ISACA Newsletter 2|2008

ISACA
Serving IT Governance Professionals
Switzerland Chapter

newsletter

After Hours Seminar • 25.3.2008

Internes Sicherheits-Kontrollsystem (IKS) im Bankenumfeld

Die Luzerne Kantonalbank betreibt seit Jahren erfolgreich ein Informations-Sicherheits-Management-System (ISMS) basierend auf ISO 27001 und ISO 27002.

➜ **Mehr auf Seite 4**

Inhalt

Der neu-alte Avaloq-Kurs – bereits ausgebucht!

Der speziell für IT-Revisoren konzipierte Avaloq-Einführungskurs stösst auf grosses Interesse.

➜ **Mehr auf Seite 2**

Erfolg mit CISA und CISM
Die erfolgreichen Absolventen der CISA- und CISM-Prüfungen 2006 (Dezember) und 2007 (Juni) trafen sich zu einem gemütlichen Abendessen.

➜ **Mehr auf Seite 3**

ISACA-Kurse und -Veranstaltungen

Die aktuellsten Veranstaltungs- und Kursdaten finden Sie auf ➜ **Seite 6**

Impressum

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

Redaktionsschluss
Nr. 3|2008: 5. April 2008

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

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

Editorial

Zeit, wieder einmal die Schulbank zu drücken

Die gerade erfolgte OR-Revision hat vor allem auf Wirtschaftsprüfer, aber auch auf interne Revisoren und die IT-Prüfer spürbare Auswirkungen. Zwar ist die «Prüfung der Existenz des IKS», wie es im neuen PS890 heisst, für die meisten internen und die IT-Prüfer schon seit Jahren Realität, ja sogar nur eine Vorstufe zur «Prüfung der Wirksamkeit des IKS» – doch hat die aktuelle Diskussion über die neue Regelung im OR und den neuen Prüfungsstandard einiges in Gang gesetzt. Plötzlich wird klar erkennbar, wie eigentliche Selbstverständlichkeiten neue Dimensionen erhalten: Wussten Sie beispielsweise, dass die Definition des IKS im neuen Prüfungsstandard ausdrücklich nur jene Vorgänge und Massnahmen in einer Unternehmung umfasst, welche eine ordnungsmässige Buchführung und finanzielle Berichterstattung sicherstellen? In meinem zarten Alter muss ich nun plötzlich feststellen, dass ich mich über 25 Jahre mit internen Kontrollen beschäftigt habe, welche für Abschlussprüfer anscheinend kaum relevant sind …

Zeit, um wieder einmal die Schulbank zu drücken. Ich habe mir fest vorgenommen, ein neues Skript zum Internen Kontrollsystem zu erstellen, das auf die verschiedenen Betrachtungsweisen eingeht und die wesentlichen Elemente eines IKS aufzeigt – wenn man so etwas schreibt, wird man ganz automatisch sehr viel über das Thema lernen. Allen anderen empfehle ich, wieder einmal die Schulbank zu drücken. Schliesslich benötigen die meisten Unternehmen kompetente Mitarbeiter auf allen hierarchischen Stufen, welche die Bedeutung von internen Kontrollen, von Governance und damit von Risiko-, Sicherheits-, Servicemanagement usw. verstehen und deren korrekte Implementation unterstützen und überwachen können.

Als Mitglied des ISACA Switzerland Chapter haben Sie zu Weihnachten einen Ausbildungsgutschein über CHF 200 erhalten. Setzen Sie den Gutschein gezielt für Ihre Aus- und Weiterbildung ein – in diesem Newsletter finden Sie verschiedene kurze Beiträge zu aktuellen Kursen und Entwicklungen.

Ihr Peter R. Bitterli
Verantwortlicher für Aus- und Weiterbildung

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

Focus

Der neu-alte Avaloq-Kurs – bereits ausgebucht!

Autor: Peter R. Bitterli, CISA

In der Schweiz haben sich in den letzten Monaten zahlreiche Banken für die neue Bankensoftware Avaloq entschieden. Nicht nur die Mitarbeiter der verantwortlichen Fachbereiche, auch die internen und externen Revisoren müssen sich an die teilweise geänderten Geschäftsprozesse und Schlüsselkontrollen gewöhnen.

Die Komplexität von Avaloq ist hoch, so dass eine wirksame Prüfung schwierig und aufwändig ist. Alleine für die erste Beherrschung der Parametrisierung bietet Avaloq einen vierwöchigen Grundkurs an – bis man die Workflow-Funktionalität, das Objektmodell und entsprechende Konzepte und all die anderen wichtigen Elemente wirklich kennt, muss man schon einiges an Lernaufwand investieren.

Es ist daher gut zu wissen, dass es eine speziell für IT-Prüfer konzipierte, einwöchige Einführung in Avaloq gibt, welche das notwendige Basiswissen über Funktionalität, Technologie und Parametrisierungsmöglichkeiten sowie spezielles Wissen u.a. in den Bereichen Security, Workflow und Order Validation vermittelt (die genauen Details finden Sie in der Kursausschreibung auf unserer Webseite).

Der bereits einmal durchgeführte Kurs wurde hinsichtlich der Prüfbelange noch spezifischer an die Bedürfnisse der Teilnehmer angepasst. Dazu wurden die im Kurs eingesetzten Trainer auf die typischen Fragen von IT-Revisoren geschult sowie die gesamten Kursunterlagen hinsichtlich einer optimalen Unterstützung durchgecheckt. Ein Erfahrungsbericht eines erfahrenen Avaloq-Prüfers rundet den aktualisierten Kurs ab.

Der erste Kurs im laufenden Jahr (31.3.-2.4.08) ist zu unserer grossen Freude aber zum Leid einiger IT-Prüfer bereits ausgebucht – wir sind derzeit daran, für das zweite Halbjahr einen neuen Termin festzulegen. Wer sich dafür interessiert, soll sich bald einmal anmelden. ■

Typische Revisorenfragen, welche im letzten Kurs gestellt wurden:
- Wie können normale Lesezugriffe geloggt werden?
- Machen nur Online-Änderungen einen Log-Eintrag oder auch Batch-Jobs?
- Was sind alles superprivilegierte Benutzer?
- Mit welchen technischen Usern kann man sich einloggen?
- Wie mache ich die Verwendung des K-Users sicher?
- Wie stelle ich die Vollständigkeit der Datenübernahme bei der erstmaligen Poduktionsaufnahme sicher?
- Wie kann ich sicherstellen, dass Reports vollständig sind?
- Wie erkenne ich direkte Fixes in der Produktion und wer sie gemacht hat?

Die Antworten auf obige Fragen erhalten Sie im nächsten Kurs.

Liebe Mitglieder

IDG Communications AG ist offizieller IT-Medienpartner der informatica08 und berichtet in der Computerworld regelmässig über die Aktivitäten und Veranstaltungen zum Jahr der Informatik 08.

informatica08 ist es ein besonderes Anliegen, die IT-Professionals und somit die Mitglieder unseres Verbandes umfassend informiert zu halten. informatica08 und IDG Communications AG haben zum Jahr der Informatik 08 ein Spezialangebot für unsere Mitglieder realisiert.

Ein Jahresabonnement der IT-Zeitschrift Computerworld zum Spezialpreis von 90 Franken (statt 259 Franken).

Wir unterstützen diese Aktion und empfehlen Ihnen das Abonnement.

Kontakt IDG: Cornelia.brunschwiler@idg.ch • Telefon 044 387 44 09

Inside

Erfolg mit CISA und CISM

Autor: Peter R. Bitterli, CISA

Am vergangenen 3. März trafen sich die erfolgreichen Absolventen der CISA- und CISM-Prüfungen 2006 (Dezember) und 2007 (Juni) zusammen mit einigen Vorstandsmitgliedern zu einem gemütlichen Abendessen – eine Tradition, welche wir im ISACA Switzerland Chapter bereits seit vielen Jahren pflegen.

Ebenfalls Tradition ist, anlässlich des Abendessens die neuesten Statistiken zum Prüfungserfolg zu zeigen – z.B. die Unterschiede zwischen den Prüfungen in Deutsch und Englisch oder zwischen den Kursteilnehmern und den anderen Prüfungskandidaten. Selbstverständlich wird auch immer ein wenig gespöttelt über die Unterschiede zwischen den Punktzahlen der zukünftigen CISAs und CISMs.

Gefeiert wurde natürlich auch, dass sämtliche Teilnehmer des CISA-Vertiefungskurses 2006|2 die anspruchsvolle Prüfung bestanden – eine Erfolgsquote von 100% hatten wir bis anhin noch nicht, der bisherige Rekord stand auf 96.4%. Klar hatten damit die CISAs für einmal den vereinsinternen Wettkampf gewonnen!

by Bitterli Consulting
itacs training

Hacking Defense Training Week
21.–25. April 2008

Wirksame Verteidigung von Hacking-Angriffen mit anspruchsvollen Fallstudien – eine Intensivwoche (nur) für Fortgeschrittene!

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

ITACS Training ist der offizielle Ausbildungspartner des ISACA Switzerland Chapter

ISACA Serving IT Governance Professionals Switzerland Chapter

Unter den Grafiken war eine, welche die Punktzahlen in den verschiedenen CISA-Areas aufzeigte. Die extrem gleichmässige Verteilung über die sechs Areas provozierte die Frage: Ist das Zufall?

Die korrekte Antwort ist relativ komplex. Zu einem grossen Teil hat das mit der unterdessen 16jährigen Erfahrung mit unserem CISA-Vertiefungskurs zu tun: Kursteilnehmer erhalten jeweils klare Lese- und Arbeitsaufträge für die Vorbereitungsphase – und im Unterricht werden aufgrund der Auswertung von gelösten kleinen Testprüfungen die Schwerpunkte immer wieder neu gesetzt. Ein Grund ist auch, dass die sechs «vollen» Testprüfungen mit insgesamt 1200 Multiple-Choice Fragen detailliert analysiert werden: Jede Frage ist einem oder mehreren der Task Statements aus dem Berufsbild zugeordnet; nach jeder Testprüfung erhalten alle Teilnehmer eine persönliche Auswertung ihrer Ergebnisse und somit pro Task Statement eine genaue Aussage über ihre diesbezüglichen Kenntnisse (siehe Abb. auf der nächsten Seite). Diese Information gibt den Kursteilnehmern deutliche Hinweise, welche Themen noch «nachgelernt» werden müssen; auf der anderer Seite dienen die Auswertungen der ersten Testprüfungen dazu, im dreitägigen Repetitionsblock und in der Besprechung der Testprüfungen die Schwerpunkte entsprechend der wirklichen Lern-Bedürfnisse der Teilnehmer zu setzen.

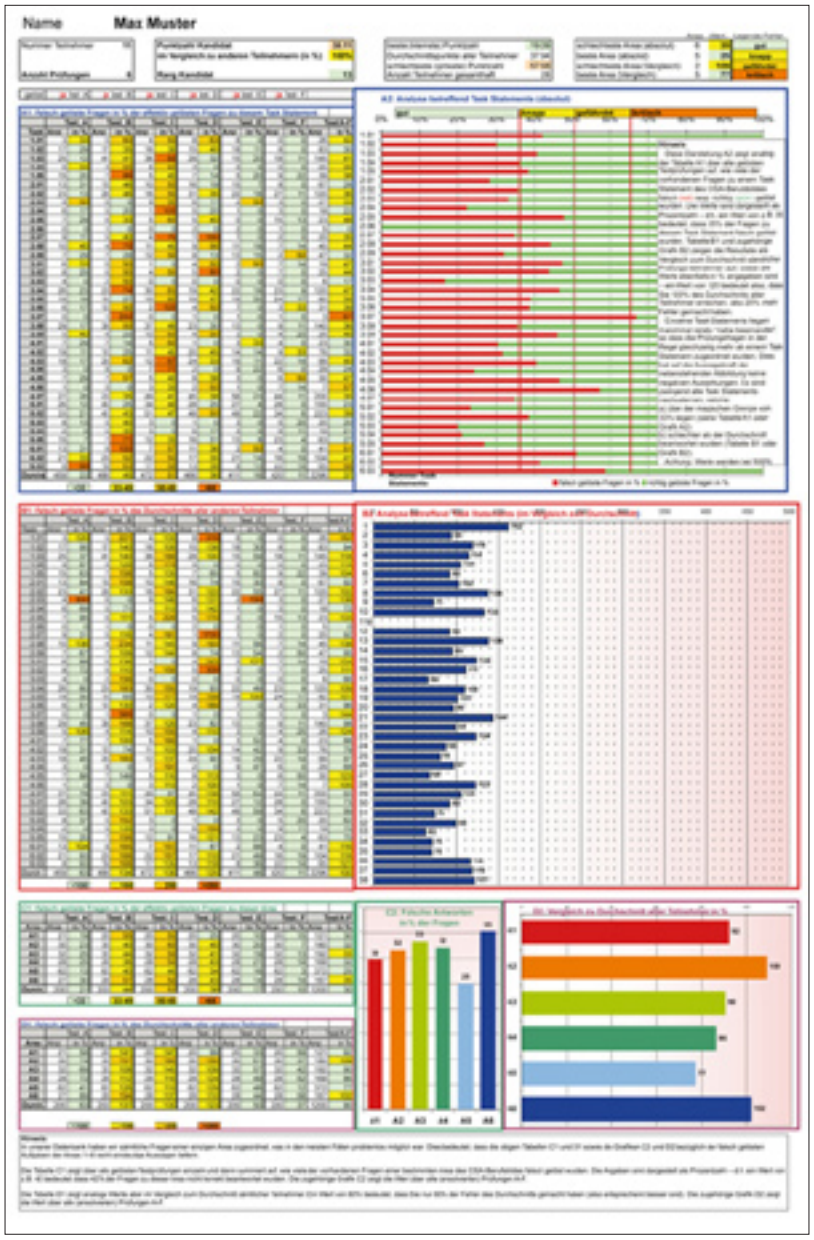
Die obige Aufzählung ist nicht abschliessend – selbstverständlich gibt es weitere Gründe für das gute Abschliessen unserer Kursteilnehmer. Wichtig ist uns die Aussage, dass wir im einzigen offiziellen CISA-Kurs des ISACA Switzerland Chapter* unsere Aufgabe – nämlich die gezielte Vorbereitung der Kursteilnehmer auf die Prüfung wie auch auf die wirklichen Anforderungen der Praxis – ernst nehmen und uns entsprechend dafür einsetzen.

Derzeit sind wir daran, auch im relativ jungen CISM-Kurs die notwendige Zuordnung der Testfragen zu

➜ **Fortsetzung**

* In der Westschweiz findet bei ISEIG ebenfalls ein offizieller CISA-Kurs des ISACA Switzerland Chapter statt: mit französischsprachigen Dozenten und den kompletten Unterlagen von ITACS Training auf Englisch

Inside



den Task Statements des Berufsbilds vorzunehmen und ähnliche Auswertungen zu erstellen. Bis zum nächsten Kurs (Start Ende Juni!) werden wir dazu ebenfalls fähig sein.

Letztlich aber hängt der Prüfungserfolg zu einem grossen Teil von der persönlichen Motivation und dem Einsatz jedes einzelnen Kursteilnehmers ab. Da gerade in den letzten Jahren der Druck im Arbeitsalltag stetig gestiegen ist, müssen sich die Kursteilnehmer umso besser fokussieren und für ihre eigenen Interessen einsetzen.

Gönnen Sie sich und/oder Ihren Mitarbeitern eine ausgewiesen hochwertige Ausbildung: melden Sie sich baldmöglichst für den nächsten CISA- oder CISM-Vertiefungskurs an!

After Hours Seminar • 25. März 2008

Internes Sicherheits-Kontrollsystem (IKS) im Bankenumfeld

Referent: Kurt Niederberger, LKB

Die Luzerne Kantonalbank betreibt seit Jahren erfolgreich ein Informations-Sicherheits-Management-System (ISMS) basierend auf ISO 27001/2.

Aus dem Inhalt:

- Internes Sicherheits-Kontrollsystem (IKS) im Bankenumfeld
  - Sicherheitsmanagement
  - Risikoanalyse mit Gefährdungskatalog
  - Kontrollaktivitäten festlegen
- Umsetzung Monitoring und IKS im Bankenumfeld
  - technische Massnahmen
  - organisatorische Massnahmen
  - persönliches Verhalten
- Messziele / Metriken festlegen
  - Informationsbeschaffung
  - Rapportierung

➜ **Zur Anmeldung**

Agenda

29. April 2008
IT-Revisionsplanung und -Durchführung - ein Praxisbericht
Referent: Christian Balmer, ZKB

27. Mai 2008
The Cycles of Security - Einführung von IT Security in einer Rückversicherungsgesellschaft
Referent: Martin Rohrer, PartnerRe

24. Juni 2008
Thema noch offen

29. Juli 2008
Keine Veranstaltung während den Sommerferien

26. August 2008
Thema noch offen

30. September 2008
Identity und Access Management als Teil von Compliance

by Bitterli Consulting
itacs training

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

Interessante Konditionen bei der Buchung von mehreren, beliebig kombinierbaren Kursen dieser Trainings-Woche

ITACS Training AG
Stampfenbachstr. 40
CH-8006 Zürich
Tel. +41 (0)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

IT Security Training Week • 5.–9. Mai 2008
Bestehend aus 5 einzeln buchbaren Tageskursen

IT-Risikomanagement
Grundbegriffe, Risikoanalysen für IT-Systeme, IT-Projekte und IT-Anwendungen. Strategisches Risikomanagement, ORM, ...

ISO 27001/2 verstehen und anwenden
Die wichtigsten Elemente eines ISMS kennen und in 30 klaren Schritten implementieren oder verbessern

Erfolgreiche Awareness-Kampagnen
Systematische Planung/Durchführung von Aktivitäten und Kampagnen für anhaltende Awareness (mit zahlreichen Beispielen/Erkenntnissen aus der Praxis)

Sichere Anwendungsentwicklung
Projekt-, Entwicklungs- und eigentliche Applikationsrisiken; Vorgehen zur Gewährleistung sicherer Anwendungen, inkl. Organisation und Durchführung von Security Penetration Testing

Grundlagen der Kryptologie
Alle notwendigen Fachbegriffe und Erkenntnisse; besonders geeignet für IT-Prüfer, Sicherheitsspezialisten, Manager

ISACA-Kurse und -Veranstaltungen

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

25.3.2008	➜ **After Hours Seminar** Internes Sicherheits-Kontrollsystem (IKS) im Bankenumfeld
9.3. – 2.4.08 **Stockholm**	➜ **European Conference on Computer Audit, Control and Security**
31.3. – 4.4.08 **AUSGEBUCHT**	➜ **Avaloq-Einführung für IT-Revisoren** Grundlagen, Konzepte und Bedienung des Avaloq Banking Systems. Vertiefung in Parametrisierung u.a. von Security-, Workflow- und Rule Engine
31.3. – 4.4.08 **Edinburgh**	➜ **ISACA Training Week**
10.4. – 20.5.08	➜ **CISM-Prüfungsvorbereitungskurs 2008|1** Für Informationssicherheitsbeauftragte: die kompakte Variante zur gezielten Vorbereitung auf die internationale CISM-Prüfung
14.4. – 19.5.08	➜ **CISA-Prüfungsvorbereitungskurs 2008|1** Für IT-Prüfer/Sicherheitsspezialisten: die kompakte Variante zur gezielten Vorbereitung auf die internationale CISA-Prüfung
21.4. – 25.4.08	➜ **Hacking Defense Training Week** Wirksame Verteidigung von Hacking-Angriffen mit anspruchsvollen Fallstudien Eine Intensivwoche (nur) für Fortgeschrittene!
5. – 9.5.08	**IT Security Week; bestehend aus 5 einzeln buchbaren Kompaktkursen** • Montag 5. Mai 2008: ➜ **IT-Risikomanagement** • Dienstag, 6. Mai 2008: ➜ **ISO 27001/2 verstehen und anwenden** • Mittwoch, 7. Mai 2008: ➜ **Erfolgreiche Awareness-Kampagnen** • Donnerstag, 8. Mai 2008: ➜ **Sichere Anwendungsentwicklung** • Freitag, 9. Mai 2008: ➜ **Grundlagen der Kryptologie** Beachten Sie das attraktive Preismodell der IT Security Training Week ➜ **Kursübersicht**
14. – 16.5.08	➜ **Business Continuity und IT Service Continuity (inkl. Workshop)** Prozesse auf Basis ITIL V3 aufsetzen und wirksam implementieren
21.– 23.5.08	➜ **Von IT Governance bis IT Security Management – wirksamer Einsatz von CobiT 4.1** Anwendung des internationalen Standards auf die wichtigsten Governance-Themen Security, Risk Management, Projekt Management, usw.
2. – 3.6.08	➜ **IT Governance Compliance Reviews** Wirkungsvolle und effiziente Durchführung von Überprüfungen bezüglich der Einhaltung von Richtlinien und anderen Vorgaben

Wo nichts anderes vermerkt, finden die Veranstaltungen/Kurse in den Schulungsräumlichkeiten von ITACS Training AG, Stampfenbachstrasse 40, 8006 Zürich, statt.