ISACA Newsletter MÄRZ 2009

ISACA 20 JAHRE ANS ANNI
Serving IT Governance Professionals
Switzerland Chapter

newsletter

After Hours Seminar

Zürich • Dienstag, 31.3.2009 • 16:40 – 17:40
After Hours Seminar und Vereinsversammlung
in den Lokalitäten von Deloitte AG,
General Guisan Quai 38, 8002 Zürich ➜ Seite 6

Focus

Enterprise Rollen – nicht nur eine IT-Herausforderung ➜ Seite 2

Inside

PMBOK 4th Edition ➜ Seite 4

CobiT im Forschungseinsatz
Rückblick auf das AHS-Referat ➜ Seite 5

ISACA-Kurse und -Veranstaltungen

Die aktuellsten Veranstaltungs- und Kursdaten ➜ Seite 7

ISACA Switzerland Chapter • Jubiläumsveranstaltung
25. August 2009 • Zürich

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o ITACS Training AG
Stampfenbachstrasse 40
8006 Zürich
kurse@isaca.ch

Redaktionsschluss
Nr. APR|2009:
5. April 2009

Redaktion:
Michael Kuss
Färberstrasse 27
8008 Zürich
mkuss@gmx.net

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

Editorial

Auch ISACA bleibt von den schlechten wirtschaftlichen Verhältnissen leider nicht verschont. Trotzdem trafen sich rund 220 Teilnehmer an der diesjährigen EuroCACS in Frankfurt vom 16-18. März 2009, je nach Pre- oder Post-Workshop auch länger. Als Mitglied vom Programm Kommittee durfte ich bei der Gestaltung des Programmes dabei sein und mithelfen, geeignete Präsentatoren zu finden. Keine einfache Aufgabe, wenn aufgrund von Vorschlägen auf Papier (Call for Papers) eine Auswahl getroffen werden soll. Sind die Speaker bereits bekannt und wurden an anderen Anlässen von den Teilnehmern positiv bewertet, ist das einfacher. Dieses Jahr kam als zusätzliche Hürde hinzu, dass auch ein paar Referenten von Sparmassnahmen ihrer Firmen betroffen worden sind, da musste kurzfristig Ersatz gefunden werden. Die Stimmung unter den Teilnehmern und das Feedback zur Qualität der Referenten und Inhalten war überwiegend positiv.

Am Wochenende vor der EuroCACS fand das Europäisch/Afrikanische Präsidententreffen statt, ebenfalls mit weniger Teilnehmern als in früheren Jahren, jedoch nicht weniger interessant. Die rund 50 Anwesenden wurden über die neuen Entwicklungen in den Bereichen Membership, Certifications, Research und Committees informiert und es wurde über Social Networks (soll ISACA auf Facebook, etc.), Student Memberships und Membership Retention diskutiert. Über einige dieser Punkte werden wir Sie an unserer Vereinsversammlung vom 31. März 2009 weiter informieren, andere werden später im Newsletter, auf dem Web und in anderen Informationsquellen zu finden sein. Neben all den Sessions und Workshops war wie immer das Networking mit Vertretern aus den verschiedenen Ländern, Firmen und Berufen äusserst interessant. Neue Kontakte zu knüpfen und "alte" Gesichter nach Jahren wiederzusehen sind für mich wertvolle Erfahrungen und Erinnerungen.

Ganz kurz möchte ich hier auf unseren Jubiläumsanlass vom 25. August 2009 hinweisen. Das ISACA Switzerland Chapter feiert sein 20-jähriges Jubiläum und diesen Anlass möchten wir mit Ihnen feiern. Neben einem Seminarteil, voraussichtlich ein Tag, wird es auch einen Abendanlass geben. Sie dürfen sich auf ein interessantes und unterhaltsames Programm freuen - und wir hoffentlich auf eine rege Teilnahme.

Herzliche Grüsse, Daniela Gschwend, Präsidentin

CISA 30 Certified Information Systems Auditor
CISM Certified Information Security Manager
CGEIT Certified in the Governance of Enterprise IT

Focus

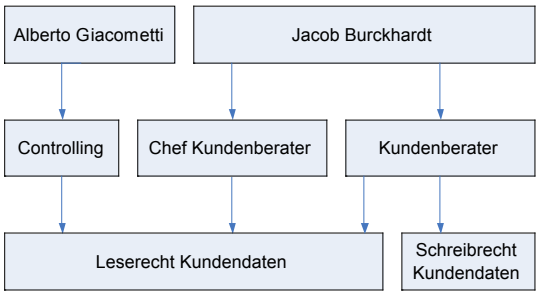
Enterprise Rollen – nicht nur eine IT-Herausforderung

Autoren: Roger Auinger und Falk Hollenwäger

Einleitung

Neben den klassischen Anforderungen im Bereich der Informationssicherheit, wie Vertraulichkeit, Integrität und Verfügbarkeit, gewinnt die Autorisierung als weitere Dimension immer mehr an Bedeutung. Es wird für viele Unternehmen zunehmend unverzichtbar, zu regeln und zu wissen, wer welche Applikationen benutzt und wer auf welche Daten zugreifen darf.

Diese Autorisierung zu steuern und zu kontrollieren ist über ein sog. unternehmensweites Rollenmodell möglich. Mit der Einführung dieser «Enterprise Rollen» wird versucht, unternehmensweit die Zugriffsberechtigungen auf Applikationen, Daten sowie IT-Systeme zu regeln. Dabei werden z.B. Risiken eines unautorisierten Datenzugriffs minimiert. Die Rechte, auf diese Entitäten zuzugreifen oder diese nutzen zu können, werden in einem rollen- und regelbasiertem Autorisierungsmodell anhand von festgelegten Regeln abgeleitet. Unter einer Enterprise Rolle wird also eine Abstraktion einer Funktion in einem Unternehmen verstanden. Eine Person kann mehrere Rollen haben, da sie auch mehrere Funktionen ausüben kann.



Nachstehend erfolgt eine Beleuchtung der Vor- und Nachteile von Enterprise Rollen, sowie der grössten Probleme bei der Einführung und deren Pflege in der Praxis.

Vorteile

Ein wesentlicher Vorteil von Enterprise Rollen ist die Gruppierung von Mitarbeitern über ihre Funktion in einer Rolle. Ist eine Rolle adäquat definiert, ist der Unterhaltsaufwand für die Autorisierung kleiner, als wenn jeder Person ein individuelles Profil zugewiesen wird.

Die Wiederverwendung von Rollen ist ein weiterer wichtiger Vorteil, da in den meisten Fällen die Funktion weniger Veränderungen ausgesetzt ist, als ein individuelles Profil. Eine zentrale Eigenschaft von Rollen ist die Parametrisierbarkeit. Solche Parameter können im Beispiel des Kundenberaters verschiedene Länder oder Divisionen sein.

Die Nutzung von Enterprise Rollen bringt auch den Gewinn eines verminderten Administrationsaufwandes mit sich. Da die Rollen zentral administriert und gepflegt werden können, entsteht ein geringerer personeller Aufwand, als wenn dies mittels individuellen Profilen dezentral gemacht werden würde. Durch den Normierungsanspruch bzw. durch das Zusammenfassen und die Abstraktion von Funktionen in einer Rolle, werden die Autorisierungskriterien vereinheitlicht und die Rollen werden somit auch besser untereinander vergleichbar. Anforderungen der internen wie auch der externen Revision wird die zentrale Administration dahingehend gerecht, dass die Zuweisung der Rollen transparent und eine Rollen-Kumulation schneller erkannt wird. Zudem ist die Nachvollziehbarkeit von Änderungen in den Zugriffsrechten dokumentiert.

Nachteile

Die Abstraktion von Funktionen in Rollen bringt aber auch eine grössere Komplexität mit sich und birgt somit das Risiko der zunehmenden Unübersichtlichkeit. Bei der Einführung von Enterprise Rollen muss deshalb entsprechendes, umfassendes

➜ Fortsetzung

Focus

Fortsetzung:Enterprise Rollen

Know-how, auch im Hinblick auf die organisatorische Eingliederung vorhanden sein. Eine der Herausforderungen wird sein, dass sowohl die Aufbau- als auch die Ablauforganisation einem ständigen Wandel ausgesetzt ist. Ein rollenspezifisches «Change Management» wird darum unabdingbar. Es versteht sich von selbst, dass es in einer Unternehmung nie möglich sein wird, alle Systeme zu integrieren. Es werden immer einzelne Systeme und Applikationen übrig bleiben, welche sich nicht sinnvoll in ein Enterprise Rollen Modell integrieren lassen. Dieses Restrisiko muss mit der notwendigen Sorgfalt behandelt werden.

Herausforderungen

Ist in einem rollenbasierten Konzept die Herausforderung, möglichst unabhängige Rollen in einem mehrdimensionalen Kontext Aufgabe; organisatorische Eingliederung; Wirkungsbereich; Stellvertreter-Regelungen; etc. zu bauen, so multiplizieren sich diese Dimensionen bei Enterprise Rollen und führen schnell zu einer Unübersichtlichkeit, die nicht mehr zu kontrollieren ist. Diesem Umstand lässt sich durch eine möglichst unabhängige Definition der Rollen begegnen. Um unabhängige Rollen zu definieren, müssen bestimmte Vereinheitlichungen durchgeführt werden. In den meisten Fällen können Rollen auf ein Niveau angehoben werden, ohne dass es den betreffenden System- und Dateneigner stört. Unbedingt zu vermeiden sind Ausnahmeregelungen. Diese bergen das Risiko, dass immer weitere Ausnahmen die Folge sind, dass sich der Pflege-Aufwand entsprechend wieder erhöht und am Ende die Vorteile der Enterprise Rollen wieder zunichte gemacht werden. Ein wichtiger Aspekt hierbei ist auch die Nachvollziehbarkeit bei Mutationen von Rollen. Für die Revision ist es unabdingbar, dass zu jedem Zeitpunkt genau definiert und insbesondere dokumentiert ist, welcher Benutzer über welche Rolle und somit über welche Rechte verfügt. Es ist somit ein geeigneter Prozess zu implementieren, welcher den Anforderungen der vollständigen Nachvollziehbarkeit Rechnung trägt. Dort wo Vereinheitlichung nicht möglich ist, sollte von Beginn an auf Enterprise Rollen verzichtet werden, da sich der Aufwand nicht lohnt.

Nach der Einführung von Enterprise Rollen ist es wichtig, sowohl die Vergabe als auch das Hinzufügen von neuen Rollen restriktiv und nach vordefinierten Regeln durchzuführen. Die Ablauforganisation muss darauf ausgerichtet werden, dass die Anforderungen wie Definition, Mutation oder Löschung einer Rolle von einer Person erfüllt werden können. Was oftmals bei der Definition von Enterprise Rollen vergessen geht, ist die Festlegung des Geltungsbereiches. Insbesondere in global tätigen Unternehmen ist der Geltungsbereich massgebend. Ein Kundenberater in der Schweiz wird nicht auf die gleichen Entitäten zugreifen dürfen, wie ein Kundenberater in den USA.

Weitere «Dimensionen» wie der beschriebene Geltungsbereich sind bspw. die Kundensegmentierung, die CO-Organisation, die Stellvertreter-Regelung oder die Sonderfunktionen eines Mitarbeiters, welche es zu definieren gilt. Diese machen aus einem «einfachen» Mitarbeiter ein komplexes Rollengebilde.

Schlussfolgerung

Eine Analyse der Systeme und die Einbindung möglicher Teilnehmer im Enterprise Rollen Konzept ist zwingend vor jeglicher technischen Diskussion notwendig. Hierzu muss eine Roadmap der einzubindenden Systeme aufgestellt werden. Dabei sollten die zwingend notwendigen und einfach zu integrierenden Entitäten zuerst angegangen werden. Die Einbindung des Personalbereichs sollte in Erwägung gezogen werden, da dort die Stellenbeschreibungen erstellt und verwaltet werden. Am Ende der Einführung von Enterprise Rollen werden diejenigen Systeme übrig bleiben, deren Aufwand zur Einbindung den Nutzen eines zentralen Enterprise Rollen Management übersteigt.

Der Nutzen steht in direktem Zusammenhang mit der Komplexität. Je komplexer ein rollenbasiertes Konzept ist, desto schwieriger ist es in das Enterprise Rollen Konzept zu integrieren und desto teurer wird auch dessen Unterhalt. Das Projekt, welches die Einführung eines Enterprise Rollen Konzept zum Ziel hat, sollte auf jeden Fall mit entsprechendem Personal ausgestattet sein, welches die Definition der Rollen im Fokus haben muss. Die Arbeit für die Informatik kommt erst viel später.

Die Einführung von Enterprise Rollen kann somit als wesentlicher Bestandteil des Risikomanagements angesehen werden, welcher einen aktiven Beitrag zur Minimierung von unautorisierten Zugriffen auf Entitäten innerhalb eines Unterhalts bildet.

Inside

PMBOK 4TH EDITION

Author: Andres Maurer

The Project Management Institute released the PMBOK 4th Edition on 1st January 2009 which replaces the 3rd Edition that has been available since 2004. The changes made to the 4th Edition are more evolutionary in character.

The major changes include:
- Standardizing the process names to the verb-noun format.
- The number of processes decreased from 44 to 42. Two processes were deleted, two processes were added and in the Project Procurement Management Knowledge Area, 6 processes were redefined into 4 processes to match the other Knowledge Areas.
- Clarification of the information contained in the Project Charter and Project Scope Statement.
- Better distinction between the Project Management Plan and other project documents.
- New Appendix with a list of key interpersonal skills that a project manager requires to manage a project.

The phase model has remained unchanged. The five process phases are:
- Initiating Processes
- Planning Processes
- Executing Processes
- Monitoring & Controlling Processes
- Closing Processes

For large projects, these 5 process phases will be executed for each project phase. For example the Design Phase and the Construction Phase both will each contain these 5 process phases.

The Knowledge Areas (Project Integration Management, Project Scope Management, Project Time Management, Project Cost Management, Project Quality Management, Project Human Resource Management, Project Communication Management, Project Risk Management and Project Procurement Management) remained unchanged.

The following processes within have been revised:
- Project Integration Management: «Develop Preliminary Scope Statement» deleted, «Close Project» renamed «Close Project or Phase«.
- Project Scope Management: «Plan Scope» deleted, «Collect Requirements» added.
- Project HR Management: «Manage Project Team» changed from a controlling process to an execution process.
- Project Communications Management: «Identify Stakeholders» added, «Managing Stakeholders» changed to «Managing Stakeholder Expectations» and as an execution process.
- Project Procurement Management: «Plan Purchases and Acquisitions» and «Plan Contracting» merged to «Plan Procurements«, «Request Seller Responses» and «Select Sellers» merged to «Conduct Procurements«.

The Mapping to CobiT can practically be taken over as is. The content of the significant match to PO10 Management Projects does not need necessarily to be revised. Of the minor matches AI2 Acquire and Maintain Application Software, AI5 Procure IT Resources, AI7 Install and Accredit Solution and Changes, ME1 Monitor and Evaluate IT Performance, only the contents of AI5 have to be slightly modified due to the process consolidation in the Knowledge Area Project Procurement Management.

The PMBOK 4th Edition Book and CD-ROM can also be ordered from:

PMI Switzerland Chapter
Wasserwerkgasse 37 • CH-3011 Berne
Tel.: 031 311 53 08 • office@pmi-switzerland.ch

Resources:
PMI Members can download the electronic version free from the PMI Website:
➜ **http://www.pmi.org/Resources/Pages/Members/Library-of-PMI-Global-Standards-Projects.aspx**

CobiT-PMBOK Mapping: ISACA Website
➜ **http://www.isaca.org/Template cfm?Section=COBIT_Mapping1&Template=/Content Management/ContentDisplay.cfm&ContentID=31448**

Inside

CobiT im Forschungseinsatz

Autor: Bruno Wiederkehr

An der AHS vom 24. Februar 2009 hat uns Andres Wohler mit seinem Referat «Service-Management im IT-Outsourcing-Umfeld» aufgezeigt, wie eine prozessorientierte Analyse mit CobiT und einem neuronalen Framework erstellt werden kann. Ausgehend von den heutigen Anforderungen und den Problemfeldern ging er detailliert auf Forschungsfragen und -design ein. Dabei ist er im Rahmen einer Social-Network-Analyse auf die Anwendung von CobiT Val IT, Schlüsselprozess und Maturitätsattribut eingegangen.

Eine zentrale Bedeutung bei dieser Analyse erhalten Rollen-Systeme (z.B. RACI-Charts in CobiT). Durch die Interpretation von Rollen kann alogisches und nicht-rationales Verhalten erklärt werden. Dieses Verhalten kann zu organisationalen Risiken führen. Diese Risiken schlagen sich in verschiedenen Kennzahlen nieder. Mit Hilfe von geeigneten Social-Network-Analysen können diese Risiken detailliert sichtbar gemacht werden.

Als Quelle seines Referates diente seine Bachelorarbeit zum gleichnamigen Thema. Besonders überraschte mich, dass ich zum ersten Mal feststellen konnte, dass CobiT für Forschungszwecke gute Dienste leistet. Hervorgehoben wurde vom Referenten, dass die Anwendung durch die sprachliche Komponente (globale Einheitlichkeit), die Flexibilität und die Offenheit des CobiT Frameworks begünstigt wird. Kritische Fragen aus dem Publikum konnte er aufgrund seiner Forschungsergebnisse und praktischer Erfahrung souverän beantworten.

Auf die Frage, wie CobiT an der Universität Zürich ankomme – kam blitzartig die Antwort – hervorragend. Schade, dass dieses Prädikat der abwesende Dozent an der Uni ZH, Peter R. Bitterli (Ski-Urlaub), nicht hören konnte. Ich hoffe, dass im Rahmen der ISACA Academic Relations noch mehrere derartige Beispiele auf Bachelor- und Masterstufe entstehen werden.

by Bitterli Consulting
itacs training

Details und andere Kurse siehe
unsere Homepage: ➜ www.itacs.ch

ISACA CobiT 4.1 Foundation Certificate • 20.–22. April 2009
Offizieller ISACA-Zertifikatskurs mit international standardisiertem Curriculum

CobiT für Manager – ein Kompaktkurs zu Projektmanagement und IT-Governance • 29.–30. April 2009
Mittels Projekt-Simulation Management-Kompetenz in CobiT erwerben

Application Security Lab • 6.–8. Mai 2009
Web-Entwickler Kurs vom Applikationssicherheits-Spezialisten Compass

Erfolgreiche Awareness-Kampagnen (Kompaktkurs) • 15. Mai 2009
Systematische Planung/Durchführung von Aktivitäten und Kampagnen für anhaltende Awareness (mit zahlreichen Beispielen/Erkenntnissen aus der Praxis)

ITACS Training AG
Stampfenbachstr. 40
CH-8006 Zürich
Tel. +41 44 444 11 01
kurse@itacs.ch

ITACS Training ist der offizielle Ausbildungspartner des ISACA Switzerland Chapter **www.isaca.ch**

ISACA Serving IT Governance Professionals Switzerland Chapter

IT Governance Institute

After Hours Seminar + Vereinsversammlung 2009

Dienstag, 31.3.2009 • Zürich • Ort: General Guisan Quai 38, bei Deloitte AG

15.15 – 16.15 • After Hours Seminar ➜ **Situationsplan Deloitte AG**

Vortrag von Bruno Jenny, Experte IT-Projektmanagement;
Hat 20 Jahre ISACA-CH im Projektmanagementumfeld etwas bewirkt?

16.20 – 17.20 • Vereinsversammlung 2009

Traktanden

1.Begrüssung
2. Wahl der Stimmenzähler
3. Protokoll der Generalversammlung vom 25. März 2008
4. Rückblick 2008 / Vorschau 2009
5. Jahresrechnung 2008
   - Bericht des Kassiers
   - Revisionsbericht
   - Abnahme/Décharge-Erteilung
6. Wahlen
7. Budget 2009
8. Verschiedenes

Anträge, über die an der Generalversammlung abgestimmt werden soll, sind bis 10 Tage vor der Versammlung schriftlich an die Präsidentin, Daniela Gschwend, zu richten.

Vor der Vereinsversammlung wird Bruno Jenny, Geschäftsführer SPOL AG, ein spannendes Referat zum Thema «Hat 20 Jahre ISACA-CH im Projektmanagementumfeld etwas bewirkt?» halten.

Wie jedes Jahr suchen wir Personen, die aktiv in unserem Chapter mitwirken oder neue Ideen einbringen möchten. Insbesondere im Jubiläumsjahr suchen wir zahlreiche Helfer und einige Referenten für unseren Spezialanlass im August. Interessiert? Bitte melden Sie sich bei unseren Vorstandsmitgliedern!

Den Nachmittag möchten wir mit einem Apéro, zu dem Sie alle herzlich eingeladen sind, abschliessen. Wir freuen uns auf Ihre Teilnahme – bitte melden Sie sich unbedingt an oder ab! Bitte retournieren Sie auch unbedingt den Datenbankauszug mit/ohne allfälligen Korrekturen.

Anmeldung für Mitglieder ➜ kurse@isaca.ch ■

Die Alumni-Organisation von NDK/NDS Informationssicherheit in Luzern SGR" startet eine neue Special Interest Group zum Thema "Secure Information Exchange".

Ziel der SIG "Secure Information Exchange"

- Ansätze und Lösungen zum sicheren Datenaustausch mit Geschäftspartnern diskutieren
- Lösungen aus Sicht des Endbenutzers / Business Kontakts durchleuchten
- Rechtliche Aspekte aus der Sicht der Schweiz und weltweit tätigen Unternehmen diskutieren
- Richtlinien und Hilfestellungen für den sicheren Datenaustausch erarbeiten
- Das Thema ganzheitlich betrachten und für eine Veranstaltung aufbereiten

Die Special Interest Group richtet sich an Security Professionals von mittleren und grösseren Unternehmen - bevorzugt werden Unternehmen, welche die Anwenderseite vertreten

Weitere Infos zur SIG findet man unter ➜ **http://www.sgrp.ch/securex**

ISACA-Kurse und -Veranstaltungen

Diese Übersicht enthält die aktuellsten Veranstaltungs- und Kursdaten. Details: ➜ www.isaca.ch

20. – 22.4.09	➜ **ISACA CobiT 4.1 Foundation Certificate** Offizieller ISACA-Zertifikatskurs mit international standardisiertem Curriculum
29. – 30.4.09	➜ **CobiT für Manager – ein Kompaktkurs zu Projektmanagement und IT-Governance** Mittels Projekt-Simulation Management-Kompetenz in CobiT erwerben
6. – 8.5.09	➜ **Application Security Lab** Web-Entwickler Kurs vom Applikationssicherheits-Spezialisten Compass
15.5.09	➜ **Erfolgreiche Awareness-Kampagnen (Kompaktkurs)** Systematische Planung/Durchführung von Aktivitäten und Kampagnen für anhaltende Awareness (mit zahlreichen Beispielen/Erkenntnissen aus der Praxis)
25.5.09	➜ **Grundlagen der Kryptologie (Kompaktkurs)** Alle notwendigen Fachbegriffen und Erkenntnisse; besonders geeignet für IT-Prüfer, Sicherheitsspezialisten, Manager
	IT Security Training Week (All Courses in English !)
8.–9.6.09	➜ **Introduction to Information Security (Days 1+2 of the IT Security Training Week)** Highly compact introduction to information security
10.6.09	➜ **Understanding and Securing the Wireless Network (Day 3 of the IT Security Training Week)** Effectively secure wireless networks
11.6.09	➜ **Using ISO27002 to Audit Mobile Technology (Day 4 of the IT Security Training Week)** Effectively audit mobile technology issues
1.6.09	➜ **Understanding and Auditing Windows Active Directory (Day 5 of the IT Security Training Week)** Effectively audit Windows Active Directory
17. – 19.6.09	➜ **ISACA CobiT 4.1 Foundation Certificate** Offizieller ISACA-Zertifikatskurs mit international standardisiertem Curriculum

Wo nichts anderes vermerkt, finden die Veranstaltungen/Kurse in den Schulungsräumlichkeiten von ITACS Training AG, Stampfenbachstrasse 40 (5 Geh-Minuten vom Hauptbahnhof), 8006 Zürich, statt.

Weitere Kurs- und Veranstaltungsanbieter

EXCLUSIF A LAUSANNE	**Accès à l'information : rôles et responsabilités** Un événement organisé par l'ISACA, le CLUSIS et l'ASAI Réservez d'ores et déjà cette date! Vous recevrez prochainement toutes les informations utiles pour vous inscrire.	**27.5.2009** Hôtel Alpha Palmier Lausanne
	IT-Migration aus Sicht des Prüfers Eine Veranstaltung der Treuhand-Kammer in Zusammenarbeit mit ISACA. Detaillierte Informationen folgen ➜ **www.treuhand-kammer.ch**	**16.6.2009** Bern
➜ **www.isss.ch**	**ISSS Zürcher Tagung:** «Digital Rights Management (DRM): the good, the bad and the ugly?«	**17.6.2009** Widder Hotel Zürich
➜ **www.isss.ch**	**12. ISSS Berner Tagung für Informationssicherheit «ICT-Riskmanagement«**	**24.11.2009** Hotel Bellevue Bern