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

Nr. 03 | September 2014 | www.isaca.ch
NEWSLETTER

Sicherheitsmanagement
In einem Unternehmen gibt es zahlreiche Sicherheitsmanagement-fragen. **Seite 69**

Ausbildung Sicherheit
Das CISM-Zertifikat der ISACA vermittelt ein umfassendes und breites Fachwissen im Bereich der Sicherheit. **Seite 73**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 73**

99% SICHERHEIT = (MENSCH + PROZESSE + TECHNOLOGIE) + RISK-MANAGEMENT

Der Titel dieses Artikels will aussagen, dass es die 100% Sicherheit nicht gibt – der Rest ist reines Risk-Management und nicht Technologie.

Von Fridel Rickenbacher

Diverse Ansätze / Methoden / Compliance Anforderungen / Regulatoren / Zertifizierungen wie z.B. Business Recovery System (BRS), Contingency Plan, CISA, CISM, ISO 22301/BCMS, IKS oder Prozesse nach CobIT, ITIL, ISACA, ISO, IEC27001 ISMS, IEC17799, SOX, IT GSHB, DSG, VDSG können schon sehr viele generische Risiken und Gegenmassnahmen abdecken.

Jedoch sind diese eben «nur generisch» und müssen daher massgeschneidert an die Firmen-ICT-Prozesslandschaft angewandt und an die ICT-Teilziele (z.B. mittels ICT-Governance) der Firmen-Gesamt-Strategie angelehnt werden.

Es bleiben immer Rest-Risiken übrig, welche im Risk-Management verwaltet werden müssen – und dies auf Ebene der Führung oder Verwaltungsrat.

Innerhalb des Risk-Management-Systems / ICT-Governance geht es um einen laufenden Loop von «Erkennung», «Bewertung und Klassifizierung», «Managen» und «Überwachung und Kommunikation».

Ich neige bei vielen Controlling-Systemen und Audits zu sagen: «Es ist vieles abdeckbar mit den Akteuren Menschen, Prozessen, ICT-Technologien und vor allem Baseline / Tests / Monitoring. Die anderen Rest-Risiken gehören ins Risk-Management und haben nicht mehr ausschliesslich etwas mit ICT-Technologie zu tun. Sicherheit ist keine reine Technologie-Frage, sondern eine Kombination von wiederkehrenden Gesamt-Audit-Prozessen».

DatenSCHUTZ in der DatenFLUT?

Ein kleines Rinnsal und dessen bescheidener Wasserfluss mit Sicht auf den Grund zu überwachen, ist einfacher als ein grosser Fluss mit einem reissenden, dynamischen Wasserstrom ohne Sicht auf den Grund…

Diese einfache Analogie zeigt das zunehmende Problem auf in diesem Sicherheits-Bereich im Zeitalter der hochdynamischen Entwicklung in z.B. Cloud, Big Data, Internet der Dinge und letztlich der fortschreitenden digitalen Transformationsprozessen.

Die digitale Transformation und Wandlungsdruck der Informationsgesellschaft hat interdisziplinäre Auswirkungen – auch im Sicherheits-Bereich

Die Bedürfnisse und dessen Auswirkungen der Informationsgesellschaft betreffen mittlerweile globale Prozesse, Technologien und lassen sich nicht mehr isoliert betrachten und abdecken. Es braucht zunehmend interdisziplinäre Zusammenarbeiten von Akteuren von z.B. Gesell-

schaft, Politik, Technologie, Wirtschaft, Wissenschaft, Ausbildung und auch Spezialthemen wie auch Psychologie oder Management-Ansätze, damit dieses entstehende Next Generation Informationsuniversum an Mensch und Maschine mehr Nutzen als Schaden mit sich bringt und so gut es geht auch beherrschbar bleibt.

Der entsprechende «Wandlungsdruck der Informatik» oder «Transformation» in ein neues Informations-Zeitalter - mit jeweilig an die Firmenstrategie orientierte ICT-Strategie - hält schon länger an. Auch hier ist die Führungsebene in der unveränderten Pflicht, den Informatik-Bereich in dieser Transformation zu begleiten. ICT (und auch die ICT-Sicherheit) wird vielfach leider immer noch als reiner Kostenfaktor und leider nicht als strategischer, innovationstreibender Vorteil gegenüber Mitbewerbern betrachtet.

The new Economy versprach und vernichtete vieles... Wertschöpfung durch «sichere» ICT

Vor zirka 15 Jahren versprachen viele Berater, Firmen, Leadership-Methoden ein ungeahntes Potential in den Bereichen Internet, E-Business etc. und viele Firmen, Organisationen, Technologien wuchsen ins Unermessliche an, ohne auch z.B. die Prozesse, Sicherheit, Risiken und nötigen Organisationsanpassungen zu prüfen und anzupassen.

Die DOT.COM-Blase platzte entsprechend und auch die ICT-Industrie litt stark als zusätzlich dadurch belasteter «reiner Kostenfaktor und Wertvernichter».

Damit die ICT zunehmend entscheidend die Wertschöpfung und Effizienzsteigerung / Business-Support unterstützen kann, braucht es zunehmend abgesicherte / überwachte Prozesse aufgrund der zunehmend business-kritischen ICT.

Ein Teil des Internet – Internet ein Teil von uns - Big Brother is watching us in our «smart» homes

Mit der fortschreitenden Entwicklung von Internet- / Cloud-Lösungen und wachsender Mobilität mittels z.B. Smartphones, Notebooks, entgrenzter HomeOffice-Arbeit schwindet die Grenze zwischen Privat und Business zunehmend – und dadurch auch die Gesamt-Sicherheit.

Weitere Entwicklungen im Bereich der Heimvernetzung und letztlich «Internet der Dinge» werden dazu beitragen, dass wir nicht mehr nur ein Teil des Internets sind, sondern das Internet ein Teil von uns wird. Dass dann hierbei Unmengen Informationen in alle Richtungen fliessen, werden im gesamten Haushalt / Haustechnik / HomeOffice-Firmen-EDV / Privat-EDV weitere Fragen und Herausforderungen der beherrschbaren Sicherheit aufwerfen.

Globale Internet-Industriegiganten wie z.B. CISCO, Google, Microsoft, Amazon, Siemens sind aufgrund deren dominanten Verbreitung im Internet und wachsenden totalen Vernetzung, auf Internet-Kern-Infrastruktur-Bereichen und dem künftigen «Internet der Dinge» letztlich überall «allzu sehr heimisch» in unseren Haushalten, Firmen und Netzwerken – und mit dem irgendwo hinterlegten «Master-Passepartout-Datenschlüssel» ausgestattet sehr «nah». Oder werden diese gar mal genötigt, regulatorisch vorgegebene Staats-Trojaner zu «akzeptieren» oder «mit zu implementieren» (?)

Hoffen wir, dass künftig Hacker oder schadhafter Programm-Code nicht «via Kühlschrank» zu uns kommen ... oder uns ein- oder raus-sperren via Türen-Management-System.

Unsere «connected smart homes» mögen zwar irgendwann smart sein... aber auch wirklich sicher?

Der Schutz der digitalen Identität im 21. Jahrhundert - ein «multifaktorieller» Widerspruch?

Ein Megatrend des plattformübergreifenden «Single Sign On (SSO) / Anmeldung mit nur einer Anmeldung» im Zuge der standort- und geräte-unabhängigen Zugangsmöglichkeiten auf z.B. Cloud, Social Media, Apps, Firma, Kreditkarte eröffnet völlig neue Konform-Stufen bei aber auch unschwer zu erkennenden, komplexeren Sicherheits-Gefahren.

Eine sehr grosse Herausforderung wird der künftige Schutz genau dieses zentralen Einstiegspunktes sein, der ja auch irgendwann mal nebst z.B. dem reinen Datenzugang auch weitergehende sehr personensensitive Informationen wie z.B. Bankzugänge, Gesundheitsinformationen, Familie, Kinder «schützen» wird (hoffentlich).

Dass hier vor allem in den Bereichen wie Social Media (Facebook, Twitter etc.) und Email dermassen viele personensensitive Daten sehr fahrlässig öffentlich verteilt werden, erschwert auch hier den Spagat zwischen Fahrlässigkeit und Sicherheitsanforderung. Leider ist der «gläserne» Mensch im Internet nicht schwer sichtbar, nur weil er aus Glas ist... im Gegenteil: er macht sich meist selbstverschuldet selber «extrem gläsern» und sichtbar...

Den Bedrohungen des 21. Jahrhunderts ist die Authentifizierung per einfacher oder auch zweifacher Anmeldung nicht mehr gewachsen. Eine neue Generation - von gar bewusst system-verteilten und voneinander unabhängigen, nicht konzentriert angreifbaren – (Cloud)-Anmeldelösungen mit dynamischer Multifaktor-Authentifizierung und Autorisierung ist unumgänglich. Diese können dann noch mehrstufig verstärkt werden mit z.B. kontextbasierten Verhaltensmustern, Standortbezug und Echtzeit-Token an persönliche Devices.

Sicherheitsoptimierung durch (Hybrid)Cloud oder Big Data?

Im Zuge der aktuellen Erkenntnisse rund um die verschiedenen Nachrichtendienste und deren grenzenlosen Datenzugangs-Möglichkeiten und dem offenbaren Trend von «jeder bespitzelt jeden» stellen sich einige Grundsatzfragen.

Eine Private Cloud ist schon längstens nicht mehr «privat» – sei es durch Schwachstellen in den Bereichen Prozess, Technologie oder vor allem des Menschen.

Wäre aus diesem Aspekt dann die Auslagerung von einzelnen ICT-Themen in die Public Cloud / Hybrid Cloud «sicherer» und «beherrschbarer», wenn nur schon mal einer der Haupt-Sicherheits-Risiko-Faktoren «Mensch» und lokale Prozesse ausgelagert sind?

Ein gezielter Sicherheits-Schwachstellen-Angriff auf eine Firmen-ICT-Infrastruktur (inkl. auch physisch vor Ort oder per Social Engineering / Trojaner / Malware etc.) ist natürlich viel einfacher als ein eher ungezielter Angriff auf eine Public Cloud oder «Mega Cloud». Die Analogie bei der «Mega Cloud» zur mühsamen und eher unendlichen Suche nach der bekannten Nadel (Firmendaten) im dann aber SEHR grossen Heuhaufen (Cloud) ist hier mehr als angebracht.

Und leider müssen hier noch weitere Fakten (oder alte Paradigmen) adressiert werden:

- Der Datenstandort wird zunehmend irrelevant für die künftigen immer globaler werdenden Sicherheitsfragen.
- Zunehmend lassen CH-Firmen sicherheits-relevante Systeme von externen oder gar ausländischen Serviceorganisationen betreiben – inkl. auch grenzüberschreitendem Informationsaustausch.
- Ein «sicherer» Weg kann also auch – trotz allen anderslautenden Meldungen – gerade darum eine gut orchestrierte Kombination von (Hybrid)Cloud-Lösungen und Managed Services sein. Hier könnte der Ansatz «the very best out of all Clouds» ein gangbarer Weg sein, wenn diese mittels den nötigen Prozessen, Technologien, Mitarbeiter und Risk-Management / ICT-Governance gestützt werden von der Führungsebene und letztlich der Firmen- / ICT-Strategie.

Kontrollen über Kontrollen = Bestandteil der unabhängigen Qualitätssicherung, aber auch echte Sicherheit?

Seit Jahren entstanden immer mehr ICT-Kontroll-Methoden oder regulatorische Vorgaben.

Bei vielen Firmen in der Schweiz wurden vielfach seitens der Treuhänder, Revisions-Stellen, Auditoren oder des eigenen Verwaltungsrates interne Kontrollsysteme (IKS) aufgebaut und eingeführt.

Viele dieser Kontrollsysteme bedienen sich an generischen und aber zum Glück auch an spezialisierteren Fragestellungen rund um ICT-Prozesse und ICT-Risk Management. Firmenvitale Prüfpunkte rund um z.B. ICT-Gesamt-Sicherheit, Datensicherheit, Datensicherungs-Prozesse, Social Engineering, Mensch als Sicherheits-Faktor 1, KnowHow-Transfer, Mitarbeiter-Eintritt / Mitarbeiter-Austritt, ICT Security Policies, Internet-Nutzungs-Richtlinien, Datenklassifizierungen etc. wurden mehr oder minder darin abgedeckt, aber dann vielfach «einfach abgehakt».

Gut orchestrierte Theorie- und Praxis-Anwendung schafft echter Mehrnutzen

Aus eigener jahrelanger Beobachtung, Anwendung und Beratung in solchen ICT-Audits oder Zweitmeinungs-Abgaben erhärtete sich der Eindruck und Fakt, dass viele dieser Kontrollsysteme in kritischen Bereichen die Tiefe und nötige Tragweite nicht erreichen.

Die besten Expertisen und Audits sind immer solche, die Theorie (Methoden, Standards, Prozesse) und Praxis (Systemtechnik, Systemengineering, Automatisierung) auf der Basis von z.B. «Best Practices» oder selber angewandten Prozessen abdecken.

Ein echter Mehrnutzen – und nicht nur eben das «Abhaken» von nur theoretischen Kontroll-Listen – kann entstehen, wenn der ICT-Auditor gemeinsam mit den Systemverantwortlichen echte Schwachpunkte und Verbesserungs-Potentiale analysiert, testet und dann effektiv auch einführt. Hierzu gilt es, sämtliche Hands-On-Praxis und besten Erfahrungen von anderen Kunden, der eigenen Infrastruktur-Umgebung und von allen taktisch gut ausgewählten KnowHow-Trägern zu nutzen und massgeschneidert passend in die ICT-Organisation einzuführen. Daraus muss letztlich ein echter nachhaltiger Mehrnutzen (und zwar nicht nur aus Sicht des ICT-Auditoren…) entstehen für z.B. die ICT-Organisation, ICT-Automatisierung, Führungs-Ebene und den Revisions-Stellen / Treuhändern und letztlich dem Risk-Management.

Und trotzdem: Innovationen durch Audits und Risk-Management

Die Erfahrung zeigt, dass durch das proaktive Anwenden und Akzeptieren von gemeinsam definierten Prozessen oder IKS – mit eben auch Blick nach vorne oder auf neue adaptierbare Technologien und Methoden – durchaus auch Innovationen entstehen in einer solchen fortwährenden Transformation in eine Art «Business Excellence in der ICT».

Dies auch unter dem Aspekt, dass sich mehrere Sichten, Bedürfnisse, Expertisen und Erfahrungswerte vereinen und das «möglichst Beste aus der Praxis und Theorie» einbringen.

Eine daraus realisierbare Standardisierung, Automatisierung, oder Homogenisierung von ICT-Prozessen oder ICT-Infrastrukturen kann hierbei ein weiteres Nebenprodukt sein.

Performance- und Sicherheits-Penetration-Tests mit Baselining – einer ist keiner

Es gibt viele Möglichkeiten, vorgegebene Sicherheits-Standards und Compliance-Vorgaben intern oder extern überprüfen zu lassen. Je nach Sicherheits-Anforderungen oder Vorgaben des IKS kann es nötig sein, erweiterte Test-Szenarien zu definieren und prüfen zu lassen durch die externe ICT-Serviceorganisation oder externe, darauf spezialisierte Dienstleister.

Auf dem Markt gibt es viele Anbieter und ab und an entpuppen sich preisgünstige Angebote als reine, simple Security Scans mit gängigen technischen Tools aber ohne weitergehende Überprüfung – mit auch Defiziten in den Lerneffekten und best practices technischen Massnahmen als Gegenwert der Überprüfung.

Die eingangs im Artikel angesprochene Analogie zum DatenSCHUTZ in der DatenFLUT (reissender Wasserstrom) zeigt die schwierige Herausforderung auf bei solchen Tests und verlangt immer mehr nach hochspezialisierten Managed Security Services Dienstleistern, welche mit z.B. nur Evaluationen von Baselines und dem fortwährenden Monitoring dieser Baselines dann Auffälligkeiten (zu grosser oder zu kleiner Fisch im Fluss…) / Angriffsmuster erkennen, eskalieren und verhindern können. Dies im Gegensatz zum einmaligen Penetration Scan, ohne Trends oder brauchbare Vergleiche zu z.B. Baselines.

Nebst dem reinen systemtechnischen Ansatz werden auch zunehmend immer mehr z.B. Prozess-, Informationsmanagement- und ICT-Forensik-Spezialisten involviert, um möglichst ein breitgefächertes Sensorium aufzubauen.

Ansatz von Szenarientechnik und Herausforderungen von dynamischen Bedrohungslagen

Weitere Erfahrungswerte aus erlebten und gesehenen Krisen und Super-GAUs zeigten auf, dass das Spannungsfeld von Theorie und Praxis sich immer mehr akzentuierten in Richtung von angewandten

Szenarien-Techniken im Bereich von Planung, Überwachung und Controlling.

Vermeintlich einfache Fragen wie zum Beispiel: (bewusst einige einfache Beispiele für die Verdeutlichung)

- «Was passiert ab wann bei einem Internet-Zugangs-Ausfall?»
- «Was passiert und wird eingeleitet bei einem Stromausfall, welcher länger dauert als 1 Stunde?»
- «Welche Systeme und ICT-basierte Prozesse können wie weitergeführt werden bei einem Komplett- oder Teil-Ausfall der ICT-Systemumgebung?»
- «Zu welchem Zeitpunkt muss der Überganges-Betrieb mit welchen «analogen» Prozessen oder auf dem «Papierweg» weitergeführt werden und welche Kunden oder Organisationen (z.B. Zoll, Spedi, Transport, Behörden, Geschäftsleitung, Verwaltungsrat, Presse) müssen wie informiert werden?»
- «Wie lange kann die Prozess-Landschaft ohne ICT-Business Unterstützung (wenn überhaupt und wie?) funktionieren?»
- «Wieviele voll- oder halb-automatische System-Redundanz wird benötigt im Gesamt-System oder klassifizierten Teil-Systemen?»
- «Was für Zusatz-Massnahmen sind nötig für die aktuelle, dynamische Bedrohungslage gegenüber des neu bekannten Sicherheits-Problems?»
- «Können die eingesetzten Sicherheits-Infrastrukturen wie z.B. Internet-Firewall, Mail-Filterung, Content-Überwachung, Viren-Malware-Filterung etc. entsprechende brauchbare proaktive Alarmierungen oder Trends reporten und auswerten. Oder braucht es übergeordnete Monitoring-Systeme?»
- «Was ist das verlangte Service Level Agreement von externen Dienstleistern hinsichtlich Reaktions- (MTTR, Mean time to react) oder Reparatur-Zeiten (MTTR, Mean time to repair)?»
- «Was passiert wie schnell bei einem schweren Mitarbeiter-Datensicherheits- oder EDV-Nutzungs-Verstoss gemäss ICT Security Policy?»
- «Sind die Mitarbeiter genügend sensibilisiert, aufgeklärt und geschult zu Basis-ICT-Sicherheits-Prozessen?»
- «Was passiert, wenn es mehrere Fehler gibt bei den Backup-Prozessen oder Backup-Wiederherstellungs-Prozessen?»
- «Was passiert ab wann bei einem externen oder internen gezielten Hacker-/ Trojaner-Angriff?»
- «Gibt es ein Change Management für kontrollierte Systemveränderungen?»
- «Sind die eingesetzten EDV-Mittel genügend dokumentiert und die entsprechenden Versicherungen / Versicherungssummen darauf korrekt ausgerichtet?»
- «Ist der KnowHow-Transfer bzw. Wissensträger-Abhängigkeit genügend geregelt und sichergestellt? Gibt es genügend internes HandsOn für Recovery-Interventionen?»
- «Ist die physische Server-Raum-Sicherheit genügend sicher für einfache Einbrüche oder Sabotagen?»
- «Ist die externe sichere Backup-Aufbewahrung sichergestellt?»

Die Gesamt-Sicherheit braucht auch eine Gesamt-Rahmen-Sicht

Die Gesamt-Sicherheit ist in einem gesamten Rahmen zu sehen – beginnen tut diese aber sicherlich in der internen, selbstkritischen Betrachtung von eigenen Prozessen und Infrastrukturen und erst danach sollte man den Fokus erweitern in Richtung der externen Abhängigkeiten, Hackern, Cloud etc.

Die ICT-Gesamtsicherheit bzw. letztlich die ICT-Strategie ist ein umfassender Gesamt-Prozess mit Verantwortlichkeit auf der Führungsebene - und nicht nur eine Ansammlung von Technologien / Produkten / Tools.

Der Faktor Mensch ist unter diesem Aspekt wichtiger und heikler als der Faktor Maschine.

Dabei ist auch der übrigbleibende Aspekt des Risk-Managements sehr wichtig.

Eine 100% Sicherheit bei Mensch und Maschine gibt es nicht und wird es nie geben und hier ist es die Aufgabe der Führungsebene oder Kontroll-Gremien (Audit, IKS, Controlling) genau diese Rest-Risiken zu identifizieren, zu werten, zu testen und mit gangbaren präventiven Massnahmen und Prozessen zu reduzieren und sporadisch zu prüfen (so gut es eben geht...)

Aus diesen Aspekten heraus empfehle ich: Bevor irgendwelcher externer, technischer Schutzwall aufgebaut wird, sollte man als Basis die internen Prozesse / Sicherheit / Risk-Management optimieren und möglichst «zukunftsgewappnet» transformieren.

Eine «sichere» Informations-Zukunft und nachhaltiges System-Wachstum braucht ein «sicheres» interdisziplinär abgestütztes Rückgrat

Letztlich ist es so, dass «sichere» ICT-Services / ICT-Prozesse das Rückgrat sind von «modern Business» und der voranschreitenden digitalen Transformations-Prozessen und dem ansteigenden Wandlungsdruck.

Auch die Globalisierung / New Economy ist mitunter mitverantwortlich für einen schon lange andauernden, grenzüberschreitenden Informations-Austausch. Und hier sprechen wir von unterschiedlichsten Grenzen (z.B. Geografie, Systeme, Private-Business, Politik, Behörden, Gesellschaft, Bildung, Health, Wissenschaft, Wirtschaft, Märkte), welche zunehmend nur in einer interdisziplinären Zusammenarbeit möglichst gut «abgesichert» werden können mit allen Akteuren und dem gemeinsamen Ziel eines nachhaltigen, sicheren Global-Informations-System-Wachstums.

DER AUTOR

Fridel Rickenbacher ist Mitbegründer, Partner und Verwaltungsrat der MIT-GROUP, einem Totalunternehmen für Informations- und Kommunikationsmanagement mit eigenem Hochsicherheits-Rechencenter in der Schweiz.
Sein erster Bildungsweg absolvierte er an der Fachhochschule FH Horw in den Bereichen Bauleiter/Projektleiter/Immobilienverwaltung und Internet-Netzwerk-Technologien (1. CISCO Academy Klasse NDK in der Schweiz, mit Dozententätigkeit an der FH Horw) und der zweite Bildungsweg an der HSLU in den Bereichen Wirtschaftsinformatik/Engineering und letztlich in diversen Microsoft-Zertifizierungen MCSE NT/2000/2003/2008/2012

Des Weiteren ist er Mitglied bei diversen Branchen- und Fach-Verbänden und Redaktionen und schreibt / bloggt über aktuelle ICT- / Management-Themen aus seinen eigenen Erfahrungen als Unternehmer, Generalist, ICT-Coach, Systemengineer, Auditor, Sparring-Partner und Transformations-Begleiter.

Informationen des Verbands

Sicherheitsmanagement – mit unserer Ausbildung

Der Artikel von Fridel Rickenbacher beleuchtet zahlreiche und teilweise recht unterschiedliche Aspekte des Sicherheitsmanagements in einem Unternehmen. Die Vielfalt der erwähnten Lösungsansätze und (inter)nationalen Standards lassen einem etwas ratlos zurück: Findet man den Zugang eher über die Gesetze wie den Sarbanes Oxley Act oder das Datenschutzgesetz – oder vielleicht doch besser über Sammlungen von bewährten Praktiken wie das deutsche IT-Grundschutzhandbuch, ISO27002 in der gültigen Ausführung von 2013 oder vielleicht COBIT 5 for Security?

Genauso wie es keine 100%ige Sicherheit geben kann (wie im Artikel mehrfach erwähnt), gibt es auch nicht den perfekten Lösungsansatz. Damit man aber aus den zahlreichen Quellen die sinnvoll anwendbaren Ansätze erkennen und auswählen kann, benötigt man eine solide Ausbildung. Nur so kann man die zahlreichen Gemeinsamkeiten erkennen oder z.B. eigentlich für andere Zwecke gedachte Lösungsvorschläge für das eigene Unternehmen adaptieren und ausreichend wirksam implementieren.

Seit 1992 bietet das ISACA Switzerland Chapter eine seriöse, sorgfältig aufgebaute und nachweislich erfolgreiche Ausbildung an – immer wieder angepasst an die neuen rsp. regelmässig aktualisierten Berufsbilder CISA, CISM, CGEIT und CRISC. Für die Sicherheitsspezialisten besteht ein 14tägiger Kurs mit einem vorgelagerten "Heimstudium", Präsenzunterricht sowie ausführlichen und klar strukturierten Unterlagen; unsere berufsbegleitende Aus- und Weiterbildung vermittelt ein umfassendes Fachwissen und bereitet auch auf die internationale CISM-Prüfung (Certified Information Security Officer) vor. Analoge Ausbildungen bestehen auch für CISA (Certified Information System Auditor), CGEIT (Certified in the Governance of Enterprise IT) und CRISC (Certified in Risk and Information Systems Control). Alle vier Kurse finden jeweils einmal pro Jahr im Juni/Juli statt (mit einem individuellen Studienbeginn ab Februar und dem nachgelagerten Prüfungstrainingsblock im Oktober).

WEITERE INFORMATIONEN

Die genauen Daten für die vier Prüfungstrainings CISA, CISM, CGEIT und CRISC finden Sie in der nachfolgenden Kursübersicht oder auch auf www.isaca.ch, wo Sie weitere Informationen zu den Zertifikaten sowie unseren Vertiefungskursen herunterladen können.

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
11.-12.09.2014	LAB-IPS B	iPhone & iPad Security (Bern)
15.09.2014		ISACA Anniversary Conference (Lausanne)
17.09.2014	JK-2014	ISACA Jubiläums-Tagung (Zürich)
09.-11.10.2014	CGEIT-PV	CGEIT-Prüfungstraining
16.-18.10.2014	CRISC-PV	CRISC-Prüfungstraining
22.-25.10.2014	CISA-PV	CISA-Prüfungstraining
30.10.-01.11.2014	CISM-PV	CISM-Prüfungstraining
www.isaca.ch		
29.09. - 01.10.2014	P-COF3	COBIT 5 Foundation
10. - 12.11.2014	P-COI3	COBIT 5 Implementation
www.glenfis.ch		

IMPRESSUM ISACA NEWS

ISACA

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Kurssekretariat, c/o ITACS Training AG, Chrummbächliweg 35, 8805 Richterswil
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