ISACA Newsletter Januar

newsletter

ISACA
Trust in, and value from, information systems
Switzerland Chapter

After Hours Seminar • Zürich

Dienstag, 25. Januar 2011 • 16:40 – 17:40 Uhr
IT Audit at UBS - a Fully Integrated Approach
(Slides in English, German spoken)

➜ Mehr auf Seite 4

Focus

Sicherheit und Compliance in SAP-Systemen: Realität und Anspruch

➜ Mehr auf Seite 2

Inside

Rückblick SVIR Erfa-Gruppe Versicherung

➜ Mehr auf Seite 6

ISACA-Kurse und -Veranstaltungen

Die aktuellsten Veranstaltungs- und Kursdaten ➜ Seite 7

Neue Upgrade-Möglichkeiten für bereits zertifizierte CISAs, CISMs, CGEITs und CRISCs

Impressum

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

Redaktionsschluss:
1. Februar 2011

Redaktion:
Peter R. Bitterli
Stampfenbachstrasse 40
8006 Zürich
prb@bitterli-consulting.ch

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

Editorial

27C3 - der 27. Chaos Communication Congress des Chaos Computer Club. Diese von weit über 3000 Teilnehmern besuchte, inzwischen global etablierte Sicherheitskonferenz fand vom 27. - 30. Dezember 2010 in Berlin statt. Vortragsthemen sind Community, Culture, Hacking, Making, Science, Society - es werden technische Sicherheitsaspekte moderner Technologie wie auch gesellschaftliche und politische Entwicklung der vernetzten Welt kritisch hinterfragt und diskutiert. Referenten und «Hacker» aus aller Welt treffen sich alljährlich zur grössten europäischen Hackerkonferenz. Der Eintritt für vier Tage hochkarätige Sicherheitsvorträge kostet 70 Euro.

ISACA-Mitglieder wurden angetroffen, die sich über die neusten Sicherheits-Schwachstellen informieren und Sicherheit und Risiko im Informationszeitalter im globalen Kontext betrachten. Es zeigt sich in vielen Vorträgen, wie lascher Umgang mit Sicherheitsaspekten zu grossen Schäden führen kann, im globalen Ausmass.

Zu den oft in bis auf den letzten Platz gefüllten Vorträgen gehören einige sehr Interessante Themen, die auch grosse Aufmerksamkeit in der Branche erhielten. Einige davon könnten auch für die ISACA-Mitglieder von Interesse sein:

- 27C3 Keynote - We Come in Peace
- Hacking Smart Phones
- Recent advances in IPv6 insecurities
- Die gesamte Technik ist sicher – Relay-Angriffe auf den neuen Personalausweis
- Adventures in analyzing Stuxnet (von Microsoft)
- Wideband GSM sniffing
- Is the SSLiverse a safe place?
- Data Recovery Techniques
- Chip and PIN is Broken - Vulnerabilities in the EMV Protocol OMG WTF PDF - What you didn't know about PDF
- Data Analysis in Terabit Ethernet Traffic
- How the Internet sees you - demonstrating what activities most ISPs see you doing on the Internet

Siehe: ➜ **events.ccc.de/congress/2010/Fahrplan/index.en.html**

Zu finden sind die Videos und Audio-Mitschnitte. Die gesamte Konferenz wird realtime im WWW auf verschiedenen Mirrors gratis zur Verfügung gestellt. Eine Liste finden Sie hier: ➜ **events.ccc.de/congress/2010/wiki/Documentation**

Falls Sie dieses Jahr mit einem neuen ISACA-Zertifikat Ihren Lebenslauf schmücken möchten, weise ich Sie auf das im Juni 2011 erstmals stattfindende CRISC-Examen hin (Certified in Risk and Information Systems Control). Early Registration Deadline ist der 9. Februar 2011.

Herzliche Grüsse
Ihr Umberto Annino,
CISA, CISM, CGEIT, CRISC Coordinator,
ISACA Switzerland Chapter

CISA Certified Information Systems Auditor — CISM Certified Information Security Manager — CGEIT Certified in the Governance of Enterprise IT — CRISC Certified in Risk and Information Systems Control

Focus

Sicherheit und Compliance in SAP-Systemen: Realität und Anspruch

Autor: Jörg Altmeier

Die Anforderungen an die Sicherheit von SAP-Systemen steigen mit der Komplexität der eingesetzten Funktionalitäten. Zahlreiche Unternehmen sind noch nicht genügend vor möglichen Bedrohungen geschützt. Bei den Verantwortlichen steigt jedoch die Awareness, dass es Zeit zum Handeln ist. Eine Roadmap gibt Hilfestellung bei Umsetzung der wichtigsten Schritte.

Sicherheit in SAP-Systemen hat viel zu tun mit Technik: Netzwerke, Betriebssysteme und Datenbanken bieten Angriffsflächen. Zu deren Schutz stellen die Anbieter von Sicherheitsprodukten ausgereifte Werkzeuge zur Verfügung, so dass das Risiko einer Bedrohung auf ein akzeptables Niveau gesenkt werden kann. Die Absicherung nach aussen ist aber heute nicht mehr das Hauptproblem. Studien haben herausgefunden, dass der Missbrauch von sensitiven Daten zu 80% im Unternehmen selbst, von den eigenen Mitarbeitenden, vorsätzlich oder fahrlässig verübt wird. Diesem Missbrauch ist aber mit technischen Hilfsmitteln alleine nicht beizukommen.

Verbesserungsbereiche

Mehr und mehr Verantwortliche erkennen, dass nicht die technischen Aspekte im Vordergrund stehen, sondern dass zuerst organisatorische und betriebswirtschaftliche Hausaufgaben zu lösen sind. So stehen bei der Analyse der Lücken nicht etwa technische Anforderungen im Vordergrund, die Top Ten Verbesserungsbereiche finden sich fast ohne Ausnahme in den organisatorischen Bereichen:

- Der Informationsaustausch zu sicherheitsrelevanten Themen zwischen dem Hersteller und den Sicherheitsverantwortlichen ist ungenügend ausgeprägt. Von der SAP erwarten die Unternehmen eine pro-aktive Kommunikation, gestehen aber auch ein, dass sie die vorhandenen Infos zu wenig nutzen und sich bis anhin mit dem Thema SAP-Sicherheit insgesamt zu wenig auseinandergesetzt haben.
- Das SAP-System bietet Standard-Tools, die ein Monitoring der sicherheitskritischen Systemereignisse ermöglichen. Diese Funktionen werden aber zu wenig eingesetzt, Security Incidents werden erst zu spät erkannt.
- Anwendern werden häufig so viele Authentifizierungs-Mechanismen zugemutet, dass diese sich ihre Passwörter nicht merken können. In der Folge sind die meisten Passwörter nicht qualifiziert, eine Passwort-Policy kann nicht durchgesetzt werden.
- Beim Export von Daten aus SAP zur Weiterverarbeitung in Office-Systemen wie auch beim Drucken findet sich aufgrund mangelnder Awareness bei den Benutzern ein zu sorgloser Umgang mit sensitiven Daten.
- Im SAP-Bereich wenig verbreitet sind Methoden zum Risikomanagement, soweit vorhanden beschränken sie sich auf die Folgenabschätzung einer technischen Unterbrechung und fokussieren wenig auf Geschäftsprozesse und geldmässige Schadensabschätzung.
- In zahlreichen Unternehmen sind die produktiven SAP-Einheiten nur rudimentär gegen böswillige oder ungewollte Veränderungen geschützt, zu viele Personen verfügen - meist historisch bedingt - über weit reichende Entwicklungsrechte.
- Die Qualität der Dokumentation sowie die Überprüfung der Einhaltung vorgegebener Richtlinien, welche Konfigurationseinheit wie verändert wurde, sind oft nicht genügend ausgeprägt. Spätestens beim nächsten Release-Wechsel sind somit Sicherheits-Probleme vorprogrammiert.
- Die Client-Server-Kommunikation sowie die Beleg-Erzeugung erfolgt in SAP-Systemen unverschlüsselt, viele Unternehmen sind gegen Netzangriffe, Mithören und Manipulation nur unzureichend geschützt.
- Sicherheitsüberprüfungen bei Mitarbeitenden, die Zugang zu besonders sensitiven SAP-Bereichen haben, werden in den meisten Unternehmen nicht oder nur sporadisch durchgeführt, Anzeichen sich

➜ Fortsetzung

Focus

Fortsetzung Sicherheit und Compliance …

verändernder Umstände meist nicht registriert.

- Die Rollen SAP-Sicherheitsbeauftragter und unabhängige Kontrollinstanz zur Überprüfung der festgelegten Sicherheits-Standards und -Massnahmen sind häufig nicht besetzt oder mit zu wenig Ressourcen, Kompetenzen und Know-how ausgestattet.

Die grössten Herausforderungen bilden jedoch nicht etwa das Erkennen und Schliessen bekannter Sicherheitslücken. Betrachtet man die für Sicherheit relevanten Komponenten losgelöst vom konkreten Umfeld, läuft man leicht Gefahr, deren Einfluss als wenig kritisch einzustufen. Häufig ergeben sich im Falle des vorsätzlichen oder fahrlässigen Störfalls durch das Zusammenspiel der einzelnen Bereiche fatale Auswirkungen. Die Kette ist eben nur so stark wie ihr schwächstes Glied.

In den meisten Unternehmen ist das technische Umfeld bedarfsgerecht ausgebaut, der organisatorische Bereich zeigt dagegen grosse Lücken. In vielen Unternehmen ist beispielsweise das Erraten oder Hacken von Passwort-Informationen nicht wirklich schwierig, da meist weder Datenverschlüsselung noch qualifizierte Authentisierung eingesetzt werden. Erlangt ein unberechtigter Dritter Zugang, ist es für ihn ein Leichtes, im Namen des wirklichen Benutzers das System zu manipulieren oder Einsicht in geheime Daten zu erhalten, ohne entdeckt und erkannt zu werden.

Sind für solche Szenarien keine Schutz- und Reaktionsmassnahmen vorbereitet, kann im schlimmsten Fall das produktive System nicht mehr aufrecht gehalten werden. Verfügbarkeit und Integrität des im Tagesgeschäft so dringend benötigten Systems sind dann nur mit hohem Aufwand wiederherzustellen, der Schaden beträchtlich.

Roadmap zur Umsetzung

Auf die geschilderte Situation sind die wenigsten Unternehmen ausreichend vorbereitet. Es bestehen zu viele Lücken und nötige Kontroll- und Monitoring-Aktivitäten sind zu schwach ausgeprägt, als dass sie zur Aufrechterhaltung der geforderten Sicherheitsziele beitragen könnten. Die folgende 10-Punkte-Roadmap kann hier Abhilfe schaffen:

➜ **Fortsetzung**

Bereits CISA, CISM, CGEIT oder CRISC? Machen Sie jetzt einen Upgrade!

Dank der modularen Vermittlung des Fachwissens können wir neu für sämtliche vier Zertifikate einen kompakten Upgrade-Kurs zu jedem anderen ISACA-Zertifikat anbieten: Sie belegen einzig die für das neue Zertifikat zusätzlich benötigten Module und sinnvollerweise auch das eigentliche Prüfungstraining (Repetitionsblock).

Kurstage für Upgrade	CISA	CISM	CGEIT	CRISC
Von CISA zu …		Risikomanagement Vertiefung Performance Measurement Sicherheitsmanagement und 4 Tage Repetitionsblock	Risikomanagement Vertiefung Performance Measurement Strategic Alignment IT-Governance Vertiefung* und 4 Tage Repetitionsblock	Risikomanagement Vertiefung Performance Measurement Risiko-Monitoring IKS-Vertiefung und 4 Tage Repetitionsblock
Von CISM zu …	(IT-) Revision* IT-Betrieb & Service Management und 5 Tage Repetitionsblock		IT-Betrieb & Service Management Strategic Alignment IT-Governance Vertiefung* und 4 Tage Repetitionsblock	Risiko-Monitoring IKS-Vertiefung und 4 Tage Repetitionsblock
Von CGEIT zu …	Anwendungsentwicklung (IT-) Revision* Sicherheit und Kultur Sicherheitstechnologie Notfall-Management und 5 Tage Repetitionsblock	Anwendungsentwicklung Sicherheit und Kultur Sicherheitsmanagement Sicherheitstechnologie Notfall-Management und 4 Tage Repetitionsblock		Anwendungsentwicklung Sicherheit und Kultur Risiko-Monitoring IKS-Vertiefung und 4 Tage Repetitionsblock
Von CRISC zu …	(IT-) Revision* Sicherheitstechnologie Notfall-Management IT-Betrieb & Service Management und 5 Tage Repetitionsblock	Sicherheitsmanagement Sicherheitstechnologie Notfall-Management und 4 Tage Repetitionsblock	IT-Betrieb & Service Management Strategic Alignment IT-Governance Vertiefung* und 4 Tage Repetitionsblock	

* 2-tägiges Modul

IT Governance Institute®

Verlangen Sie eine persönliche Offerte – wir haben attraktive Upgrade-Preise: kurse@itacs.ch

Focus

Fortsetzung Sicherheit und Compliance …

- Wesentliche Grundlage zur Erhöhung der Systemsicherheit ist Prozess-Transparenz. Es sollte nachvollziehbar dokumentiert werden, welche Prozesse vom SAP-System abgedeckt sind und welche Mitarbeitenden damit arbeiten. In vielen Unternehmen existieren zwar Projektdokumente mit System-Beschreibungen, diese sind aber zu wenig abteilungsübergreifend und erlauben kein «Big Picture». Davon abzuleiten sind Rollenbeschreibungen, die die wirklich benötigten Zugriffsrechte transparent machen, und eine Risikomatrix, die Auswirkungen von Sicherheitsvorfällen auf einzelne Prozess-Schritte auch geldmässig bewertet.
- Im Unternehmen bestehende Sicherheits-Organisation sollte um SAP-spezifische Aufgabenstellungen in Betrieb und Projekten erweitert werden. Zur Erfüllung der Hauptaufgaben Awareness-Bildung, Kommunikation und Security Monitoring sind die entsprechenden Ressourcen bereitzustellen und Trainingsmassnahmen durchzuführen.
- Unternehmensvorgaben bezüglich Sicherheit sollten auf SAP-Besonderheiten wie beispielsweise System-Konfiguration, Dokumentation, Schutz sensitiver Daten oder Projektablauf detailliert, mit geeigneten Massnahmen erzwungen und regelmässig auf Einhaltung überprüft werden.
- Für die Kontinuitätsplanung sollte ein formalisiertes Konzept erstellt werden, das eine klare Aufgabenteilung zwischen den verantwortlichen Aufgabenträgern sicherstellt. Zusätzlich sollte eine aktuelle und vollständige Inventarliste vorhanden sein, die einen Überblick über die eingesetzten Hard- und Software-Komponenten, das Netzwerk sowie über die Sicherungsmassnahmen des Rechenzentrums gibt.
- Im Bereich Perimeter-Schutz ergeben sich bezüglich Gebäudesicherheit und Zutrittskontrolle keine SAP-spezifischen Anforderungen. Bei der Ausgestaltung des Netzwerks sollten die von SAP strikt empfohlenen Massnahmen zur Firewall- und Router-Konfiguration und zum Domänenkonzept umgesetzt werden. Ausserdem sollten die zwischen Clients und Servern ungeschützt transportierten Daten durch eine zusätzliche Verschlüsselung geschützt werden. Diese Empfehlung gilt auch insbesondere für Zugriffe von Mitarbeitenden sensitiver Bereiche wie beispielsweise Personal oder Finanzen und auch für das Drucken von kritischen Daten auf ungeschützten Druckern.
- S
ind Datenbank und Betriebssystem nicht restriktiv gegen unerlaubten Zugriff geschützt, ist das beste Benutzer-Berechtigungs-Konzept wertlos. Für die jeweiligen Kombinationen stellt SAP spezifische Security Guidelines bereit, die helfen, geeignete Sicherungsmassnahmen zu implementieren.
- Die im Betrieb durchzuführenden Tätigkeiten wie System-Management und -Kontrolle, Job Management oder Benutzerverwaltung sollten durch eine eindeutige Beschreibung Aufgabenträgern zugeordnet werden. Dies gilt insbesondere dann, wenn wie im Falle eines Basis-Outsourcings die Verantwortlichkeiten auf unterschiedliche Gruppen verteilt sind.
- Viele Unternehmen haben in ihren Business Prozessen das 4-Augen-Prinzip so realisiert, dass es den

➜ **Fortsetzung**

After Hours Seminar • Zürich

IT Audit at UBS - a Fully Integrated Approach

Dienstag, 25. Januar 2011 • 16:40 – 17:40 Uhr • (Slides in English, German spoken)

Das Referat stellt den integrierten Ansatz der UBS für das Audit von Businessprozessen mit einem hohen Anteil an automatisierten Kontrollen vor. Dabei wird dieser dem «klassischen» Ansatz reiner IT-Kontrollen in einem Business-Audit gegenübergestellt und die resultierenden Vorteile aus IT- wie auch aus Business-Sicht aufgezeigt sowie allfällige Herausforderungen besprochen.

Inhalt:
- Übersicht über das UBS Group Internal Audit
- Früherer «klassischer» IT Audit Ansatz
- Neuer integrierter Audit Ansatz
- Vorteile und Herausforderungen

Referent: Gerd Lierhaus, CISA

➜ **Zur Anmeldung**

Focus

Fortsetzung Sicherheit und Compliance …

allgemein akzeptierten Grundsätzen eines internen Kontrollsystems entspricht. Für die eher technischen Funktionalitäten wie beispielsweise Benutzerverwaltung, Entwicklung, Transport, Support, Tabellenpflege oder Systempflege gilt dies oftmals nicht. Eine in SAP versierte Person könnte mit den zugeordneten Rechten absichtlich oder fahrlässig die vermeintlich wirksame Aufgabenteilung überwinden. Es ist daher notwendig, bestehende Benutzer-Berechtigungs-Konzepte genau zu prüfen und soweit nötig anzupassen.

- Viele Unternehmen erlauben im kritischen Produktivsystem zahlreiche Benutzer mit weit reichenden Entwicklungsrechten, teilweise sogar von extern. Begründet wird diese Tatsache mit historisch gewachsenen Strukturen oder der Notwendigkeit eines raschen und unbehinderten Eingreifens im Notfall. Diese Rechte sollten soweit als möglich reduziert werden, am besten auf maximal zwei inaktive Notfalluser, die nur im Eintretensfall frei geschaltet werden. Mal abgesehen davon, wie selten tatsächlich in ein produktives System notfallmässig eingegriffen wird. Diese Vorgehensweise schützt Administratoren in ihrer täglichen Arbeit, indem gravierende Fehlhandlungen reduziert werden können.
- Fast kein Unternehmen nutzt die von SAP zur Verfügung gestellten Standard-Tools zum System Monitoring, die bereits eine vernünftige Überwachung von Sicherheitsvorfällen ermöglichen. Für die Nutzung des Security Audit Log sowie das Audit Information System (AIS) sollte ein unternehmensspezifisches Konzept erstellt werden. Dieses legt fest, welche Vorfälle aufgezeichnet und ausgewertet werden und wie auch im Hinblick auf eine umfassende Qualitätssicherung auf die Ergebnisse zu reagieren ist.

Fazit

Mit der Umsetzung dieser Empfehlungen werden nicht nur Sicherheitslöcher «gestopft». Die Etablierung eines adäquaten Security Levels der eingesetzten SAP-Systeme schafft auch geschäftlichen Nutzen. Zahlreiche Unternehmen haben durch die Beschäftigung mit sicheren Prozessen und Systemen Kosteneinsparungen erreicht, sei es durch die jetzt optimierte Prozessabwicklung, eine effizientere Wartung oder der quasi nebenbei erreichten Erfüllung von Anforderungen seitens internationaler Regulatoren wie beispielsweise Datenschutzgesetze oder Sarbanes Oxley Act. ■

Qualitätsmanagement für Interne (IT-) Revisionen

Montag/Dienstag, 21/22. März 2011 • 09:15 – 17:15 Uhr • Zürich • Fr. 1'600.- für ISACA-Mitglieder

Bringen Sie Ihre eigene Revisionstätigkeit auf ein ausreichendes Qualitätsniveau!

Dieser 2-tägige, praxisorientierte Kurs richtet sich an erfahrene IT-Revisoren, interne Revisoren und Berater für IT-Revision, die interne IT-Prüfungen planen, koordinieren und überwachen sowie ihre Arbeitsweise optimieren wollen. Der Workshop ist weiter für regelmässige Bezieher und Nutzer interner IT-Prüfungen geeignet, die Arbeitsweise und operative Schnittstelle der IT-Prüfung hinterfragen wollen, um Nutzen und Effizienz der Zusammenarbeit mit IT-Prüfern zu verbessern.

Referent: Dr. Ulrich Hahn, CISA, CIA

➜ **Melden Sie sich jetzt an!**

by Bitterli Consulting
itacs training

➜ **www.itacs.ch**

Inside

Rückblick SVIR Erfa-Gruppe Versicherung

Autor: Bruno Wiederkehr

Am 25.10.2010 hat die Suva in Luzern zur offenen Erfa-Tagung zum Thema «Risikomanagement in der Versicherung» eingeladen. Der gut besuchte Event (42 Teilnehmende) wurde von der Leiterin der Erfa-Gruppe, Mirja Platzer, Allianz, in der Aula eröffnet. Erfreulicherweise konnten auch einige ISACA-Mitglieder ausgemacht werden.

Am Vormittag haben drei Referenten die folgenden Schwerpunkte beleuchtet und mit einer Fragerunde abgeschlossen:

Gabe Shawn Varges FINMA, Head of Governance
Grundlagen: Anforderungen der FINMA an Risk Management Governance

Bruno Wiederkehr Autor der Neuerscheinung, ISACA Vorstandsmitglied, langjähriger Konzernprüfer, Swiss Life
Theorie: «Risikomanagement im Unternehmen» in Verbindung mit Versicherung

Dr. Peter Bamert Leiter Corporate Finance & Risk Management, Helvetia Gruppe
Praxisbeitrag: Risikomanagement in der Helvetia

Bruno Wiederkehr weist auf die die Vorteile und Kompatibilität der Rahmenwerke CobiT, Risk IT und Val IT im Zusammenhang mit dem COSO ERM (Enterprise Risk Management) hin.

Nach dem Mittagessen wurden in drei Arbeitsgruppen zu den folgenden Detailaspekten Erfahrungen ausgetauscht:

Arbeitsgruppe1
Erwartungen der FINMA an das Risikomanagement

Arbeitsgruppe 2:
Erarbeiten eines Prüfansatzes an das Risikomanagement

Arbeitsgruppe 3:
Erhebung von Aspekten für die Zusammenarbeit IT-Revision und IT-Risikomanagement

Im Anschluss wurden im Plenum die wichtigsten Erkenntnisse aufgrund der Workshopergebnisse diskutiert. Alles in Allem war die Tagung für die Teilnehmenden einen aufschlussreichen Event. Auch das Networking kam beim Mittagessen im Culinarium Rösslimatt der Suva sowie beim Willkommens- und Abschiedskaffee nicht zu kurz.

ISACA-Kurse und -Veranstaltungen

25.1.2011	➜ **After Hours Seminar • ISACA Switzerland Chapter**
10.2.2011 **Garantierte Durchführung**	➜ **Risikomanagement-Methoden wirksam anwenden (Kompaktkurs)** Identifikation, Bewertung und Management von (IT-) Risiken wirksam implementieren
11.2.2011 **Garantierte Durchführung**	➜ **Effizientes Messen der Performance (Kompaktkurs)** Gute Leistungsindikatoren effizient erheben
3. – 4.3.2011	➜ **Wirksames Projekt- und Portfolio-Controlling** (IT-) Projekte effizient und wirksam überwachen und steuern
7.3.2011 **Garantierte Durchführung**	➜ **ISMS gemäss ISO 2700x implementieren und verbessern (Kompaktkurs)** Wirkungsvolles Sicherheitsmanagementsystem auf Basis ISO 27001/2/4/5 in 30 Schritten entwickeln und festigen (mit detaillierten Tipps aus langjähriger Praxis)
14.3.2011 **Garantierte Durchführung**	➜ **Risikoprüfungen und kontinuierliche Risikoüberwachungen (Kompaktkurs)** Wirksame Überwachung von Risiken
15.3.2011 **Garantierte Durchführung**	➜ **Design, Betrieb, Überwachung & Unterhalt von Kontrollen (Kompaktkurs)** Effizientes Design & wirksame Überprüfung von anwendungsabhängigen Kontrollen
21.–22.3.2011	➜ **Qualitätsmanagement in der Internen (IT-) Revision** Bringen Sie Ihre eigene Revisionstätigkeit auf ein ausreichendes Qualitätsniveau!
23.–25.3.2011	➜ **Projektmanagement für Controller, Sicherheitsfachkräfte und Revisoren** Softwareentwicklungsprojekte optimal begleiten und prüfen
30.3.2011	➜ **Wireless Security • Security Labor mit Compass Security**
6.–7.4.2011	➜ **Networking & Penetration Testing • Security Labor mit Compass Security**
6.4.–10.5.2011 **Garantierte Durchführung**	➜ **CISA-Prüfungsvorbereitungskurs 2011|1** Kompakte Variante zur Vorbereitung auf die internationale CISA-Prüfung

Weitere Kurs- und Veranstaltungsanbieter

➜ **www.isss.ch**	➜ **Cloud Computing – rechtlich und technisch erfolgreiches Risikomanagement**	**19.1.2011 • Bern** Casino Restaurant
➜ **Glenfis**	➜ **CobiT 4.1 – IT Governance Foundation Kurs**	**24. – 26.1.2011** bei Glenfis AG, Zürich
➜ **www.isss.ch**	➜ **ISSS Security Lunch: «Wirksames Informations-sicherheitsmanagement für KMU»**	**28.1.2011 • Zürich** Restaurant Certo
➜ **www.isss.ch**	➜ **Cloud Storage Security**	**10.2.2011 • Zürich** Restaurant Certo
➜ **Glenfis**	➜ **Implementing Governance of Enterprise IT Using CobiT**	**21. – 22.2.2011** bei Glenfis AG, Zürich
➜ **Glenfis**	➜ **RISK IT Enterprise RM Kurs**	**3. – 4.3.2011** bei Glenfis AG, Zürich
➜ **Wildhaber**	➜ **Records Management im Zeitalter von Web 2.0** Rabatt für ISACA-Mitglieder (Fr. 750.- statt Fr. 850.-)	**9. + 10.3.2011 • Zürich** Technopark

IT Governance Institute

Retrouvez dès maintenant les membres «ISACA Suisse romande» sur LinkedIn