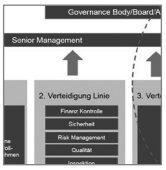
Trust in, and value from, information systems

Switzerland Chapter

Nr. 02 | Juni 2015 | www.isaca.ch

NEWSLETTER



Audit Vorgehen
Die Business-kritische Bedeutung von Cyber-Governance und strukturierten Darstellung der Cyber-Risiken **Seite 77**

Risikomanagement
ISACA Switzerland Chapter bietet eine solide Grundausbildung in Risikomanagement an **Seite 81**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 81**

Audit von Cyber Risiken: Verantwortung der Unternehmensleitung und Herausforderung für den Auditor

Die Audit-Methodik und der Prüfungsumfang müssen laufend den technologischen Veränderungen angepasst und erweitert werden um die effektive Cyber-Sicherheit beim zu prüfenden Unternehmen wirksam beurteilen zu können. Hier kommt die Frage des „Wie", da zurzeit keine Cyber Gesetze oder Regulationen existieren

Von Jiri Cejka und Markus Martinides

Für den Auditor stellt dies eine sehr grosse Herausforderung dar, denn er muss die mit den enormen Veränderungen in der IT Entwicklung verbundenen Cyber-Risiken und Herausforderungen beim Vorgehen im Audit berücksichtigen. Obwohl die Auditing Standards, bspw. ISA 315 (International Standard on Auditing) die Ausgangsschritte für das Vorgehen aufzeigen, muss der Auditor in der Lage sein, die technische Vielfalt der Angriffsmöglichkeiten, die neuen Methoden zur Erkennung der Angriffe, sowie die Verantwortlichen im Unternehmen (Management, Verwaltungsrat) in seinen Audit mit einzubeziehen.

Der sich laufend ausweitende Einsatz des Cloud-Computings hat die Cyber-Risiken massiv verstärkt.

1. Entwicklung in der IT: Geschäftsvorteile und Bedrohungspotential

Die Entwicklungen in der IT haben im letzten Jahrzehnt ein schnelles Tempo erreicht: Mobile-Wireless und Netz-Technologie, Cloud-Computing, vernetzte und virtualisierte Plattformen oder Big-Data Anwendungen. Die Fortschritte ermöglichen strukturierte Veränderungen der IT Umgebung, wie Einführung alternativer Sourcing-Strukturen, Hosting oder Cloud-Computing. Diese Veränderungen haben für die Unternehmen grosse Kostenvorteile gebracht: Sie können ihre Anbindungen an Dritt-Lieferanten und Kunden verbessern. Ein Beispiel dafür ist die Cloud-Lösung, welche wesentliche Kosteneinsparungen gegenüber der Verwaltung der Daten im eigenen Rechenzentrum bietet:

➤ Aus strategischer Sicht ist das Unternehmen effizienter, dynamischer und unabhängiger von Investitionen in die IT.

➤ Aus ökonomischer Sicht werden die globalen operativen Kosten reduziert, die Verfügbarkeit und Kapazität der Daten erhöht und der Einsatz neuer und effektiverer IT-Produkte oder IT-Dienstleistungen ermöglicht.

Folglich fragt das Management «Wie schnell und wie kann vom Cloud-Einsatz profitiert werden?» Der Auditor hingegen wird die Geschäftsleitung mit anderen Fragen adressieren:
➤ Wie ist die strategische Geschäftsausrichtung mit der Informatik synchronisiert?
➤ Wie unterstützt die Informatik das Geschäft?
➤ Basieren die IT-Investment-Entscheide auf Business-Anforderungen?
➤ Bleibt die Verantwortung für die Daten innerhalb der Firma, auch wenn sie von der Sicherheit externer Systeme abhängig ist?

Verändertes Geschäftsumfeld generiert neues Bedrohungspotential
Der Drang nach Geschäftsvorteilen aus der Entwicklung neuer Informatik- und Telekommunikationstechnologien ist gross, kann jedoch auch erhebliche Risiken und Governance-Herausforderungen mit sich bringen.

Zwar bringen diese Technologien viele Annehmlichkeiten bei der täglichen Arbeit mit der Informatik, gleichzeitig aber eröffnen sie Hackern, Betrügern und Virenprogrammierern unzählige Möglichkeiten um Computersysteme anzugreifen und – für den Benutzer nicht erkennbar – dabei die Vollkontrolle des Computers zu übernehmen. Für das Unternehmen entsteht eine neue Bedrohung - die Cyber-Kriminalität.

Cyber-Kriminalität – die globale Bedrohung
Bei Cyber-Attacken können Kriminelle bestehende Schutzmassnahmen häufig einfach umgehen. Die existierenden Sicherheitsmassnahmen bspw. die Absicherung der logischen Schichten durch Firewalls genügen nicht mehr, um solche Angriffe mit Erfolg abzuwenden. Durch die weltweite Vernetzung unzähliger Informatik-Systeme über das Internet haben Angreifer innerhalb Sekundenbruchteilen Zugriff auf alle am Internet angeschlossenen Systeme. Dabei können unsere traditionellen Rechtssysteme praktisch beliebig umgangen werden. Als Reaktion haben bereits 44 Staaten die Konvention über Cyber-Kriminalität ratifiziert, 9 Staaten haben sie unterzeichnet.

Situation in der Schweiz
«Eines der grössten Probleme im Zusammenhang mit der Nutzung des Internets ist heute die Datensicherheit», erklärt Markus Martinides, Cyber-Experte von der im Bereich Sicherheitsanalysen spezialisierten Firma SUA Telenet GmbH. «Insbesondere für Firmen, die über vertrauliche Daten verfügen, aber auch für Private ist es wichtig, kontrollieren zu können, wer auf interne Daten zugreift und ob diese unerlaubt verändert oder sogar gelöscht werden.» Aus diesem Grund sind in der Schweiz nicht nur die grossen Institutionen wie Versicherungen, Banken oder Industrieunternehmen sondern auch KMU Betriebe wie Arztpraxen und Anwaltskanzleien ebenso wie Spitäler, Gemeinden und Kantone bedroht.

Die gängigen Firewalls bieten dabei immer weniger Schutz. Denn sogenannte Zombies (Codes, die sich via Internet auf dem System installieren und dann Daten vom System nach aussen schicken), können sich oft völlig unbemerkt installieren und bleiben von Antivirenprogrammen und Firewalls vollkommen unerkannt. «Oftmals sind solche Programme lange Zeit aktiv und spionieren das Netzwerk aus, bevor sie bemerkt werden», so Markus Martinides. Tür und Tor werden Viren und Hackern beispielsweise durch die Verwendung von nicht überprüfter USB-Sticks geöffnet. Ein weiteres Problem ist, dass immer mehr Angriffe über sehr komplexe Technologien wie Javascripts laufen die verstärkt im Bereich der Internet-Browser zum Einsatz gelangen.

2. Cyber-Governance ist Management Aufgabe

«Cyber-Kriminalität wächst und ist auf dem 4.Platz aller kriminellen Taten. Cyber-Kriminalität ist nicht das Technologie Problem, es ist das Business- und das Strategie-Problem». Quelle: PWC 2014 Crime-Survey

Die Verantwortung für die Daten des Unternehmens liegt beim Management. Dem Verwaltungsrat sollten die Cyber-Risiken deshalb bewusst sein. Folgende Corporate Governance Prinzipien können helfen, die Cyber-Risiken aktiv zu managen.

Prinzipien für Corporate Governance
➤ Der Verwaltungsrat soll das Vorgehen bei Cyber-Sicherheit als unternehmensweites Risk-Management positionieren, nicht nur als IT-Risiko.
➤ Der Verwaltungsrat soll die juristischen Konsequenzen der Cyber-Risiken verstehen, da sie sich auf unternehmens-spezifische Umstände beziehen.
➤ Der Verwaltungsrat soll Zugriff zur Cyber-Sicherheit Expertise haben und die Diskussionen über Cyber-Risiko-Management sollten ausreichend Zeit auf seiner Agenda einnehmen.
➤ Der Verwaltungsrat erlässt eine Richtlinie an das Management, dass ein unternehmensweites Cyber-Risiko-Management-Framework aufgebaut und mit genügend Personal und Budget unterstützt wird.
➤ Cyber-Risiken können nicht einfach durch Abschluss einer Daten-Verlustversicherung gelöst werden.
➤ Die Diskussion zwischen VR und Management sollte die Identifikation der tatsächlichen Cyber-Risiken und deren effektiven Abwehr durch organisatorische und technische Massnahmen beinhalten.

Audit Fragen an Verwaltungsräte
Der Auditor soll die Unternehmensleitung und den Verwaltungsrat aktiv unterstützen, das Risikobewusstsein gegenüber Cyber Attacken zu schärfen und konkret zu formulieren. Folgende Fragen des Auditors an den Verwaltungsrat können dabei eine Hilfe sein:
➤ Wendet das Unternehmen ein Sicherheitsframework an?
➤ Welche sind die Top fünf Risiken im Unternehmen, welche auf Cyber-Sicherheit bezogen sind?
➤ Ist bei dem Mitarbeiter ein Bewusstsein in Bezug auf Cyber-Sicherheit vorhanden?
➤ Wurden bei der Planung des Cyber-Sicherheit Programms externe und interne Bedrohungen beachtet?
➤ Wie ist die Sicherheits-Governance innerhalb des Unternehmens geregelt?
➤ Gibt es einen konkreten Notfallplan im Falle einer Cyber-Attacke?

3. Darstellung von Cyber-Risiken und Vorgehen im Audit

Die Cyber-Kriminalität «profitiert» von den, durch IT-Fortschritt erzeugten, neuen Risiko Quellen, welche vor allem mit dem Cloud-Computing Einsatz, mit Konzepten

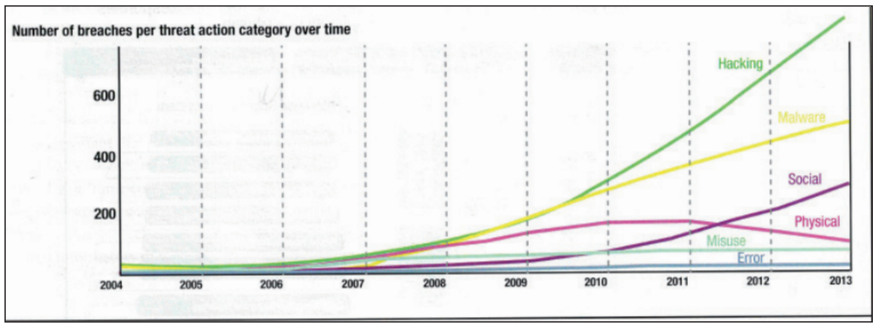


Bild 1: Zunehmende Anzahl der Hacker Angriffe
(Quelle: Verizon 2014 Data Breach Investigation Report)

wie «Bring-Your-Own-Device» (BYOD) mobilen Geräten und Applikationen sowie mit der Auslagerung der für Business kritischen IT-Bereichen, entstanden sind. Die neuen Risiko Quellen haben die Cyber-Angriffsflächen vergrössert.

Die Risiken der Cyber-Kriminalität sind: i) Datenverlust, ii) Bedrohungen im Datenschutz-Bereich, iii) Verlust der Kontrolle über Zugriff auf die Daten iv) Verlust der Verfügbarkeit der Daten im Betrieb. Die Folgen der Cyber-Attacke können dem Unternehmen weitreichenden Schaden zufügen wie bspw. Verlust der Wettbewerbsfähigkeit, Kosten, Reputationsschaden oder Compliance-Probleme.

Die Cyber-Bedrohung wird kritisch, da die Hacker sich auf den Missbrauch sensitiver oder finanziell wertvoller Information oder auf die Störung der wichtigen operativen Bereiche fokussieren. Dabei ist der Anstieg von Attacken drastisch, da die Hacker-Bedrohungen und Sicherheits-Einbrüche nicht nur in der Anzahl exponentiell wachsen (Bild 1), sondern ihre Methoden kontinuierlich weiterentwickelt und ausgeklügelter konstruiert werden.

In vielen Fällen werden Hacker-Attacken viel zu spät erkannt. Sehr viele Daten des Unternehmens können in dieser Zeit unbemerkt ausgeforscht, verändert und gelöscht werden. Viele Angreifer erstellen einen versteckten Remote-Zugang, der es ermöglicht Informationen erst bei «Bedarf» als bezahlte Dienstleistung gegenüber Ihren Auftraggebern bereitzustellen.

Themen & Aufgaben im Cyber Audit

Der Audit der Cyber-Risiken erweitert sich um spezifische Themen in den Bereichen i) IT Governance und Assurance, ii) IT Sicherheitsstrategie inkl. Richtlinien und Vorgaben, iii) Implementierungen iv) Projekt Risk-Management.

Zu den Aufgaben des Auditors gehören die Beurteilung der Cyber-Bedrohungen und Risiken, der Kontrollprozesse inkl. ihrer Maturität sowie der Kommunikation mit Verwaltungsrat, Management, Geschäfts und IT Verantwortlichen. Essentiell ist weiter auch ein Verständnis über interne Kontrollen, wie das Unternehmen auf die durch die IT initiierten Risiken reagiert.

Cyber relevante IT-Umgebung und Cyber Sicherheits-Framework

Der Auditor verschafft sich eine Übersicht im Unternehmen betreffend IT-Organisation, Compliance Regeln, IT-Infrastruktur und den assoziierten Risiken. Weiter geht es darum wie IT-Prozesse und Applikation gemanagt werden und welche Dienstleistungen an Drittfirmen ausgelagert sind. Dabei muss er in seinem Bericht die Risiken nachweisen und beurteilen können.

Für den Aufbau der Cyber-Sicherheit ist es wichtig, das Gesamtbild in einem Framework darzustellen, welches die aktuelle Situation und Ausblick umfasst, damit das Vorgehen beim Audit mit dem Kunden festgelegt werden kann. Das Cybersecurity Framework NIST (National Institute of Standards and Technology, Feb 2014) hilft dem Auditor die Situation abgestimmt und transparent in Quervergleichen beurteilen zu können. Dieses Framework besteht aus den drei Bereichen Basis Framework, Implementierung in Schichten und Framework Profilen.

Das **Basis Framework** -beinhaltet Funktionen, Aktivitäten, Resultate und Referenzen, welche die Priorisierung der Cyber Sicherheit relevanten Entscheide ermöglichen. In diesem Basis Framework wird der Aufbau der Cyber Sicherheit als ein kontinuierlicher Prozess mit fünf Funktionen definiert: Identifikation, Schutz, Detektieren, Reagieren und Recovery.

Die **Implementierung in Schichten** beinhaltet vorhandene Cyber-Sicherheit Messwerte, mit welchen die Tiefe der erfüllten Vorgaben der Sicherheitsprozesse (Maturität) beurteilt werden kann. Dabei wird unterschieden zwischen ‚partiell', ‚Risiko informativ' und ‚wiederholbar'.

Mit den **Framework Profilen** wird die Beurteilung der existierenden Position (Ist Zustand) sowie die Definition der zu erreichenden Ziele der Cyber-Sicherheit formuliert.

Entlang dieses Frameworks kann das Cyber-Security-Program mit den nachfolgenden sechs Schritten erfasst und formuliert werden:

1. Priorisierung und Festlegung des Umfangs (Business Ziele, organisatorisches Umfeld, Umfangs des Cyber-Security-Programms).
2. Positionierung und Identifizierung der Systeme, Anforderungen, Risiko-Ansatz, Schwachstellen und Bedrohung.
3. Das Erstellen des Profils der aktuellen Situation sowie Bestimmen der Maturität der bestehenden Prozesse.
4. Risk-Assessments: Durchführung der Risiko-Impact-Analyse, Bewertung der Ereignis-Eintritts-Wahrscheinlichkeit und die Bestimmung der Risiko-Eskalation.
5. Das Erstellen des Ziel-Profils: Festlegung der geforderten Ziele unter Berücksichtigung der Business-Strategie
6. IST-SOLL Analyse und Priorisierung der Verbesserungs-Schritte.

Die Bedeutung des «Three Lines of Defense Model»

Im Kontext eines Audits zu Cyber-Security liegt eine grosse Bedeutung auf dem

Bild 2: Die 5 Funktionen im Basis Framework

Three Lines of Defense Models (IAA: The Institute of Internal Auditors). Das Externe und Interne Audit rapportiert das Assessment und die erstellten IST- und SOLL-Profile des Cyber-Security-Programms direkt an den Verwaltungsrat und das Management um entsprechende Risiken dort zu adressieren. Damit soll sichergestellt werden, dass Cyber-Risiken in der Unternehmensleitung bekannt sind und das Management die Verantwortung übernimmt.

Auditors Fokus und Vorbereitung

Der Auditor soll sich bei seinem Audit auf drei Themen fokussieren: Zuerst eine Priorisierung auf Bereichen, bei denen die Cyber-Bedrohung besonders relevant ist: Cloud Computing, Mobile Applikationen, Sozial-Engineering und Soziale Netze, Angestellte und externe Firmen Berater. Die zweite Voraussetzung für ein effizientes Audit Vorgehen ist die Erweiterung eigener Kenntnisse der neuen Methoden, welche vor allem bei der Analyse von grossen Datenmengen hilfreich sind, sowie die Monitoring und Logging Techniken, mit welchen die Spuren der Cyber-Attacke erkannt werden können.

Das letzte Fokus-Thema ist die Entwicklung der Fähigkeit der Erkennung des Cyber-Betrugs im Geschäftsumfeld sowie am Arbeitsplatz.

Die Vorbereitung auf den Cyber-Sicherheits-Audit sollte Fragen beinhalten, welche sich auf die Benutzung der Mobile-und/oder Internet in geschäftskritischen Prozessen sowie auf die Verarbeitung und Speicherung der geschäftskritischen Daten konzentrieren. Weiterhin sollten die Bereiche der Überwachung und Aufzeichnung der Transaktionen und der Daten angefragt werden. Wichtige Fragenthemen sind auch das Change Management, Implementierung neuer Funktionen sowie die Qualität der Sicherheitsmassnahmen in der Organisation.

Cyber-Audit-Programm

Im Cyber-Audit-Programm werden zehn typische Bereiche für den Plan des Auditors aufgeführt:

➤ Planung und Umfangsabschätzung des Audits – was gehört zum Audit und was ist ausgeschlossen?

➤ Kenntnisse und Verständnis der vorhandenen IT-Architektur. Sind diese bekannt?

➤ Governance - Wie sollte die Governance für die Cyber-Kriminalität strukturiert werden?

➤ Organisation - Wie ist VR & Management bei Cyber-Themen involviert und in welcher Rolle?

➤ Richtlinien und Verordnungen – welche sind spezifiziert und werden diese in der Praxis angewendet?

➤ Geschäftsunterstützende Rolle in Cyber-Verbrechen Prävention – wie ist die Business-Gruppe in der Prävention von der Cyber-Kriminalität involviert?

➤ IT Management – welches Know-How ist vorhanden und welche Massnahmen sind implementiert?

➤ Störfallmanagement Richtlinien und Prozesse – welche sind vorhanden und wurden getestet?

➤ Störfallmanagement Implementierung – welche Schutzmassnahmen sind eingeführt?

➤ Krisenmanagement - wenn eine Cyber-Attacke passiert, wie ist die Organisation auf die Krisen Situation vorbereitet?

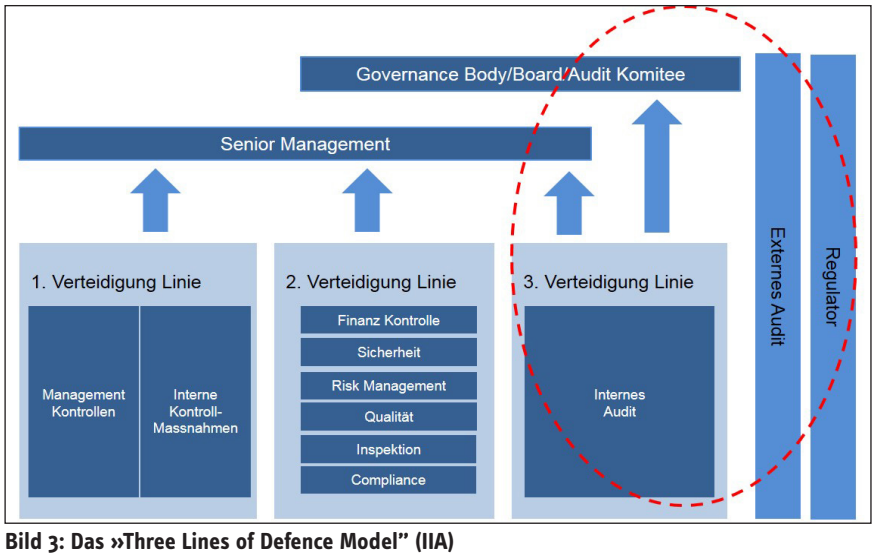


Bild 3: Das »Three Lines of Defence Model" (IIA)

Zusammenfassung: Wichtige Schlüsse für den Audit der Cyber-Risiken:

➤ Cyber-Governance hat Business-kritische Bedeutung. Das Management muss wissen, wo die Risiken liegen.

➤ Jede Organisation kann von Cyber-Attacken betroffen werden.

➤ Cyber-Sicherheit kann in der Organisation mit Hilfe des Frameworks aufgebaut werden.

➤ Auditors Fokus soll Kenntnis neuer Methoden und Erkennung der Cyber-Risiken im Geschäftsumfeld beinhalten.

➤ Vorbereitung für Cyber-Audit besteht aus Fragen/Programm zu neuer Technologie und geschäftskritischen Daten.

Weitere Informationen

Der vollständige Artikel, das Literaturverzeichnis inkl. des Beispiels des Cyber Audits beim Cloud Einsatz kann hier heruntergeladen werden: www.acons.ch und www.sua-tele.net.

DIE AUTOREN

Jiri Cejka, Senior Manager, Acons Governance & Audit AG
Dipl. El.-Ing, Fach technische Kybernetik, CISA, Quality Auditor ISO 9000
jiri.cejka@acons.ch
www.acons.ch

Bereiche & Kompetenzen: GRC, BCM, IT & Cyber Sicherheit, IT Risikomanagement, Programm Management
Jiri Cejka prüft bei ISACA HQ weltweit das Lernprogramm «IS Audit and Control» für Universitäten. Er war langjähriger Entwickler der Börsen-Systeme, tätig im IT Audit der KPMG sowie Leiter IT Audit OC Oerlikon.

Markus Martinides,
CEO SUA Telenet GmbH
Studium: ETH Zürich Nachrichten- und Informationstechnologien (1986)
info@sua-tele.net
www.sua-tele.net /
www.sec-check.net

Bereiche & Kompetenzen: Informatik, Mobil-, Richtfunk-, Daten- und Sprachkommunikation, IT-Sicherheit, Projektmanagement, Betriebssysteme, Cloud Architektur.
Mitglied ISACA, Information Security Society Switzerland (ISSS) und Dozent UZH MedLAW

Informationen des Verbands

Risikomanagement – (auch) für Cyber Risk unabdingbar

Der vorangehende Artikel von Jiri Cejka zum Audit von Cyber-Risiken zeigt sehr gut auf, mit welchen Fragestellungen sich nicht nur der Revisor sondern auch der eigentlich für dieses Thema zuständige Risikomanager beschäftigen muss. Neben der Analyse der Entwicklungen innerhalb des Unternehmens selbst (z.B. Geschäftsstrategie oder Sourcing-Strategie), den Veränderungen im Markt (neue Gesetze und regulatorischen Anforderungen, veränderte Konkurrenzsituation, Devisenkursentwicklung usw.) sind auch die spezifischen Risiken in den jeweiligen Fachbereichen zu identifizieren, zu bewerten, wo sinnvoll zu vermindern und ganz grundsätzlich zu überwachen. Dabei darf man Spezialrisiken wie die Cyber-Risiken weder überbewerten noch vernachlässigen.

Was wir für so einen »Job" benötigen, sind umfassend ausgebildete Risikomanager, wie sie zum Beispiel im CRISC-Berufsbild von ISACA vorgestellt werden. Gemäss CRISC muss ein Risikomanager insgesamt 39 verschiedene Aufgaben in fünf übergeordneten Themen¬bereichen abdecken: Von der Identifikation, Einschätzung und Bewertung von Risiken bis zu deren Management und Überwachung. Ein Schwerpunkt im CRISC-Berufsbild ist aber auch die Informationstechnologie (IT), wo spezifische IT-Massnahmen entworfen und implementiert werden müssen.

Das ISACA Switzerland Chapter bietet eine solide Grundausbildung zum CRISC an. Jeweils ab Februar bis anfangs Juni bereitet sich die Teilnehmer zuerst mit einem strukturierten Selbststudium vor. Im Sommer (Juni/Juli) findet dann der eigentliche Präsenzunterricht in Zürich statt. Mit einem separaten Prüfungstraining im Spätherbst wird dann die Vorbereitung auf die internationale Zertifikatsprüfung anfangs Dezember (insgesamt 13 Kurstage) abgeschlossen.

Der durch ITACS Training AG im Auftrag des ISACA Switzerland Chapter durchgeführte Kurs vermittelt und vertieft theoretisches wie praktisches Fachwissen im breiten Feld von Risikomanagement und internen Kontrollen, bereitet aber auch intensiv auf die von ISACA organisierte CRISC-Prüfung vor.

WEITERE INFORMATIONEN

Weitere Details zum CRISC-Zertifikat und zur entsprechenden Ausbildung finden Sie auf www.isaca.ch

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
15.06.2015	CISA-VK	CISA Zertifikatskurs 2015
15.06.2015	CISM-VK	CISM Zertifikatskurs 2015
15.06.2015	CGEIT-VK	CGEIT Zertifikatskurs 2015
15.06.2015	CRISC-VK	CRISC Zertifikatskurs 2015
01.10.2015	CGEIT-PV2	CGEIT Prüfungsvorbereitung 2015
08.10.2015	CRISC-PV2	CRISC Prüfungsvorbereitung 2015
www.isaca.ch		
15. - 17.6.2015	P-COF3	COBIT 5 Foundation
22. - 24.6.2015	P-COI3	COBIT 5 Implementation
27.7. - 29.7.2015	P-COF3	COBIT 5 Foundation
www.glenfis.ch		

IMPRESSUM ISACA NEWS

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Sekretariat ISACA c/o BDO AG, Biberiststrasse 16, 4501 Solothurn
Erscheinungsweise: 4x jährlich in Swiss IT Magazine
Mitgliedschaft: Wir begrüssen alle, die Interesse an Audit, Governance und Sicherheit von Informationssystemen haben. Es ist nicht notwendig, dass Sie Sicherheitsspezialist oder Revisor sind, um bei uns Mitglied zu werden. Weitere Informationen finden Sie unter www.isaca.ch

Copyright: © Switzerland Chapter der ISACA