ISACA Newsletter Februar 2010

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

newsletter

Vereinsversammlung

Zürich • Dienstag, 23. 2. 2010
Ort • Ernst & Young AG, Brandschenkestrasse 100
Vereinsversammlung • 15:00 – 16:15 Uhr
Referat von Andreas Toggwyler • 16.30 – 17.30 Uhr

Andreas Toggwyler, Partner bei der KPMG, welcher 2 Jahre in den USA war, wird ein spannendes Referat zum Thema «Der kleine Unterschied – Erfahrungsbericht eines Heimkehrers» halten.

➜ Detaillierte Informationen

Focus

IT-Sicherheit verbessern hat hohe Priorität für Unternehmen

Die Erhebung zum Thema IT-Sicherheit und Risiko-Management wurde zwischen Juni und Juli 2009 durchgeführt. Die Ergebnisse basieren auf Interviews mit Führungskräften aus über 1'900 Unternehmen sämtlicher Branchen.

➜ Mehr auf Seite 2

ISACA-Kurse und -Veranstaltungen

Die aktuellsten Veranstaltungs- und Kursdaten ➜ Seite 6

Impressum

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

Redaktionsschluss:
11. März 2010

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

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

ISACA/SVIR-Tagung

Donnerstag, 29. April 2010 • Zürich
Tagungsthema: «Zusammenarbeit zwischen interner und externer (IT-) Prüfung»

Editorial

Liebe ISACA Schweiz Mitglieder,

Wir haben ein ereignisreiches und in vielen Gebieten erfolgreiches Vereinsjahr hinter uns. Im August 2009 durften wir unser 20-jähriges Bestehen als Chapter mit einem Jubiläumsevent feiern: an der Tagung zu IT-Governance-Themen nahmen rund 200 Personen teil, am gemütlichen Abendanlass für ISACA-Mitglieder und deren Partner/innen waren es rund 160 Personen. Bestimmt können Sie sich vorstellen, dass die Vorbereitungszeit intensiv war und uns einigen Aufwand und graue Haare gekostet hat. Der überwiegend positive Feedback zu diesem Event hat uns für diese Arbeit jedoch entschädigt. Verbesserungsvorschläge sind uns jedoch ebenfalls ein Ansporn, im Vorstand fortwährend am Service-Angebot unseres Chapters zu arbeiten. Natürlich fliessen Ihre Anregungen während des Jahres auch in unsere Aktivitäten ein.

Die Arbeiten über das Jahr hindurch sind hauptsächlich auf den Schultern der Vorstandsmitglieder verteilt. Während unseren Vorstandssitzungen finden wir immer wieder Aufgaben, die eine Einzelperson oder ein kleines Team lösen könnte und die eigentlich "frische" Ansichten und Ideen fordern. In solchen Fällen wären wir froh, wenn wir auf weitere Resourcen zugreifen könnten - Resourcen in Form von freiwilligen Helfern. Es kann sich dabei um das Schreiben eines Artikels, um das Erstellen und Umsetzen eines Sponsoringkonzeptes, um Hilfeleistung bei der Organisation eines Events oder Kontakte mit Universitäten handeln. Sind Sie interessiert, uns zu unterstützen? Melden Sie sich bitte beim ISACA-Vereinssekretariat.

Die Vereinsversammlung findet am 23. Februar 2010 statt und wir freuen uns, Ihnen dort über unsere Aktivitäten berichten zu dürfen. Wir werden dabei Ideen vorstellen und Ihre Meinung dazu abholen. Wie jedes Jahr wird die Versammlung von einem spannenden Vortrag begleitet. Details zur Versammlung und zum Vortrag entnehmen Sie bitte diesem Newsletter oder unserer Webseite.

Bezüglich einer zukünftigen EuroCACS in der Schweiz haben wir noch keine weiteren Informationen vom ISACA Headquarter, werden Sie jedoch über Entwicklungen in dieser Richtung auf dem Laufenden halten.

Ich würde mich freuen, Sie an der Vereinsversammlung oder einem anderen Anlass begrüssen zu dürfen.

Freundliche Grüsse,
Daniela Gschwend, Präsidentin

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

Focus

IT-Sicherheit verbessern hat hohe Priorität für Unternehmen

Autor: Yan Borboen

Der Ernst & Young 2009 Global Information Security Survey wurde in über sechzig Ländern entwickelt. Die Erhebung wurde zwischen Juni und Juli 2009 durchgeführt. Die Ergebnisse basieren auf Interviews mit Führungskräften aus über 1'900 Unternehmen sämtlicher Branchen.

IT-Sicherheit verbessern hat hohe Priorität für Unternehmen
1. Drei Viertel der Führungskräfte in Unternehmen weltweit befürchten mögliche Vergeltungsaktionen von kürzlich ausgeschiedenen Mitarbeitern.
2. Für die Hälfte der Befragten ist die Durchsetzung eines adäquaten Budgets für IT-Sicherheit eine grosse Herausforderung.
3. Nur 41 Prozent der Unternehmen weltweit verschlüsseln Daten auf ihren Laptops.
4. Unternehmen wollen sich vor zunehmendem Datendiebstahl mit Data Leakage Prevention-Technologien (DLP) schützen.
5. Regulierung ist noch immer ein wichtiger Treiber für IT-Sicherheit.

Vergeltung durch ausgeschiedene Mitarbeiter

Risiken bzgl. Vergeltungsaktionen durch ausgeschiedene und unzufriedene Mitarbeiter werden für Unternehmen weltweit zunehmend zur Herausforderung und erschweren die bereits in den vergangenen Jahren aufgezeigten Schwierigkeiten durch unzureichende Budgets und Ressourcen für IT-Sicherheit. Gleichzeitig nehmen die Fälle von Datendiebstahl zu und viele Unternehmen wollen sich mittels entsprechender Technologien schützen. Das ergab der zwölfte Ernst & Young Global Information Security Survey, welcher unter 1.900 Führungskräften in Unternehmen aus mehr als 60 Ländern durchgeführt wurde.

Drei Viertel der Führungskräfte in Unternehmen weltweit befürchten mögliche Vergeltungsaktionen durch Mitarbeiter, von denen man sich unlängst trennen musste. 42 Prozent setzen sich intensiv mit den potentiellen Risiken dieser Thematik auseinander und bereits 26 Prozent ergreifen aktiv Gegenmassnahmen.

In der Schweiz ist dies auch ein akutes Thema, allerdings wird nur von 17 Prozent der Unternehmen angegeben, dass dies als sehr hohes Risiko eingestuft wird und bereits aktiv Gegenmassnahmen ergriffen wurden. 34% der Unternehmen sind noch dabei, die potentiellen Risiken zu evaluieren, um dann über geeignete Gegenmassnahmen zu entscheiden.

➜ **Fortsetzung**

by Bitterli Consulting
itacs training
➜ www.itacs.ch

Avaloq-Einführung für IT-Revisoren und IT-Sicherheitsbeauftragte

Dieser Kurs richtet sich an Sie als IT-Revisor mit einem guten Verständnis für Bank- und IT-Prozesse. Sie wollen einen Einstieg ins Avaloq-Umfeld und wollen erste praktische Erfahrungen mit dem System machen. Im Rahmen des Kurses erhalten Sie Zugriff auf die Avaloq Academy IT-Infrastruktur mit einer speziellen Modell-Bank für die Übungen am Avaloq-System.

Montag, 8. März – Freitag, 12. März 2010

Focus

Fortsetzung: IT-Sicherheit verbessern …

Zu wenig Budget für Informationssicherheit

Für etwa die Hälfte der Befragten ist die Zuteilung adäquater Budgets für Informationssicherheit eine grosse Herausforderung. Verglichen mit den Befragungsergebnissen 2008 bedeutet dies einen deutlich spürbaren Zuwachs von 17 Prozentpunkten. Nur 6 Prozent aller Befragten in der Schweiz geben an, dass sie keine Herausforderung in ihrem aktuellen Budget sehen. Dies reflektiert die erhöhten Ansprüche an die IT-Sicherheit, sowie die wirtschaftlichen Zwänge, welcher sich auch die Informationssicherheit nicht entziehen kann. Dennoch wollen 40 Prozent ihr Jahresbudget für IT-Sicherheit im Verhältnis zu den Gesamtausgaben erhöhen, während 52 Prozent planen, es eher konstant zu halten.

Laptops grossteils unzureichend geschützt

Nur 41 Prozent der Befragten weltweit geben an, Daten auf Laptops zu verschlüsseln, und lediglich 17 Prozent planen, dies im kommenden Jahr noch zu tun. Und das, obwohl die Zahl der bekannt gewordenen unberechtigten Zugriffe aufgrund von Verlust oder Diebstahl zunimmt.

Dies ist sicherlich ein alarmierendes Ergebnis, jedoch sind in der Schweiz die Laptops bei 80% aller befragten Unternehmen verschlüsselt, und 16 Prozent planen dies innerhalb der nächsten zwölf Monate noch zu implementieren.

Einsatz von Technologien für die Informationssicherheit

Durch zunehmende Datenschutzverstösse mit erheblicher Publizität steht der Datenschutz für viele Führungskräfte im Bereich der Informationssicherheit ganz oben auf der Agenda. Die Implementierung oder Verbesserung sogenannter Data Leakage Prevention (DLP)-Technologien ist insgesamt die zweitwichtigste Priorität für das kommende Jahr – für 40% Prozent der Befragten ist DLP eine der Top-3-Prioritäten. In der Schweiz wollen rund 45 % der Befragten mehr in DLP-Technologien investieren.

➜ Fortsetzung

by Bitterli Consulting
itacs training

Leadership-Seminar für Revisoren und Sicherheitsbeauftragte

Das zweitägige Leadership-Seminar richtet sich an Revisoren und Sicherheitsbeauftragte, die ihre Führungsfunktion weiterentwickeln wollen, neu in einer Teamleiterrolle sind oder sich auf eine solche Funktion vorbereiten möchten.
Das Leadership-Seminar ermöglicht den Teilnehmenden, sich intensiv mit ihrer Führungsrolle als Teamleiter im Revisions- oder Sicherheitsumfeld auseinander zusetzen und anspruchsvolle Führungssituationen kompetent zu bewältigen.

Dienstag, 16. März/Mittwoch, 17. März 2010

Einführung in Enterprise Risk Management

Der Kurs richtet sich primär an Personen, welche mit dem Aufbau oder der Beurteilung des unternehmensweiten und operativen Risikomanagement betraut sind. Von grossem Interesse ist dieser als Workshop aufgebaute Kurs für Risikomanager aus allen betrieblichen Bereichen wie Finanzen, IT oder Technik, für Leiter der Organisationsentwicklung, Geschäftsleitungsmitglieder und Inhaber von KMU's.

Donnerstag, 18. März 2010

ISMS gemäss ISO 27001/2/4/5 implementieren und verbessern

Der Kurs richtet sich an alle Personen, welche in kurzer Zeit alles Wesentliche über den internationalen Standard ISO 27001 – ISO 27005 erfahren und diesen im Rahmen ihrer Tätigkeiten produktiv einsetzen wollen: Sicherheitsverantwortliche, Datenschutz-Beauftragte, Risikomanager, ISO 27001-Auditoren und IT-Revisoren. Informatik-Kenntnisse sind nicht notwendig.

Mittwoch, 31. März 2010

➜ www.itacs.ch

Focus

Vereinsversammlung 2010

- **Dienstag, 23. Februar 2008 • Zürich**
- **Bei Ernst & Young AG, Brandschenkestrasse 100 • ➜ Anfahrts- und Situatuionsplan**

- **Vereinsversammlung** 15.00 – 16.15 Uhr
- **Referat** 16.30 – 17.30 Uhr
  Andreas Toggwyler, Partner bei der KPMG, welcher 2 Jahre in den USA war, wird ein spannendes Referat zum Thema «Der kleine Unterschied – Erfahrungsbericht eines Heimkehrers» halten.
- **Apéro**

ISACA/SVIR-Tagung

Am **Donnerstag, 29. April 2010** findet die ISACA/SVIR-Tagung zum Thema «Zusammenarbeit zwischen interner und externer (IT) Prüfung» in Zürich statt. Bitte reservieren Sie sich den Termin.

Fortsetzung: IT-Sicherheit verbessern …

DLP bezeichnet die Kombination verschiedener Massnahmen und Prozesse zur Identifikation, Überwachung und zum Schutz von sensiblen Daten und Informationen vor unzulässigem Abfluss bzw. Entwendung.

Regulierung als Treiber für IT-Sicherheit

Die Sicherstellung der Einhaltung gesetzlicher Anforderungen hat für viele der befragten Führungskräfte seit mehreren Jahren eine Top-Priorität: 2009 gaben 55 Prozent der Befragten an, dass Compliance-Anforderungen die Ursache für eine moderate bis deutliche Erhöhung ihrer Kosten im Bereich Informationssicherheit waren. Während diese Zahl von 65 Prozent in den letzten drei Jahren rückläufig ist, geben nur 5% aller Befragten an, dass sie dieses Jahr weniger ausgeben werden.

Lediglich 7% der Befragten in der Schweiz wollen in den kommenden zwölf Monaten ihre Ausgaben in diesem Bereich senken, während 90% mit denselben Kosten wie im Vorjahr planen.

Grund dafür ist möglicherweise, dass zu viel vom Budget für Informationssicherheit für Projekte benötigt wird, mit denen eine rechtzeitige und ge-

➜ **Fortsetzung**

by Bitterli Consulting
itacs training

Design und Prüfung von anwendungsabhängigen Kontrollen (IKS)

Der bewährte Kurs wurde auf zwei Tage erweitert und richtet sich primär an Personen, welche an der Entwicklung oder Prüfung von anwendungsabhängigen Kontrollen beteiligt sind, also IKS-Verantwortliche, IT-Projektleiter, Anwendungsentwickler, Sicherheitsspezialisten und Finanz- wie IT-Prüfer.

Donnerstag, 11. März und Freitag, 12. März 2010

Einführung in das Interne Kontrollsystem (IKS-Kompaktkurs)

Der Kurs richtet sich an alle, welche mit Betrieb, Beurteilung und Optimierung des IKS betraut sind (Geschäftsleitung, Finanzverantwortliche, Risikomanager, Controller und Revisoren) und ist insbesondere für Praktiker aus der Unternehmung – auch ohne entsprechende Vorkenntnisse – geeignet.

Freitag, 19. März 2010

➜ www.itacs.ch

Focus

Fortsetzung: IT-Sicherheit verbessern …

zielte Einhaltung von spezifischen Regulierungsvorgaben erreicht werden muss. Diese Mittel stehen dann nicht für systematische Informationssicherheitsprogramme zur Verfügung, bei denen die Einhaltung regulatorischer oder gesetzlicher Vorgaben ein Nebenprodukt und nicht der primäre Treiber ist.

Wenn der Fokus primär auf Risiken und nicht die Einhaltung von Regulierungsvorgaben gelegt wird, können Kosteneinsparungen oder Leistungsverbesserungen in der Informationssicherheit erreicht werden.

Die Top-Prioritäten für Unternehmen im Bereich Informationssicherheit

- **Risikomanagement verbessern**
  - Verbesserung des Risikomanagements im Bereich Informationssicherheit
  - Zunehmende externe und interne Attacken auf Informationssysteme
  - Ausgeschiedene Mitarbeiter als Informationssicherheitsrisiko
- **Herausforderungen bewältigen**
  - Professionelle und qualifizierte IT-Sicherheitsressourcen sind der Schlüssel zu erfolgreichen Initiativen in diesem Gebiet
  - Zu wenig Budget für IT-Sicherheit
  - Interne Trainings und Bewusstmachung zum Thema IT-Sicherheit kommen in den meisten Unternehmen zu kurz
- **Regulatorische Vorgaben einhalten**
  - Regulatorische Anforderungen sind noch immer ein wichtiger Treiber für IT-Sicherheit
  - Kosten zur Einhaltung regulatorischer Anforderungen sind nach wie vor hoch
  - Nur wenige Unternehmen schützen persönliche Daten ausreichend
- **Technologien richtig nutzen und Potentiale ausschöpfen**
  - Einführung von Data Leakage Protection (DLP)-Technologien ist aktuell eine hohe Priorität für viele Unternehmen
  - Nichtverschlüsselung von Laptops und Desktop Computers bleibt ein Risiko für viele Unternehmen
  - Virtualisierung- und Cloud Computing-Techno-logien werden zunehmend eingesetzt, aber nur wenige Unternehmen bedenken die damit verbundenen Sicherheitsrisiken

by Bitterli Consulting
itacs training

Projekt- und Portfoliocontrolling

Das Zielpublikum sind Verantwortliche von Projekten wie z.B. Controller, Portfolio- Manager, Programmleiter, Auftraggeber oder Projektausschussmitglieder, welche Projekte aus projektexterner Sicht kontrollieren und damit die besten Voraussetzungen schaffen wollen, um zum geplanten Erfolg zu kommen.

Donnerstag, 25. März und Freitag, 26. März 2010

IKS in IT revisionssicher implementieren (Kompaktkurs)

Der Kompaktkurs richtet sich primär an das Zielpublikum der Revisionstätigkeiten – also Mitarbeiter und Führungskräfte von Fach- und IT-Abteilungen. Wertvoll ist der Kurs insbesondere für Mitarbeitende im Informatikbereich, da für diese Prüfungen bis anhin eher selten waren.

Montag, 29. März 2010

➜ www.itacs.ch

ISACA-Kurse und -Veranstaltungen

23.2.10	➜ **ISACA Vereinsversammlung 2010**
8.–12.3.10	➜ **Avaloq-Einführung für IT-Revisoren & Sicherheitsbeauftragte • Anmeldung noch möglich** Grundlagen, Konzepte und Bedienung des Avaloq Banking Systems. **Der Kurs findet bei Avaloq Evolution Corp., Allmendstr. 140, statt**
11.–12.3.10	➜ **Design und Prüfung von anwendungsabhängigen Kontrollen** **(Bewährter Kurs auf 2 Tage erweitert!)** Wirtschaftliches Design und wirksame Überprüfung von anwendungsabhängigen Kontrollen
16.–17.3.10	➜ **Leadership-Seminar für Revisoren & Sicherheitsbeauftragte** Verbesserung des persönlichen Kommunikationsverhaltens in kritischen Situationen
18.3.10	➜ **Einführung in Enterprise Risk Management (ERM)** Sicherheit durch proaktive Handhabung der Risiken
19.3.10	➜ **Einführung in das Interne Kontrollsystem (IKS-Kompaktkurs)** Konzeption, Betrieb und Prüfung des IKS
25.–26.3.10	➜ **Projekt- und Portfoliocontrolling** (IT-) Projekte effizient und wirksam überwachen und steuern
29.3.10	➜ **IKS in IT revisionssicher implementieren (Kompaktkurs)** Effiziente Vorbereitung auf (angekündigte) Revisionen und Schutz vor übertriebenen Forderungen
30.3.10	➜ **ISACA After Hours Seminar** • ➜ **sekretariat@isaca.ch**
31.3.10	➜ **ISMS gemäss ISO 27001/2/4/5 implementieren und verbessern (Kompaktkurs)** Ein ISMS in 30 effizienten Schritten implementieren oder verbessern
8.4.–11.5.10	➜ **CISM-Prüfungsvorbereitungskurs 2010l1** 4tägiger Kompaktkurs für erfahrene Sicherheitsbeauftragte, welche das gesamte Berufsbild und das CISM Review Manual bereits selbständig durchgearbeitet haben und beherrschen. Die gezielte Vorbereitung auf die internationale CISM-Prüfung.
12.4.–10.5.10	➜ **CISA-Prüfungsvorbereitungskurs 2010l1** 5tägiger Kompaktkurs für erfahrene Kursteilnehmer, welche das gesamte Berufsbild und das CISA Review Manual bereits selbständig durchgearbeitet haben und beherrschen. Die gezielte Vorbereitung auf die internationale CISA-Prüfung.
29.4.10	➜ **ISACA/SVIR-Tagung** Zusammenarbeit zwischen interner und externer (IT-) Prüfung

Wo nichts anderses vermerkt finden die Kurse in Zürich, bei ITACS Training AG, Stampfenbachstrasse 40, statt.

Weitere Kurs- und Veranstaltungsanbieter

➜ **www.glenfis.ch**	**RISK IT Overview Kurs** Risk IT - das Risiko Management Framework von ISACA	**25.3.2010 • Glenfis AG** Badenerstrasse 623 8048 Zürich
➜ **www.glenfis.ch**	**CobiT Foundation Kurs mit optionaler Zertifizierung** CobiT® 4.1 - IT Governance Foundation Kurs	**14.4.2010 • Glenfis AG** Badenerstrasse 623 8048 Zürich
➜ **www.isss.ch**	**Cyber Crime und die Schweiz** Verschaffen Sie sich einen Überblick über das Thema «Cyber Crime». Erfahren Sie aus erster Hand die aktuellen, realen Bedrohungen.	**29.4.2010** Hotel Einstein St. Gallen
➜ **www.glenfis.ch**	**VAL IT Overview Kurs** VAL IT - Das Value Management Framework von ISACA	**21.5.2010 • Glenfis AG** Badenerstrasse 623 8048 Zürich

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