ISACA Newsletter FEBRUAR 2009

newsletter

ISACA 20 JAHRE ANS ANNI
Serving IT Governance Professionals
Switzerland Chapter

After Hours Seminar

Zürich • Dienstag, 24.2.2009 • 16:40 – 17:40
Service-Management im IT-Outsourcing-Umfeld
Eine prozessorientierte Analyse mit Hilfe von CobiT und einem neuronalen Framework

➜ Mehr auf Seite 5

Focus

Haben Sie die neuen Schweizer Gesetze im Griff?

➜ Mehr auf Seite 2

Inside

Congratulation Glenfis! ➜ Mehr auf Seite 4

Swiss Cyber Storm II
Das grösste europäische Computer Wargame

➜ Mehr auf Seite 4

ISACA-Kurse und -Veranstaltungen

Beachten das neue Kusangebot auf ➜ www.itacs.ch

Die aktuellsten Veranstaltungs- und Kursdaten ➜ Seite 6

ISACA Switzerland Chapter • Vereinsversammlung 2009
31. März 2009 • Zürich

Impressum

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

Redaktionsschluss
Nr. MAR|2009:
5. März 2009

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

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

Editorial

In Zeiten weltweiter Rezession bekommt der Megatrend des Jahres – Virtualisierung – ein neues Gesicht. Unternehmer reduzieren ihre IT-Ausgaben, indem sie ressourcenhungrige Server in virtuelle Maschinen zusammenfassen. Einsparungen von 30 bis 50 % betreffen nicht nur Speichertechniken, Raum und Energie, sondern auch Unterhalt von Betriebssystemen und Applikationen. Ausschlaggebend ist auch die Kostenfrage bei Entscheidungen für das Outsourcing oder Offshoring.

Bei den erwähnten Fällen stehen ebenso die Komplexität des IT-Umfeldes sowie die Fähigkeiten der Betroffenen im Mittelpunkt. Insbesondere beim Outsourcing/Offshoring nach Osteuropa oder Fernost sind zusätzlich kulturelle und sprachliche Kompetenzen gefragt. Doch nicht alles, was technisch machbar ist, erweist sich im Unternehmen als praktikabel und profitabel. Es gilt vielmehr auch für Compliance-Anforderungen, wie jahrelanges Speichern und Schützen von unternehmensrelevanten Daten und Informationen, gerüstet zu sein. Trotz allem bleibt dem Wirtschaftsinformatiker, IT-Revisor oder IT-Sicherheitsbeauftragen nichts anderes übrig, als sich den neuen Anforderungen nachhaltig zu stellen.

Dank den ISACA IS Auditing Standards, Guidelines und Procedures sowie den vorhandenen Workpapers (Knet), Fachbüchern (Bookstore), Kursen und Konferenzen können die notwendigen Fähigkeiten angeeignet werden. Empfehlenswert für neue Prüfungsbereiche wie z.B. Virtualisierung und Outsourcing ist auch die Bildung von Interessengruppen (IG), welche von unserem ISACA IG-Koordinator unterstützt werden. Ziel sollte sein, das notwendige Know-how zu erarbeiten, um risikoorientierte Prüfungen durchführen und das IKS sicherstellen zu können. Gerade im Zusammenhang mit neuen rechtlichen Anforderungen kann die Glaubwürdigkeit und das Know-how eines «State of the Art» Revisors von Vorteil sein.

Unternehmen erwarten, dass Mitarbeitende egal welchen Alters lernbereit und lernfähig sind, um neues Wissen gewinnbringend anzuwenden. Es ist daher wichtig, die Aus- und Weiterbildung proaktiv und prophylaktisch anzugehen und nicht erst dann, wenn man feststellt, dass sie fehlt.

Bruno Wiederkehr, ISACA Vorstandmitglied

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

Focus

Haben Sie die neuen Schweizer Gesetze im Griff?

Autor: Bruno Wiederkehr

Die vom Gesetzgeber beschlossenen Neuerungen und nicht zuletzt im Zuge der internationalen Entwicklungen – Finanzkrise, Subprime-Sumpf, Milliardenskandal um Parmalat, Steuerskandal mit Datenklau LGT und nationalen Wirtschaftsskandale – Swissair Grounding, Konkurs der Erb-Gruppe zielen darauf ab, das Vertrauen in die Unternehmen und in die Schweizer Wirtschaft insgesamt zu stärken. Mit der abgelaufenen Referendumsfrist hat der Bundesrat die betroffenen Änderungen im Revisions- und Gesellschaftsrecht per 1.1.2008 in Kraft gesetzt.

Welche Unternehmen werden durch die Gesetzesbestimmungen beeinflusst?

Neue Gesetze bringen wesentliche Änderungen für Unternehmen. Sie betreffen auch den Inhalt und den Umfang der internen und externen Revision. Folgende Gesellschaftsformen sind davon betroffen: AG, GmbH, Genossenschaft, Stiftungen und Vereine.

- Kleinere Unternehmen zwischen 10 und 50 Vollzeitstellen können ihre Bücher noch eingeschränkt prüfen lassen. Trotzdem besteht die Pflicht, jährlich eine Risikobeurteilung durchzuführen.
- Für grössere Unternehmen mit mehr als 50 Vollzeitbeschäftigten gibt es keine Erleichterung aber den gesetzlichen Zwang für eine Risikobeurteilung durch den Verwaltungsrat und für die Bestätigung der Existenz eines IKS (Internes Kontrollsystem) durch die Revisionsstelle.

Welche Änderungen in den neuen Gesetzesbestimmungen betrifft die ICT?

Die Änderungen im Gesellschaftsrecht und das Bundesgesetz über die staatliche Überwachung der Revisionsstelle betreffen die ICT im Umgang mit Risiken sowie technischen und organisatorischen Kontrollen bzw. Massnahmen, soweit die betroffenen Unternehmensteile oder Software-Programme einen Beitrag zur Finanzberichterstattung leisten.

Welche Gesetzesartikel sind von Bedeutung?

OR 663b Ziffer 12 verlangt, dass die Risikobeurteilung als Bestandteil der Jahresrechnung durchgeführt und darüber Bericht erstattet wird.

OR 728a und b verlangen, dass bei grösseren Unternehmen durch die Revisionsstelle die Existenz eines IKS geprüft wird und die Risiken im Anhang des Geschäftsberichtes aufgezeigt werden.

Wer in den Unternehmen ist für die Umsetzung der OR-Artikel verantwortlich?

Die beiden erwähnten Gesetzesartikel sind eng miteinander verbunden. Für die Risikobeurteilung und -bewältigung sowie die Kontrolle der Wirksamkeit des IKS sind der Verwaltungsrat bzw. das Audit Committee und die Geschäftsleitung verantwortlich. Durch die Verflechtung von Risikomanagement und interner Kontrolle ergibt sich ein zuverlässiges Frühwarn- und Kontrollsystem.

Welche Fragen muss heute ein Unternehmen dem ICT-Revisor beantworten können?

1. Wie werden Wirksamkeit und Wirtschaftlichkeit der wesentlichen ICT-Kontrollen vom Verwaltungsrat bzw. Audit Committee und von der Geschäftsleitung erörtert?

2. Erfolgt eine regelmässige Neubeurteilung der wesentlichen ICT-Risiken und -Kontrollen verbunden mit den Geschäftsanforderungen?

3. Werden die Kosten der ICT Kontroll- und Sicherheitsmassnahmen unter Berücksichtigung des Nutzens und im Verhältnis zum Unternehmens-Risiko beurteilt?

4. Wo und in welcher Form findet die Rapportierung über die gesetzlichen Neuerungen hinsichtlich Risiken und Kontrollen statt?

➜ **Fortsetzung**

Inside

Fortsetzung: Haben Sie die neuen Schweizer Gesetze im Griff?

Unter Mitwirkung des ISACA Switzerland Chapters hat eine Fachveranstaltung «IKS sicher und OR konform» zu diesen Fragestellungen stattgefunden. Dabei wurden bei der ordnungsgemässen Berichterstattung folgende Aspekte hervorgehoben:

Gesetzliche Anforderung	Formale Berichterstattung: Aussteller / Empfänger
OR 663 Risikobeurteilung durchgeführt mit Angabe vorhandener Risiken	Im Anhang des Geschäftsberichtes des Unternehmens z.Hd. der Aktionäre / Generalversammlung
OR 728 die Existenz des IKS mit Angaben vorhandener Kontroll-Lücken	Revisionsbericht der Abschlussprüfer z.Hd. des Verwaltungsrates und der Geschäftsleitung

Fazit

Mit einem integrierten Risikomanagement-Prozess und der laufenden Überprüfung des IKS eröffnen sich dem Unternehmen und der ICT die Chance zwei wesentliche Führungsinstrumente systematisch und kostengünstig zu verbinden sowie die geforderte Compliance sicherzustellen.

Die Umsetzung der neuen Anforderungen setzen ein aktives Engagement sowohl der Führungsgremien als auch von der internen und externen Revision voraus. Insgesamt führen die betroffenen Gesetzesartikel zu weitreichenden Veränderungen der Corporate und IT Governance.

Ausblick

Auf Änderungen im Bundesgesetz über den Datenschutz (DSG) und deren Auswirkungen auf die ICT wird in einem folgenden ISACA eNewsletter eingegangen. Die Neuerungen wurden ebenfalls am 1.1.2008 mit einer Übergangsfrist bis 1.1.2009 in Kraft gesetzt. ■

SPOL
WHAT PROJECTS WANT

Tagesseminar PM-Excellence Controlling

10. März 2009 • Mit Bruno Jenny • Hotel Spirgarten am Lindenplatz • Zürich-Altstetten

Lernen Sie am PM-Excellence-Tag Controlling mit dem Projektmanagement-Spezialisten Bruno Jenny, wie Sie ein Projekt effizient und ergebnisbezogen kontrollieren können.

Projekt-Controlling ist ein wichtiger Bestandteil des Projektmanagements! Wir befähigen Sie, mit den richtigen Methoden und Instrumenten ein Projektcontrolling aufzubauen und effizient zu nutzen.

Bruno Jenny:
«Wir kontrollieren nicht zu wenig, sondern oftmals zuviel das Falsche!»

Weitere Informationen und Anmeldung unter ➜ www.spol.ch

Exklusiv für ISACA-Mitglieder CHF 750.00 statt CHF 850.00

Inside

Swiss Cyber Storm II

Autor: Ivan Bütler

Bereits zum zweiten Mal findet über das Wochenende vom 18./19. April 2009 in der Aula der FH Rapperswil das grösste europäische Computer Wargame «Swiss Cyber Storm II» statt. Wie macht man sicheres E-Banking? Wie schütze ich mich vor aktuellen Viren und Trojanern? Warum können Hacker in Computersysteme eindringen? Was ist ein Botnet? Warum ist die Firewall nicht das Allerheilmittel im Kampf gegen Computer-Kriminalität? Wie sicher sind Social Networks wie Facebook oder Xing?

Die Veranstaltung richtet sich sowohl an Fach-Spezialisten als auch an Informatik-Studenten und andere an Computern interessierten Personen. In leicht verständlichen Präsentationen informieren Security-Spezialisten über die Gefahren im Internet und geben praktische Tipps für einen sicheren Umgang im Alltag. Für jene, die auch selbst am Computer in die Rolle des Angreifers schlüpfen wollen, stehen über 25 Computer-Rätsel in sogenannten Wargames bereit, um sich intensiver mit den Hacker-Methoden und der notwendigen Abwehr auseinander zu setzen.

Zuschauen ist gratis – mitmachen kostet für ISACA-Mitglieder nur gerade CHF 22.– (50% Rabatt).

Veranstalter sind gemeinsam unser Ausbildungspartner Compass Security AG sowie die Fachhochschule Rapperswil. Weitere Informationen sowie die Möglichkeit zur Online-Registrierung finden Sie unter:

➜ **http://www.hacking-lab.com**

Congratulation Glenfis!

Autor: Bruno Wiederkehr

Anlässlich eines Besuches bei unserem Ausbildungspartner Glenfis AG gratuliert Bruno Wiederkehr, als Vorstandsmitglied der ISACA, Glenfis Geschäftsführer Martin Andenmatten zum CGEIT Certified in the Governance of Enterprise IT (Bild unten).

Ebenso erfreulich und wertvoll für das ISACA Switzerland Chapter ist, dass Martin Andenmatten als Erster in der Schweiz im Jahre 2008 den «Certified CobiT Foundation Course Trainer» erworben hat.

Auf der ISACA-Website und in der neuen Kursbroschüre 2009|1 ist der neue ISACA-Zertifikatskurs CobiT 4.1 Foundation mit international standardisiertem Curriculum und abschliessendem Zertifikat beschrieben.

ISACA 20 JAHRE ANS ANNI
Serving IT Governance Professionals
Switzerland Chapter

Bitte reservieren Sie sich den
25. August 2009
für den Jubiläumsanlass
Weitere Informationen folgen

After Hours Seminar

Dienstag, 24.2.2009 • 16:40 – 17:40 • Zürich • Stampfenbachstrasse 40

Service-Management im IT-Outsourcing-Umfeld – eine prozessorientierte Analyse mit Hilfe von CobiT und einem neuronalen Framework

Referent: Andres Wohler

Auf Grund regulatorischer Bestimmungen ist es für Unternehmen immer entscheidender, engmaschige Kontroll- und Risiko-Management-Systeme zu etablieren. Im IT-Umfeld können Konkretisierungen anhand erprobter und verbreiteter Standards in diesem Zusammenhang sinnvoll sein. Dabei prägen sich IT-Organisationen als komplexe und mehrdimensionale Organisationen. Diese richten sich auf die Geschäftsprozesse aus und umgekehrt. Jede Organisation ist massgebend von dieser Vernetzung ihrer Agenten mit der Umwelt und deren Knowledge abhängig.

Kombiniert man diese Aussagen in ein wissenschaftliches Framework, so entsteht in Anlehnung an Gehms organisationspsychologisches Model der kooperativen Informationsverarbeitung die Idee, Organisationen analog einem neuronalen Netzwerk zu analysieren. Welches Potenzial diese Denkschule in Bezug auf das Management von IT-Outsourcing-Cases mit sich bringt, ist Gegenstand des Referates.

Andres Wohler beschreibt in Anlehnung an seine wirtschaftswissenschaftliche Arbeit Verfahren, wie durch die Vernetzung von Personen branchenübliche Standards und Prozesse entstehen können. Unter Zuhilfenahme von CobiT geht er der Frage nach, wie Menschen mit Prozessen interagieren und welchen Einfluss Wahrnehmung und die Interpretation von Rollen auf diese Interaktion hat. Daraus können Analysemethoden und grundlegende Schlüsse für das Management von IT-Organisationen aufgezeigt werden.

Anmeldung für Mitglieder ➜ kurse@isaca.ch ■

by Bitterli Consulting
itacs training

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

Avaloq-Einführung für IT-Revisoren/Sicherheitsbeauftragte
9.–13. März 2009 • wird durchgeführt • ➜ **Anmeldung noch möglich**
Avaloq verstehen als Grundlage für effiziente Prüfungen

Virus/Trojan/Backdoor Security Lab • 16.–18. März 2009
Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung durch mobile Technologien und aktuelle Malware

Von IT Governance bis IT Security Management – wirksamer Einsatz von CobiT 4.1 • 23.–25. Mätz 2009
Anwendung des internationalen Standards auf die wichtigsten Governance-Themen Security, Risk Management, Projekt Management, usw.

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

ISACA-Kurse und -Veranstaltungen

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

9.3.09 – 13.3.09	➜ **Avaloq-Einführung für IT-Revisoren/Sicherheitsbeauftragte • Garantierte Durchführung** Bedienung des Avaloq Banking Systems. Vertiefung in Parametrisierung u.a. von Security-, Workflow- und Rule Engine
19.3.09 – 20.3.09	➜ **Leadership-Seminar für Revisoren und Sicherheitsbeauftragte** Verbesserung des persönlichen Kommunikationsverhaltens von Revisoren/Sicherheitsbeauftragten in kritischen Situationen
23.3.09 – 25.3.09	➜ **Von IT Governance bis IT Security Management – wirksamer Einsatz von CobiT 4.1** Praxisorientierte Anwendung von CobiT 4.1 für IT-Governance in ausgewählten Schwerpunktbereichen – mit dem Herausgeber des ersten deutschsprachigen CobiT-Buches
23.3.09 – 13.5.09	➜ **CGEIT Zertifikatskurs 09|1 (verkürzter Kurs für Prüfung im Juni 09)** Vertieftes theoretisches wie praktisches Fachwissen im breiten Feld von IT-Governance wie: strategische Ausrichtung, Wertschöpfung, Risikomanagement, Ressourcenmanagement und Leistungsmessung in der Informationstechnologie (IT). Intensive Vorbereitung auf die von ISACA organisierte CGEIT-Prüfung.
26.–27.3.09	➜ **Prüfung und Berichterstattung bei Outsourcing-Providern** Standardisierte Prüfungen im Outsourcing-Umfeld – ein Kurs für Provider und deren Kunden (mit Provider-Gastreferat!)
30.3.09	➜ **ISMS gemäss ISO27001/2 implementieren und verbessern** Die wichtigsten Elemente eines ISMS kennen und in 30 klaren Schritten implementieren oder verbessern
31.3.09	➜ **ISACA Switzerland Chapter Vereinsversammlung 2009**
1.4.09	➜ **IKS in IT revisionssicher implementieren (Kompaktkurs)** Effiziente Vorbereitung auf (angekündigte) Revisionen und Schutz vor übertriebenen Forderungen
2.4.09 – 12.5.09	➜ **CISM-Prüfungsvorbereitungskurs 2009|1** 4tägiger Kompaktkurs für erfahrene Sicherheitsbeauftragte. Die gezielte Vorbereitung auf die internationale CISM-Prüfung

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

➜ RSSI 2009	**RSSI 2009, Rencontre Suisse de la Sécurité Informatique** Tarif préférentiel pour les membres de l'ISACA	**17. 3. 2009** Four Seasons Hôtel des Bergues, Genève
➜ www.hacking-lab.com	**Swiss Cyber Storm II** Security Event and Wargames 50% Rabatt für alle ISACA-Mitglieder	**18. + 19.4.2009** Aula Fachhochschule Rapperswil
➜ 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