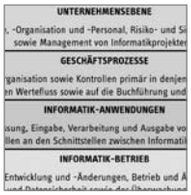
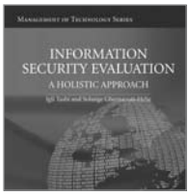
ISACA®
Trust in, and value from, information systems
Switzerland Chapter
Nr. 04 | Dezember 2012 | www.isaca.ch
NEWSLETTER



IKS IT
Dokumentierte IT-Kontrollen erhöhen die Zuverlässigkeit der Geschäftsabwicklung.
Seite 73



Information Security
The Information Security Assurance Assessment Model (ISAAM) can be used to evaluate the information security posture. **Seite 76**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 77**

Internes Kontroll-System im Informatikbereich von KMU

Auf Risiken und Bedürfnisse ausgerichtete, systematisch aufgebaute und dokumentierte Kontrollen im Informatikbereich erhöhen die Zuverlässigkeit der Geschäftsabwicklung und helfen, die Funktionsfähigkeit, Sicherheit und Wirtschaftlichkeit der Informatik zu gewährleisten – dies gilt auch für kleinere und mittlere Unternehmen!

Von Peter Steuri

Ausgangslage

Erfahrungen und Beobachtungen aus der Tätigkeit als Informatik-Prüfer und -Berater zeigen, dass in kleineren und mittleren Unternehmen oftmals Unsicherheit und Fragen zum Umfang und Inhalt sowie insbesondere auch zum konkreten Nutzen des Internen Kontroll-Systems (IKS) bestehen. Dies gilt für das IKS auf Unternehmens- und Prozessebene sowie, in noch stärkerem Mass, auch für die Kontrollen im Informatikbereich.

Der Schweizer Prüfungsstandard «Prüfung der Existenz des Internen Kontrollsystems» (PS 890) definiert die Bedeutung der Informatik für das interne Kontroll-System wie folgt: «Kontrollen im Informatikbereich sind umso wichtiger, je stärker der Rechnungslegungs- und Berichterstattungs-Prozess von Informatik-Systemen abhängig ist und je höher das Risiko ist, dass Fehler ihre Ursache im Aufbau von und Umgang mit Informatik-Systemen haben könnten.»

Informatikeinsatz in Schweizer KMU

In kleineren und mittleren Unternehmen (KMU) weichen die Anforderungen an die Informatik nicht wesentlich von denjenigen in grossen Unternehmen ab: Anwendungen mit breitem Funktionsumfang sowie hohe Verfügbarkeit und Sicherheit sind wesentliche Voraussetzungen für die effiziente und zuverlässige Abwicklung der Geschäftsprozesse.

Gegenüber grösseren Unternehmen mit bezüglich Knowhow und Kapazität gut dotierten Informatikabteilungen ist die Situation in KMU, obwohl deren Informatik-Systeme und -Infrastruktur noch «überschaubar» sind und als Kern-Anwendungen in der Regel Standard-Software eingesetzt wird, oft von folgenden «typischen» Risiken geprägt:

- fehlendes Knowhow zu den Informatik-Anwendungen sowie den Daten- und Werteflüssen (d.h. den Schnittstellen zwischen den Anwendungen); daraus resultieren eine fehleranfällige, ineffiziente Nutzung der Software, Schwachstellen in der internen Kontrolle und eine hohe Abhängigkeit von externen Partnern (Dienstleistern und Lieferanten);
- starke Konzentration des Knowhow auf Einzelne, sehr oft einher gehend mit wenig strukturierten und kaum dokumentierten Prozessen im Informatikbereich; daraus ergibt sich eine hohe Abhängigkeit von solchen Schlüsselpersonen;

- angemessener Zugriffsschutz auf der Ebene von Netzwerk und Betriebssystem, aber innerhalb der einzelnen Anwendungen kaum differenzierte Zugriffsberechtigungen sowie «schwache» Passworte und Verzicht auf periodische Passwort-Wechsel;

- Individual-Lösungen und -Auswertungen in Excel oder Access, die von einzelnen Anwendern erstellt und kaum dokumentiert werden; deren Weiterentwicklung und Funktionsfähigkeit sowie oft auch deren Nutzung (v.a. im Bereich Kennzahlen und MIS) sind vollumfänglich von dieser einen Person abhängig;

- Schwachstellen im Bereich der physischen Sicherheit (Zutritt, Rauch- und Feuererkennung, Klimatisierung und Stromversorgung) des Rechenzentrums resp. des Serverraumes;

- regelmässige Erstellung von Datensicherungen, aber oftmals Schwachstellen in deren Aufbewahrung (kein Datenträger-Safe) sowie ungenügende Auslagerung und fehlende Restore-Tests (als Grundlage für Wiederherstellung nach einem gravierenden Ereignis);

- fehlende Vorsorge und Vorbereitung für die Bewältigung von gravierenden Ereignissen (bspw. Zerstörung des Rechenzentrums resp. des Serverraumes), obwohl die Geschäftsprozesse in hohem Mass von der Verfügbarkeit der Informatikmittel abhängig sind.

Das «ideale» IKS im Informatikbereich

Auch für ein KMU ist wichtig, im Informatikbereich eine angemessene interne Organisation und Kontrolle zu gewährleisten sowie zweckmässige Dokumentationen zu pflegen.

Ein umfassendes IKS beinhaltet Kontrollziele und Kontrollen auf mehreren Ebenen: Den Geschäftsprozessen, den Informatik-Anwendungen und deren programmierten Kontrollen sowie dem Informatik-Bereich.

Als «Dach» sind unternehmensweite Kontrollziele und Kontrollen in den Bereichen Informatik-Strategie, -Organisation und -Personal, Risiko- und Sicherheits-Management sowie Steuerung und Management von (Informatik-)Projekten zu implementieren.

Inhalte des IKS im Informatikbereich

Im anwendungsunabhängigen Bereich, d.h. der Informatik «an sich», sollten Kontrollziele und Kontrollen mindestens folgende Themen abdecken:

- Informatik-Strategie und -Planung
- Organisation und Personal im Informatikbereich
- Übersicht zum Informatikeinsatz (Anwendungen, Systeme und Netzwerk) und Inventar der Informatikmittel
- Verträge / Service Level Agreements (intern und mit externen Dienstleistern)
- Projekt-Management
- Beschaffung von Informatikmitteln (Hard- und Software)
- Inbetriebnahme von Informatikmitteln
- Programm-Entwicklung und -Unterhalt (genereller Prozess)
- Konfigurations-Management
- Risiko-Management / Versicherungen
- Physische Sicherheit
- Logische Sicherheit / Daten- und Zugriffsschutz (Grundlagen)
- Datensicherung / Archivierung
- Notorganisation / Katastrophenvorsorge
- Führungsgrundlagen, Richtlinien, Weisungen
- relevante Gesetze, Vorschriften und Verträge
- Interne Kontrollen

Im Bereich der Kern-Anwendungen zur Unterstützung der Geschäftsprozesse sollten Kontrollziele und Kontrollen für jede wesentliche Anwendung folgende Themen abdecken:

- Organisation (Zusammenspiel von Informatik und Fachabteilungen) / Benutzer-Schulung und -Support
- System- und Betriebs-Dokumentationen / Benutzer-Dokumentationen
- Systemumgebungen (Entwicklung, Test, Produktion)
- Antrags-, Genehmigungs-, Test- und Abnahmeverfahren für Programm-Entwicklung und -Unterhalt
- Antrags-, Genehmigungs-, Test- und Abnahmeverfahren für die Pflege der Steuerungsparameter (Customizing)
- Pflege der Stammdaten (Berechtigte, Kontrolle und Nachvollzug)
- Datenerfassung (Berechtigte, Kontrolle und Nachvollzug)
- Datenverarbeitung (Kontrolle und Nachvollzug)
- Datenspeicherung (Kontrolle und Nachvollzug) / Datensicherung, -aufbewahrung und -archivierung
- Datenausgabe (Journale, Kontrolle)
- (Jahres-)Abschlussarbeiten (Durchführung, Kontrolle und Nachvollzug)
- Schnittstellen (Kontrolle und Nachvollzug)
- Zugriffsschutz (Berechtigungskonzept)
- Pflege und Überwachung von Benutzern und Berechtigungen (Prozess, Verantwortliche)

Erster Schritt zum IKS: Erhebung und Beurteilung des IST-Zustandes

Als Hilfsmittel für die Erhebung und Beurteilung des IST-Zustandes kann das vom Stab Informatik der Treuhand-Kammer erarbeitete «Vorgehensmodell IT-Risikoanalyse» dienen. Obwohl das Vorgehensmodell als «Arbeitshilfe für KMU-Prüfer» bezeichnet ist, eignet es sich auch für Self-Assessments.

Das Modell beinhaltet zwei Checklisten und beschreibt die drei Vorgehensschritte, um sich mit angemessenem Aufwand ein klares Bild über den IST-Zustand zu verschaffen:

1) Bedeutung der Informatik für das Unternehmen und die mit dem Informatikeinsatz verbundenen Risiken erkennen. Dazu dient eine Checkliste mit 16 Fragen und jeweils 4 möglichen Antworten. Aus den Antworten gehen potentielle Risikofaktoren hervor: Einschätzungen in den Stufen 4 und 3 weisen auf

IKS IM INFORMATIKBEREICH

UNTERNEHMENSEBENE Informatik-Strategie, -Organisation und -Personal, Risiko- und Sicherheits-Management sowie Management von Informatikprojekten.
GESCHÄFTSPROZESSE Aufbau- und Ablauforganisation sowie Kontrollen primär in denjenigen Geschäftsprozessen, die einen Einfluss auf den Wertefluss sowie auf die Buchführung und die Jahresrechnung haben.
INFORMATIK-ANWENDUNGEN Kontrollen bei der Erfassung, Eingabe, Verarbeitung und Ausgabe von Transaktionen und Daten sowie Kontrollen an den Schnittstellen zwischen Informatik-Anwendungen.
INFORMATIK-BETRIEB Kontrollen bei Programm-Entwicklung und -Änderungen, Betrieb und Änderung der Informatikmittel, der System- und Datensicherheit sowie der Überwachung der Informatik.

Bei der Gestaltung des IKS im Informatikbereich sind Kontrollziele einzubeziehen, welche die Funktionsfähigkeit, Sicherheit und Wirtschaftlichkeit der Informatik in einem weiteren Sinn unterstützen.

geringe Risiken hin; die Stufen 2 und 1 weisen auf erhebliche bis hohe Risiken hin.

2) Stark- / Schwachstellen in IT-Organisation und -Prozessen identifizieren, d.h. die «Reife» der Informatik beurteilen. Dazu dient eine Checkliste mit rund 90 Fragen zu 20 für den IT-Einsatz relevanten Themen. Die einzelnen Fragen werden in einem 4-stufigen Maturitätsmodell bewertet. Bewertungen im Bereich der Maturitätsstufen 4 und 3 weisen auf einen guten Reifegrad und geringe Risiken hin; die Maturitätsstufen 2 und 1 weisen auf einen ungenügenden Reifegrad resp. erhebliche bis hohe Risiken hin.

3) Übersicht über die (Kern-)Anwendungen sowie die wesentlichen Werte- und Datenflüsse gewinnen und (grafisch) darstellen; dazu ist es hilfreich, die Anwendungen (Standard-Software / angepasste Standard-Software / Individual-Software) und deren Schnittstellen (manuell / maschinell als Stapelverarbeitung / maschinell/automatisch) zu kategorisieren.

Das Vorgehensmodell und die Checklisten werden vom Autor auf Anfrage hin zur Verfügung gestellt.

Zweiter Schritt: Aufbau resp. Optimierung des IKS

In der Praxis haben sich verschiedene Werkzeuge und Methoden durchgesetzt, die hilfreich sind, um die Informatik «im Griff» zu halten resp. in den Griff zu bekommen und das IKS zu optimieren:

Zum einen ist das **COBIT Framework**, das international anerkannte Standardwerk zur IT-Governance von ISACA, zu nennen. Das 1996 erstmals veröffentlichte COBIT-Framework (1998, 2000, 2005 und erneut auf 2012 wesentlich überarbeitet) betont die Rolle und den Einfluss der Informationstechnologie auf die Geschäftsprozesse. COBIT stellt ein Modell von generell anwendbaren und akzeptierten Governance- und Management-Praktiken bereit, um in einem Unternehmen einen verlässlichen Umgang mit der Informationstechnologie zu gewährleisten. Das COBIT-Framework integriert die Anforderungen der bekanntesten Standards und Modelle für das Management und die Kontrolle der Informationstechnologie wie bspw. COSO, Basel III, ISO27000 und ITIL.

Wenn bei der Gestaltung des IKS ein hohes Gewicht auf die Informations- und Informatik-Sicherheit gelegt werden soll, kann auch auf der **ISO-Normenreihe 27000** abgestellt werden:

1) Die ISO-Norm 27001 spezifiziert die Anforderungen an ein Informationssicherheits-Managementsystem (ISMS). Die Norm umfasst die Erstellung, die Einführung, den Betrieb, die Überwachung, die Wartung und die kontinuierliche Verbesserung eines dokumentierten ISMS unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Über die Erfüllung der Anforderungen von ISO 27001 ist auch eine Zertifizierung des ISMS möglich.

2) Die ISO-Norm 27002 beschreibt Kontrollziele im Bereich der Informationssicherheit. Grundlage bildete eine breite Sammlung von Erfahrungen, Verfahren und Methoden aus der Praxis, um einen «best practice» Ansatz umzusetzen. Sie umfasst Weisungen und Richtlinien zur Informationssicherheit, organisatorische Sicherheitsmassnahmen und Managementprozess, Verantwortung und Klassifizierung von Informationswerten, personelle Sicherheit, Physische Sicherheit und öffentliche Versorgungsdienste, Netzwerk- und Betriebssicherheit, Zugriffskontrolle, Systementwicklung und Wartung, Umgang mit Sicherheitsvorfällen, Notfallvorsorgeplanung, Einhaltung rechtlicher Vorgaben und der Sicherheitsrichtlinien sowie Überprüfungen durch Audits.

Eine Zertifizierung nach ISO 27002 ist nicht möglich, da die Norm «nur» eine Sammlung von Vorschlägen (Massnahmen) beinhaltet, die entsprechend umgesetzt werden müssen.

Wenn im ersten Schritt, d.h. bei der Erhebung und Beurteilung des IST-Zustandes mit dem «Vorgehensmodell IT-Risikoanalyse» gearbeitet wurde, kann dieses auch als Grundlage für die Optimierung dienen: Die Beschreibungen zu den «höheren» Stufen der Checkliste mit den rund 90 Fragen zeigen, was im jeweiligen Prozess / Thema als guter (Stufe 3) resp. als optimaler (Stufe 4) Reifegrad erachtet wird.

Fokussieren Sie auf Ihre betrieblichen Anforderungen

Wichtig bei der Gestaltung des IKS, und dies nicht nur im Informatikbereich, ist eine klare Fokussierung auf das für das Unternehmen und dessen spezifischen Verhältnisse Notwendige und Zweckmässige – das IKS darf nicht eine «Pflichtübung» sein, sondern kann einen wesentlichen Beitrag zur «sicheren» (im weitesten Sinn) und effizienten Geschäftsabwicklung leisten.

Bei der Gestaltung der Kontrollen im Informatikbereich müssen neben der Buchführung und Rechnungslegung vor allem auch die Leistungserbringungs-Prozesse einbezogen werden: Häufig sind die Entwicklung, die Produktion, der Vertrieb und der Service in einem viel höheren und direkteren Ausmass abhängig von einem funktionierenden und sicheren Informatikeinsatz als das Rechnungswesen!

Last but not least - Unterstützung beiziehen

Für eine sorgfältige Erhebung und neutrale Beurteilung des IST-Zustandes sowie die nachhaltige Verbesserung des IKS im Informatikbereich fehlen in KMU oftmals die notwendigen Ressourcen und häufig auch die erforderlichen Kenntnisse.

Experten mit entsprechendem Knowhow und umfassender Erfahrung können eine gegebene Situation rasch beurteilen sowie mit vertretbarem Aufwand konkrete Massnahmen zu wirksamen Verbesserungen, und damit zur Reduktion der Risiken, aufzeigen!

DER AUTOR

Peter Steuri Certified Information Systems Auditor / eidg. dipl. Wirtschaftsinformatiker
Partner und Leiter CC Informatik bei BDO AG in Solothurn /
peter.steuri@bdo.ch

IMPRESSUM ISACA NEWS

Herausgeber, Redaktion:	ISACA Switzerland Chapter
Adresse:	Kurssekretariat, c/o ITACS Training AG, Stampfenbachstr. 40, 8006 Zürich
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

Information security evaluation: a holistic approach

By Igli Tashi, Solange Ghernaouti-Hélie. Management of Technology Series. EPFL Press 2011

Context and scope

You can only have real confidence in your information security programme if it's based on a strong foundation and if it has been developed with conviction. The main challenge for security practitioners is to increase the level of trust over their business partners and stakeholders believing that their business is protected by a robust information security practice.

In order to capture the intent «to be appropriately and commensurately» protected, an evaluation should be based on a targeted assessment, aligned with the organisation's business needs. In doing that, an information security function should have a consistent and coherent structure, operate as expected, and respond to specific business needs.

This book presents a global, systemic, and multidimensional integrated approach to the holistic evaluation of the information security posture of an organization. It is based on, and integrates, a number of information security best practices, standards, methodologies and sources of research expertise, in order to provide a generic model that can be implemented in organizations of all kinds as part of their effort towards the improved governance their information security.

This approach contributes to improving the identification of security requirements, measures and controls. At the same time, it provides a means of enhancing the recognition of evidence related to the assurance, quality and maturity level of the organisation's security function thus driving improved security effectiveness and efficiency.

The problem

Executives, in spite of all the papers and theories published in hundred of books and newspapers, still have a limited view of the importance of the information security practice. Fundamental questions with regards to the position of the information security within the value chain of the organization, as well as the nature and the extent of the resources and efforts dedicated to it, are very often considered a posteriori. The PwC 2012 Global Information Security Survey outlines that the lack of an actionable vision or understanding from Executives is identified as one of the greatest obstacles to effective information security from a strategic point of view. This is the case for 37 % of the CISO and for 30 % of CIOs that responded to the PwC's security survey. Executives are motivated by the fear or after the occurrence of a crisis, but when problems arise this is unfortunately too late.

The approach

The Information Security Assurance Assessment Model (ISAAM) can be used to evaluate the information security posture in a given period of time and aiming to provide a faithful picture of the protection level achieved by being as pragmatic as possible.

In doing that, ISAAM uses a system based on a triple evaluation aiming to quantify the level of trust that can be put into a given subject of the evaluation (a security measure or process) as well as into the security system as a whole. This is the result of three different evaluation angles, namely

- the resilience of the security structure;
- the quality of the security processes; and,
- the level of the alignment of the security practice with regards to the business objectives.

ISAAM's structured assessment approach enables organizations to perform a holistic assessment of their overall security protection system rather than the traditional piecemeal or compliance-driven evaluation approach. This rigor makes the assessment much more valuable to the organization by reducing the complexity arising from the number of security safeguards and practices, and the evaluation methods of a multiple nature and scope.

ISAAM focuses more on the consistency of the security practices in place and the related constituent elements of security rather than on their overall compliance level against a single best practice or methodology. To holistically evaluate the information security program, ISAAM clearly sets out the various relevant multidimensional aspects of information security. This enables us to identify the specific concerns and safeguards put in place to address those concerns. As a consequence, the level of confidence senior management can expect from their information security programme by assessing the four dimensions against the three evaluation axis, is related as previously mentioned to the capability to respond and quantify the output of the following:

- Resilience of the structure: is my security programme consistent and coherent over all the dimensions?
- Quality of processes: is my security programme delivering as expected?
- Maturity level of the programme: is my security programme aligned with my expectations and business needs?

The solution

The holistic evaluation based on the methodology proposed by ISAAM, will allow organizations to obtain:

- a greater and a more meaningful understanding for senior business decision makers over their security practices;
- the gap between security performance that is put in place for their specific business needs ; and
- continuously monitor and improve their information security position.

The added value of the ISAAM evaluation approach is that it is easy to implement and operate and it addresses the concrete needs of the business in terms of reliance on an efficient and dynamic evaluation tool, using a coherent system of evaluation. This book gives to the Executives, for whom information security is a priority, a valuable tool, based on a global and integrated approach for information risks and security management and also enables them to effectively run the information security function within their organization.

Igli Tashi: PhD in Information Systems / Master of Advanced Studies in Legal Issues, Crime and ICT Security /expert on information security and risk management at PwC
http://www.pwc.ch

Solange Ghernaouti-Hélie: PhD in Computer Science / professor of the University of Lausanne / founder and director of the Swiss Cybersecurity Advisory and Research Group
http://www.hec.unil.ch/sgh/

Information des Verbandes

Skyfall und CISA – der faszinierende Beruf als IT-Prüfer

Vom Himmel fallen sie kaum, und auch über eine 00-Lizenz verfügen die hochspezialisierten Agenten für ihre Tätigkeit beim Aufspüren von Risiken im Informatikumfeld nicht – aber ansonsten ist der Job als IT-Prüfer fast so spannend wie ein Leben als James Bond 007.

Die Identifikation von Bedrohungen, Verwundbarkeiten und der daraus resultierenden Risiken ist ein Schwerpunkt der Tätigkeit als IT-Prüfer. Auch wenn sich die Risiken in den grossen wie kleinen Unternehmen ähneln (siehe vorhergehender Artikel von Peter Steuri), muss man sie als Prüfer zuerst finden. Manchmal verstecken sich die IT-Risiken hartnäckig und man muss sie zwischen den Zeilen der Handbücher oder Prozessbeschreibungen, mittels Befragungen (nicht à la James Bond) oder aus den technischen Innereien der Informatik «herausholen». In aller Regel arbeitet ein IT-Prüfer mit (sehr) beschränkten Ressourcen und muss oft in kurzer Zeit nicht nur «alle» vorhandenen Risiken aufspüren sondern auch noch bewerten und in einem Bericht Management-tauglich zusammenfassen. Die grosse Schwierigkeit dabei ist, aus den manchmal widersprüchlichen und oft unvollständigen Informationen ein klares Bild zu erstellen.

Die Tätigkeit als IT-Prüfer ist teilweise vergleichbar mit dem Zusammensetzen eines 1000teiligen Puzzles. Jedoch müssen die Puzzle-Teilchen zuerst in der riesigen Informationsflut gefunden und dann korrekt zusammengesetzt werden. Zudem verändern die Puzzleteilchen – im Unterschied zum «klassischen» Puzzlen – während der Prüfungstätigkeit immer wieder Form und Farbe, da laufend neue Erkenntnisse einfliessen und mitberücksichtigt werden müssen. Das kann dann gerade im oft hochkomplexen, technischen Informatikumfeld zu einer riesigen Herausforderung werden.

Wer solche Herausforderungen liebt, sollte sich ernsthaft Gedanken über einen Berufswechsel zum IT-Prüfer und eine entsprechende seriöse Aus- und Weiterbildung machen. Seit 1977 (!) besteht ein international akzeptiertes, immer wieder an die laufenden Entwicklungen in der Wirtschaft und Informatik angepasstes Berufsbild – die Zertifizierung als CISA (Certified Information Systems Auditor) des internationalen Berufsverbandes ISACA mit deutlich über 100,000 Mitgliedern. Seit 1992/93 bieten wir in der Schweiz eine berufsbegleitende, fünfmonatige Ausbildung an, die mit 15 Tagen Präsenzunterricht, ausführlichen und klar strukturierten Unterlagen (und Hausaufgaben!) auf die Tätigkeit im Beruf sowie auf die internationale Prüfung vorbereitet.

Der nächste Kurs startet im Januar 2013 – mit einem «obligatorischen» Einführungstag am 14. Dezember 2012 – melden Sie sich baldmöglichst an! Informieren Sie sich auf unserer Website www.isaca.ch

WEITERE INFORMATIONEN

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

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
11.-12.12.12	ERM-UF	**Risk Management Workshop featuring ISACA's Risk IT Framework and Guidance** Unternehmensweites Risikomanagement wirksam umsetzen
14.12.12-13.5.13	CISA-VK	**CISA-Zertifikatskurs 2013|1** Vertiefungskurs IT-Revision, IT-Kontrolle, IT-Sicherheit, IT-Governance und CISA-Prüfungsvorbereitungskurs. Offizieller CISA-Kurs des ISACA Switzerland Chapter
14.12.12-14.5.13	CISM-VK	**CISM-Zertifikatskurs 2013|1** Vertiefungskurs Konzeption, Governance und Management der Informationssicherheit, Risiko-Management, Reaktionsmanagement und CISM-Prüfungsvorbereitungskurs. Offizieller CISM-Kurs des ISACA Switzerland Chapter
14.12.12-15.5.13	CGEIT-VK	**CGEIT-Zertifikatskurs 2013|1** Vertiefungskurs IT-Governance: strategische Ausrichtung, Wertschöpfung, Risikomanagement, Ressourcen-Management und Leistungsmessung und CGEIT-Prüfungsvorbereitungskurs. Offizieller CGEIT-Kurs des ISACA Switzerland Chapter
14.12.12-16.5.13	CRISC-VK	**CRISC-Zertifikatskurs 2013|1** Vertiefungskurs Identifikation, Management und Überwachung von (IT) Risiken, Einführung, Betrieb und Überwachung des IKS und CRISC-Prüfungsvorbereitungskurs. Offizieller CRISC-Kurs des ISACA Switzerland Chapter
07.02.2013	RM-KK	**Risikomanagement-Methoden wirksam anwenden** Identifikation, Bewertung, und Management von (IT-) Risiken
08.02.2013	PER-KK	**Effizientes Messen von Leistungs- und Risko-Indikatoren** Gute Leistungsindikatoren effizient erheben und auswerten
www.isaca.ch		
4.3.-5.3.13	COB-IG	**ISACA Implementing Governance of Enterprise Using COBIT (Deutsch)**
18.3.13-20.3.13	COB-FB	**ISACA COBIT 5 Foundation Zertifikat**
www.glenfis.ch		