisse
2. Festlegen Weiteres Vorgehen
Themen, Ziele und Organisation der nächsten Sitzung

IG Romandie

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

IG Outsourcing/Insourcing

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

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

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

IG MIS/EIS/DWH

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

Nach einer längeren Pause hat die IG ihre Arbeit wieder aufgenommen.
- Wrap-Up/Standortbestimmung

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

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

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

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

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

IG SAP R/3

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

Nächste Sitzung: 28. November 2005 in Bern, bei der Eidg. Finanzkontrolle, Monbijoustrasse 45, 09.45–16.45 Uhr ***(bitte anmelden)***
Traktanden:
- Fachpräsentation
- Erfahrungsaustausch
- gemeinsames Mittagessen, dann Führung durchs Parlamentsgebäude und anschliessend auf der Tribüne Miterleben der Herbstsessionseröffnung des Nationalrates ***(Personalausweis mitbringen)***

Neue Interessenten können sich bei Monika Galli, IG-Leiterin, anmelden.

Veranstaltungen

SSI-Fachtagung: Der neue und sichere Arbeitsplatz	13. September 2005 Zürich,1 Tag, MediaSec
Application Security Lab – Workshop zum Thema Sicherheit von Web-Anwendungen	14. – 16. September 2005 Zürich, 3 Tage, ISACA/Compass
Einführung BS7799	19. September 2005 Zürich, 1 Tag, Infosec
Wirtschaftskriminalität – Krisenmanagement und Beweismittelsicherung	19. – 20. September 2005 Zürich, 2 Tage, ISACA/CMC
Vertiefung BS7799	20./21. September 2005 Zürich, 2 Tage, Infosec
Technische Sicherheit	26.–29. September 2005 Bern, 5 Tage, Infosec
After Hour Seminar: Automatisiertes Backup	27. September 2005 Zürich, 16.40–17.40, ISACA
Service Management – ITIL Foundation Training Auf der Basis des de facto-Standards ITIL mit Links zur BS 15000 Zertifizierung	28.–30. September 2005 Zürich, 3 Tage, ISACA/glenfis
Security Awareness & Social Engineering	5. Oktober 2005 Zug, 1 Tag, Infoguard
Praxisgerechte Anwendung des BS7799 / ISO17799	5. – 7. Oktober 2005 Zürich, 3 Tage, ISACA/ ITACS
After Hour Seminar: SOX-light bei der SBB AG	25. Oktober 2005 16.40–17.40, Zürich, ISACA
Network Security	14. – 16. November 2005 Hotel Hilton in Amsterdam 3, Tage, ISACA
Information Security Management Conference	14. – 16. November 2005 Hotel Hilton in Amsterdam 3, Tage, ISACA
Internet Security Lab	16.–18. November 2005 Zürich, 3 Tage, ISACA/Compass
CISA/CISM-Infoveranstaltung	28. November 2005 Zürich, 16.45–18.45, ISACA/ITACS
BS7799 Auditoren-Lehrgang	5.–9. Dezember 2005 Zürich, 5 Tage, Infosec
Evidence Lab – Workshop über die Spurensuche in Computersystemen	7.–9. Dezember 2005 Zürich, 3 Tage, ISACA/Compass
CISM-Vertiefungskurs	12. Januar–16. Mai 2005 Zürich, 12 Tage, ISACA/ITACS
CISA-Vertiefungskurs	16. Januar–15. Mai 2005 Zürich, 14 Tage, ISACA/ITACS

Kontaktadressen Veranstalter

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

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

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

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

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

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

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

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

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

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

ISACA CH Kurssekretariat
c/o ITACS Training AG
Stampfenbachstrasse 40
CH-80006 Zürich
Tel. + 41 44 444 11 01
Fax +41 44 444 11 02
info@isaca.ch
www.isaca.ch

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

ITACS Training AG
Stampfenbachstrasse 40
CH-80006 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

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

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

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

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

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

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

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

Vereinsadressen

Germany Chapter

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

Präsidentin
Karin Thelemann
Tel. +49 6196 99626 488
karin.thelemann@de.ey.com

Konferenzen
Markus Gaulke
Tel. +49 69 9587 2313
MGaulke@kpmg.com

Mitgliederverwaltung und Kassenwart
Norbert Gröning
Tel. +49 201 438 0
Norbert.Groening@de.pwcglobal.com

Public Relations
Heinrich Geis
Tel. +49 692 101 5149
heinrich.geis@deutsche-boerse.com

Arbeitskreise und Facharbeit
Bernd Wojtyna
Tel. +49 251 288 4253 oder
+49 251 210 4539
bernd_wojtyna@gmx.net

Publikationen
Ingo Struckmeyer
Tel. +49 4106 704 2336
ingo.struckmeyer@pf.comdirect.de

CISA-Koordinator
Holger Klindtworth
Tel. +49 (40)41522863
h.klindtworth@susat.de

www.isaca.de

Austria Chapter

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

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

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

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

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

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

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

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

www.isaca.at

Switzerland Chapter

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

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

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

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

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

Sekretär
c/o Präsidentin

Information & Kommunikation
Monika Josi
Tel. +41 61 697 72 41
monika.josi@novartis.com
Adressmutationen bitte hier melden.

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

Représentant Suisse Romande
Paul Wang
Tel. +41 22 748 56 01
paul.wang@ch.pwcglobal.com

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

www.isaca.ch