ISACA Newsletter JANUAR 2010

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

# newsletter

## After Hours Seminar

**Zürich • Dienstag, 26. 1. 2010 • 16:40 – 17:40 Uhr**

**Enterprise Governance of IT zur Prävention von Wirtschaftskriminalitätsdelikten?**
Das Referat befasst sich mit der Prävention von Wirtschaftskriminalitität (WK) in Unternehmen. Es wird am Beispiel eines realen Betrugsfalles untersucht, ob mit den 'Enterprise Governance of IT'-Modellen CobiT und Val IT präventive Wirkung gegen WK-Delikte erzielt werden kann.

➜ Detaillierte Informationen

## Focus

**10 Tips for Risk Management by Victor Chapela**

➜ Mehr auf Seite 2

## Inside

**ISACA Announces New CRISC Certification for Risk Professionals Inside**

➜ Mehr auf Seite 3

## 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:**
**4. Februar 2010**

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

**Satz und Gestaltung:**
ITACS Training AG
Felice Lutz
8006 Zürich

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

## Editorial

Liebe Leser

das neue Jahr hat gerade erst begonnen und die meisten von uns sind wohl damit beschäftigt, ihre guten Vorsätze in Taten umzusetzen. Wie jedes Jahr wird auch 2010 wieder ein Jahr der Veränderungen und Neuerungen, ein Jahr der Herausforderungen.

In der ersten Ausgabe unseres Newsletters beschäftigen wir uns vorwiegend mit dem Thema Risiko-Management.

- Am 13. Januar hat ISACA offiziell seine neue Zertifizierung CRISC (Certified in Risk and Information Systems Control) vorgestellt. Diese soll ab 2011 die bestehende Zertifizierungsreihe (CISA, CISM, CGEIT) ergänzen.
- Darüber hinaus geben wir unter der Rubrik Inside noch Tipps für das Risiko-Management und verweisen auf das neue ISACA Risk IT Framework.
- Das erste After Hours Seminiar in diesem Jahr befasst sich mit der Prävention von Risiken wirtschaftskrimineller Handlungen.

Auch in diesem Jahr freuen wir uns natürlich wieder über Ihre Zusendung von Fachartikeln oder Praxisbeiträgen.

Wir wünschen Ihnen noch Viel Glück und Erfolg für 2010!

Ihre Redaktion ISACA Newsletter

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

Focus

# 10 Tips for Risk Management by Victor Chapela

Author: Victor Chapela

1. Use «intent» to separate intentional risks (hacking or fraud) from unintentional risks (availability). The types of risk are completely different to manage and each requires different types of controls to mitigate.

2. For unintentional risks, most of which are availability incidents, use a standard business impact analysis (BIA) to assess risks and business continuity plan (BCP) to mitigate them.

3. For intentional risks, however, determine impact as the external value of your information. How much is it worth to an employee, to the press, to your competition or to organized crime?

4. Classify your information based on this external value, and define policies and standards to protect high-risk information.

5. From the universe of possible risks, prioritize by focusing on those that have occurred and have been published. Out of those, determine which are applicable to your organization. Finally, establish which have a higher, recurrent long-term value to an attacker. The latter group should have the highest priority in the risk management plan.

6. In protecting intentional risks, determine which assets store, process or transmit high-risk information. But most important, create an inventory of the accounts, groups and privileges that have access to it.

7. Evaluating, filtering, restricting and monitoring the accounts with access to high-risk information are the most efficient ways to mitigate intentional risk.

8. If a specific risk cannot be mitigated, have the data owners sign a temporal risk acceptance statement. Always include an expiration date, after which the risk should be addressed.

9. Implement a risk management process that can periodically reassess risk, recommend mitigation controls, collect risk acceptance statements, manage mitigation projects and maintain a risk inventory.

10. Senior management sponsorship is essential for risk management to be efficient and effective. Fortunately, it tends to be easier for them to understand risk management than other security-related disciplines.

For more information on IT risk management, download ISACA's new Risk IT framework publications.

Victor Chapela is founder and CEO of Sm4rt Security Services. He is coauthoring a book on the evolution of risk and is a frequent speaker at conferences around the world.

## Unterlagen der 12. Berner Tagung für Informationssicherheit

Aufgrund unserer Partnerschaft mit ISSS möchten wir unsere Mitglieder auf die 12. Berner Tagung für Informationssicherheit im vergangenen Jahr aufmerksam machen.

In der Keynote widerrief Dr. Rudolf Bär die bekannte Risikoformel Risiko = Eintretenswahrscheinlichkeit x Schadensausmass und zeigte nachvollziehbar auf, warum diese nur in den wenigsten Fällen überhaupt sinnvoll anwendbar ist. Die Slides seines Referates sowie auch das Video des Referates des Leaders der Patrouille Suisse «Risikomanagement aus einer etwas anderen Optik - Teamwork bei Tempo 1000» lassen sich von der nachfolgenden Webadresse herunterladen.

Detaillierte Informationen ➜ **www.isss.ch**

Inside

# ISACA Announces New CRISC Certification for Risk Professionals

Rolling Meadows, IL, USA (13 January 2010)

**ISACA, a global association of 86'000 IT audit, risk, governance and security professionals, is responding to market demand by introducing a new risk-related certification. The Certified in Risk and Information Systems Control (CRISC) designation is for IT professionals who identify and manage risks through the development, implementation and maintenance of information systems (IS) controls. These professionals help enterprises accomplish business objectives such as effective and efficient operations, reliable financial reporting, and compliance with regulatory requirements.**

A grandfathering program, through which experienced professionals can earn the certification without passing an exam, will open in April. The first CRISC exam will be administered in 2011.

ISACA established CRISC (pronounced «see risk») to recognize IT professionals with skills and abilities related to:

- Risk identification, assessment and evaluation
- Risk response
- Risk monitoring
- IS control design and implementation
- IS control monitoring and maintenance

«The CRISC designation will demonstrate to employers that the certification holder is able to identify and evaluate the risks unique to a specific organization and help the enterprise accomplish its business objectives by designing, implementing, monitoring and maintaining risk-based, efficient and effective IS controls,» said Urs Fischer, chair of ISACA's CRISC Task Force. «We conducted an extensive amount of research globally and found that enterprises are becoming more risk-aware and are looking to identify professionals who possess the skills to help them protect their assets and enhance their businesses. CRISC fills a gap that currently exists in the marketplace.»

➜ Fortsetzung auf Seite 4

by Bitterli Consulting
itacs training

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

**Szenario-basiertes IT-Risikomanagement (Kompaktkurs)**

Der Kurs vermittelt anhand verschiedener Beispiele, wie ein wirkungsvoller Risikomanagement-Prozess basierend auf IT-Risikoszenarien implementiert und betrieben werden kann.

Dieser Kompaktkurs richtet sich an alle Personen, welche
- *entweder* bereits über viel Erfahrung in verschiedenen Aspekten von IT-Risikomanagement verfügen und das so erworbene Wissen vervollständigen und mit praktischen Tipps abrunden wollen
- *oder* über wenig(er) Erfahrung in der Thematik verfügen und sich in kurzer Zeit einen qualitativ hochstehenden Überblick – gepaart mit viel Praxis-Knowhow – verschaffen wollen

**Freitag, 12. Februar 2010 • ➜ Anmeldung noch möglich!**

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

## Inside

Fortsetzung: ISACA Announces …

CRISC complements ISACA's three existing certifications: Certified Information Systems Auditor (CISA), established in 1978 and earned by more than 70'000 professionals since its inception; Certified Information Security Manager (CISM), earned by more than 12,000 professionals since it was launched in 2002; and the newer Certified in the Governance of Enterprise IT (CGEIT), earned by more than 4,000 professionals since it was developed in 2006:

- CISA is designed for IT professionals who perform independent reviews of control design and operational effectiveness; CRISC is for IT and business professionals who identify, evaluate and manage risk, and design, implement and maintain IS controls.
- CISM is for individuals who manage, design, oversee and/or assess an enterprise's information security, including the identification and management of information security risks; CRISC is for IT professionals whose roles also encompass operational and compliance considerations.
- CGEIT is for IT and business professionals who have a significant management, advisory or assurance role relating to the governance of IT, including risk management; CRISC is for IT and business professionals who are engaged at an operational level to mitigate risk.

### About ISACA

With more than 86,000 constituents in more than 160 countries, ISACA® (➜ **www.isaca.org**) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems assurance and security, enterprise governance of IT, and IT-related risk and compliance. Founded in 1969, ISACA sponsors international conferences, publishes the ISACA® Journal, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ CISA®, Certified Information Security Manager® CISM®, Certified in the Governance of Enterprise IT® CGEIT® and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA developed and continually updates the CobiT®, Val IT™ and Risk IT frameworks, which help IT professionals and enterprise leaders fulfill their IT governance responsibilities and deliver value to the business.

**Contact:**
Kristen Kessinger ➜ **kkessinger@isaca.org**
Deborah Vohasek ➜ **dvohasek@isaca.org**
Joanne Duffer ➜ **jduffer@isaca.org**

Additional information about the CRISC certification is available at ➜ **www.isaca.org/crisc**. ■

by Bitterli Consulting
itacs training

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

**Von IT Governance bis IT Security Mgmt – wirksamer Einsatz von CobiT 4.1**

Der Kurs richtet sich an alle Personen, welche mehr über sinnvolle Einsatzmöglichkeiten von CobiT und die Neuerungen in CobiT 4.1 erfahren möchten resp. verantwortlich sind für (Teilbereiche des) IT Governance; insbesondere an Unternehmer, IT-Manager, IT-Projektleiter, (IT) Security Manager, Risikomanager und Informatikrevisoren. Dieser Kurs setzt voraus, dass die Teilnehmenden Grundkenntnisse der Informationstechnologie sowie der Unternehmensführung (Management) mitbringen.

**Montag, 15. Februar, bis Mittwoch, 17. Februar 2010**

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

Inside

# ISACA-Vereinsversammlung 2010

**Dienstag, 23. Februar 2010**

15.00 – 16.15 Uhr: Vereinsversammlung
16.30 – 17.30 Uhr: Spannendes Referat mit dem IT-Prüfer Andreas Toggwyler

Ort: Ernst & Young AG, Brandschenkestrasse 100, 8002 Zürich (Nähe Bahnhof Enge)

Anschliessend an die Vereinsversammlung wird Andreas Toggwyler, welcher 2 Jahre für die KPMG in den USA war, ein spannendes Referat zum Thema «Der kleine Unterschied – Erfahrungsbericht eines Heimkehrers» halten. Den Nachmittag möchten wir mit einem Apéro abschliessen, zu dem Sie alle herzlich eingeladen sind.

Wir freuen uns auf Ihre Teilnahme!

---

# SVIR – ISACA-Tagung

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

---

by Bitterli Consulting
itacs training

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

**Clevere IT-Risikoanalysen für Sicherheitsprofis und Wirtschafts-/IT-Prüfer**

Der Fokus des Kurses liegt auf pragmatischen Ansätzen für Risikoanalysen, welche sich in der Praxis mehrfach bewährt haben. Ziel dieser Risikoanalysen ist jeweils, potentielle Gebiete für vertiefende Untersuchungen zu identifizieren sowie Informationen für die strategische Prüfungsplanung zu gewinnen.

Dieser Kompaktkurs richtet sich primär an Personen, welche Anwendungen, Systeme und Plattformen zu überprüfen haben und eine diesbezügliche Auswahl effizient aber risikoorientiert treffen. Neben Wirtschafts- und IT-Prüfer sind dies primär Sicherheitsbeauftragte (ISMS), Risiko Manager und IKS-Verantwortliche – aber auch IT-Governance Spezialisten, Controller, Compliance-Zuständige usw.

**Donnerstag, 11. Februar 2010 ➜ Anmeldung noch möglich!**

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

## ISACA-Kurse und -Veranstaltungen

| | |
|---|---|
| 26.1.10 | ➜ **ISACA After Hours Seminar** • ➜ **sekretariat@isaca.ch** |
| 11.2.10 | ➜ **Clevere IT-Risikoanalysen für Sicherheitsprofis und Wirtschafts-/IT-Prüfer (Kompaktkurs)**<br>Effiziente Durchführung von IT-Risikoanalysen in allen Schichten der «Cremeschnitte« |
| 12.2.10 | ➜ **Szenario-basiertes IT-Risikomanagement (Kompaktkurs)**<br>Hochwirksamer szenario-basierter Vorgehensansatz für Risikomanagement |
| 15.–17.2.10 | ➜ **Von IT Governance bis IT Security Management – wirksamer Einsatz von CobiT 4.1**<br>Anwendung des internationalen Standards auf die wichtigsten Governance-Themen Security, Risk Management, Projekt Management / Software Development, IT Audit, ... |
| 23.2.10 | ➜ **ISACA Vereinsversammlung 2010** • **Anschliessend Referat von Andreas Toggwyler**<br>**Die Veranstaltung findet bei Ernst & Young, Brandschenkestr. 100, statt • Beginn: 15:00 Uhr** |
| 8.–12.3.10 | ➜ **Avaloq-Einführung für IT-Revisoren & Sicherheitsbeauftragte**<br>Grundlagen, Konzepte und Bedienung des Avaloq Banking Systems.<br>**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!)**<br>Wirtschaftliches Design und wirksame Überprüfung von anwendungsabhängigen Kontrollen |
| 16.–17.3.10 | ➜ **Leadership-Seminar für Revisoren & Sicherheitsbeauftragte**<br>Verbesserung des persönlichen Kommunikationsverhaltens in kritischen Situationen |
| 18.3.10 | ➜ **Einführung in Enterprise Risk Management (ERM)**<br>Sicherheit durch proaktive Handhabung der Risiken |
| 19.3.10 | ➜ **Einführung in das Interne Kontrollsystem (IKS-Kompaktkurs)**<br>Konzeption, Betrieb und Prüfung des IKS |
| 25.–26.3.10 | ➜ **Projekt- und Portfoliocontrolling**<br>(IT-) Projekte effizient und wirksam überwachen und steuern |
| 29.3.10 | ➜ **IKS in IT revisionssicher implementieren (Kompaktkurs)**<br>Effiziente Vorbereitung auf (angekündigte) Revisionen und Schutz vor übertriebenen Forderungen |
| 31.3.10 | ➜ **ISMS gemäss ISO 27001/2/4/5 implementieren und verbessern (Kompaktkurs)**<br>Ein ISMS in 30 effizienten Schritten implementieren oder verbessern; ISO-Normen werden abgegeben |
| 8.4.–11.5.10 | ➜ **CISM-Prüfungsvorbereitungskurs 2010\|1**<br>Die gezielte Vorbereitung auf die internationale CISM-Prüfung. |
| 12.4.–10.5.10 | ➜ **CISA-Prüfungsvorbereitungskurs 2010\|1**<br>Die gezielte Vorbereitung auf die internationale CISA-Prüfung. |

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

## Weitere Kurs- und Veranstaltungsanbieter

| | | |
|---|---|---|
| ➜ **www.isss.ch** | **Security Dinner** • **Model Driven Security** | **4.3.2010** • Zürich |
| ➜ **www.svir.ch** | **ISACA/SVIR-Tagung**<br>**Zusammenarbeit zwischen interner und externer (IT-) Prüfung** | **29.4.2010**<br>Hotel Four Point, Zürich |
| ➜ **www.isss.ch** | **Security Dinner** • **Cyber Crime und die Schweiz** | **29.4.2010** • St.Gallen |
| ➜ **www.isss.ch** | **ISSS Zürcher Tagung 2010**<br>**Datendiebstahl verhindern, entdecken, und bewältigen. Möglichkeiten und Grenzen von DLP.** | **1.6.2010**<br>Hotel Widder<br>Rennweg 7, Zürich |

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