ISACA Newsletter 7|2008

ISACA
Serving IT Governance Professionals
Switzerland Chapter

newsletter

After Hours Seminar • 30.9.2008

Identity und Access Management als Teil von Compliance
Identity- und Access-Management-Lösungen (IAM) identifizieren Mitarbeitende und regeln ihre Zugriffsrechte auf Daten und Applikationen ➜ **Mehr auf Seite 4**

Inside

Does Your Control System Pass the COSO Test?
➜ **Mehr auf Seite 2**

CISA- und CISM-Prüfungen Juni 2008
➜ **Mehr auf Seite 3**

ISACA-Kurse und -Veranstaltungen

Sicherheit von Web-Anwendungen: Für den definitiv durchgeführten Kurs «Application Security Lab» 1.–3.10. sind kurzfristige Anmeldungen noch möglich. Attraktive Konditionen für weitere Teilnehmer aus derselben Firma!
➜ **Mehr auf Seite 4**

(IT-) Projekte und Projektportfolios erfolgreich prüfen und managen. Eine von ISACA gemeinsam mit dem Schweiz. Verband für Interne Revision (SVIR) durchgeführte Veranstaltung. Reservieren Sie sich den Donnerstag, 27. November.
➜ **Mehr auf Seite 3**

Die aktuellsten Veranstaltungs- und Kursdaten finden Sie auf
➜ **Seite 5**

Impressum

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

Redaktionsschluss
Nr. 9|2008:
5.Oktober 2008

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

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

Editorial

IT-Governance: Professionals und Wirtschaft in der Schweiz

Von der Global Leadership Conference, am 25. und 26. Juli 2008, in Toronto hat unsere Chapter-Präsidentin Daniela Geschwend Zahlen zu den Certification Programs mitgebracht. Demnach gab es per 26. Juli 2008 weltweit über 45'000 aktive CISAs, mehr als 8'000 aktive CISMs und bereits 364 CGEITs.

Und wie sehen die Zahlen in der Schweiz aus? Per August 2008 gab es im Switzerland Chapter 476 ISACA-zertifizierte Personen. Davon verfügten 372 über den CISA-Titel, 45 über den CISM, 54 über den CISA und den CISM, 2 über den CISA und den CGEIT sowie 3 über den CISA, den CISM und den CGEIT.

Für die Grösse unseres Landes stellt dies ein respektables Mass an IT-Governance, -Control und -Audit-Wissen dar.

Wo sind diese IT-Governance-Professionals im Einsatz? Etwa 30% sind im Finanzbereich beschäftigt, 21% in Prüf- und Beratungsfirmen, 12% in der Industrie, 9% bei IT-Dienstleistern, 7% in der öffentlichen Verwaltung, 4% bei nicht-IT-Dienstleistern und 17% lassen sich mangels genauerer Informationen nicht kategorisieren.

Gering ist der Anteil zertifizierter IT-Governance-Professionals bei den kleinen und mittleren Unternehmen (KMU). Er ist wesentlich kleiner als ihr Anteil an der schweizerischen Wertschöpfung.

Unsere Schwesterverband, die SwissICT, hat ein Programm lanciert, um der Schweizer Wirtschaft das Thema IT-Governance näher zu bringen. Erste Resultate von Umfragen sind allerdings ernüchternd: IT-Governance scheint gerade bei KMU ein Thema mit geringem Stellenwert zu sein.

Die Abhängigkeit der Wertschöpfung der KMU von Informations-Systemen ist heute schon gross und sie wird weiter zunehmen. Die SwissICT hat dies erkannt und sie glaubt, dass damit

➜ **Fortsetzung**

CISA 30 Certified Information Systems Auditor
CISM Certified Information Security Manager
IT Governance Institute

Insida

Does Your Control System Pass the COSO Test?

Offered to you by Peter R. Bitterli, CISA, CISM

In our eNewsletter 2008-5 we have already shown you some «tough» questions for members of executive management, the board and audit committees on effective internal control systems, published originally in March 1998 by the Institute of Internal Auditors. This time the questions are about the Internal Audit Function and the Audit Committee.

How Do You Know that the Internal Auditing Function is Effective?

Properly organized and effectively operated, internal auditing can give management and the audit committee a way to help monitor the reliability and integrity of financial and operating information.

- Does internal auditing have the support of top management, the audit committee, and the board of directors as a whole?
- Has the written scope of internal auditing responsibilities been reviewed by the audit committee for adequacy?
- Is the organizational relationship between internal auditing and senior executives appropriate?
- Does internal auditing have and use open lines of communication and private access to all senior officers and the audit committee?
- Are audit reports covering the right subjects, distributed to the right people, and acted upon in a timely manner?
- Do key audit executives possess an appropriate level of expertise?

How Can You Determine that the Board of Directors' Audit Committee is an Effective Process?

An enlightened and proactive audit committee is a powerful agent for corporate self-regulation.

- Has the board recently reviewed adequacy of the audit committee's written charter?
- Are audit committee members functioning and independent of management?
- Do audit committee members possess an appropriate mix of operating and financial control expertise?
- Does the audit committee understand and monitor the broad organizational control environment?
- Does the audit committee oversee appropriateness, relevance, and reliability of operational and financial reporting to the board, as well as to investors and other stakeholders and external users?
- Does the audit committee oversee existence of and compliance with ethical standards?
- Does the audit committee or full board have a meaningful but challenging relationship with independent external auditors, internal auditors, senior financial control executives, and key business-unit operating executives?

If you want to read more, look for the 1998 March issue No 2 published by The Institute of Internal Auditor.

IT-Governance: Professionals und Wirtschaft in der Schweiz

IT-Governance auch für Schweizer KMU zu einem wichtigen Thema werden muss. Dazu bedarf es der zielgruppengerechten Aufarbeitung.

«ISACA Serving IT Governance Professionals» sagt es: IT-Governance ist eines der Kernthemen der ISACA und das Switzerland Chapter mit 476 zertifizierten IT-Governance-Professionals ist in einer guten Ausgangslage, unsere Kollegen vom SwissICT im Bereich IT-Governance fachlich zu unterstützen.

Der Vorstand ist deshalb im Kontakte mit der IT-Governance Fachgruppe der SwissICT und diese ist stark an einer Zusammenarbeit interessiert.

Es wird an den Interessengruppen und Mitgliedern unseres Chapters liegen, die konkrete Unterstützungsarbeit zu leisten.

Hans.W. Kramer,
Koordinator IT-Governance

Inside

CISA- und CISM-Prüfungen Juni 2008

Autor: Umberto Annino, CISA-/CISM-Koordinator ISACA Switzerland Chapter

In meiner Rolle als CISA-/CISM-Koordinator des ISACA Switzerland Chapter durfte ich im Juni 2008 die «Feuertaufe» im Zürcher Marriott Hotel erleben, wo ich als Ansprechperson des Switzerland Chapter vor Ort an der «exam site», für mich erstmalig, zur Verfügung stand.

Glücklicherweise gab es keine Zwischenfälle oder Probleme bis auf wenige no-shows von angemeldeten Personen. Das Prüfungsreglement wurde diesmal von einem neuen Herrn des «examination body», der prüfungs-durchführenden Organisation, vorgelesen. Leider liegen bis heute noch keine detaillierten Statistiken (Punktzahlen pro knowledge area) vor, somit kann ich keine genauen Zahlen zu den Erfolgsquoten nennen. Wir (ISACA Switzerland) wissen durch die verfügbaren Statistiken jetzt schon, dass der CISM-Prüfungsvorbereitungskurs von Peter Bitterli bereits zum zweiten Mal 100% erfolgreiche Prüfungsabsolventen hervor gebracht hat!

Weitere interessante Zahlen im Zusammenhang mit den diesjährigen CISA-/CISM-Prüfungen:
36 erfolgreiche Absolventen der CISM-Prüfung (ISACA Members)
91 erfolgreiche Absolventen der CISA-Prüfung (ISACA Members)

Total 127 erfolgreiche Absolventen. Verglichen mit 4 CISM «non-member» Absolventen und 6 CISA «non-member» Absolventen zeigt sich, dass der grösste Teil der Prüfungskandidaten auch ISACA-Members sind. Wir würden uns natürlich freuen, auch die non-members bald zu Vereinsmitgliedern zählen zu dürfen!

Ein weiteres Novum dieses Jahres ist die Durchführung des traditionellen «CISA-/CISM Dinner» in der französischsprechenden Schweiz, nebst der Durchführung in Zürich. Die Einladung an die erfolgreichen Absolventen folgt separat durch das Sekretariat (wo angegeben per Email, sonst schriftlich); das Essen wird durch ISACA bezahlt. Sofern genügend Plätze vorhanden sind, dürfen «gestandene» CISA's und CISM's ebenfalls, auf eigene Kosten, teilnehmen.

Die Daten sind wie folgt:
Montag, 13. Oktober 2008, 19.00 Uhr
Café la Bruschetta, Avenue de la Gare 20, Lausanne

Montag, 20. Oktober 2008, 19.00 Uhr
Restaurant Au Premier, 1. Stock, im Hauptbahnhof Zürich

Anmeldungen mit Hinweis auf vegetarisch oder nicht-vegetarisch nimmt ➜ umberto.annino@swiss-life.ch entgegen.

Den bereits angemeldeten Kandidaten für die CISA- und CISM-Prüfungen im Dezember 2008 wünsche ich hiermit viel Erfolg! ■

„Top Scorer" der Juni-2008 Prüfungen

CISA
Stefan Zurkirch
Roger Hacmac
Christian Lochmatter

CISM
Peter R. Bitterli
Richard Lebeda
Martin Leuthold

Projekte und Projektportfolios erfolgreich prüfen und managen

Tagung in Zürich • 27. November 2008

Investitionen in (IT-) Projekte sollen einen klaren Geschäftsnutzen hervorbringen. Dabei müssen die Risiken von Projekten und Projektportfolios überwacht und durch ausreichend wirksame Massnahmen auf ein akzeptables Niveau reduziert werden. Einige Themenschwerpunkte aus dem Tagungsprogramm: Projektrisiken auf verschiedenen Ebenen, Projektmanagement (PM)-Governance, PM-Instrumente, Projektauswahl der Revision, Durchführung von Projektportfoliomanagement-Prüfungen, …

ISACA Serving IT Governance Professionals Switzerland Chapter

SVIR ASAI ASRI SIIA
SVIR Schweizerischer Verband für Interne Revision
ASAI Association suisse d'audit interne
ASRI Associazione svizzera di revisione interna
SIIA Swiss Institute of Internal Auditing

ISACA- und SVIR-Mitglieder erhalten noch eine detaillierte Kursausschreibung

After Hours Seminar • 30. September 2008 • 16:40 – 17:40

Identity und Access Management als Teil von Compliance

Referent: Marco Rohrer, ipg ag

Identity- und Access-Management-Lösungen (IAM) identifizieren Mitarbeitende und regeln ihre Zugriffsrechte auf Daten und Applikationen.

Erfahren Sie, wie mit «Role Life Cycle Management» und «Role-Based Access Control» solche Lösungen einfacher sowie effizienter werden und dabei helfen, relevante Gesetze und Standards einzuhalten

Aus dem Inhalt:
- Traditionelle Rechteverwaltung
- Inhärente Risiken
- Compliance Anforderungen
- Umfassende IAM-Suite: Transition und Benefit

Agenda

28. Oktober 2008
aktuelles Thema siehe: ➜ **www.isaca.ch**

25. November 2008
Spezialthema
Referent: Peter R. Bitterli, Bitterli Consulting AG

Seit Jahren ist es Tradition, dass das letzte After Hours Seminar des Jahres einem Thema im Umfeld unseres Berufs gewidmet ist und durch den Gastgeber abgedeckt wird.

25. Dezember 2008
Keine Veranstaltung über die Feiertage

Anmeldung für Mitglieder ➜ kurse@isaca.ch

Anmeldung für Gäste ➜ Bitte per Fax (PDF)

by Bitterli Consulting
itacs training

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

ITACS Training AG
Stampfenbachstr. 40
CH-8006 Zürich
Tel. +41 (0)44 444 11 01
kurse@itacs.ch

Application Security Lab • 1.–3. Oktober 2008

Workshop zum Thema Sicherheit in Web-Anwendungen mit praktischen Beispielen zu HTTP/S, J2EE, Web-Services und Datenbanken.

Der Kurs vermittelt Ihnen das notwendige Verständnis für die Sicherheit im Umfeld von Web-Anwendungen und -Services:
- Authentisierung & Autorisierung
- Cross-Site-Scripting
- SQL-Injection
- Phishing-Attacken
- Sichere E-Business-Infrastrukturen

Achtung: Ab dem 2. Teilnehmer derselben Firma kostet der Kurs die Hälfte!

➜ Detaillierte Informationen zum Kurs

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

ISACA Serving IT Governance Professionals Switzerland Chapter

ISACA-Kurse und -Veranstaltungen

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

1 – 3.10.2008	➜ **Application Security Lab** Web-Entwickler Kurs vom Applikationssicherheits-Spezialisten Compass
21. – 23.10.2008	➜ **Expertenkurs ISO27001/2** Ein Muss für Sicherheitsverantwortliche, Risikomanager und alle anderen, welche den Zwillingsstandard erfolgreich in ihrem Unternehmen umsetzen wollen
27.10.2008 Hotel Marriott, Zürich	**Projekte und Projektportfolios erfolgreich prüfen und managen** Gemeinsame Veranstaltung von ➜ SVIR und ➜ ISACA-CH
30.10 – 18.11.2008	➜ **CISM-Prüfungsvorbereitungskurs 2008|2** Für Informationssicherheitsbeauftragte: die kompakte Variante zur gezielten Vorbereitung auf die internationale CISM-Prüfung
5.11 – 19.11.2008	➜ **CISA-Prüfungsvorbereitungskurs 2008|2** Für IT-Prüfer/Sicherheitsspezialisten: die kompakte Variante zur gezielten Vorbereitung auf die internationale CISA-Prüfung
10. – 11.11.2008	➜ **ISO/IEC 20000 Auditor (Prüfung von Service Management-Prozessen)** Effiziente Prüfung von Service Management-Prozessen
12. – 14.11.2008	➜ **Virus/Trojan/Backdoor Security Lab** Sicherheit bei Anwendung von mobilem Code
26.11.2008	➜ **IT-Risikomanagement wirksam umsetzen** Grundbegriffe, Risikoanalysen für IT-Systeme, IT-Projekte und IT-Anwendungen. Strategisches Risikomanagement, ORM, ...
5.12.2008	➜ **ISMS gemäss ISO27001/2 implementieren und verrbessern** Die wichtigsten Elemente eines ISMS kennen und in 30 klaren Schritten implementieren oder verbessern
8. – 12.12.2008	➜ **Hacking Defense Training Week** Wirksame Verteidigung von Hacking-Angriffen mit anspruchsvollen Fallstudien – eine Intensivwoche (nur) für Fortgeschrittene!

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

➜ www.unige.ch	**La sécurité informatique** Enjeux juridiques et responsabilités	**28.11.2008** Université de Genève Genève

ISACA-Kurse und -Veranstaltungen

Audit des systèmes d'information

Préparation à la certification internationale CISA

La formation traite tous les domaines de l'audit des systèmes d'information, des aspects les plus techniques aux aspects les plus organisationnels. Elle couvre les thèmes suivants :

- processus d'audit des systèmes informatiques,
- gouvernance des SI,
- gestion du cycle de vie et de l'infrastructure des systèmes,
- fourniture et support des services,
- protection des avoirs informatiques,
- plan de continuité et de secours informatique.

La certification CISA démontre que son titulaire dispose des connaissances, des compétences et de l'expérience pratique pour assurer que les technologies de l'information et les systèmes de son organisation sont protégés et contrôlés.

Cycle printemps 2009 à Genève
www.iseig.ch

14 jours, du 12 février au 16 mai 2009, de 9:00 à 17:00

ISEIG
Av. des Boveresses 52
CH-1010 Lausanne
Tél. +41 21 654 40 60
info@iseig.ch

ISEIG est le partenaire officiel et exclusif du Chapitre suisse de l'ISACA pour la Suisse romande

Management de la sécurité des systèmes d'information

Préparation à la certification internationale CISM

La formation orientée métier et gestion des risques informatiques aborde les problématiques de sécurité en terme de management, de conception et de mise en oeuvre. Elle couvre les thèmes suivants :

- gouvernance de la sécurité,
- management des risques,
- schéma directeur de la sécurité des systèmes d'information,
- gestion de la sécurité,
- gestion de crise.

Cette formation est destinée aux managers expérimentés en sécurité des systèmes d'information. Elle se base sur le programme défini et constamment actualisé par l'ISACA. Celui-ci regroupe les connaissances indispensables exigées pour faire d'un collaborateur en sécurité un véritable manager en sécurité des systèmes d'information.

Cycle printemps 2009 à Genève
www.iseig.ch

12 jours, du 16 février au 15 mai 2009 de 14:00 à 21:00

ISEIG
Av. des Boveresses 52
CH-1010 Lausanne
Tél. +41 21 654 40 60
info@iseig.ch

ISEIG est le partenaire officiel et exclusif du Chapitre suisse de l'ISACA pour la Suisse romande