

ISACA Switzerland Chapter

Die ISACA ist ein weltweites Netzwerk von Spezialisten, die sich mit der Sicherheit, Kontrolle, Audit und Governance von Informationssystemen befassen. Das bereits 1988 gegründete ISACA Switzerland Chapter hat heute rund 900 Mitglieder und wurde für seine umfassenden Dienstleistungen für die eigenen Mitglieder und die internationale Berufsgemeinschaft 2005 zum "Best Very Large Chapter Worldwide" gekürt – eine Auszeichnung, welche die zahlreichen Freiwilligen zu weiteren Höchstleistungen anspornt. Interessieren Sie sich für Sicherheit, Risikomanagement, Governance oder Revision im Informatikumfeld? Dann werden Sie doch Mitglied!

Weitere Informationen finden Sie auf www.isaca.ch



ITACS Training AG

Der 1992/93 erstmals angebotene Vertiefungskurs für "Revision und Sicherheit von Informationssystemen" mit den im internationalen Vergleich erstklassigen Erfolgsquoten an der CISA-Prüfung stand ursprünglich im Zentrum unserer Ausbildungstätigkeit. Seit 2003 bieten wir unter dem neuen Firmennamen ITACS Training weitere Spezialistenkurse sowie den offiziellen CISM-Kurs des ISACA Switzerland Chapter für Certified Information Security Manager an. Als Ausbildungsprofis organisieren wir für Unternehmen interne Schulungen und Sensibilisierungskampagnen und bieten neu im Auftrag des ISACA Switzerland Chapter pro Jahr rund 40 verschiedene Kurse an.

Weitere Informationen finden Sie auf www.itacs.ch



**Auch im zweiten Halbjahr:
Top-Kurse zu aktuellen Themen**

Juli bis Dezember 2008

KURSÜbersicht_2008|2

- Audit
- Security
- Risikomanagement
- Governance
- Zertifikats-Kurse



	Seite
Inhaltsverzeichnis	2
Kursübersicht nach Daten	3
Kursübersicht nach Themen	4
ISACA – der Berufsverband für Governance, Sicherheit und Audit	6
ITACS Training – Ihr Ausbildungs-Provider	8
Kurse: Details	10
Partnerfirmen	48
Schulungsräume	50
Allgemeine Geschäftsbedingungen	52

	Seite
14.8.–18.11.08 12,5 Tage CISM-VK CISM-Vertiefungskurs 2008 2	38
20.8.–19.11.08 14,5 Tage CISA-VK CISA-Vertiefungskurs 2008 2	40
25.–29.8.08 5 Tage AVA-IR Avaloq-Einführung für IT-Revisoren/Sicherheitsbeauftragte	14
27.–29.8.08 3 Tage GOV-GL Von IT Governance bis IT Security Management – wirksamer Einsatz von CobiT 4.1	10
1.–3.9.08 3 Tage AVA-REP Avaloq – Reporterstellung für Revisoren/Sicherheitsbeauftragte	16
3.9.2008 1 Tag AUD-KK Hilfe, die Revisoren kommen – sind wir vorbereitet?	18
4.–5.9.08 2 Tage KOM-BT Wirkungsvoll kommunizieren in kritischen Situationen	36
11.9.–22.11.08 14 jours CISA-CE CISA Cours d’approfondissement 2008 2	42
25.–26.9.08 2 Tage COB-MA CobiT für Manager – ein Kompaktkurs zu Projektmanagement und IT-Governance	12
1.–3.10.08 3 Tage LAB-AS Application Security Lab	30
21.–23.10.08 3 Tage ISMS-EXP Expertenkurs ISO27001/2	24
30.10.–18.11.08 4 Tage CISM-PV CISM-Prüfungsvorbereitungskurs 2008 2	44
3.–4.11.2008 2 Tage AUD-OS Prüfung und Berichterstattung bei Outsourcing-Providern	20
5.–19.11.08 5 Tage CISA-PV CISA-Prüfungsvorbereitungskurs 2008 2	46
10.–11.11.08 2 Tage AUD-SM ISO/IEC 20000 Auditor (Prüfung von Service Management-Prozessen)	22
12.–14.11.08 3 Tage LAB-VTB Virus/Trojan/Backdoor Security Lab	32
26.11.08 1 Tag ITRM-KK IT-Risikomanagement wirksam umsetzen	26
5.12.08 1 Tag ISMS-KK ISMS gemäss ISO27001/2 implementieren und verbessern	28
8.–12.12.08 5 Tage LAB-TW Hacking Defense Training Week	34

Hinweis

Alle Kursausschreibungen enthalten unter der Überschrift "Referenzen" Angaben zu den CISA resp. CISM Task Statements (also den Aufgaben aus dem entsprechenden CISA- resp. CISM-Berufsbild) sowie Hinweise zu den CobiT 4.1 IT-Prozessen, welche im Rahmen der jeweiligen Kurse abgedeckt werden.

Details zu diesen Berufsbildern und dem CobiT-Framework können Sie der Broschüre "Zertifizierung als CISA oder CISM" entnehmen, welche von der ISACA-Homepage (www.isaca.ch) herunterladbar ist.

IT-Governance			
GOV-GL 27.–29.8.08	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.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Seite 10
COB-MA 25.–26.9.08	CoBIT für Manager – ein Kompaktkurs zu Projektmanagement und IT-Governance Mittels Projekt-Simulation Management-Kompetenz in CoBIT erwerben	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Seite 12

(IT-) Revision/Audit			
AVA-IR 25.–29.8.08	Avaloq-Einführung für IT-Revisoren/Sicherheitsbeauftragte Wirksame Kontrollen im Avaloq-Umfeld prüfen und implementieren	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Seite 14
AVA-REP 1.–3.9.08	Avaloq – Reporterstellung für Revisoren/Sicherheitsbeauftragte Effiziente Erstellung von verlässlichen Reports aus dem Avaloq Banking System	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Seite 16
AUD-KK 3.9.08	Hilfe, die Revisoren kommen – sind wir vorbereitet? (Kompaktkurs) Sinnvolle und wirksame Vorbereitung auf angekündigte Revisionen	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Seite 18
AUD-OS 3.–4.11.08	Prüfung und Berichterstattung bei Outsourcing-Providern Standardisierte Prüfungen im Outsourcing-Umfeld – ein Kurs für Provider und deren Kunden (mit Provider-Gastreferat!)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Seite 20
AUD-SM 10.–11.11.08	ISO/IEC 20000 Auditor (Prüfung von Service Management-Prozessen) Effiziente Prüfung von Service Management-Prozessen	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> ⚡	Seite 22

Risikomanagement/Sicherheit			
ISMS-EXP 21.–23.10.08	Expertenkurs ISO27001/2 Ein Muss für Sicherheitsverantwortliche, Risikomanager und alle anderen, welche den Zwillingsstandard erfolgreich in ihrem Unternehmen umsetzen wollen	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Seite 24
ITRM-KK 26.11.08	IT-Risikomanagement wirksam umsetzen (Kompaktkurs) Grundbegriffe, Risikoanalysen für IT-Systeme, IT-Projekte und IT-Anwendungen. Strategisches Risikomanagement, ORM, ...	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Seite 26
ISMS-KK 5.12.08	ISMS gemäss ISO27001/2 implementieren und verbessern (Kompaktkurs) Die wichtigsten Elemente eines ISMS kennen und in 30 klaren Schritten implementieren oder verbessern	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Seite 28

Security Labor			
LAB-AS 1.–3.10.08	Application Security Lab Web-Entwickler Kurs vom Applikationssicherheits-Spezialisten Compass	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Seite 30
LAB-VTB 12.–14.11.08	Virus/Trojan/Backdoor Security Lab Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung durch mobile Technologien und aktuelle Malware	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Seite 32
LAB-TW 8.–12.12.08	Hacking Defense Training Week Wirksame Verteidigung von Hacking-Angriffen mit anspruchsvollen Fallstudien – eine Intensivwoche (nur) für Fortgeschrittene!	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Seite 34

Spezielles Fachwissen für alle			
KOM-BT 4.–5.9.08	Wirkungsvoll kommunizieren in kritischen Situationen Verbesserung des persönlichen Kommunikationsverhaltens von Revisoren/Sicherheitsbeauftragten in kritischen Situationen	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Seite 36

Offizielle Zertifikatskurse des ISACA Switzerland Chapter			
CISM-VK 14.8.–18.11.08	CISM-Vertiefungskurs 2008 2 Die intensive, berufsbegleitende Aus- und Weiterbildung für Informationssicherheitsbeauftragte; inkl. gezielte Vorbereitung auf die internationale CISM-Prüfung	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> ⚡	Seite 38
CISA-VK 20.8.–19.11.08	CISA-Vertiefungskurs 2008 2 Für IT-Prüfer/Sicherheitspezialisten: der international erfolgreiche CISA-Kurs zur Vermittlung eines umfassenden Fachwissens	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> ⚡	Seite 40
CISA-CE 11.9.–22.11.08	CISA Cours d'approfondissement 2008 2 Audit des systèmes d'information Préparation à la certification internationale CISA	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> ⚡	Seite 42
CISM-PV 30.10.–18.11.08	CISM-Prüfungsvorbereitungskurs 2008 2 Für Informationssicherheitsbeauftragte: die kompakte Variante zur gezielten Vorbereitung auf die internationale CISM-Prüfung	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> ⚡	Seite 44
CISA-PV 5.11.–19.11.08	CISA-Prüfungsvorbereitungskurs 2008 2 Für IT-Prüfer/Sicherheitspezialisten: die kompakte Variante zur gezielten Vorbereitung auf die internationale CISA-Prüfung	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> ⚡	Seite 46

Folgende Referenzierungen können Ihnen bei der Auswahl der Kurse helfen:

Audit Security Risikomanagement Governance ⚡ mit Zertifikat

Governance, Sicherheit und Audit von Informationssystemen

Die ISACA ist ein weltweites Netzwerk von Berufsleuten und Spezialisten, welche sich mit Risiken, Sicherheit, Kontrolle, Audit und Management von Informationssystemen befassen. Die Anzahl Mitglieder ist in den letzten Jahren rasant auf über 75,000 gestiegen. Die ISACA-Dachorganisation hat über 170 Chapter in rund 100 Ländern.

ISACA organisiert weltweit zahlreiche Konferenzen und Ausbildungsveranstaltungen und unterstützt die lokalen Chapter mit verschiedenen Standardkursen. ISACA publiziert neueste Forschungsergebnisse, erstellt ein breites Angebot an professionellen Broschüren, Büchern & Präsentationen und bietet unzählige Fachbücher in einem spezialisierten Internet-Bookstore an. Seit Jahrzehnten publiziert ISACA weltweit akzeptierte, professionelle Kontroll-, Sicherheits- und Audit-Standards – wovon das aktualisierte CoBIT-Framework in der Version 4.1 wahrscheinlich das bekannteste ist.

Als ISACA-Mitglied können Sie von folgenden Vorteilen profitieren

- Zugriff auf mehrere Tausend Dokumente und Links u.a. zu IT Governance, Risk-, Project- und Business-Management, E-Business, IT Audit, IT Security
- Gratis Downloads von praktischen Broschüren, Standards und Präsentationen (inkl. CoBIT auf Deutsch und Englisch)
- Rabatte bei sämtlichen nationalen und internationalen Konferenzen und anderen Aus- und Weiterbildungsveranstaltungen
- Rabatte auf dem Sortiment des ISACA-Bookstore
- Periodische Informationen via E-Mail und den Zeitschriften IS Control Journal, Global Communiqué US

Das ISACA Switzerland Chapter wurde 1988 als Verein gegründet. Es richtet sich an Spezialisten, welche sich mit Fragen der Informationssicherheit und der Qualitätskontrolle beschäftigen, sowie an Vertreter der internen und externen Revision. Wir haben heute bereits 900 Mitglieder, von denen nur noch ein kleiner Teil aus den "klassischen" Revisionsberufen stammt. Das ISACA Switzerland Chapter genießt im internationalen Dachverband einen hervorragenden Ruf und hat in den vergangenen Jahren immer wieder Preise gewonnen; 2005 wurden wir sogar zum "Best Very Large Chapter Worldwide" gekürt.

Seit Beginn ist das ISACA Switzerland Chapter aktiv in der Aus- und Weiterbildung. Unzählige Personen haben einen der zahlreichen angebotenen Kurse oder Tagungen besucht. Bereits zwei Mal organisierte das Switzerland Chapter die "European Conference on Audit, Control & Security (EuroCACS)", welche zu den grössten derartigen Konferenzen in Europa gehört. Seit 2007 können wir dank einer engeren Zusammenarbeit mit ITACS Training AG unseren ISACA-Mitgliedern pro Jahr über 40 Kurse anbieten. Alle unsere Mitglieder (Stichtag 15.11.2007) erhielten zudem einen persönlichen Ausbildungsbeitrag von CHF 200.-, anrechenbar auf sämtliche ISACA-Kurse bis 31.12.2008.

Als Mitglied des ISACA Switzerland Chapter profitieren Sie auch in Zukunft von ermässigten Kurspreisen auf dem gesamten Ausbildungsangebot. Weitere spezielle Vorteile der Mitglieder in der Schweiz:

- ausgezeichnete Vorbereitungsunterlagen und Kurse mit anerkanntem Zertifikat für CISA und CISM
- interessante monatliche After Hours Seminare (gratis)
- Möglichkeit zur Mitarbeit in verschiedenen Interessengruppen, welche spezifische Themen behandeln und Hilfsmittel (z.B. Prüfprogramme, Checklisten) erarbeiten
- deutschsprachige Mitglieder erhalten gratis die renommierte Fachzeitschrift IT-Governance, französischsprachige die "Revue de l'AFAI"
- durch das Switzerland Chapter herausgegebener eNewsletter
- enge Zusammenarbeit mit den grossen Revisionsgesellschaften, der Schweizerischen Treuhand-Kammer, der Schweizerischen Akademie für Wirtschaftsprüfer, dem Schweizerischen Verband für interne Revision (SVIR), der Information Security Society Switzerland (vormals SI Fachgruppe Security) und Clusis

www.isaca.ch

Jedermann mit Interesse an Audit, Governance und Sicherheit von Informationssystemen ist als Mitglied willkommen. Weitere Informationen finden Sie auf unserer Website.



Haben Sie Interesse? Werden Sie Mitglied!

Daniela Gschwend, CISA
Präsidentin ISACA Switzerland Chapter

ITACS Training AG – Ihr Ausbildungs-Provider

Unsere Partnerschaft mit dem ISACA Switzerland Chapter

Seit 2003 sind wir der offizielle Ausbildungspartner des ISACA Switzerland Chapter. Wir verstehen diese Partnerschaft als Verpflichtung, dem Switzerland Chapter und seinen Mitgliedern nicht nur finanzielle Vergünstigungen, sondern ein ausgewogenes Kursangebot zu bieten, das die spezifischen Bedürfnisse der Mitglieder abdeckt. Wir stehen daher in engem Kontakt mit dem Vorstand und den Vereinsmitgliedern, haben ein offenes Ohr für neue Ideen und fragen in sämtlichen Kursen konsequent nach weiteren Verbesserungsmöglichkeiten.

Praxisgerechte Ausbildung

Als Ausbildungsanbieter setzen wir uns für sorgfältig konzipierte Seminare mit einem hohen Praxisanteil ein. Wir wählen dazu unsere Kurspartner und Referenten gewissenhaft aus. Wir legen besonderen Wert darauf, dass unsere Ausbildungspartner auch in der Praxis eine hohe Akzeptanz haben. Wo immer möglich, passen wir die Kursinhalte an die speziellen Bedürfnisse unserer Zielgruppen an und verknüpfen die Inhalte mit den einschlägigen Standards (z.B. COBIT, ISO27001/ISO27002) und den spezifischen Berufsbildern (z.B. CISA, CISM). Auch wenn Sie bei anderen Kursanbietern eventuell ähnliche Kurse finden, sind die von uns angebotenen Kurse in dieser speziellen Form einzigartig.

Ganzheitlicher Schulungsansatz

Nach den ausgezeichneten Erfahrungen im Jahr 2007 setzen wir uns auch im 2008 für einen ganzheitlichen Schulungsansatz ein, der neben dem themenspezifischen Fachwissen über Technologien und Prozesse wenn möglich auch den Aspekt Mensch einbezieht. Wir legen grossen Wert darauf, diese drei Elemente Technologie, Prozesse und Mensch in jedem einzelnen Kurs zu berücksichtigen – gerade weil es Kurse mit bewusst gesetzten Schwerpunkten gibt, achten wir auch auf ein ausgeglichenes Gesamtangebot.

“Ehrliche“ Preise

Unsere Seminargebühren beinhalten alle notwendigen Kursunterlagen sowie die Kosten für die Pausen- und Mittagsverpflegung – in bestimmten Fällen auch die Übernachtungsgebühren. Wir berücksichtigen dabei die minimale und maximale Teilnehmerzahl, die Anzahl der im Unterricht gleichzeitig eingesetzten Referenten, Art und Umfang der benötigten Hilfsmittel usw. Als privates Ausbildungsinstitut ohne jegliche staatliche Förderung und Unterstützung sind wir auf kostendeckende Preise angewiesen. Für 2008 haben wir die Preise weiterer Kurse nach unten anpassen können, so dass das Preis-/Leistungs-Verhältnis hervorragend ist.

Wie steht es mit Ihrer persönlichen Weiterbildung?

Wir sind der Überzeugung, dass eine professionelle Aus- und Weiterbildung sowohl für die Arbeitnehmer als auch die Arbeitgeber immer wichtiger wird:

- Für die *Arbeitnehmer* ist es aufgrund des raschen Wandels in den Unternehmen, den immer häufigeren Restrukturierungen, Unternehmensübernahmen und -zusammenschlüssen und dem anhaltenden Trend zum Outsourcing und Offshoring wichtig, ihr Fachwissen ständig anzupassen und zu erweitern und so den persönlichen Marktwert zu erhalten.
- Für die *Arbeitgeber* ist es gerade wegen dem verschärften Konkurrenzdruck aber auch den zunehmenden Anforderungen von staatlichen wie privaten Regulatoren (z.B. Sarbanes-Oxley, Basel II) unabdingbar, qualifizierte Mitarbeiter zu haben, welche alle für ihre Aufgaben notwendigen Kenntnisse und Fähigkeiten besitzen. Dies setzt eine gezielte, auf Tätigkeit und Mitarbeiter ausgerichtete Aus- und Weiterbildung voraus.



Peter R. Bitterli, CISA, CISM
Inhaber ITACS Training AG

www.itacs.ch



Einführung

Das 1996 erstmals veröffentlichte COBIT-Framework (1998, 2000 und 2005 wesentlich überarbeitet) betont die Rolle und den Einfluss der Informationstechnologie auf die Geschäftsprozesse. COBIT stellt ein Modell von generell anwendbaren und international akzeptierten Kontrollzielen (die wesentlichsten Zielsetzungen für ein Kontrollsystem innerhalb der IT) bereit, die in einem Unternehmen implementiert werden sollten, um eine verlässliche Anwendung der Informationstechnologie zu gewährleisten.

Das COBIT-Framework integriert in verblüffend einfacher Weise die Sicherheits- resp. Kontrollanforderungen der bekanntesten Standards und Modelle für Management und Kontrolle der Informationstechnologie (z.B. Prince, TickIT, ITIL, ...). Die Prinzipien von COBIT lassen sich dabei auf jede Plattform und in jedem Geschäftsumfeld anwenden.

Mit der Veröffentlichung von COBIT 4.0 wurde nun der in der Version 3.2 bereits erkennbare Schritt zu IT Governance vollständig und konsequent vollzogen. Ebenso wurde die Verbindung von Unternehmenszielen zu Informatikzielen konkreter beschrieben und die COBIT-Prozesse haben eine inhaltliche und formale Verbesserung erfahren. In Anbetracht der gestiegenen Anforderungen zur angemessenen Sicherstellung der (IT) Governance (Basel II, Sarbanes-Oxley, etc.) erlangt COBIT so eine noch grössere Bedeutung als bisher. Die im Frühling 2007 veröffentlichte Version 4.1 wurde noch leicht gestrafft und enthält wertvolle Hinweise für die Umsetzung in die Praxis.

Lernziele

Nach unserem informationsreichen Kurs sind Sie in der Lage:

- die zahlreichen Ausprägungen von IT-Governance zu verstehen;
- die verschiedenen Elemente des COBIT 4.1 Frameworks zu bezeichnen;
- den Strukturaufbau des Frameworks zu verstehen;
- die inneren Zusammenhänge von COBIT zu erkennen;
- Inhalte von COBIT 4.1 in Ihrem Umfeld nutzbringend einzusetzen;
- Elemente auch für nicht offensichtliche Zwecke zielführend in der eigenen Praxis anzuwenden.

Zielpublikum

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.

Kurs-Spezialitäten

Erleben Sie den Herausgeber des ersten deutschsprachigen Buchs zu COBIT in einem intensiven Seminar mit zahlreichen praxisrelevanten Fallbeispielen und Zusatzinformationen. Nur wenige beschäftigen sich schon so lange mit dem Framework wie der Kursleiter Peter R. Bitterli, der be-

reits 1997 anlässlich einer internationalen Konferenz sein erstes Referat zum Framework hielt, alle Entwicklungen des Framework intensiv verfolgt und 2006 grosse Teile von COBIT 4.0 ins Deutsche übersetzt sowie an der Qualitätssicherung der Übersetzung des gesamten Frameworks mitgearbeitet hat.

Der Referent hat im Verlaufe seiner Beratungstätigkeit COBIT immer wieder eingesetzt für die Planung und Durchführung von Revisionen, Sicherstellung der Governance und Beurteilung der Informationssicherheit. Bereits zum vierten Mal wird das dabei angesammelte Wissen in unserer dreitägigen, intensiven Lehrgang in dieser Form und Zusammenstellung präsentiert und abgeben.

Alle Teilnehmer erhalten neben den üblichen Kursunterlagen eine CD-ROM mit wertvollen Hilfsmitteln (Word und Excel), welche im Kurspreis enthalten sind.

Kursinhalte

- Einführung in die Elemente von COBIT 4.1 (Control Objectives, Management Guidelines, Maturity Model, IT Assurance Guide, IT Control Practices, Implementation Tool Set, COBIT Quickstart und COBIT Online)
- Projektmanagement mit COBIT (mit Link zu aktuellen Projektmanagement- und Entwicklungsstandards)
- Service Management (mit detailliertem Abgleich zwischen COBIT und ITIL)
- Management der Informationssicherheit nach COBIT und entsprechende Verknüpfung zu ISO27001 und ISO27002

- Optimaler Einsatz von COBIT für die Vorbereitung einer IT-Revision (als Revisor und als Geprüfter)
- IT-Risikomanagement mit COBIT (mit Link zu Basel II)
- IT-Governance und ihre Bedeutung aus Optik der Regulatoren (Wirtschaftsprüfung allg., Sarbanes Oxley)

Referenzen

- CISA Task Statements: 2.2 (2.5) (2.8) 5.5
- CISM Task Statements: 1.7 2.2 2.5 2.6 3.8 3.9 4.4 4.5
- COBIT IT-Prozesse: alle; mit Schwerpunkten bei PO1 PO4 PO9 PO10 AI1 AI2 AI6 DS1 DS2 DS5 DS8–10 DS13 ME1–4

Referent

- Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG

Seminargebühren

CHF 2'850.– für ISACA-Mitglieder (alle anderen plus CHF 200.–)

Anmeldeformular:
www.itacs.ch

Einführung

IT-Governance ist ein Schlagwort, über dessen Bedeutung sich erst wenige Manager im Klaren sind – und CobiT das zugehörige Governance-Framework, das jeder Manager kennen und einsetzen müsste. IT-Governance ist jedoch zu facettenreich und CobiT zu umfangreich, als dass man sich so auf die Schnelle das entsprechende Wissen aneignen könnte. Unser Management-Seminar unter der Leitung von zwei top-gesetzten Referenten vermittelt innert kürzester Zeit die wichtigsten Informationen und verhilft dank der eingebauten Simulation zu den notwendigen Handlungskompetenzen.

Unterrichtsmethodik

Wesentliches Element dieses Kompaktkurses ist eine Kombination von (wenig) Theorie mit der beispielhaften Anwendung von vorhandenem Wissen und dem Neugelerten im Rahmen einer praxisnahen Management-Simulation: Zentrale Governance-Themen wie Projektmanagement, Risikomanagement, Ressourcenmanagement usw. werden in einer vier-phasigen Simulation behandelt – jede Phase wird dabei von kurzen Theorieblöcken, Besprechungen und Hinweisen zu CobiT-Themen begleitet.

Jeder der Teilnehmer übernimmt im Rahmen der vielfach bewährten Simulation eine Rolle beim Bau der Pyramiden im alten Ägypten. Was hier so leicht scheint, ist in der (Kurs-) Realität ein hartes Stück Arbeit: Wie sonst soll man Millionen Steine an den richtigen Platz bringen und dafür sorgen, dass Zehntausende Arbeiter effizient und effektiv arbeiten?

Das Projektteam als Ganzes bekommt den Auftrag, die Pyramide innerhalb eines festgelegten Zeitrahmens zu errichten. Diese Aufgabe wird durch realistische Ereignisse der damaligen Zeit (z.B. Wetterlagen, Krankheiten, Kriege, sich ändernde Wünsche des Pharaonen) beeinflusst.

Als erstes geht es darum, basierend auf Rollenbeschreibungen eine geeignete Projektorganisation zu definieren. Anhand der vorliegenden Informationen muss eine erste Risikoanalyse durchgeführt werden; für eine entsprechende Risikovorsorge sind mit einem limitierten Budget Gegenmassnahmen zu implementieren. Jeder der darauf folgenden Simulationsphasen ist fokussiert auf ein Schwerpunktthema: So geht es z.B. in der ersten Phase primär um die Gewinnung wichtiger Erkenntnisse im Zusammenhang mit der Dynamik von Projekten. Bereits in der zweiten Runde wird das Team mit der plötzlichen Änderung des Projektumfangs konfrontiert. In Absprache zwischen Projektleiter, Team, Support und Qualitätssicherung müssen Entscheidungsgrundlagen für das Steering Committee aufbereitet werden. In der dritten Phase drohen die in der Planung zugesagten Termine und Funktionen in Gefahr zu geraten. Das Team muss geeignete Massnahmen einleiten, um das Projekt zu retten. Prozessverbesserungen müssen besprochen und umgesetzt werden. Jetzt zeigt sich zunehmend, wie gut das Risikomanagement zu Beginn des Projektes durchgeführt wurde. In der letzten Simulationsphase werden die Prozesse gut abgestimmt gelebt und die Ressourcen zielgerichtet eingesetzt. Die Vorzüge der Qualitätssicherung im Projekt werden erkannt und helfen, das Projekt erfolgreich abzuschliessen.

Nach jeder Phase werden die wichtigsten Erkenntnisse zusammengefasst und mit entsprechenden Führungsinformationen aus dem CobiT-Framework verknüpft.

Lernziele

Nach dem Seminar sind die Teilnehmer in der Lage:

- die verschiedenen Ausprägungen von IT-Governance zu verstehen;
- den Nutzen der wichtigsten Elemente des CobiT-Frameworks zu erkennen;
- ausgewählte Elemente des Frameworks in der eigenen Praxis einzusetzen;
- im Schwerpunktbereich (IT-) Projektmanagement Entscheide mit hoher Kompetenz treffen.

Zielpublikum

Manager auf unteren und mittleren Führungsstufen, welche eigene Erfahrungen im Umfeld von IT-Governance und CobiT machen wollen sowie alle Personen, welche eine Rolle im Projektmanagement tragen (Projektleiter, Portfoliomanager, Steuerungsausschuss-Mitglieder, ...).

Kurs-Spezialitäten

Das zweitägige Management-Seminar mit Projekt-Simulation und der im Kurspreis eingeschlossenen Übernachtung im einzigartigen 4Sterne-Hotel auf dem Üetliberg findet in einem kleinen Kreis (max. 12 Teilnehmer) statt. Der Abend vom ersten zum zweiten Kurstag wird zur Vernetzung untereinander und der Klärung allfälliger Fragen mit den beiden als Experten anerkannten Referenten verwendet.

Kursinhalte

- Grundlagen von IT-Governance
- Aus Optik des Management wichtigste Elemente des CobiT-Frameworks
- Projektmanagement-Grundlagen, Projektorganisation mit Rollen, Verantwortlichkeiten und Kompetenzen
- Analyse von Projektrisiken, Finden von Gegenmassnahmen, Lösen von Problemen in Projekten
- Ausfertigen von Arbeitspaketen und ihre Überwachung (Finanzen, Zeit, Projektumfang, Qualität)
- Projekt(risiko)beurteilungen
- Umgang mit Änderungen im Projekt
- Steuern/Kontrollieren von Projekten
- Umgang mit Steering Committees und Projektmanagement

Referenzen

- CISA Task Statements: 2.1 2.2 2.6 2.8 2.9 3.2 3.5
- CISM Task Statements: 2.2 2.3 2.6
- CobiT IT-Prozesse: PO8–10 (AI5 DS8 DS10) ME1 ME4

Referenten (Co-Teaching)

- Martin Andenmatten, CISA, ISO20000 Consultant & Auditor, Glenfis AG
- Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG

Seminargebühren

CHF 3'500.– für ISACA-Mitglieder (alle anderen plus CHF 150.–); inkl. Kursunterlagen, Übernachtung im 4Sterne-Hotel und Verpflegung



Anmeldeformular:
www.itacs.ch

Einführung

Das Avaloq Banking System ist ein das ganze Banking umfassendes Produkt. Es liefert Werkzeuge zur individuellen Realisation aktueller und zukünftiger Marktleistungen von Retail-, Kommerz-, Privat- und Universalbanken. Avaloq arbeitet mit Standards, nutzt State-of-the-Art-Technologien und bietet offene Schnittstellen im Blick auf vernetztes Banking.

Die Komplexität von Avaloq ist hoch, so dass eine wirksame Prüfung schwierig und aufwändig ist. Mit diesem Kompaktkurs bieten wir IT-Revisoren die Möglichkeit, sich einen Überblick über wesentliche Funktionalitätselemente zu verschaffen sowie detailliertes Parametrierungs-Knowhow in einzelnen ausgewählten Schwerpunktthemen wie Security oder Workflow zu gewinnen.

Präsentationen und praktische Übungen werden ergänzt durch einen Erfahrungsbericht von IT-Revisoren mit dem Avaloq-System.

Lernziele

Der Kurs vermittelt theoretische Grundlagen und praktische Beispiele in den Bereichen

- Benutzerschnittstelle, Konzepte, Objektmodell
- Release Upgrade, Compilerklassen, Source Management
- Workflow-Funktionalität und -Limitierungen
- System- und benutzerdefinierte Checks

- Security Konzepte, Benutzerprofile sowie Benutzerverwaltung
- Buchung und Bilanzierung mit dem Avaloq Banking System
- Avaloq Audit Trail, Logs sowie spezielle Orderbooks

Nach der Schulung verfügen Sie:

- über Basiswissen in Funktionalität, Technologie und Parametrisierungsmöglichkeiten sowie
- spezielles Wissen u.a. in den Bereichen Security, Workflow und OrderValidation.

Zielpublikum

Dieser Kurs richtet sich an interne und externe IT-Revisoren und Sicherheitsbeauftragte mit einem guten Verständnis für Bank- und IT-Prozesse, die Avaloq-Systeme prüfen und erste praktische Erfahrungen mit dem System machen wollen.

Kurs-Spezialitäten

Im Rahmen des Kurses erhalten Sie Zugriff auf die Avaloq Academy IT-Infrastruktur mit einer speziellen Modell-Bank für die Übungen am Avaloq-System.

Bei der Kurszusammenstellung wurden Themen ausgewählt, welche für die (IT-) Revision und Sicherheitsbeauftragte besonders relevant sind; zudem wurden die Referenten durch die ITACS Training AG entsprechend ausgebildet.

Am Nachmittag des letzten Tages können Sie am System selbständig weitere Fragen abklären und Übungen durchführen.

Kursprache Deutsch
Unterlagen Englisch

Kursinhalte

Sie erhalten Einblicke in folgende Bereiche des Avaloq Banking Systems (P = beinhaltet praktische Übungen):

- Foundation (P)
 - Funktionalitätsübersicht, Benutzerschnittstelle, Konzepte, Objekt-Modell
- Parametrisierung Overview
 - Parametrisierungsarten, Source Management, Compilerklassen
- Release Management
 - Change-Request Prozess, Release Migration, Initialinstallation, Migration alter Daten
 - Standard Avaloq-Umgebungen (Implementierung, Integration, Testen, Produktion und Training)
- Rule Loader (P)
 - Konzept, Prozeduren, Anwendungsbereiche
- Workflow
 - Features und Limitierungen
 - Rule-based Workflow
- Order Validation
 - Benutzerdefinierte und vom System vorgegebene Validierungen von Aufträgen (Orders)
- Security (P)
 - Konzepte, Features und Grenzen.
 - Benutzerprofile und -verwaltung
- Accounting
 - Buchung und Bilanzierung mit dem Avaloq Banking-System
- Cost & Fees
 - Aufsetzen verschiedener Preismodelle
 - Parametrisierung von Kostenregeln
- Auditing
 - Aufsetzen sog. Audit Trails, d.h., Protokollierung von Änderungen einzelner Objekte

- Experience
 - Erfahrungsbericht von erfahrenen IT-Revisoren aus der Praxis mit Avaloq-Kunden

Referenzen

- CISA Task Statements: 3.4 3.6 3.9 (5.1)
- CISM Task Statements: 3.9 (4.5)
- CoBIT IT-Prozesse: A16 DS5 ME2

Referenten

Diverse Referenten von Avaloq Academy, und PriceWaterhouseCoopers (Teil Erfahrungsbericht)

Seminargebühren

CHF 4'500.– für ISACA-Mitglieder (alle anderen plus CHF 250.–)

Kursort

Avaloq Academy
Allmendstrasse 140, 8027 Zürich



Anmeldeformular:
www.itacs.ch

Einführung

Bereits ist die Avaloq-Plattform in zahlreichen Banken im Einsatz. Der sichere Betrieb sowie eine wirksame Überwachung dieser komplexen Plattform wie auch eine effiziente Prüfung durch den Informatikrevisor ist schwierig und bedingt fundierte Fachkenntnisse. Die effiziente Sammlung, Auswertung und Darstellung relevanter Informationen ist in diesem Zusammenhang von zentraler Bedeutung.

In unserem Avaloq-Einführungskurs (AVA-IR; siehe Seiten 16|17) haben die Teilnehmer einen Überblick über die wesentlichen Funktionalitätselemente von Avaloq sowie detailliertes Parametrierungs-Knowhow in ausgewählten Schwerpunktthemen wie Security oder Workflow gewonnen.

Auf diesem Fachwissen sowie den in der eigenen Praxis gewonnenen Erfahrungen baut unser zweite Avaloq-Kurs auf – er schult die Fähigkeit, revisionsrelevante Informationen (Berechtigungen, Zugriffsmöglichkeiten auf Objekte oder manuelle Eingriffe in Buchungsabläufe) zu sammeln und zu einem aussagekräftigen Nachweis (Evidence) zusammenzustellen, und verhilft damit den Teilnehmern zu einer hohen Handlungskompetenz.

Lernziele

Nach unserem Kurs sind die Teilnehmer in der Lage:

- aus der gesamten Avaloq-Plattform einfache Berichte selber zusammenzustellen und
- die Parametrierung komplexer Berichte zu überwachen.

Zielpublikum

Der Kurs richtet sich an alle Personen, die für die Überwachung oder Prüfung von Prozessen, IKS und Sicherheit in Unternehmen zuständig sind, welche Avaloq als zentrales Bankensystem einsetzen und zu diesem Zweck Avaloq-Auswertungen erstellen müssen.

Dieser Kurs ist speziell geeignet für interne und externe Sicherheitsspezialisten, IKS- oder Compliance-Verantwortliche sowie für IT-Revisoren mit einem guten Verständnis für Bank- und IT-Prozesse.

Die Teilnehmer sollten unseren Avaloq-Einführungskurs besucht haben oder für das Avaloq-System zertifiziert sein; andere Teilnehmer mit sehr guten Avaloq- und Praxiskenntnissen müssen bestätigen, dass sie die Inhalte des Einführungskurses beherrschen. Eine Kombination beider Kurse wird empfohlen.

Kurs-Spezialitäten

Im Rahmen des Kurses erhalten Sie Zugriff auf die Avaloq Academy IT-Infrastruktur mit Beispieldaten für die Übungen.

Bei der Kurszusammenstellung wurden die speziellen Bedürfnisse der (IT-) Revision besonders berücksichtigt; ein eigener Kursblock vermittelt die wesentlichen regulatorischen Anforderungen an die Sammlung und Darstellung von Nachweisen (Beweismittel) in Form von Avaloq-Berichten, die im Rahmen einer Überprüfung (Revision) verwendet werden sollen.

Kurssprache Deutsch
Unterlagen Englisch

Kursinhalte

Unser praxisnaher Kurs vermittelt die folgenden Inhalte:

- Regulatorische Anforderungen an Nachweise (Beweismittel) zur Benutzung z.B. in der Revision
- Script-Sprache "Avaloq Script"
- Avaloq Data Dictionary und Identifikation von Informationen im Avaloq Data Dictionary
- Erstellung einfacher Avaloq-Scripts unter Verwendung der Informationen aus dem Avaloq Data Dictionary
- Verstehen komplexer Scripts (Ziel: einen Experten diesbezüglich beauftragen zu können)
- Ordervvalidierung mit Avaloq-Script als Komponente des IKS
- Berichtskonzept (Report Writer) in Avaloq
- Report Datamart Sprache zur Aufbereitung der Informationen für Berichte
- Möglichkeiten, in Avaloq Informationen zu strukturieren und zu gestalten, um aussagekräftige Nachweise und benutzerfreundliche interaktive Auswertungen zu parametrieren
- Übung der Berichterstellung an revisionsrelevanten Beispielen

Am Nachmittag des letzten Kurstages steht die Schulungsinfrastruktur für freies Üben zur Verfügung.

Referenzen

- CISA Task Statements: 1.3 (3.4) (3.5) (5.1)
- CISM Task Statements: 3.9 (4.5)
- COBIT IT-Prozesse: (DS5) ME1–3

Referenten

Diverse Referenten von Avaloq Academy und PriceWaterhouseCoopers (Teil regulatorische Anforderungen an Beweismittel).

Seminargebühren

CHF 2'850.– für ISACA-Mitglieder (alle anderen plus CHF 200.–)

Kursort

Avaloq Academy
Allmendstrasse 140, 8027 Zürich



Anmeldeformular:
www.itacs.ch

Einführung

Aufgrund der gesetzlichen und regulatorischen Auflagen, aber auch aufgrund eines verbesserten Bewusstseins beim Management, werden immer mehr Bereiche durch die interne oder externe Revision überprüft.

Die Ankündigung einer Revision führt häufig zu hektischen Reaktionen: da werden innert kürzester Zeit Krisensitzungen durchgeführt, Prozesse angepasst sowie Dokumentationen erstellt oder aktualisiert. Dabei hat die Revision häufig ganz andere Bedürfnisse – ein grosser Teil der investierten Arbeit dürfte (mindestens aus Sicht der Revision) unwirtschaftlich und überflüssig sein.

Zudem gibt es aufgrund des Nachfrageüberhangs leider immer mehr Revisoren, welche ihre eigene Tätigkeit zu wenig kompetent beherrschen, kaum auf die Bedürfnisse des geprüften Unternehmens eingehen und daher von den Geprüften oft Unsinniges verlangen. Hier ist es sinnvoll und auch notwendig, solches Tun kritisch zu hinterfragen und allenfalls auch abzulehnen – das kann man aber nur, wenn man die Aufgaben und Grenzen der Revision versteht.

Lernziele

Nach diesem Kompaktkurs werden die Teilnehmer:

- Aufgaben und Tätigkeiten der Fach-/ Finanzrevision und der IT-Revision verstehen;
- die zentralen Elemente eines internen Kontrollsystems (IKS) im IT-Umfeld aufzählen können;
- die grundsätzlichen IKS-Anforderungen verstehen und in die Praxis umsetzen können;
- eine risikoorientierte Prüfungsplanung nachvollziehen und sich damit besser auf die Prüfung vorbereiten können;
- die Bedürfnisse der Revision verstehen und antizipieren;
- aus Revisionsicht notwendige Dokumente bereitstellen (oder nötigenfalls erstellen) können;
- Rechte und Pflichten der Revision korrekt interpretieren;
- Argumente zur Verfügung haben, um unsinnige Prüfungstätigkeit und/oder Empfehlungen bremsen zu können.

Zielpublikum

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.

Besonders wertvoll ist der Kurs für Beteiligte an Projekten in den Bereichen IKS und IT-Governance sowie für (interne) Koordinatoren/Kontaktpersonen für Revisionen.

Kurs-Spezialitäten

Der Fokus der Prüfungstätigkeit liegt in der Regel auf den Schlüsselkontrollen. Was das genau ist und welche typischen Schlüsselkontrollen die Revision in den Fachbereichen oder der IT immer wieder prüfen möchte, ist ein wesentlicher Bestandteil dieses Kompaktkurses.

Im Weiteren werden echte aber anonymisierte Feststellungen im Plenum diskutiert, um ähnliche Beanstandungen in den "eigenen" Revisionen zu vermeiden.

Kursinhalte

Einführung und Grundlagen

- Zweck und Aufgabe der internen und externen Revision
- Internes Kontrollsystem und Ordnungsmässigkeit (unter besonderer Berücksichtigung der IT)
- Phasen der Revisionsdurchführung (Vorbereitung, Planung, Durchführung, Berichterstattung, Nachrevision)
- Standards und Hilfsmittel der Revision
- Wichtige Schlüsselkontrollen in Fachbereichen und IT

Vorbereitung auf angekündigte Prüfungen

- Typische, von der Revision einverlangte Informationen/Unterlagen

Handhabung der Ergebnisse der Prüfungen

- Analyse der Revisionsempfehlungen
- Planung von entsprechenden Aktivitäten
- Umgang mit "übertriebenen" Revisionsanforderungen

Referenzen

- CISA Task Statements: 1.1–1.5
- CISM Task Statements: –
- CoBIT IT-Prozesse: (alle)

Referent

- Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG

Seminargebühren

CHF 1'000.– für ISACA-Mitglieder (alle anderen plus CHF 100.–)



Anmeldeformular:
www.itacs.ch

AUD-KK

Effiziente Vorbereitung auf (angekündigte) Revisionen und Schutz vor übertriebenen Forderungen

Einführung

Beim Outsourcing von (IT-) Prozessen darf nicht übersehen werden, dass die Verantwortung für den ausgelagerten Geschäftsbereich und damit für die einwandfreie Durchführung der ausgelagerten Verarbeitung vom Auftraggeber weiterhin vollständig getragen wird. Dieser sollte deshalb ein grosses Interesse daran haben, ein adäquates Netz von Kontrollen über diesen Bereich zu spannen. Eine Überprüfung des Outsourcing-Providers kann für alle Auftraggeber sinnvoll sein – in manchen Fällen ist diese sogar vorgeschrieben!

Durch die steigenden Anforderungen an ein Internes Kontrollsystem (IKS) in der Schweiz sind Fragen nach Kontrollen über finanzrelevante IT-Prozesse zu einem wichtigen Thema für die Geschäftsleitung und den CIO geworden. Da heutzutage kaum noch ein Geschäftsbereich ohne IT-Unterstützung auskommt, sind finanzrelevante Kontrollen auch in jeder IT-Umgebung zu finden – ihnen kommt bei der Prüfung der Informatik im Rahmen der Jahresabschlussprüfungen eine zentrale Bedeutung zu.

Prüfungen des Providers müssen daher sorgfältig geplant und durchgeführt werden. Ein Vorgehen nach SAS-70 wie auch PS402 bieten für Auftraggeber wie Service Provider neu die Möglichkeit, die zahlreichen störenden Einzel-Audits ihrer Kunden auf ein "standardisiertes" Audit pro Service zu minimieren.

Lernziele

Der Kurs vermittelt theoretische Grundlagen und praktische Beispiele, wie eine Prüfung eines Providers sinnvollerweise durchgeführt wird:

- Prüfungsstandards mit Relevanz für Outsourcing (Fokus auf SAS-70)
- Grundbegriffe und Anforderungen an Interne Kontrollsysteme
- Definition, Dokumentation und Nachvollziehbarkeit von Kontrollen
- Aufbau von Prüfungen und Berichten
- Anwendungsgebiete und Unterscheidung der verschiedenen SAS-70 Typen
- Verantwortlichkeiten der beteiligten Parteien
- Planung, Vorgehen und Timing aus Sicht aller beteiligten Parteien
- Nutzen für die beteiligten Parteien
- Fallstudien aus Sicht Kunde und Outsourcer

Nach der Schulung sind Sie in der Lage:

- die wesentlichen Unterschiede zwischen SAS-70 und PS402 aufzuzeigen;
- zu erkennen, welcher Prüfstandard in einer bestimmten Situation Sinn macht;
- zu verstehen, wie Prüfungen nach SAS-70 resp. PS402 aufgebaut sind, wer daran beteiligt ist und wem sie in welchem Fall einen Nutzen bringen;
- Kontrollziele und Kontrollen zu definieren;
- zu verstehen, wie solche Prüfungen durchgeführt werden und welche Partei dabei für welche Aufgabe verantwortlich ist;
- zu verstehen, wie ein entsprechender Bericht aufgebaut und welche Partei für welche Teile verantwortlich ist.

Zielpublikum

Dieser Kurs richtet sich an Geschäftsführer, Account-Manager, Verantwortliche für Betrieb, Management und Kontrolle von operativen Dienstleistungen sowie an Revisionsleiter und IT-Revisionen. Erfahrungen in der Konzeption und Betreuung von IT-Outsourcing wie auch Vorkenntnisse über Interne Kontrollsysteme sind von Vorteil. Für das Verständnis der Unterlagen sind Englischkenntnisse notwendig (Unterrichtssprache ist Deutsch).

Dieser Kurs richtet sich gleichzeitig an (potentielle) Outsourcing-Auftraggeber und Outsourcing-Provider. SAS-70 und PS402 sind zwar Prüfungsstandards, doch unser Kurs richtet sich nicht nur an die Revisoren sondern vor allem an Personen, welche das IKS von ausgelagerten IT- und Geschäftsprozessen wirksam überprüfen lassen wollen.

Kurs-Spezialitäten

Die Teilnehmer sind aufgefordert, im Zusammenhang mit den Fallstudien eigene Praxiserfahrungen einzubringen.

Im Kurs eingebaut ist das Referat "Erfahrungen beim Aufbau und Unterhalt eines Control Framework auf Basis SAS-70 bei einem IT-Provider mit sehr heterogenem Kundenkreis" von Georges Lichtsteiner.

Kursinhalte

Theoretische Grundlagen SAS-70/PS402:

- Hintergrund, Ziel und Umfang
- Allgemeines Konzept von Internen Kontrollsystemen (COSO, CoBIT, etc.) und Zusammenhang mit SAS-70
- Andere SAS

- Bestandteile eines Reports
- Unterscheidung und Anwendung von Type I und II Reports
- Verantwortlichkeiten der Parteien
- Dokumentation und Nachvollziehbarkeit von Kontrollen
- Einsatzgebiet von SAS-70 und PS402
- Unterscheidung von Business Controls und IT General Controls
- Multifirm Engagements
- Berichtsperioden
- Zusammenhang SOX 404 und OR IKS
- Schweizer Richtlinien für Outsourcing (z.B. EBK)
- IKS-Anforderungen anderer Länder

Fallstudien:

- SAS-70 aus der Sicht der Service Organization (Outsourcer)
- SAS-70 aus der Sicht der User Organization (Kunde)
- SAS-70 aus der Sicht der Service und User Auditors (Unabhängige Prüfer)

Referenzen

- CISA Task Statements: 1.1–1.5
- CISM Task Statements: (3.8) (4.5)
- CoBIT IT-Prozesse: DS1–DS6 DS8–DS10 DS12 DS13

Referenten

- Christoph Protz, CISA, KPMG

Gastreferent

- Georges Lichtsteiner, CISA, Swisscom

Seminargebühren

CHF 2'000.– für ISACA-Mitglieder (alle anderen plus CHF 150.–)



AUD-OS

für alle Auftraggeber sinnvolle Überprüfung von Outsourcing

Anmeldeformular:
www.itacs.ch

Einführung

ISO20000 ist der erste weltweite Standard, der sich speziell auf das IT Service Management auf Basis von ITIL® Best Practice fokussiert. Dieser Standard beschreibt integrierte Management-Prozesse für die Lieferung von IT Services. ISO20000 soll bei der Anwendung und Umsetzung von IT Service Management sicherstellen, dass Anbieter den vereinbarten Service professionell liefern.

Mit der Implementierung von ITIL® auf Basis des neuen Standards ISO20000 steht die kontinuierliche Verbesserung der Servicequalität im Vordergrund. Das Risiko, die Business-Anforderungen nicht erfüllen zu können, wird mit der konsequenten Ausrichtung auf diese Norm reduziert. Mit einer durch eine unabhängige externe Stelle erteilten Zertifizierung wird offiziell besiegelt, dass eine Service-Organisation über stabile Verfügbarkeit und hinreichende Flexibilität verfügt, um auf neue Anforderungen adäquat zu reagieren.

Lernziele

Nach dem Seminar sind die Teilnehmer in der Lage:

- den ISO20000-Standard und seine Inhalte zu beschreiben;
- den damit verbundenen Zertifizierungsprozess zu erläutern;
- den Reifegrad von Organisationen basierend auf ISO20000 zu bestimmen;
- die Vorgehenssystematik, wie Organisationen die ISO20000-Zertifizierung erreichen, zu verstehen;

- die Prüfung zum ISO20000 Auditor-Zertifikat zu bestehen (ausreichende Vorkenntnisse vorausgesetzt).

Zielpublikum

Interne und externe ISO20000-Auditoren von IT Service Management-Prozessen; IT-Prüfer und IT-Berater mit Fokus auf Audits und Assessments. ITIL®-Grundkenntnisse werden empfohlen.

Kurs-Spezialitäten

Zur Qualitätssicherung hat itSMF eine offizielle Ausbildung zum ISO20000-Auditor bzw. zum ISO20000-Consultant festgelegt. Nur akkreditierte Trainingsinstitute dürfen auf die offiziellen Prüfungen zum zertifizierten BS15000-Consultant oder -Auditor vorbereiten. Die Glenfis AG ist seit September 2005 das erste akkreditierte schweizerische Trainingsinstitut für solche Ausbildungen.

Kursinhalte

- Einführung und Entwicklungsgeschichte von ISO20000
- Das ISO20000-Zertifizierungsschema
- ISO20000: Überblick, Terminologie, Prozesse und Zielsetzungen
- ISO/IEC 20000:1-2005 Part 1 im Detail: The Specification for Service Management
- ISO/IEC 20000:2-2005 Part 2 im Überblick: The Code of Practice for Service Management
- Anwendung von ISO20000
- Umsetzung von ISO20000
- Vorbereitung zum formalen Audit
- Die Rolle der Service Management Toolsets bei der Zertifizierung
- Eignung und Scope-Festlegung (Eligibility & Scoping) der ISO20000-Zertifizierung

Referenzen

- CISA Task Statements: 4.1–4.6 (4.7)
- CISM Task Statements: (4.3) (4.5) 5.1–5.4 5.7–5.9
- CoBIT IT-Prozesse: DS1–DS3 (DS4 DS5 DS6) DS8–DS10 DS13

Referenten

- Martin Andenmatten, CISA, ISO20000 Consultant & Auditor, Glenfis AG
- Adrian Müller, ISO20000 Consultant, Glenfis AG

Seminargebühren

CHF 1'800.– für ISACA-Mitglieder (alle anderen plus CHF 150.–)

Zertifizierung

Erforderliche Vorkenntnisse

- Qualifizierter Auditor gemäss ISO 9000, BS7799, TickIT oder eine «Internal Auditor Zertifizierung» (Nachweis erforderlich)
- Drei Jahre Auditerfahrung
- Die umfangreichen Prüfungen (Multiple Choice und schriftliches Assignment/Praxis-Anwendung; Dauer 60 Min.) sind in Englisch durchzuführen. Englischkenntnisse in Wort und Schrift sind daher unerlässlich.

Prüfungsgebühr

CHF 300.–



Anmeldeformular:
www.itacs.ch

AUD-SM

Effiziente Prüfung von Service Management-Prozessen



Einführung

Der Leitfaden für das Management der Informationssicherheit ISO27001/ISO27002 (Code of Practice for Information Security Management) dient in erster Linie als Basis für Sicherheits-Zertifizierungen. Zudem benützen viele Sicherheitsbeauftragte von Unternehmen ihn auch als "Inspirationsquelle" für ihre internen Tätigkeiten.

Die Referenten dieses Expertenkurses setzen den Standard im Rahmen ihrer Beratungstätigkeiten bereits seit 1995 mit grossem Erfolg für unterschiedlichste sicherheitsrelevante Tätigkeiten ein: vom internen Sicherheits-Benchmarking über die Definition von Sicherheitsstrategien bis hin zur Anwendung im Bereich des Operational Risk Management – und von der Prioritätenbestimmung im Rahmen der Budgetplanung über Security Reviews bis zur konkreten Umsetzung von massgeschneiderten Sicherheitskonzepten. Das dabei angesammelte Wissen – sowie auch ein grosser Teil der dafür entwickelten Werkzeuge – werden in unserem dreitägigen, intensiven Lehrgang in einer praxisbezogenen Form und Zusammenstellung präsentiert und abgegeben.

Lernziele

Nach dem dreitägigen Seminar sind Sie in der Lage:

- Werdegang und Struktur des ISO27001/ISO27002 vorzustellen;
- den Unterschied zwischen ISO27001 und ISO27002 zu erläutern;
- die wesentlichen Elemente eines Information Security Management System (ISMS) nach ISO27001 zu bestimmen;

- die Anwendungsmöglichkeiten des ISO27001/ISO27002 zu verstehen;
- Control Self Assessment Workshops selber vorzubereiten und durchzuführen (Moderations-Fähigkeiten vorausgesetzt);
- basierend auf ISO27001/ISO27002 unternehmensspezifische Sicherheitskonzepte zu erstellen;
- die abgegebenen Hilfsmittel nutzbringend einzusetzen und weiterzuentwickeln.

Zielpublikum

Der Kurs richtet sich an alle Personen, welche mehr über den internationalen Standard ISO27001 resp. ISO27002 erfahren und diesen im Rahmen ihrer Tätigkeiten produktiv einsetzen wollen: Sicherheitsverantwortliche, Datenschutz-Beauftragte, Risikomanager, ISO27001-Auditoren und IT-Revisoren. Informatik-Kenntnisse sind nicht notwendig.

Hinweis: Der Kurs ist weder eine Ausbildung zum zertifizierten ISO27001-Auditor noch zeigt er im Detail die umfangreichen unternehmensinternen Vorbereitungen im Zusammenhang mit einer ISO27001-Zertifizierung auf – der Kurs liefert aber wertvollste Informationen über Aufbau und Betrieb eines ISMS weit über diese beiden Aspekte hinaus.

Maximal 12 Teilnehmer!

Kurs-Spezialitäten

Alle Teilnehmenden erhalten die aktuelle Version von ISO27001 und ISO27002 sowie zusätzlich zu den üblichen Kursunterlagen eine CD-ROM mit wertvollen Hilfsmitteln:

- Excel-Tool für Erfassung und Visualisierung von Benchmark-Resultaten
- verschiedene Excel-Tabellen für weitergehende Auswertungen

Der Kurs findet extern im Tagungs-/Konferenzhotel Uto Kulm statt, so dass die Teilnehmer auch am Abend einen intensiven Gedankenaustausch pflegen können.

Kursinhalte

- Werdegang CoP, BS7799, ISO 17799 und ISO27001/2
- Inhalte und Unterschiede ISO27001/ISO27002

Vergleich zu anderen Standards

- CoBIT
- IT-Grundschutzhandbuch (BSI)
- ITIL Security Management

Anwendungsmöglichkeiten von ISO27001 und ISO27002

- Erstellung/Unterhalt ISMS
- Zertifizierung
- Benchmarking
 - Vorgehen
 - Maturitätsmassstäbe
 - Hilfsmittel für Benchmarking
- Control Self Assessment (CSA)
 - Vorbereitung
 - Regeln
 - Erfolgsfaktoren
 - Durchführung
 - Rollenspiel "CSA-Workshop"

- Review IT-Sicherheit
- Sicherheitsstrategien
- Sicherheitskonzepte
- Planung/Priorisierung von Massnahmen
- Risikoanalysen
 - Radarchart und Entwicklung Risk Landscape
 - Integration in Operational IT Risk Management
- Schrittweise ISMS-Verbesserung
- Zusammenfassung/Abschluss

Referenzen

- CISA Task Statements: (2.1) 2.8 5.5
- CISM Task Statements: praktisch alle
- CoBIT IT-Prozesse: (PO4) (PO6) (PO7) PO9 (AI2) (DS4) DS5 (DS7) ME2 (ME3)

Referenten (z.T. Co-Teaching)

- Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG
- Hans Peter Riess, CISA, CISM, Ixact Security Inspection and Consulting AG

Seminargebühren

CHF 3'400.– für ISACA-Mitglieder (alle anderen plus CHF 200.–)

Inkl. 2 Übernachtungen, Verpflegung, Kursunterlagen sowie CD-ROM mit wertvollen Hilfsmitteln, welche im Rahmen der speziellen Lizenz-Bestimmungen unternehmensintern beliebig einsetzbar sind.

Anmeldeformular:
www.itacs.ch

Einführung

Der wirtschaftliche Umgang mit den vielfältigen Risiken der Informationstechnologie erfordert ein planmässiges und strukturiertes Vorgehen, das als Risikomanagement bezeichnet wird. In dessen Rahmen werden Risiken systematisch identifiziert, aussagekräftig bewertet und ggf. durch geeignete Massnahmen auf ein tolerierbares Mass reduziert.

Wegen aktueller Regulatorien und Gesetzgebungen (z.B. Anpassung Schweiz. Obligationenrecht, neue Richtlinien vom Bundesamt für Privatversicherungen, Basel II, Sarbanes Oxley) sowie aufgrund von zunehmendem Druck von Geschäftspartnern bezüglich der Einhaltung von Standards und Zertifizierungen (ISO27001, ITIL, CMM, ...) wird ein systematisches Risikomanagement immer wichtiger. Dies erfordert nicht nur die Bewertung der Risiken bestehender IT-Systeme und Anwendungen sondern auch die Verankerung des Risikomanagements in Entwicklungs- und Beschaffungsprozessen. Zudem müssen die Risiken der Informationstechnik mit operativen Risiken aus anderen Bereichen zusammengeführt und auf strategischer Ebene dargestellt und bewertet werden.

ITRM-KK

Hochkonzentriertes
Fachwissen und
Praxistipps

Lernziele

Nach unserem Kompaktseminar:

- kennen Sie die korrekten Begriffe aus dem Gebiet des Risikomanagement;
- kennen Sie die Bedeutung und die Aufgaben des IT-Risikomanagement;
- sind Sie mit unterschiedlichen Ansätzen und Ideen für das IT-Risikomanagement vertraut;
- sind Sie in der Lage, einen wirkungsvollen Risikomanagement-Prozess zu entwerfen;
- kennen Sie mögliche Lösungen für dessen Aufbau und die Implementierung.

Zielpublikum

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.

Kurs-Spezialitäten

Der Kurs vermittelt anhand verschiedener Beispiele, wie die konkreten Lösungsansätze an die spezifischen Unternehmensbedürfnisse angepasst werden können.

Die beiden gleichzeitig agierenden Referenten haben die vorgestellten Methoden in unterschiedlichsten Varianten vielfach in der Praxis eingesetzt und können daher im Unterricht auf diesbezügliche Verständnis- und Vertiefungsfragen situationsgerecht eingehen.

Kursinhalte

- Systematische Einführung in die Begriffswelt: z.B. Risikoanalyse, Risikomanagement
- Risikoanalyse für IT-Systeme, IT-Projekte und IT-Anwendungen: Vorstellung und Vergleich verschiedener Ansätze
- Strategisches IT-Risikomanagement als hybrider Lösungsansatz: szenario-basierte Risikolandschaft gekoppelt mit Grundschatz-Ansatz
- Implementierungsdetails: Erstellung und Pflege einer Risiko-Landschaft und deren Einbettung in Risikomanagement-Prozesse
- Abgrenzungsproblematik IT-Risikomanagement zu Operational Risk Management
- Zusammenfassung und Abschluss

Referenzen

- CISA Task Statements: (1.1) 2.8 (5.1–5.3)
- CISM Task Statements: 2.1–2.7
- CoBIT IT-Prozesse: PO9

Referenten (Co-Teaching)

- Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG
- Hans Peter Riess, CISA, CISM, Ixact Security Inspection and Consulting AG

Seminargebühren

CHF 1'200.– für ISACA-Mitglieder
(alle anderen plus CHF 100.–)



by Bitterli Consulting
itacs
training

Anmeldeformular:
www.itacs.ch

Einführung

An ISO27001 (vormals BS7799-2) und ISO27002 (vormals ISO17799) kommt heute kaum eine Sicherheitsspezialist oder IT-Revisor vorbei. Die beiden Standards sind allen bekannt; viele Sicherheitsbeauftragte von Unternehmen benützen sie (vor allem ISO27002) als "Inspirationsquelle" für ihre internen Tätigkeiten. Doch kaum jemand versteht beispielsweise, wie eine Zertifizierung auf Basis ISO27001 abläuft und was so ein Zertifikat in Realität wirklich bedeutet.

Die beiden Referenten dieses Kompaktkurses setzen den Standard ISO27001/2 resp. dessen Vorläufer im Rahmen ihrer Beratungstätigkeiten bereits seit 1995 mit grossem Erfolg für unterschiedlichste sicherheitsrelevante Tätigkeiten ein und kennen daher seinen Nutzen aber auch die Grenzen. Peter R. Bitterli überwacht zudem seit vielen Jahren als Fachexperte des Bundes die akkreditierten Zertifizierungsunternehmen und beurteilt deren Prozesse und die eingesetzten Audit-Teams.

Das Kompaktseminar hat zum Ziel, den Teilnehmern die wichtigsten Schritte zur Implementierung und Verbesserung eines ISMS nach ISO27001 und ISO27002 zu vermitteln sowie einen Überblick zu geben über sonstige Anwendungsmöglichkeiten.

Lernziele

Nach diesem Kompaktseminar sind Sie in der Lage:

- Werdegang und Struktur des ISO27001 (vormals BS7799) und ISO27002 (vormals ISO17799) vorzustellen;
- den Unterschied zwischen ISO27001 und ISO27002 zu erläutern;
- die wesentlichen Elemente eines Information Security Management System (ISMS) nach ISO27001 zu erläutern;
- die Einführung eines ISMS in rund 30 Schritten wirksam voranzutreiben resp. ein bestehendes ISMS zu erweitern und verbessern.

Zielpublikum

Der Kurs richtet sich an alle Personen, welche in kurzer Zeit alles Wesentliche über den internationalen Standard ISO27001 resp. ISO27002 erfahren und diesen im Rahmen ihrer Tätigkeiten produktiv einsetzen wollen: Sicherheitsverantwortliche, Datenschutz-Beauftragte, Risikomanager, ISO27001-Auditoren und IT-Revisoren. Informatik-Kenntnisse sind nicht notwendig.

Hinweis: Teilnehmer mit grosser Erfahrung bezüglich ISO27001/2 empfehlen wir das dreitägige Expertenseminar "Praxisgerechte Anwendung von ISO27001 und ISO27002, in das die Erfahrungen zahlreicher ISMS-Untersuchungen und Beratungsprojekte der beiden Referenten eingeflossen sind (siehe Seite 24).

Kurs-Spezialitäten

Alle Teilnehmenden erhalten die aktuelle Version von ISO27001 und ISO27002 sowie ausführliche Kursunterlagen.

Kursinhalte

- Werdegang CoP, BS7799, ISO 17799 und ISO27001/2
- Inhalte und Unterschiede ISO27001 / ISO27002
- Vorgehen bei einer Zertifizierung nach ISO27001
- Erstellung/Unterhalt eines ISMS nach ISO27001/2 (inkl. schrittweise Verbesserung eines bestehenden ISMS)
- Nutzen und Grenzen von ISO27001/2
- Zusammenfassung/Abschluss

Referenzen

- CISA Task Statements: (2.1) (2.8) 5.5
- CISM Task Statements: praktisch alle – aber nicht sehr detailliert
- COBIT IT-Prozesse: (PO4) (PO6) (PO7) PO9 (AI2) (DS4) DS5 (DS7) ME2 (ME3)

Referenten (Co-Teaching)

- Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG
- Hans Peter Riess, CISA, CISM, Ixact Security Inspection and Consulting AG

Seminargebühren

CHF 1'200.– für ISACA-Mitglieder (alle anderen plus CHF 100.–)



Anmeldeformular:
www.itacs.ch

ISMS-KK

Ein ISMS in
30 Schritten
implementieren
oder verbessern

Einführung

Der sichere Betrieb einer Web-Anwendung setzt zahlreiche technische und organisatorische Sicherheitsmassnahmen voraus, deren Kenntnis und praktische Anwendung zum Rüstzeug "jedes" Informatik-Spezialisten gehören sollten. Insbesondere im Zeitalter von Web 2.0, AJAX und neuen Technologien im Web-Bereich werden auch Sicherheitsaspekte immer wichtiger. Viele Unternehmen wöhnen sich bereits in Sicherheit, wenn sie Firewalls und Proxies einsetzen und auf dem Server die aktuellsten Security-Patches eingespielen. Was allerdings oftmals unterschätzt wird, sind Attacken gegen die Web-Applikation und Web-Services selber.

Der Kurs "Web Application Security Lab" konzentriert sich auf applikatorische Schwächen. Zu diesem Zweck hat Compass Security eine Demo-Infrastruktur bereitgestellt, mit welcher die verschiedenen Testszenarien praktisch erlebt und durchgeführt werden können. Diese Szenarien sind so aufgebaut, dass sie von "no security" bis "high security" alle Sicherheitsniveaus enthalten. Dabei geht der Kurs auf aktuelle Gefahren ein und beschreibt Massnahmen für deren Behebung.

Theoretische Angriffsszenarien werden am System illustriert, wobei Sie diese in Hands-on-Übungen gleich selbst bearbeiten und nachvollziehen können. Im Anschluss zu einem einzelnen Angriff wird die entsprechende Verbesserung am System eingespielt und der nächste Schritt (oder Angriff) getätigt, bis keine weiteren Angriffsszenarien mehr vorhanden sind.

Lernziele

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

Die Lösungen der Übungen werden durch den Kursleiter vorgeführt, so dass diese am Schluss von allen verstanden werden sollten. Diese Kombination von Theorie und Praxis gibt dem Teilnehmer einen guten Einblick in die Welt der elektronischen Straftaten, so dass er sich danach eine realistischere Einschätzung der "wirklichen" Gefahren machen kann.

Zielpublikum

Dieser Kurs richtet sich an IT-Sicherheitsverantwortliche, IT-Revisoren, Software-Entwickler sowie Sicherheitsinteressierte, die einen Einblick in die applikatorische IT-Sicherheit erhalten wollen. Der Kurs ist anspruchsvoll in Theorie und Praxis. Dabei wird ca. 50% der Zeit im Labor verbracht.

Um die Laborübungen lösen zu können, ist eine gewisse Vertrautheit auf der Windows-Kommandozeile notwendig. Auch sollten Sie Kenntnisse über E-Business-Applikationen haben und wissen, wie grundlegende Internetdienste funktionieren. Da einige Tools lediglich unter Linux verfügbar sind, wird der Teilnehmer auch auf Linux arbeiten.

Kurs-Spezialitäten

Jeder Teilnehmer verfügt im Kurs über einen eigenen Notebook, der mittels WLAN auf die verschiedenen vorbereiteten Fallstudien und Server zugreifen kann. Der Kurs "Application Security Lab" ist eine Ergänzung zu den sehr erfolgreichen Compass-Kursen "Virus/Trojan/Backdoor Security Lab" (eine Weiterentwicklung von "Content and Mobile Security Lab") und "Forensic Lab".

Kursinhalte

Zu Beginn wird die Angriffstheorie eingeführt. Der erste Schwerpunkt beschäftigt sich mit Session-Handling-Mechanismen und den dazugehörigen Attacken. Durch Übungen in der Labor-Infrastruktur gelangt das Gelernte gleich zur Anwendung:

- Angriffstheorie
- Einführung in die Applikationssicherheit
- Lauschattacken
- Session Handling-Methoden & -Angriffe
- Session Handling mit Entry Server

Der zweite Block geht auf die Bedrohungen ein, wenn die Eingaben eines Benutzers ungenügend validiert werden. Es resultieren Gefahren wie SQL-Injection oder Cross-Site Scripting. Dabei können die Daten vom Client sowohl binär als auch im ASCII-Textformat übertragen werden:

- Vergleiche zwischen verschiedenen Session-Methoden
- Authentisierung und Login-Attacken
- Autorisation
- Cross-Site-Scripting und -Tracing
- E-Business Referenz-Architektur (J2EE, EJB)
- HTML-Injection

- SQL-Injection
- HTTP-Response-Splitting
- Java Application Hacking mit Object Inspector
- Ein- und Ausgabvalidierung

Der dritte Block geht aufgrund der Aktualität auf Phishing-Attacken ein. Im Weiteren wird über eine forensische Analyse einer Anwendung auf Schwachstellen im Logging-Konzept eingegangen. Anschliessend wird die Sicherheit von Web-Services und XML-Parsern behandelt und auf Sicherheitsaspekte neuer Technologien eingegangen:

- Phishing-Attacken
- Warsearching
- Forensische Untersuchung in einer Web-Anwendung
- Logging-Konzept in Applikationen
- Web-Services Security (SOAP)
- XML-Parser-Schwachstellen
- Web 2.0 und AJAX

Referenzen

- CISA Task Statements: 3.4 (3.8) (4.7) 5.2
- CISM Task Statements: (2.4) (4.4) (4.8)
- CoBIT IT-Prozesse: (A13) DS5

Referent

- Ivan Bütler, Compass Security
- Daniel Röthlisberger, Compass Security

Seminargebühren

CHF 2'850.– für ISACA-Mitglieder (alle anderen plus CHF 200.–)



LAB-AS

Dreitägiger Workshop zum Thema Sicherheit in Web-Anwendungen mit praktischen Beispielen zu HTTPS, J2EE, Web-Services und Datenbanken

Anmeldeformular:
www.itacs.ch

Einführung

Durch den Einsatz von mobilen Technologien (z.B. Wireless-LAN, VPN, PDA, USB-Stick oder Terminal-Server) zur Anbindung von externen Partnern, Kunden und Mitarbeitern gibt es immer mehr Schnittstellen ins Intranet eines Unternehmens. Diese Vielfalt bietet den Angreifern diverse Möglichkeiten, Malware einzuschleusen oder Daten zu entwenden und dadurch die Perimetersicherheit in Form von Firewalls und Virens Scanner zu untergraben.

Immer häufiger gelangen speziell auf das Opfer ausgerichtete Trojaner zum Einsatz. Nebst dem klassischen Verbreitungsweg über E-Mail verwenden die Angreifer immer öfter Schwachstellen in Client-Anwendungen. Auch Mitarbeiter können als Angreifer aktiv werden und Sicherheitsinfrastrukturen bewusst oder unbewusst umgehen und somit das Unternehmen gefährden.

Der Kurs "Virus/Trojan/Backdoor Security Lab" zeigt die aktuellen Bedrohungen in den oben genannten Bereichen auf und stellt mögliche Gegenmassnahmen und deren Wirksamkeit vor. Nebst theoretischen Blöcken, die in die Themen einführen, können die Teilnehmenden mittels Hands-On-Übungen die Angriffsszenarien und Abwehrmechanismen in einer von Compass Security zur Verfügung gestellten Laborinfrastruktur live erleben. Im Anschluss daran werden mögliche Gegenmassnahmen und deren Wirksamkeit diskutiert.

Lernziele

Der dreitägige Kurs mit hohem Laboranteil hat folgende Ziele:

- Kennen der Hacker Methodik und des Viren Live Cycle;
- Kennen der Angriffe von aussen und innen;
- Kennen der Reverse Shell's und Inside-Out-Attacken;
- Kennen von Server-Attacken, Terminal Server Hacking;
- Wirksamkeit von Viren-Scannern und Content-Filtern;
- Wirksamkeit von Anti-Hacker Bypass-Massnahmen;
- Wissen um das Restrisiko.

Zielpublikum

Dieser Kurs richtet sich an IT-Sicherheitsverantwortliche, IT-Revisoren, System-Engineers sowie Sicherheitsinteressierte, die einen Einblick in die aktuellen Sicherheitsthemen erhalten wollen. Der Fokus des Kurses liegt in der Perimeter Security in Kombination mit Viren/Trojanern und Reverse Shells. Der Kurs ist anspruchsvoll in Theorie und Praxis. Um die Laborübungen lösen zu können, ist eine gewisse Vertrautheit mit der Windows-Kommandozeile notwendig.

Kurs-Spezialitäten

Jeder Teilnehmer verfügt im Kurs über einen eigenen Notebook, der mittels WLAN auf die verschiedenen vorbereiteten Fallstudien und Server zugreifen kann. Rund 50% der Zeit wird mit Labor-Übungen verbracht.

Der Kurs "Virus/Trojan/Backdoor Security Lab" ist eine Weiterentwicklung des

Kurses "Content and Mobile Security Lab" sowie eine Ergänzung zu den sehr erfolgreichen Labor-Kursen "Application Security Lab" und "Forensic Lab".

Kursinhalte

Als erster Schwerpunkt wird aufgezeigt, auf welchen Wegen Daten und Code in ein Unternehmensnetzwerk gelangen oder dieses verlassen können. Anschliessend werden Schwachstellen in neueren Access-Technologien aufgezeigt. Der erste Tag zeigt verschiedene Angriffskanäle auf und wie Malware in ein Unternehmen gelangen kann:

- Angriffstheorie
- Perimetersicherheit, direkte Attacken
- Gefahren durch mobile Geräte wie PDA, Mobiltelefone oder USB-Sticks
- Device-Locker, Indirekte Attacken

Falls ein Virus zur Ausführung kommt, versucht dieser, seine Schadfunktion zu starten. Vielleicht muss der Trojaner erst Admin-Privilegien erreichen? Wie sieht es mit Würmern aus, die sich selbständig verbreiten? Was kann man tun, um den Wirkungskreis der Verseuchung einzudämmen? Damit ist gemeint:

- Keystroke-Sniffer, Screen-Scraping
- Inside-Out-Attacken, Remote Administration Toolkits (RAT)
- Content-basierende Buffer Overflows (JPEG-Exploit) – IE Sicherheitslücke
- Schwachstellen in Client-Anwendungen wie Web-Browser oder Real-Player
- Applikationen, die Malware-Verhalten aufweisen (GoToMyPc, Skype)

Doch neben den Angriffen von aussen muss sich jedes Unternehmen auch mit Angriffen von innen auseinandersetzen. Was kann ein frustrierter Mitarbeiter tun,

wenn er die Firewall Policy umgehen will? Welche Möglichkeiten gibt es? Wie kann man diese verhindern?

- Umgehung einer Firewall über Tunneling
- Umgehung einer Firewall über Anonymizer
- Terminal Server als Virenschleuder?

Im Weiteren wird auf Terminal Server-spezifische Schwachstellen eingegangen, die es einem Angreifer ermöglichen, erweiterte Privilegien zu erlangen. Ist SBC (Server based Computing) die strategische Lösung für den Zugriff von unsicheren Devices? Welche Gefahren gibt es?

- Ausbrechen aus Applikationen
- Einschleusen von unerwünschten Programmen
- Stehlen von Dateien, welche auf dem Terminal Server hinterlegt sind
- Ausweitung der Privilegien
- Schwachstellen in Logon-Scripts, Treiber-Trojaner oder Stehlen der Passwortdateien
- Möglichkeiten und Grenzen von Software Restriction Policies

Referenzen

- CISA Task Statements: (4.7) 5.2
- CISM Task Statements: (2.4) (4.8)
- COBIT IT-Prozesse: (A13) DS5

Referenten (Co-Teaching)

- Walter Sprenger, Compass Security
- Martin Süss, Compass Security

Seminargebühren

CHF 2'850.– für ISACA-Mitglieder (alle anderen plus CHF 200.–)



LAB-VTB

Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung durch mobile Technologien und aktuelle Malware

Anmeldeformular:
www.itacs.ch

Einführung

Angriffe auf Internet-Plattformen, webbasierte Anwendungen oder mobile Systeme nehmen geradezu dramatisch zu. Die notwendigen Abwehrmassnahmen werden immer anspruchsvoller, weshalb die entsprechenden Entwickler und Security Engineers immer besser Bescheid wissen müssen über die verwendeten Angriffsmethoden und sinnvollen Abwehrkonzepte.

Basierend auf den in unzähligen Beratungsmandaten gesammelten Erfahrungen, den seit Jahren immer wieder aktualisierten Kursen "Application Security Lab", "Content & Mobile Security Lab" und "Evidence Lab" sowie dem tollen Erfolg mit dem "Hacking Weekend" haben wir einen einwöchigen Kurs für fortgeschrittene Teilnehmer mit hands-on Erfahrung konzipiert: Aus insgesamt über 20 vorbereiteten Cases können die Teilnehmer die ihren spezifischen Bedürfnissen entsprechenden Fragestellungen auswählen und alleine oder in Kleinteamen lösen. Dazu steht ihnen eine komplette Infrastruktur mit den notwendigen Servern, Arbeitsplätzen sowie Angriffswerkzeugen zur Verfügung.

Jeder Kurstag wird eingerahmt von einer Vorstellung des "Fall des Tages" am Vormittag und der Erläuterung der für die Abwehr dieses Angriffstyps sinnvollen Massnahmen am Spätnachmittag. Dazwischen sind die Teilnehmer aufgefordert, entsprechend ihren Kenntnissen und Fähigkeiten in ihrem eigenen Rhythmus die verschiedenen Fälle zu lösen. Ein Fall gilt dann als gelöst, wenn nicht nur der Angriff gelang sondern ein sinnvolles Abwehrdispositiv beschrieben wurde.

Verantwortungsbewusste Betreiber von aus dem Internet zugänglichen Plattformen und Anwendungen sowie auch von mobilen Systemen haben jetzt erstmals die Möglichkeit, ihre Mitarbeiter gezielt für die im eigenen Umfeld wichtigen Fragestellungen auszubilden.

Lernziele

Durch den Besuch der Trainingswoche ist der Kursteilnehmer in der Lage:

- gezielt entsprechend den persönlichen Bedürfnissen Fälle auszuwählen und zu bearbeiten;
- unterschiedlichste Angriffsszenarien bis ins letzte Detail zu analysieren;
- die jeweilige Gefährdung wirklich zu verstehen und entsprechend der möglichen Auswirkungen zu beurteilen;
- entsprechend der konkreten technologischen Gefährdung sinnvolle Massnahmen zu konzipieren;
- die Lösungsansätze strukturiert zu beschreiben.

Zielpublikum

Dieser Kurs richtet sich an IT Security Engineers, Systemadministratoren, Softwareentwickler, Sicherheitsverantwortliche und Revisoren, die über ausreichende theoretische Grundlagen und konkrete Praxiserfahrungen verfügen.

Die Laborübungen sind anspruchsvoll; um sie lösen zu können, müssen die Teilnehmer selbstständig mit Windows arbeiten können. Auch sollten die Teilnehmer Netzwerkkenntnisse haben und wissen, wie grundlegende Internetdienste funktionieren. Da viele Tools lediglich unter Linux verfügbar sind, wird der Teilnehmer auch auf Linux arbeiten.

Kurs-Spezialitäten

Der grösste Teil wird mit Laborübungen verbracht, die unterschiedlichste Themen behandeln und teilweise recht anspruchsvoll sind. Die Teilnehmer werden bei Bedarf betreut und mit Tipps versehen – das selbständige Analysieren und Lösen der Problemstellungen steht aber im Vordergrund. Der Kurs ist daher nicht geeignet für Teilnehmer, die eine Schritt-für-Schritt-Anleitung erwarten.

Wir rechnen damit, dass ein Teilnehmer ca. 1 bis max. 3 Fälle pro Tag lösen kann; inkl. der zwingend verlangten Beschreibung der für die jeweiligen Angriffe benötigten Abwehrmassnahmen. Für die gelösten Fälle erhalten die Teilnehmer eine vertiefte Beschreibung und einen vollständigen Lösungsvorschlag.

Kursinhalte

Am ersten Kurstag erhalten die Teilnehmer eine Einführung in die vorhandene Infrastruktur mit den unterschiedlichsten Servern und Anwendungen sowie die jedem Teilnehmer zur Verfügung stehenden Notebooks und Hacking-Tools.

An jedem Kurstag wird zu Beginn der "Fall des Tages" vorgestellt – dieser Fall wird am Spätnachmittag dann aufgelöst und die wichtigsten Schutzmassnahmen zur Abwehr dieses Angriffstyps konkret erläutert. U.a. stehen die folgenden Lernmodule zur Verfügung:

- Netzwerk Security
- Layer2 Security
- Web Application Security
- Web Service Security und XML
- Server-based Computing
- Content Injection Attacken

- Spyware Analyse – Forensik
- Unix Forensik
- Netzwerk Forensik
- Windows Security
- Tunneling und Firewalling/Inside-Out Attacken
- Man in the Middle Attacken
- Hardening
- Intrusion Detection und Prevention
- Nachvollziehbarkeit von Ereignissen – Korrelation und Aggregation
- Client Security

Referenzen

- CISA Task Statements: 4.2 4.7 5.1 5.2 5.5
- CISM Task Statements: (2.2) 2.4–2.6 4.8
- CoBIT IT-Prozesse: DS5

Referenten

- Ivan Büttler, Compass Security
- Daniel Röthlisberger, Compass Security

Seminargebühren

Die ersten drei Tage kosten CHF 3'300.–; die beiden weiteren Tage sind zusätzlich zu je CHF 600.- buchbar (Alle Preise für ISACA-Mitglieder, alle anderen Personen plus CHF 250.–)

Speziell zu beachten

Unterlagen sind teilweise auf Englisch.



LAB-TW

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

Anmeldeformular:
www.itacs.ch

Einführung

Für Revisoren oder Sicherheitsbeauftragte ist die Kommunikation ein wichtiges Mittel, um ihren Auftrag erfolgreich ausführen zu können. Normalerweise gelingt das Kommunizieren problemlos und ist auch erfolgreich. Es ist aber wichtig, dass die Kommunikation auch in schwierigen Situationen wirkungsvoll bleibt und das eigentliche Gesprächsziel erreicht wird.

Schwierig wird es dann, wenn wir z.B. bei Interviews oder in wichtigen Besprechungen mit unseren (internen oder externen) Kunden in eine unvorhergesehene Situation geraten, die für uns neu oder befremdend ist. Vielleicht haben Sie sich auch schon darüber geärgert, dass es Ihnen in einer solchen Gesprächssituation nicht gelungen ist, souverän zu reagieren. Oft sind wir in diesen Fällen überfordert, weil wir überrascht wurden und sprachlos sind. Der Überraschungseffekt löst bei uns Stress aus und beeinflusst unser Kommunikationsverhalten negativ: Die Konzentration geht verloren, die Wahrnehmung bezüglich des Gesprächspartners und das aktive Zuhören sind eingeschränkt, die Ausdrucksweise verändert sich. Die Trennung zwischen Sache und Person ist nicht mehr eindeutig, und damit verlieren wir das Gesprächsziel schnell aus den Augen.

Um in solchen Momenten kompetent und überzeugend reagieren zu können, ist ein gezieltes Training der verschiedenen sinnvollen Verhaltensweisen notwendig. Gleichzeitig ist von Bedeutung, die eigenen Stärken und Schwächen im Kommunikationsverhalten zu kennen, um die Kommunikationskompetenz gezielt weiterentwickeln zu können.

Lernziele

Das Kommunikationstraining ermöglicht den Teilnehmenden, sich intensiv mit Ihrem Kommunikationsverhalten auseinanderzusetzen und dieses gezielt weiterzuentwickeln. Im Vordergrund steht das Training des Kommunikationsverhaltens in schwierigen Kundensituationen.

Die Teilnehmenden:

- erkennen ihre Stärken und Schwächen in ihrem Kommunikationsverhalten;
- sind in der Lage, in schwierigen Gesprächssituationen souverän zu reagieren;
- entwickeln ihr Kommunikationsverhalten gezielt weiter;
- können anspruchsvolle Kundengespräche kompetent führen;
- sind in der Lage, ihre Rolle als Revisor oder Sicherheitsbeauftragter trotz der nicht immer einfachen Umstände überzeugend wahrzunehmen.

Zielpublikum

Interne und externe Revisoren/Wirtschaftsprüfer, Mandatsleiter, Sicherheitsbeauftragte, Projektleiter, Kommunikationsverantwortliche und alle anderen Personen, die ihr Kommunikationsverhalten in ihrem beruflichen Umfeld überprüfen und gezielt weiterentwickeln wollen. Dies setzt von den Teilnehmenden die Bereitschaft zur engagierten Mitwirkung im Training voraus.

Kurs-Spezialitäten

Im Vordergrund steht die aktive Auseinandersetzung mit dem eigenen Kommunikationsverhalten. Dies erfolgt im Zusammenhang mit:

- Kurzreferaten und Lehrgesprächen,
- der Bearbeitung von Praxisbeispielen,
- Kommunikationsübungen (mit Video-Feedback),
- dem persönlichen Feedback, das die Teilnehmenden am zweiten Tag vom Trainingsleiter erhalten.

Die Teilnehmenden haben die Möglichkeit, im Seminar eigene Praxisituationen einzubringen, die sie zum Beispiel aufgrund ihrer Aktualität lösungsorientiert bearbeiten wollen.

Kursinhalte

Die Schwerpunkte des Seminars sind:

- Rolle des Revisors / Beraters
- Anforderungen an die Sozialkompetenz des Revisors / Beraters
- Wichtige Grundsätze der Kommunikation
- Führen von zielorientierten Gesprächen
- Vorbereitung und Durchführung von Interviews
- Sachbezogenes Verhandeln
- Verhaltensstrategien in schwierigen Gesprächssituationen (Konflikte usw.)
- Überprüfen und entwickeln des eigenen Kommunikationsverhalten

Referenzen

- CISA Task Statements: (1.3) (1.4) (1.5)
- CISM Task Statements: (4.6) (4.7)
- COBIT IT-Prozesse: (PO6)

Referent

- Ruedi Wyssen,
Wyssen Unternehmensberatung

Speziell zu beachten

Einzelne der Übungen werden auf Video aufgezeichnet und teilweise im Plenum ausgewertet. Die Aufzeichnungen werden nach Kursabschluss vernichtet. Die Teilnehmer sind mit diesem Vorgehen ausdrücklich einverstanden.

Der Kurs wird mit maximal 12 Teilnehmern durchgeführt, um eine hohe Trainingsintensität zu erreichen.

Seminargebühren

CHF 2'000.– für ISACA-Mitglieder
(alle anderen plus CHF 150.–)

**KOM-BT**

Bewusste Gesprächsführung (auch) in kritischen Situationen – mit vielen praktischen Übungen und in einer kleinen Gruppe

Anmeldeformular:
www.itacs.ch

Einführung

Seit Herbst 2002 bietet die ISACA den Certified Information Security Manager (CISM) an. Nach dem riesigen Erfolg mit dem Certified Information Systems Auditor (CISA) ist zu erwarten, dass das neue CISM-Zertifikat relativ schnell eine ähnliche Bedeutung erlangen wird. Bereits sind über 7,000 Personen Träger des begehrten CISM-Zertifikates. Mit dem CISM-Zertifikat erwirbt man einen Leistungsausweis in allen Teilbereichen des Informationssicherheitsmanagement. Das CISM-Berufsbild wurde auf die Prüfung 2007 aktualisiert und umfasst fünf Areas, 45 Tasks (Aufgaben) und 93 Knowledge Statements (Aussagen zum benötigten Fachwissen).

Der CISM-Kurs vermittelt und vertieft theoretisches wie praktisches Fachwissen im breiten Feld von Risikomanagement und Governance der Informationssicherheit, bereitet aber auch intensiv auf die von ISACA organisierte CISM-Prüfung vor.

Lernziele

In unserem berufsbegleitenden CISM Kurs werden die Teilnehmer:

- die Anforderungen an einen CISM kennen und verstehen lernen (aktuelles Berufsbild von 2006);
- in die Lage versetzt, die CISM-Prüfung zu bestehen;
- ein praxisbezogenes Fachwissen für das Management der Informationssicherheit auf hohem Niveau erwerben;
- nach klaren Vorgaben alleine und gemeinsam das benötigte Wissen erarbeiten und dieses anhand von Fallbeispielen aus der Praxis vertiefen.

Zielpublikum

Der CISM-Kurs richtet sich an alle Personen, die unternehmensweit oder auch in Teilbereichen für das Management der Informationssicherheit verantwortlich sind – also Beauftragte für (Informations-) Sicherheit, Risikomanager, Verantwortliche für Business Continuity. Ein CISM beschäftigt sich mit allen Aspekten des Sicherheitsmanagement, ist also beispielsweise dafür verantwortlich,

- dass die Informationssicherheitsstrategie ausgerichtet ist auf die Unternehmensziele und übereinstimmt mit den anwendbaren Gesetzen und Richtlinien,
- dass Risiken identifiziert und gemanaged werden,
- dass ein Informationssicherheitsprogramm definiert und implementiert ist, und
- dass Auswirkungen von Unterbrüchen auf die Geschäftstätigkeit minimiert werden.

Der CISM-Kurs richtet sich also vor allem an Personen, welche eine Funktion in der Sicherheitsorganisation eines Unternehmens haben und sich vorwiegend mit dem Management der Informationssicherheit beschäftigen. Die Informatik ist zwar für die Informationssicherheit von Bedeutung, doch für einen CISM ein Faktor von vielen.

Kurs-Spezialitäten

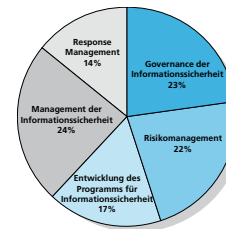
- Klar strukturierte Kursunterlagen grösstenteils in Deutsch, welche zur Prüfungsvorbereitung und als Nachschlagewerk dienen;
- Alle im Kurs direkt eingesetzte Fachliteratur wird abgegeben;
- Permanente Bestimmung des Lernfortschritts mittels 10 kleiner und 4 grosser Testprüfungen

Kursinhalte

Bitte beachten Sie das detaillierte Kursprogramm mit sämtlichen Aufgaben eines CISM (www.itacs.ch)!

- Area 1: Governance der Informationssicherheit
- Area 2: Informations-Risikomanagement
- Area 3: Entwicklung des Informationssicherheits-Programmes
- Area 4: Management des Informationssicherheits-Programms
- Area 5: Ereignis-Management und -Reaktion

- Area 1: 23%
- Area 2: 22%
- Area 3: 17%
- Area 4: 24%
- Area 5: 14%



Referenzen

- CISA Task Statements: 2.8 3.4 (3.8–3.10) (4.6) 5.1–5.5
- CISM Task Statements: alle
- CoBIT IT-Prozesse: DS4 DS5 (DS7) ME2 ME3

Referenten

- Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG

Seminargebühren

CHF 7'800.– für ISACA-Mitglieder (alle anderen plus CHF 300.–)

Inkl. 1 auswärtige Übernachtung

Zertifizierung

Für die Zertifizierung als CISM muss ein Kandidat zusätzlich zur bestandenen CISM-Prüfung fünf Jahre Berufspraxis in der Informationssicherheit in mindestens drei der fünf CISM-Areas nachweisen. Mindestens drei dieser fünf Jahre müssen in der Rolle eines Informationssicherheits-Managers ausgeübt worden sein. Bestimmte Titel/Diplome sind bis maximal 2 Jahre Praxis anrechenbar.

Prüfungsgebühr

US\$ 375.– bis 555.– (je nach Anmeldezeitpunkt und Mitglieder-Status)

Speziell zu beachten

Dies ist ein 12.5tägiger, berufsbegleitender Kurs mit ausserordentlichen Erfolgsquoten an den internationalen Prüfungen. Verlangen Sie den detaillierten Spezialprospekt oder laden Sie das entsprechende PDF herunter. Eine schriftliche Anmeldung ist zwingend.



CISM-VK

Vertiefungskurs für Sicherheitsbeauftragte; offizieller Kurs des ISACA Switzerland Chapter

Anmeldeformular: www.itacs.ch

Einführung

CISA ist das einzige weltweit anerkannte Zertifikat im Bereich Revision, Kontrolle und Sicherheit von Informationssystemen und geniesst seit Jahren international ein grosses Ansehen, da die Anforderungen hoch und weltweit identisch sind. Das CISA-Berufsbild wurde 2005 erneut aktualisiert und umfasst sechs Areas, 38 Tasks (Aufgaben) und 79 Knowledge Statements (Aussagen zum benötigten Fachwissen). Da die Task Statements auch auf die jeweiligen CoBIT-Prozesse referenziert sind, wird CoBIT de facto zu einem integrierenden Bestandteil der CISA-Ausbildung und -Zertifizierung.

Der CISA-Kurs vermittelt und vertieft theoretisches wie praktisches Fachwissen im breiten Feld von Revision und Sicherheit; bereitet aber auch intensiv auf die von ISACA organisierte CISA-Prüfung vor.

Lernziele

In unserem berufsbegleitenden CISA-Kurs werden die Teilnehmer:

- die Anforderungen an einen CISA kennen und verstehen lernen (aktuelles Berufsbild von 2005);
- in die Lage versetzt; die CISA-Prüfung zu bestehen;
- ein praxisbezogenes Fachwissen für IT-Governance; IT-Sicherheit und IT-Revision auf hohem Niveau erwerben;
- nach klaren Vorgaben alleine und gemeinsam das benötigte Wissen erarbeiten und dieses anhand von Fallbeispielen aus der Praxis vertiefen.

Zielpublikum

Der CISA-Kurs richtet sich an alle Personen, die sich mit Sicherheit, Governance und Ordnungsmässigkeit von Informationssystemen beschäftigen – also Sicherheitsbeauftragte, Compliance-Officer, Informatikrevisoren, IT-Projektleiter oder Projektcontroller und viele andere mehr. Der Kurs ist offen für alle, die Interesse an der Revision, Kontrolle und Sicherheit von Informationssystemen haben, und ist nicht an das Ablegen der CISA-Prüfung gebunden. Vorbedingung für die Teilnahme ist hingegen eine ein- bis zweijährige "qualifizierte" Berufspraxis sowie umfassende Informatik-Kenntnisse. Über jedes Thema aus dem breiten CISA-Berufsbild sollte ein Kursteilnehmer – nach Absolvieren des Kurses – die folgenden Fragen beantworten können:

- Was versteht man unter diesem Begriff? Um was handelt es sich hier?
- Was sind die mit diesem Begriff verbundenen Risiken?
- Welche Sicherheitsanforderungen (Kontrollziele) sind wichtig?
- Mit welchen Massnahmen (Kontrollen) lassen sich diese Anforderungen erfüllen?
- Wie prüfe ich, ob die implementierten Massnahmen die Risiken wirksam abdecken?

Der CISA-Kurs richtet sich also vor allem an Personen, welche überprüfen wollen, ob die dafür verantwortlichen Personen ihre Informatik "im Griff" haben, resp. selber genau dafür verantwortlich sind. Die Informatik (Informationsverarbeitung) nimmt für einen CISA einen grossen Stellenwert ein.

Kurs-Spezialitäten

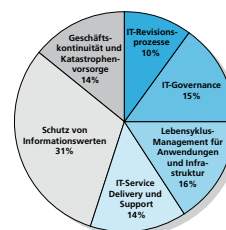
- Klar strukturierte Kursunterlagen grösstenteils in Deutsch (rund 2000 Seiten), welche zur Prüfungsvorbereitung und als Nachschlagewerk dienen (für CHF 500 auch zusätzlich auf Englisch erhältlich);
- Alle im Kurs direkt eingesetzte Fachliteratur wird abgegeben (Ausnahme CoBIT, da die meisten Firmen dieses Standardwerk bereits besitzen)
- Permanente Bestimmung des Lernfortschritts mittels 12 kleiner und 6 grosser Testprüfungen

Kursinhalte

Bitte beachten Sie das detaillierte Kursprogramm mit sämtlichen Aufgaben eines CISA (www.itacs.ch)!

- Area 1: IT-Revisionsprozess
- Area 2: IT-Governance
- Area 3: Lebenszyklus-Management für Anwendungen und Infrastruktur
- Area 4: IT Service Delivery und Support
- Area 5: Schutz von Informationswerten
- Area 6: Geschäftskontinuität und Katastrophenvorsorge

- Area 1: 10%
- Area 2: 15%
- Area 3: 16%
- Area 4: 14%
- Area 5: 31%
- Area 6: 14%



Referenzen

- CISA Task Statements: alle
- CISM Task Statements: (alle)
- CoBIT IT-Prozesse: alle

Referenten

- Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG
- Luc Pelfini, CISA, CISM

Seminargebühren

CHF 10'300.– für ISACA-Mitglieder (alle anderen plus CHF 300.–)

Inkl. 2 auswärtige Übernachtungen

Zertifizierung

Für die Zertifizierung als CISA muss ein Kandidat zusätzlich zur bestandenen CISA-Prüfung fünf Jahre Berufspraxis in den Bereichen Revision, Kontrolle oder Sicherheit von Informationssystemen nachweisen, wobei davon in der Regel maximal drei durch entsprechende Tätigkeiten in der Informatik, der Wirtschaftsprüfung oder durch einen anerkannten Abschluss z.B. an einer Fachhochschule substituiert werden können. Genauere Angaben entnehmen Sie bitte der detaillierten Kursausschreibung.

Prüfungsgebühr

US\$ 375.– bis 555.– (je nach Anmeldezeitpunkt und Mitglieder-Status)

Speziell zu beachten

Dies ist ein 14.5-tägiger, berufsbegleitender Kurs mit ausserordentlichen Erfolgsquoten an den internationalen Prüfungen. Verlangen Sie den detaillierten Spezialprospekt oder laden Sie das entsprechende PDF herunter. Eine schriftliche Anmeldung ist zwingend.

Anmeldeformular:
www.itacs.ch

Introduction

En exclusivité pour la Suisse romande, l'ISEIG propose une formation d'audit informatique complète de haut niveau basée sur les standards de l'ISACA - Information Systems Audit and Control Association.

Cette formation permet :

- d'acquérir, compléter et systématiser ses connaissances méthodologiques dans l'audit et la sécurité des systèmes d'information
- de se préparer à la certification internationale CISA.

Cette certification 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
- exprime sa volonté d'augmenter son rendement professionnel ou d'obtenir une promotion ou un nouveau poste
- se conforme aux exigences de formation continue définies par le programme de certification pour répondre aux nouvelles exigences et nouvelles technologies.

Objectifs d'apprentissage

- avoir une vision structurée et complète de l'approche orientée risque proposée par ISACA pour l'audit des systèmes d'information en termes d'organisation, de processus et de technologie
- connaître l'environnement réglementaire actuel pour les professionnels de l'audit interne et externe :

prise de position sur l'environnement bancaire selon art. 44oOB, circulaire d'outsourcing 99/2, Bâle II, Sarbanes-Oxley Act (SOX)

- analyser les différents domaines du programme sur lequel porte l'examen
- acquérir les stratégies de réponse au questionnaire et s'entraîner au déroulement de l'examen de certification CISA de l'ISACA

Public cible

- toute personne ayant l'intérêt et la volonté de se spécialiser dans l'audit et la sécurité des systèmes d'information, comme par exemple :
- auditeur IT (junior/senior/manager)
- auditeur financier souhaitant compléter ses compétences dans les aspects de l'audit IT
- gestionnaire confronté aux aspects risques, contrôles et sécurité de l'information et des systèmes d'information
- informaticien souhaitant compléter et faire reconnaître ses compétences d'audit informatique

Particularités

Un partenariat entre le Chapitre suisse de ISACA, ITACS Training AG. et ISEIG a permis d'organiser cette formation basée sur les meilleures pratiques actuelles selon le programme et les expériences menés en Suisse alémanique depuis 1992. Pour les entreprises exerçant des 2 côtés de la Sarine, cette solution permet aux collaborateurs romands et alémaniques d'avoir la même formation, chacun dans sa langue. La formation se compose de 2 modules complémentaires et indépendants :

- la formation à l'audit des systèmes d'information : pour acquérir, compléter et systématiser ses connaissances et compétences d'audit en termes d'approche, de méthodologie, de meilleures pratiques et de retour d'expériences
- la préparation à la certification internationale CISA : pour se préparer de manière optimale à l'examen de certification CISA

La formation complète, dispensée en français, se base sur un support de cours d'environ 7 classeurs en anglais, la dernière version du CISA Review Manual, 1 CD-ROM avec des questions d'examen ISACA officielles et différents documents techniques.

Programme

1. processus d'audit des systèmes d'information: effectuer les audits conformément aux normes et aux directives généralement acceptées
2. gouvernance des technologies de l'information: évaluer les stratégies, politiques, normes, procédures et pratiques en matière de gestion, planification et organisation des systèmes d'information
3. gestion du cycle de vie des systèmes et des infrastructures: évaluer l'efficacité et l'efficience des pratiques de gestion en matière de développement, acquisition, test, mise en oeuvre, maintenance et enterrement des systèmes d'information
4. distribution et support de services informatiques: évaluer les pratiques de gestion des services de la technologie de l'information

5. protection de l'information: évaluer la sécurité de l'infrastructure logique, environnementale et informatique
6. continuité opérationnelle et recouvrement en cas de sinistre: évaluer le processus visant à élaborer et maintenir des plans de continuité des affaires et de traitement de l'information documentés, communiqués et testés en cas de désastre.

Référence

- CISA Review Manual de l'ISACA

Animateurs

- Marc Barbezat, auditeur certifié CISA
- Jeff Primus, auditeur certifié CISA
- Alexis Sgard, manager de projet PMP, certifié CISA

Prix du cours

Formation complète, avec préparation à l'examen, 14 jours : CHF 8260.-*, incluant le matériel pédagogique.

Préparation à l'examen, 5 jours : CHF 2950.-*, incluant le support de cours et un CD d'examen à blanc
* Réduction de 5 % pour les membres de l'ISACA

Certification

Deux sessions par année, à Zürich pour la Suisse, en juin et décembre

Taxe d'examen

Entre USD 375.- et USD 555.- en fonction de la date d'inscription et le statut de membre ou non membre de l'ISACA



CISA-CE

En exclusivité pour la Suisse romande, une formation officielle à l'Audit des systèmes d'information avec préparation à la certification internationale CISA

Pour plus d'informations :
www.iseig.ch

Einführung

Seit Herbst 2002 bietet die ISACA den Certified Information Security Manager (CISM) an. Nach dem riesigen Erfolg mit dem Certified Information Systems Auditor (CISA) ist zu erwarten, dass das neue CISM-Zertifikat relativ schnell eine ähnliche Bedeutung erlangen wird. Bereits sind über 7,000 Personen Träger des begehrten CISM-Zertifikates. Mit dem CISM-Zertifikat erwirbt man einen Leistungsausweis in allen Teilbereichen des Informationssicherheitsmanagements. Das CISM-Berufsbild wurde auf die Prüfung 2007 aktualisiert und umfasst fünf Areas, 45 Tasks (Aufgaben) und 93 Knowledge Statements (Aussagen zum benötigten Fachwissen).

Lernziele

Aufbauend auf der bereits durchgeführten "privaten" Vorbereitung der Teilnehmer vermitteln wir die wichtigsten Tätigkeiten eines CISM und ergänzen diesen Kompaktblock mit einer realistischen Testprüfung sowie nachfolgender Auswertung und Besprechung.

In unserem CISM-Prüfungsvorbereitungskurs werden die Teilnehmer:

- das selbständig erworbene Wissen vervollständigen und abrunden;
- bei entsprechender persönlichen Vorbereitung in die Lage versetzt; die CISM-Prüfung zu bestehen.

Unser erklärtes Ziel ist, Sie optimal auf die scharfe Prüfung vorzubereiten. Nach der systematischen Besprechungen aller im Berufsbild festgehaltenen Aufgaben ("Task Statements") führen wir eine möglichst realistische Testprüfung durch.

Zielpublikum

Teilnehmer, welche bereits über langjährige Berufserfahrung verfügen und die sich privat auf die CISM-Prüfung vorbereiten und nicht an einem von uns durchgeführten Vertiefungskurs teilnehmen (können). Voraussetzungen sind genaue Kenntnisse des entsprechenden Berufsbildes, ein vollständiges Durcharbeiten des CISM Review Manual vor Kursbeginn sowie idealerweise mehrjährige Praxiserfahrung in möglichst vielen Teilbereichen der Informationssicherheit.

Der CISM-Kurs richtet sich an alle Personen, die unternehmensweit oder auch in Teilbereichen für das Management der Informationssicherheit verantwortlich sind – also Beauftragte für (Informations-) Sicherheit, Risikomanager, Verantwortliche für Business Continuity.

Kurs-Spezialitäten

2 vollständige Testprüfungen mit personenbezogener Detailauswertung

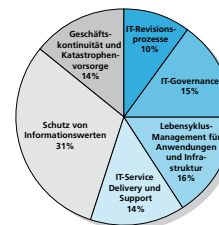
Kursinhalte

Systematische und hochkonzentrierte Durchsicht aller Aufgaben eines CISM gemäss dem aktuellen Berufsbild in zwei Tagen. Dabei werden die aus Prüfungssicht wichtigen Details vorgestellt, ohne auf die einzelnen Aufgaben vertieft einzugehen. Es geht in diesem Kurs also ausschliesslich um eine prüfungsbezogene Fokussierung – das notwendige Fachwissen wird vorausgesetzt. Wer die Aufgaben eines CISM wirklich beherrschen will, soll am eigentlichen Vertiefungskurs teilnehmen.

Anschliessend an diesen Block führen wir in Zürich eine möglichst realistische Prüfung auf Englisch durch. Nach dieser vierstündigen Testprüfung erstellen wir für Sie eine persönliche Auswertung der 200 gelösten Multiple-Choice-Fragen und besprechen diese an einem separaten Kurstag. Anschliessend erhalten Sie noch eine zweite Prüfung, welche Sie selbständig lösen können. Ihre Resultate werden wiederum von uns ausgewertet und Ihnen zugestellt.

- Area 1: Governance der Informationssicherheit
- Area 2: Informations-Risikomanagement
- Area 3: Entwicklung des Informationssicherheits-Programmes
- Area 4: Management des Informationssicherheits-Programms
- Area 5: Ereignis-Management und -Reaktion

- Area 1: 23%
- Area 2: 22%
- Area 3: 17%
- Area 4: 24%
- Area 5: 14%



Referenzen

- CISA Task Statements: –
- CISM Task Statements: alle
- COBIT IT-Prozesse: PO9 DS5

Referent

- Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG

Seminargebühren

CHF 2'900.– für ISACA-Mitglieder (alle anderen plus CHF 150.–)

Inkl. 1 auswärtige Übernachtung

Zertifizierung

Für die Zertifizierung als CISM muss ein Kandidat zusätzlich zur bestandenen CISM-Prüfung fünf Jahre Berufspraxis in der Informationssicherheit in mindestens drei der fünf CISM-Areas nachweisen. Mindestens drei dieser fünf Jahre müssen in der Rolle eines Informationssicherheits-Managers ausgeübt worden sein. Bestimmte Titel/Diplome sind bis maximal 2 Jahre Praxis anrechenbar.

Prüfungsgebühr

US\$ 375.– bis 555.– (je nach Anmeldezeitpunkt und Mitglieder-Status)

Speziell zu beachten

Dies ist ein 4tägiger Kompaktkurs für erfahrene Kursteilnehmer, welche das gesamte Berufsbild und das CISM Review Manual bereits selbständig durchgearbeitet haben und beherrschen.



Anmeldeformular:
www.itacs.ch

Einführung

CISA ist das einzige weltweit anerkannte Zertifikat im Bereich Revision, Kontrolle und Sicherheit von Informationssystemen und geniesst seit Jahren international ein grosses Ansehen, da die Anforderungen hoch und weltweit identisch sind. Mit dem CISA-Zertifikat erwirbt man einen Leistungsausweis in den Bereichen Revision, Kontrolle und Sicherheit von Informationssystemen. Das CISA-Berufsbild wurde 2005 erneut aktualisiert und umfasst sechs Areas, 38 Tasks (Aufgaben) und 79 Knowledge Statements (Aussagen zum benötigten Fachwissen). Da die Task Statements auch auf die jeweiligen COBIT-Prozesse referenziert sind, wird COBIT de facto zu einem integrierenden Bestandteil der CISA-Ausbildung und -Zertifizierung.

Lernziele

Aufbauend auf der bereits durchgeführten "privaten" Vorbereitung der Teilnehmer vermitteln wir die wichtigsten Tätigkeiten eines CISA und ergänzen diesen Kompaktblock mit einer realistischen Testprüfung sowie nachfolgender Auswertung und Besprechung.

In unserem CISA-Prüfungsvorbereitungskurs werden die Teilnehmer das selbständig erworbene Wissen vervollständigen und abrunden und, bei entsprechender persönlicher Vorbereitung, in die Lage versetzt, die CISA-Prüfung zu bestehen.

Unser erklärtes Ziel ist, Sie optimal auf die scharfe Prüfung vorzubereiten. Nach der systematischen Besprechungen aller im Berufsbild festgehaltenen Aufgaben ("Task Statements") führen wir eine möglichst realistische Testprüfung durch.

Zielpublikum

Teilnehmer, welche bereits über langjährige Berufserfahrung verfügen und die sich privat auf die CISA-Prüfung vorbereiten und nicht an einem von uns durchgeführten Vertiefungskurs teilnehmen (können). Voraussetzungen sind genaue Kenntnisse des entsprechenden Berufsbildes, ein vollständiges Durcharbeiten des CISA Review Manual vor Kursbeginn sowie idealerweise mehrjährige Praxiserfahrung in möglichst vielen Informatik-Teilbereichen.

Der CISA-Prüfungsvorbereitungskurs richtet sich an alle Personen, die sich mit Sicherheit, Governance und Ordnungsmässigkeit von Informationssystemen beschäftigen – also Sicherheitsbeauftragte, Compliance-Officer, Informatikrevisoren, IT-Projektleiter oder Projektcontroller.

Kurs-Spezialitäten

2 vollständige Testprüfungen mit personenbezogener Detailauswertung

Kursinhalte

Systematische und hochkonzentrierte Durchsicht aller Aufgaben eines CISA gemäss dem aktuellen Berufsbild in drei Tagen. Dabei werden die aus Prüfungssicht wichtigen Details vorgestellt, ohne auf die einzelnen Aufgaben vertieft einzugehen. Es geht in diesem Kurs also ausschliesslich um eine prüfungsbezogene Fokussierung – das notwendige Fachwissen wird vorausgesetzt. Wer die Aufgaben eines CISA wirklich beherrschen will, soll am eigentlichen Vertiefungskurs teilnehmen.

Anschliessend an diesen Block führen wir in Zürich eine möglichst realistische Prüfung wahlweise in Deutsch oder Englisch durch. Nach dieser vierstündigen Testprüfung erstellen wir für Sie eine persönliche Auswertung der 200 gelösten Multiple-Choice-Fragen und besprechen diese an einem separaten Kurstag. Anschliessend erhalten Sie noch eine zweite Prüfung, welche Sie selbständig lösen können. Ihre Resultate werden wiederum von uns ausgewertet und Ihnen zugestellt.

Area 1: IT-Revisionsprozess

Area 2: IT-Governance

Area 3: Lebenszyklus-Management für Anwendungen und Infrastruktur

Area 4: IT Service Delivery und Support

Area 5: Schutz von Informationswerten

Area 6: Geschäftskontinuität und Katastrophenvorsorge

Area 1: 10%

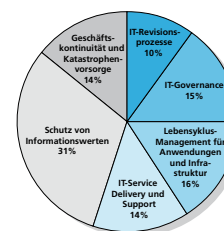
Area 2: 15%

Area 3: 16%

Area 4: 14%

Area 5: 31%

Area 6: 14%



Referenzen

- CISA Task Statements: alle
- CISM Task Statements: –
- COBIT IT-Prozesse: (alle)

Referent

- Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG

Seminargebühren

CHF 3'500.– für ISACA-Mitglieder (alle anderen plus CHF 150.–)

Inkl. 2 auswärtige Übernachtungen

Zertifizierung

Für die Zertifizierung als CISA muss ein Kandidat zusätzlich zur bestandenen CISA-Prüfung fünf Jahre Berufspraxis in den Bereichen Revision, Kontrolle oder Sicherheit von Informationssystemen nachweisen, wobei davon in der Regel maximal drei durch entsprechende Tätigkeiten in der Informatik, der Wirtschaftsprüfung oder durch einen anerkannten Abschluss z.B. an einer Fachhochschule substituiert werden können. Genauere Angaben entnehmen Sie bitte der detaillierten Kursausschreibung.

Prüfungsgebühr

US\$ 375.– bis 555.– (je nach Anmeldezeitpunkt und Mitglieder-Status)

Speziell zu beachten

Dies ist ein 5tägiger Kompaktkurs für erfahrene Kursteilnehmer, welche das gesamte Berufsbild und das CISA Review Manual bereits selbständig durchgearbeitet haben und beherrschen.

A R 5

by Bitterli Consulting
itacs
training

Anmeldeformular:
www.itacs.ch

Avaloq Evolution AG



essential for banking

Die Kernkompetenzen der Avaloq umfassen die Analyse der Anforderungen und Veränderungen der Finanzbranche und die Konzeption und den Bau von High-End-Software. Entsprechend zeigt sich auch die personelle Zusammensetzung des Unternehmens: Die Software-Ingenieure kennen das Bankgeschäft ebenso hervorragend wie die Bankexperten die Informationstechnologie. Aus der Kombination resultiert die ausserordentliche Leistungsfähigkeit des Unternehmens in seinem Kerngeschäft. Um den Fokus auf das Kerngeschäft zu bewahren, überträgt die Avaloq die Durchführung von Implementationsprojekten zertifizierten, in der Avaloq Academy ausgebildeten Partnern. Sie unterstützen den Kunden zusammen mit der Avaloq bei der Inbetriebnahme des Avaloq Banking System. Parametrisierung, Daten-Migration, Schnittstellenbau sowie das Change Management gehören zu den Kernkompetenzen der Implementationspartner. Die Partner der Avaloq, mit zusammen über 140 zertifizierten Beratern, bauen ihre Teams auf hohem Qualitätsniveau weiter aus.

www.avalog.ch

Bitterli Consulting AG



Bitterli Consulting wurde 1996 gegründet, um die wachsende Zahl der Beratungs- und Revisionsmandate der ursprünglichen Einzelfirma vor allem im Ausland optimal bewältigen zu können. Seit Anbeginn unterstützt Bitterli Consulting interne Revisionsabteilungen bei der risikoorientierten Prüfungsplanung und Durchführung von Informatikrevisionen und führt auch eigentliche IT-Revisionsmandate z.B. im Auftrag der externen Revision durch – die Firma hilft auch den internen Informatikabteilungen, sich effizient auf angekündigte Revisionen vorzubereiten. Ein weiterer Schwerpunkt liegt bei der Durchführung von Analysen von Informationssicherheitsmanagementsystemen (ISMS), bei Security Reviews und bei entsprechenden Beratungsmandaten in technisch hochkomplexen Umgebungen. Zahlreiche Unternehmen in der Schweiz und im Ausland bauen heute ihre Tätigkeiten auf Security-Policies und Verfahrensbeschreibungen (z.B. für IT-Governance) auf, welche durch Bitterli Consulting (mit)entwickelt wurden.

www.bitterli-consulting.ch

Referenten

Hinweise zu den Referenten finden Sie direkt auf unserer Webseite.

www.itacs.ch

Compass (Compass Security Network Computing AG)

Compass Security Network Computing AG ist eine auf Security Assessments und forensische Untersuchungen spezialisierte Firma (Aktiengesellschaft) mit Sitz in Rapperswil SG. Im Auftrag des Kunden werden Penetration Tests und Security Reviews durchgeführt, um die IT Sicherheit in Bezug auf Hacking Attacken zu beurteilen als auch geeignete Massnahmen für die Verbesserung des Schutzes aufzuzeigen. Mit forensischen Untersuchungen unterstützt Compass Security die Kunden bei der Beweismittelerhebung und Analyse in Bezug mit Computerdelikte, Phishing, Trojanern oder Urkundenfälschungen. Diese unabhängigen Gutachten von Compass Security werden als Grundlage für eine Schuld- oder Unschuldsvermutung benützt.



Compass Security verfügt über grosse Erfahrung in nationalen aber auch internationalen Projekten. Die enge Zusammenarbeit mit den Fachhochschulen Rapperswil und Luzern ermöglicht es angewandte Forschung zu betreiben, so dass die Sicherheitsspezialisten von Compass immer auf dem neusten Wissensstand sind. Compass ist zu 100% neutral, weder von einem Produkthersteller noch finanziell von Dritten abhängig.

www.csnc.ch

Glenfis AG

Die Glenfis AG ist eine private Aktiengesellschaft und wurde im September 1999 mit Firmensitz in Hünenberg/ZG gegründet. Glenfis ist ein IT Beratungs- und Schulungsunternehmen in der Schweiz und hat die strategische Ausrichtung für IT Service Management nach ITIL, COBIT, ISO20000 und ISO27001. Glenfis hat sich von Beginn an in der Schweiz als "first mover" intensiv mit der ITIL Best Practice Philosophie und Methode sowie der Zertifizierung von Service Management-Organisationen auseinandergesetzt. Getreu nach dem Motto "We walk the Talk" hat sich Glenfis nach ISO20000 ausgerichtet, ist seit Februar 2005 als erstes Unternehmen in der Schweiz zertifiziert und wurde beim vorgeschriebenen Nachaudit im April 2006 erfolgreich bestätigt.



Die derzeit neun Mitarbeiter sind zertifizierte ITIL Service Manager. Ergänzt werden diese Kompetenzen durch eigene ISO20000 und BS7799-zertifizierte Consultants/Auditoren. Als akkreditiertes ITIL-Trainingsunternehmen bei EXIN & itSMF schult Glenfis seit Jahren mit grossem Erfolg ITIL Foundation, Practitioner und ITIL Service Manager.

www.glenfis.ch

Beschreibung

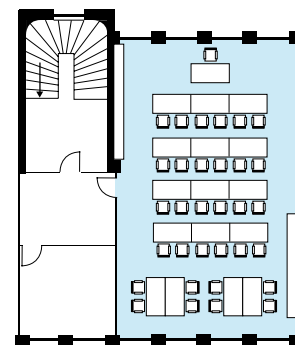
Unser grosszügiger Schulungsraum ist 500 Meter vom Hauptbahnhof Zürich entfernt gelegen und sowohl zu Fuss als auch mit dem Tram in 5 Minuten vom Hauptbahnhof aus zu erreichen. Der Schulungsraum befindet sich im 3. OG in einem ruhigen Bürohaus, gleich neben den Büroräumen der ITACS Training AG. Für Referenten steht ein Parkplatz im Innenhof zur Verfügung und umfangreiches Schulungsmaterial kann mit unserem Materialwagen transportiert werden. Teilnehmern mit langem Anreiseweg können wir mehrere Hotels in nächster Nähe mit gutem Preis-/Leistungsverhältnis empfehlen. Mehrere preiswerte Restaurants in der Umgebung ermöglichen eine abwechslungsreiche Gestaltung der Mittagspausen ohne längere Regiezeiten.

Der Schulungsraum wird für Schulungen mit bis zu 30 Teilnehmern eingesetzt und zeichnet sich durch eine Vielzahl möglicher Möblierungsvarianten aus. Bei Konzertbestuhlung können auch grössere Anlässe mit bis zu 50 Teilnehmern durchgeführt werden.

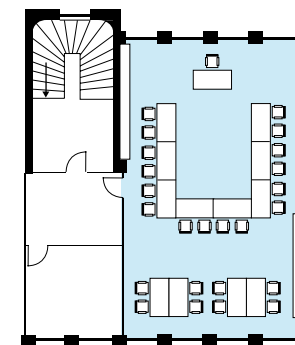
Die Räumlichkeiten können Sie für eigene Veranstaltungen zu folgenden Konditionen mieten:

1 Tag (8.00–18.00 Uhr)	Halbtag (8.00–12.30 Uhr oder 13.30–18.00 Uhr)	Kurz-Anlass (z.B. 16.00–18.00 Uhr)
Schulungsraum ca 90m ² , inkl. 1 Flipchart, 1 Pinwand und Hellraumprojektor, Stereoanlage		
CHF 500.–	CHF 300.–	CHF 200.–
Beamer , mit Auflösung 1400 x 1050, montiert an Decke		
CHF 80.–	CHF 50.–	CHF 30.–
Breitband Internet-Anschluss im Schulungsraum (Kabel oder WLAN)		
CHF 30.–	CHF 20.–	CHF 10.–
Zwischenverpflegung (Getränke, Gebäck, Früchte) pro Person pauschal*		
CHF 15.–*	CHF 8.–*	nach Aufwand
Verpflegung Mittagessen		
nach Aufwand (gemäss Rechnung Restaurant)	nach Aufwand (gemäss Rechnung Restaurant)	–

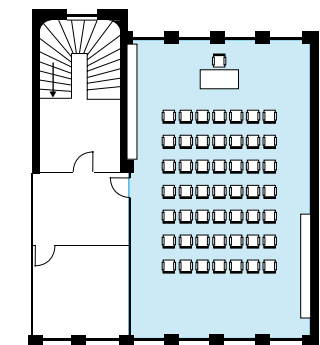
*Spezielle Wünsche nach Vereinbarung
Für mehrtägige Kurse offerieren wir interessante Rabatte.



Bestuhlung Standard,
max. 24 Teilnehmer
mit z.B. zwei Inseln für
Gruppenarbeiten



Bestuhlung U-Form,
12-24 Teilnehmer
mit z.B. zwei Inseln für
Gruppenarbeiten



Bestuhlung für Vortrag/Konzert,
max. 50 Teilnehmer

Kursbeschreibungen

Die Kursbeschreibungen enthalten in der Regel Details zu Kursinhalten, Lernzielen, Zielgruppen, Teilnehmvoraussetzungen, Referenten, Dauer, Preis, abgegebenen Unterlagen und allenfalls zusätzlichen Leistungen wie Computerarbeitsplatz, Hotel-übernachtung usw. Diese veröffentlichten Kursbeschreibungen (inkl. Seminargebühr) können jederzeit ohne besondere Ankündigung geändert werden.

Kurszeiten/Kursort

Wenn nichts anderes angegeben ist, dauern unsere Kurse von 09:15–17:15 Uhr mit einer Mittagspause von 12:15–13:30 Uhr (mit zusätzlichen Kaffeepausen am Vor- und Nachmittag). Unser Schulungszentrum ist vom Hauptbahnhof Zürich aus in 5–8 Gehminuten erreichbar.

Anmeldung

Anmeldungen können per Post, Fax, E-Mail oder Internet erfolgen – entsprechende, kursspezifische Anmeldeformulare finden Sie auf unserer Webseite. Für die mehrmonatigen, berufsbegleitenden Zertifikats-Kurse ist eine schriftliche Anmeldung per Post zwingend. Anmeldungen werden in der Reihenfolge ihres Eintreffens berücksichtigt. Die Kursteilnehmer sind damit einverstanden, dass die Daten der Anmeldung für interne Zwecke elektronisch gespeichert und verarbeitet werden. ITACS Training AG gibt keine derartigen Daten an Dritte weiter.

Anmeldebestätigung und Rechnung

Nach Eingang Ihrer Anmeldung erhalten Sie eine schriftliche Anmeldebestätigung sowie eine Rechnung, welche innert zehn Tagen, spätestens am ersten Kurstag zu entrichten ist. Die Zahlung muss in Schweizer Franken erfolgen. Bitte achten Sie darauf, dass die korrekte Rechnungsadresse auf der Anmeldung angegeben wird.

Im Kurspreis enthaltene Leistungen

Die Seminargebühr hängt ab von zahlreichen Faktoren wie Kursdauer, Art des Kurses, Anzahl gleichzeitig eingesetzter Referenten, usw. Die genauen Leistungen sind der jeweiligen Kursbeschreibung zu entnehmen. Immer im Kurspreis enthalten sind sämtliche Kursunterlagen, die für den Unterricht notwendige Literatur sowie die Pausen- und Mittagsverpflegung an allen Kurstagen. Wo in der Kursbeschreibung separat aufgeführt, sind zusätzliche Leistungen wie die Verwendung von Computern in unseren "hands-on"-Kursen, Zugang zu einer allenfalls vorhanden "Closed User Group" im Internet oder die Übernachtung mit Vollpension im Kurspreis enthalten.

Im Kurspreis nicht enthaltene Leistungen

Reisekosten und nicht in der Ausschreibung aufgeführte Unterkunftskosten gehen zu Lasten des Kursteilnehmers. Bei Kursen mit fakultativen Zertifikaten sind die Prüfungsgebühren im Seminarpreis nicht inbegriffen. Bei einigen Kursen kann zusätzliche Literatur bestellt werden, welche separat bezahlt werden muss.

Teilnahmebestätigungen/Zertifikate

Nach Kursabschluss wird Ihnen eine vom Kursleiter oder Ausbildungsverantwortlichen unterzeichnete Teilnahmebestätigung ausgehändigt, falls Sie an mindestens 80% des Unterrichts teilgenommen haben. Bei einigen Kursen erhalten die Teilnehmer zusätzlich ein international anerkanntes Zertifikat, in der Regel nach Bestehen einer entsprechenden Prüfung und Bezahlung einer separaten Prüfungsgebühr. Die genauen Konditionen sind der jeweiligen Kursbeschreibung zu entnehmen.

Durchführung eines Kurses

In der Regel wird ein Monat vor dem Kurstermin über die Durchführung eines Kurses entschieden. In Ihrem eigenen Interesse melden Sie sich vor diesem Datum an. Spätere Anmeldungen werden berücksichtigt, falls dies aus Zeit- und Platzgründen möglich ist.

Seminarabsage

Die Veranstalter behalten sich vor, ein Seminar wegen Erkrankung der Referenten, ungenügender Teilnehmerzahl oder anderen Gründen abzusagen. In diesem Fall erfolgt eine sofortige schriftliche oder telefonische Benachrichtigung und eine bereits einbezahlte Seminargebühr wird Ihnen ohne Abzüge gutgeschrieben oder ausbezahlt. Weitergehende Ansprüche werden nicht anerkannt.

Mehrwertsteuer

ITACS Training AG ist für sämtliche Dienstleistungen (inkl. Ausbildung) mehrwertsteuerpflichtig. Die Mehrwertsteuer wird auf den Rechnungen für die verschiedenen Kategorien separat gemäss den geltenden Sätzen ausgewiesen (z.B. Kurs 7.6%, Bücher 2.4%, Verpflegung 7.6% und Übernachtung 3.6%) und ist zusätzlich zur Seminargebühr zu entrichten.

Abmeldungen

Die Anmeldung ist verbindlich. Sollten Sie an einer Teilnahme verhindert sein, können Sie sich schriftlich (Brief, Fax) abmelden. Dabei gelten in der Regel die folgenden Konditionen: Bis 15 Arbeitstage vor dem ersten Kurstag kostenlos; 14 bis 5 Arbeitstage vor dem ersten Kurstag werden 50%, später als 5 Arbeitstage vor Kursbeginn oder bei Nichterscheinen sind 100% der gesamten Seminargebühr geschuldet. Gerne akzeptieren wir ohne zusätzliche Kosten einen Ersatzteilnehmer.

Vergünstigungen für Mitglieder des ISACA Switzerland Chapter

Mitglieder des ISACA Switzerland Chapter erhalten bei Nachweis ihrer Mitgliedschaft auf sämtlichen Kursen einen Rabatt, wobei die Seminargebühren mit und ohne Rabatte ausgewiesen werden. In aller Regel lohnt sich eine ISACA-Mitgliedschaft schon aus diesem Grund bereits bei einem Kursbesuch ab 3–5 Kurstagen pro Jahr.

Andere Vergünstigungen

Qualifizierte Fachjournalisten mit Nachweis der entsprechenden Publikationstätigkeit im Themenbereich der Kurse können nach Absprache mit dem Anbieter und bei Vorhandensein von genügend freien Plätzen jeden Kurs zu 50% des nicht-vergünstigten Seminarpreises besuchen.

Urheberrecht

Sämtliche Rechte für die im Kurs abgegebenen oder benutzten Unterlagen, Programme etc. verbleiben beim Inhaber der jeweiligen Rechte (ITACS Training AG, Partnerunternehmen, Referent, Buchautor, etc.). Der Kursteilnehmer verpflichtet sich, nicht gegen die geltenden Bestimmungen und Gesetze bezüglich Urheberrecht und Copyright zu verstossen und die abgegebenen Unterlagen weder vor, während oder nach dem Kurs zu kopieren oder Dritten zu überlassen.

Anwendbares Recht und Gerichtsstand

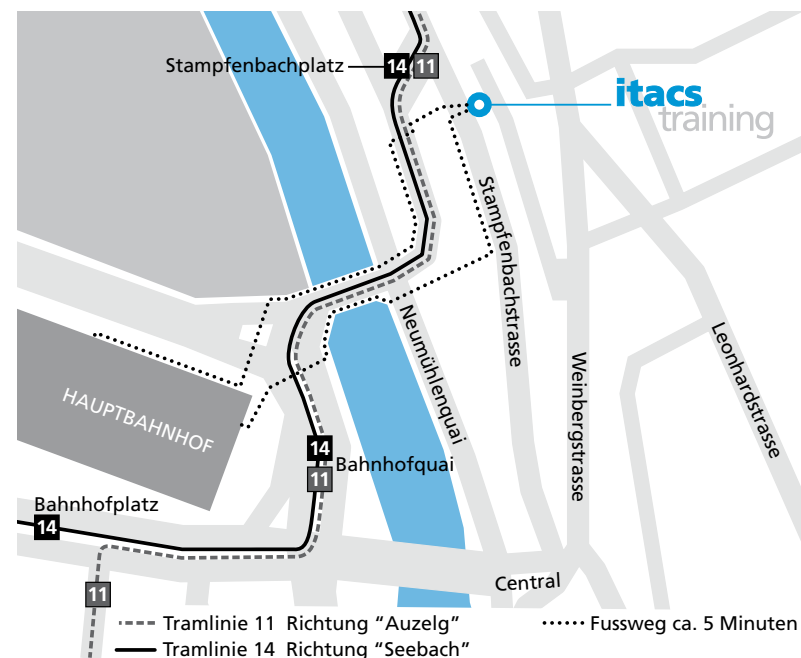
Auf alle Dienstleistungen der ITACS Training AG ist Schweizerisches Recht anwendbar. Als Gerichtsstand gilt **Zürich**.

Informationen zu weiteren Veranstaltungen finden Sie auf unserer Homepage: www.itacs.ch

Eine gedruckte Fassung der Kursübersicht erhalten Sie über unser Kurssekretariat:

ITACS Training AG

Stampfenbachstrasse 40
CH-8006 Zürich
Phone +41 (0)44 444 11 01
Fax +41 (0)44 444 11 02
kurse@itacs.ch



ITACS Kursübersicht 2008|2

© ITACS Training AG

Text und Redaktion: Peter R. Bitterli

Layout und Produktion: Felice Lutz

Druck: Print Production, 8240 Thayngen