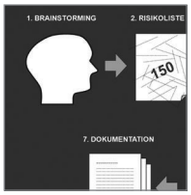
ISACA®
Trust in, and value from, information systems
Switzerland Chapter
Nr. 02 | Juni 2013 | www.isaca.ch
NEWSLETTER



IT-Risiken
Herausforderungen, Tipps und Vorgehensbeispiel für IT-Risiken und deren Management **Seite 59**

Neues CRISC-Zertifikat
IT-Risikomanagement sowie Design und Implementation von IT-Kontrollen **Seite 63**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 63**

IT-Risiken: Wo die Theorie die Praxis kennenlernt

Literatur, Frameworks und Methodologien zu IT-Risikomanagement gibt es viele, auch viele gute. In der Realität treten aber immer wieder ähnliche Probleme bei der Umsetzung auf. Nachfolgend einige Herausforderungen, Tipps und ein Vorgehensbeispiel aus der Praxis.

Von Matthias Peissert und Raphael Blatter

Zum Suchbegriff «IT Risk» findet Amazon 250'051 Treffer. Der Grossteil davon besteht sicherlich aus «False Positives». Trotzdem können wir ohne Risiko – oder eher Bedrohung – einer Lüge bezichtigt zu werden, behaupten, dass hunderte von Autoren zehntausende von Seiten zu diesem Thema verfasst haben. Kaum eine grössere Organisation, die irgendetwas mit IT zu tun hat (schliesslich auch die ISACA), hat nicht irgendwann mindestens ein Framework, eine Methodologie oder eine Publikation zu IT Risk veröffentlicht.

Die Zahl von Bäumen, die zum Druck all dieser Bücher und anderer Dokumente gefällt wurden, zeigt:

- Das Thema IT Risk ist zentral.
- Die Umsetzung ist alles andere als einfach. und
- es macht wenig Sinn, hier nochmals die Grundlagen zu erklären.

Wir gehen also nicht auf Begriffsdefinitionen ein und verweisen für detailliertere Ausführungen auf die 250'051 Amazon-Treffer. Allerdings kommen wir nicht darum herum, die Grundsätze kurz zusammenzufassen. Wir verweisen auf ein paar veröffentlichte Frameworks und Methodologien, bevor wir ausgewählte Herausforderungen aus der Praxis zeigen. Zum Schluss stellen wir an einem Praxisbeispiel ein mögliches Vorgehen zur Identifikation und Bewertung von Risiken vor.

Die Theorie weiss viele Antworten. Fragen bleiben.

Die Grundsätze des IT-Risikomanagements sind schnell erklärt: Abstrakte Bedrohungen können zu einem konkreten Risiko führen, also einer möglichen negativen und unerwünschten Zielabweichung. Um mit diesen Risiken umzugehen, müssen die Risikoverantwortlichen zuerst Bedrohungen und dann mögliche Szenarien identifizieren. Jedem relevanten, repräsentativen Szenario ordnen sie dann eine Eintretenswahrscheinlichkeit und ein Schadensausmass zu. Zur Visualisierung – und nicht zuletzt zur Kommunikation nach oben – dient zum Beispiel eine Risikomatrix (siehe Abbildung 4 aus dem Praxisbeispiel). Unter Berücksichtigung von Risikoappetit und -fähigkeit des Unternehmens, aber auch mit Kosten-Nutzen-Überlegungen werden wo nötig Massnahmen eingeleitet, um das Risiko auf ein akzeptables Mass (Restrisiko) zu senken. Dazu reduziert man die Eintretenswahrscheinlichkeit und/oder das erwartete Schadensausmass des entsprechenden Szenarios. Massnahmen zur Reduktion von IT-Risiken stammen häufig aus dem Bereich der IT-Sicherheit. Auch ungewöhnlichere Varianten wie zum Beispiel Versicherungen lassen sich anwenden.

Die zahlreichen Bücher sind zu Recht länger als der vorhergehende Absatz, denn hier gehen die Fragen weiter:

- Wie stelle ich sicher, dass ich alle relevanten Szenarien in Betracht ziehe?
- Wie bestimme ich die jeweiligen Eintretenswahrscheinlichkeiten und Schadensausmasse? Genügen Modelle basierend auf Vergangenheitsdaten?
- Sind die einzelnen Szenarien wirklich so unabhängig voneinander wie angenommen? Wie stehen aggregierte Einzelrisiken im Verhältnis zur Risikofähigkeit des Unternehmens, falls sie doch korrelieren?

Der seriöse Umgang mit diesen Fragen ist entscheidend, das mussten die Finanzinstitute bei Markt- und Kreditrisiken in den letzten sechs Jahren schmerzlich feststellen. Die Herausforderungen von IT-Risiken sind keineswegs grundlegend anders. Auch wir können keine abschliessenden Antworten auf diese Fragen geben, doch erläutern wir nachfolgend eine mögliche Technik aus einem realen Projekt, die die erwähnten Fragen aus verschiedenen Blickwinkeln betrachtet.

Bunte Vielfalt von Anleitungen

Neben der umfangreichen Literatur zum Thema IT-Risiken existieren zahlreiche Frameworks und Methodologien. Ohne Anspruch auf Vollständigkeit und Details seien in der untenstehenden Tabelle einige davon aufgelistet. Jedes Framework hat seine Befürworter und Gegner; wir nehmen absichtlich keine Bewertung vor. Mit einer Ausnahme: Die frei verfügbaren Dokumente «The Risk IT Framework» und «The Risk IT Practitioner Guide» von ISACA (letzteres für Mitglieder) gewähren einen hervorragenden Überblick und geben nützliche Tipps für die Umsetzung ab.

FRAMEWORK(S)/METHODOLOGIE(N)

	QUELLE	BEZUG
The Risk IT Framework The Risk IT Practitioner Guide	ISACA	isaca.org
NIST 800-30-r1: Guide for Conducting Risk Assessments (Information Security)	National Institute of Standards and Technology, Computer Security Division	csrc.nist.gov
IRAM (Information Risk Analysis Methodology)	ISF	securityforum.org
ISO 31000:2009: Risk management – Principles and guidelines ISO 31010:2009: Risk management – Risk assessment techniques	International Organization for Standardization	iso.org
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	CERT, Software Engineering Institute der Carnegie Mellon Universität	cert.org
CRAMM (CCTA Risk Analysis and Management Method)	Siemens Enterprise Communication Limited	cramm.com
FAIR (Factor Analysis of Information Risk)	Risk Management Insight	riskmanagementinsight.com

Integration als Herausforderung in der Praxis

Auch wenn IT-Risiken und deren Management keineswegs ein neues Thema sind, und trotz der vielen Fachliteratur, finden sich in der Praxis zahlreiche verbesserungswürdige Situationen. Wir zeigen hier eine Auswahl der wichtigsten Herausforderungen aus der Umsetzung exemplarisch auf. Natürlich betreiben auch zahlreiche Unternehmen ein mustergültiges IT-Risikomanagement.

In vielen Fällen existiert eine Stelle, die sich mit dem Thema IT Risk befasst – ganz vorbildlich. Das Risiko wird regelmässig analysiert und ins unternehmensweite Risikomanagement rapportiert. Der Link zur IT und/oder Informationssicherheit funktioniert aber häufig nur in eine Richtung. Heisst: Zur Analyse der Restrisiken werden Massnahmen der IT-Sicherheit in Betracht gezogen, aber Entscheidungen der IT-Sicherheit basieren nur in Ansätzen auf diesen Analysen. Es kommt vor, dass aus identifizierten Risiken notwendige Projekte in der IT-Sicherheit eingeleitet oder laufende Projekte priorisiert werden, die Durchführung der Projekte selbst und die gewählte Lösung hingegen basiert mehrheitlich auf Good Practice, Erfahrungen der Mitarbeitenden oder nicht selten auf den Möglichkeiten der naheliegendsten technischen Lösung. Das Beiziehen von Good Practice und das Nutzen von Erfahrungen sind durchaus angebracht. Aber der Risikoappetit – wenn überhaupt vom oberen Management bestimmt und kommuniziert – und die Einbettung von IT Risk in die unternehmensweite Risikolandschaft kommen nicht selten zu kurz.

Nebenbei möchten wir hier kurz die Verwendung von Return-on-Investment-Berechnungen in der IT-Sicherheit ansprechen. Solche Methoden sollen einen unternehmerischen Blick auf ein Projekt ermöglichen. Allerdings werden sie, wenn überhaupt, vor allem zur Kommunikation und Rechtfertigung genutzt. Seltener dienen sie für Projektentscheide, da die quantitative Berechnung des Nutzens für die Sicherheit – häufig zu einem beträchtlichen Teil in Form von reduziertem Risiko auf immaterielle Güter wie Reputation – sehr schwierig und von vielen ungenauen Annahmen abhängig ist. Die unternehmerische Perspektive auf die Sicherheit ist zwar angebracht, doch bleiben auch bei dieser Betrachtung der Risikoappetit und das Einbetten von IT-Risiken in die unternehmensweite Risikolandschaft häufig aussen vor.

Folglich betrifft eine weitere Herausforderung aus der Praxis die Einbettung eines IT-Risikos in das Risikomanagement des Unternehmens. Häufig analysiert die verantwortliche Stelle IT-Risiken isoliert und rapportiert sie gesondert. Als separater Block gelangen diese auf die Liste der von anderen Stellen im Unternehmen identifizierten Risiken – häufig als operative Risiken – und fliessen so in die Berechnung des Gesamtrisikos ein. Wie Abbildung 1 zeigt, ist der Sachverhalt in der Realität nicht ganz so simpel: Die Betrachtung von IT Risk als isoliertes Thema und deren einfache Addition zu anderen Risiken bilden die Realität nur beschränkt ab. IT-Risikomanagement muss interaktiver und in enger Kooperation mit anderen Stellen durchgeführt werden. Das Unternehmen muss Überschneidungen, gegenseitige Beeinflussung und Korrelationen von unternehmensweiten Risiken ausmachen und berücksichtigen.

Mögliche Klassifizierungen von IT-Risiken und hilfreiche Listen mit zu berücksichtigenden Risiken liefert die Literatur ausreichend. In der Praxis kommt es jedoch immer wieder vor,

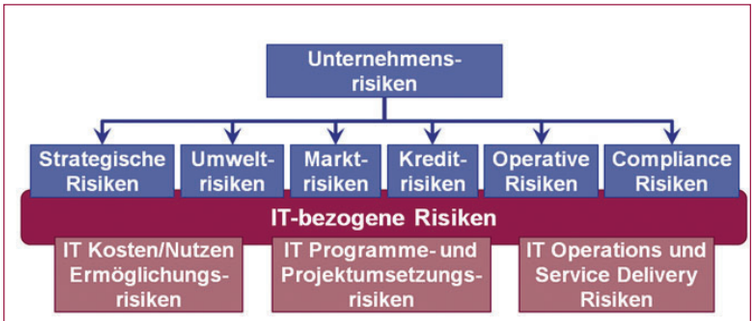


Abb. 1: IT Risk in der Risikohierarchie aus «The Risk IT Framework» von ISACA

Abb. 2: Ablauf eines moderierten Workshops

dass die analysierten Risiken durch eine zu enge Linse betrachtet werden. Aussergewöhnlichere Risiken werden in der Praxis häufig unzureichend berücksichtigt. So etwa die Frage, ob die IT wirklich die richtigen Leute hat (angemessene Ausbildung und Erfahrung, guter Mix von demographischen Hintergründen und Ansichten usw.), zeitlich beschränkte Risiken aus der Durchführung eines IT-Projekts oder das Risiko, das die IT für ein umfangreicheres Projekt bedeutet, um nur drei Beispiele zu nennen.

IT-Risiken ganzheitlich identifizieren und bewerten

Zur Identifikation bestehender IT-Risiken in einer Organisation reicht es nicht, nur die IT selbst zu analysieren. Die Verantwortlichen müssen weitere Kreise der Organisation (z. B. die Benutzer) einbeziehen, um eine umfassende Sicht auf die existierenden IT-Risiken zu erhalten.

In unserem nachfolgenden Praxisbeispiel ging es darum, die IT-Risiken eines Handelsunternehmens gemeinsam zu identifizieren, zu bewerten und Verbesserungsmassnahmen zu entwickeln. Dies geschah im Rahmen eines mehrstündigen, moderierten Workshops, zu dem Vertreter verschiedener Unternehmensbereiche eingeladen waren, so etwa Vertreter aus Niederlassungen und Verteilzentren/Lagern, Vertreter zentraler Dienste wie Beschaffung, Personal, Finanzen & Rechnungswesen, Logistik, Werbung und interne Revision und natürlich IT-Vertreter. Um den Workshop trotz der vielen Teilnehmern (ca. 20 Personen) effizient abzuwickeln, griffen die Moderatoren auf technische Unterstützung zurück: Jeder Teilnehmer erhielt einen speziellen PC und konnte dort seinen Input eingeben. Die Beiträge aller Teilnehmer wurden dann zentral konsolidiert. Abbildung 2 zeigt den Ablauf des Workshops.

Mit Hilfe des Brainstormings zu Beginn wurden zunächst alle Risiken aufgelistet, die den Teilnehmern aus ihren Bereichen bekannt waren. In der Folge haben die Moderatoren diese bereinigt und kategorisiert, indem sie Mehrfachnennungen beseitigten, die Risiken verständlicher und eindeutiger formulierten und diversen Kategorien zuordneten.

In einem nächsten Schritt wurden die Risiken diskutiert und bewertet, um pro Kategorie die zentralen Risiken herauszuschälen. Die folgende Übersicht zeigt beispielhaft einige Schlüsselrisiken:

Die Priorisierung machte deutlich, dass auch solche Risiken als Schlüsselrisiken erkannt wurden, die nur indirekt etwas mit dem Betrieb der IT zu tun haben (z. B. Unternehmensstrategie, Service-Outsourcing). Diese Erkenntnis zeigt, dass weitere Unternehmenskreise unbedingt in die Risikoüberlegungen einbezogen werden sollten und dass freies Brainstormings zu Beginn eines derartigen Workshops äusserst wertvoll ist. Um die ausgemachten Risiken passend anzugehen, definierten die Teilnehmer zum Schluss erste Massnahmen.

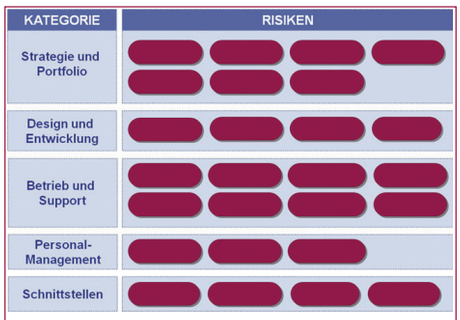


Abb. 3: Beispiel für Risikokategorien

Frameworks nutzen und Theorie sinnvoll umsetzen

Literatur und veröffentliche Frameworks bieten ausgezeichnete Grundlagen, um ein effektives und effizientes IT-Risikomanagement einzuführen und zu betreiben. Um zuverlässig mit IT Risk umzugehen, muss auch in der Praxis – wie aus der Theorie bekannt – IT Risk ganzheitlich angeschaut und Korrelationen berücksichtigt werden. Risikoanalysen sind ein gutes Hilfsmittel, um Projekte zu priorisieren, sollten aber auch zur Auswahl der Lösungen und zur Definition des Projektumfangs genutzt werden. Technologisch unterstützte Workshops mit Vertretern verschiedener Unternehmensbereiche haben sich als einfaches aber mächtiges Werkzeug erwiesen, um in der Praxis aus dem häufig anzutreffenden Silo-Denken von IT Risk auszubrechen.

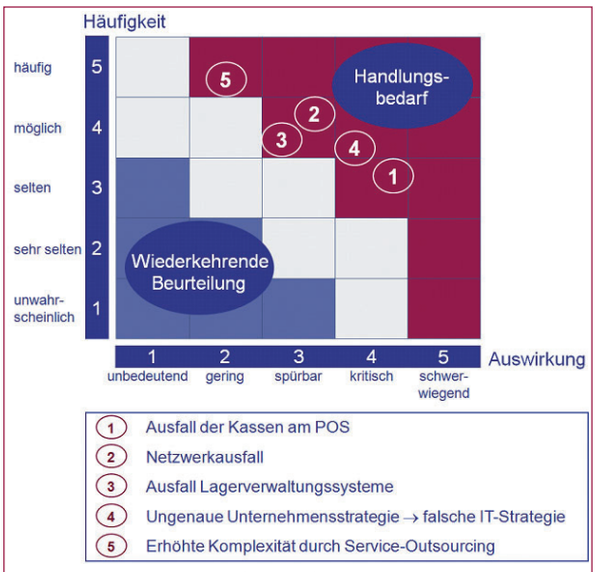


Abb. 4: Schlüsselrisiken (Auszug) nach der Priorisierung

DIE AUTOREN

Matthias Peissert ist als Berater für Informationstechnologie in Financial Services in den Bereichen Business Continuity, IT Risk und Document Management der PwC tätig.

Raphael Blatter ist seit dem Abschluss des Studiums in Wirtschaftsinformatik und Informatik vor zwei Jahren bei PwC hauptsächlich im Bereich Information Security für den Finanzsektor tätig.

Risikomanagement – alles andere als risikolos !

Sind Ihnen die vielen Artikel über Risikomanagement schon mal aufgefallen? Haben Sie aber auch realisiert, dass diese zwar grundsätzlich mehr oder weniger dieselben Prozessschritte aufzeigen und erläutern, aber oft höchst unterschiedliche Anwendungsschwerpunkte haben? Da gibt es Risikomanagement aus Optik von Compliance (Einhaltung von Gesetzen, regulatorischen Auflagen oder Verträgen), operationelles Risikomanagement oder z.B. das Management von Kredit-, Markt- oder strategischen Risiken. Und – last but not least – gibt es noch Informationssicherheits-Risikomanagement oder auch IT-Risikomanagement.

Damit Risikomanagement wirklich funktioniert, benötigt das Unternehmen gemäss einer Untersuchung der KPMG (Risikomanagement und Solvency II bei Versicherungsunternehmen) über entsprechend qualifizierte Mitarbeiter im Kernteam, eine offene Risikokultur und eine entsprechend offene Kommunikation über Risiken sowie ausreichende Kapazität und Knowhow zur Umsetzung der notwendigen Massnahmen. Darüber hinaus sind klar definierte Verantwortlichkeiten für Risikomanagement von zentraler Bedeutung – betrachtet man jetzt nochmals die Abbildung 1, so kommen leise Zweifel auf, ob dieser wichtige Punkt in einem durchschnittlichen Unternehmen auch erfüllt ist.

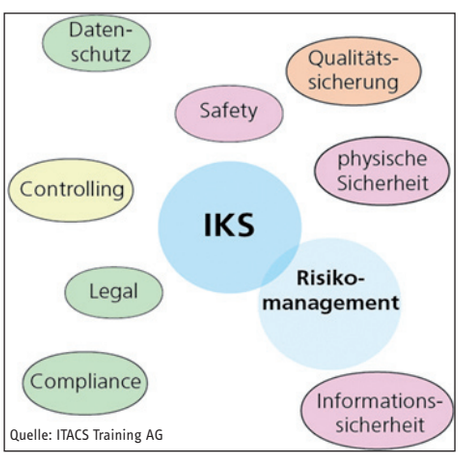


Abb. 1: Verschiedene verwandte Themen, die alle ein eigenes Risikomanagement betreiben.

Ein ebenfalls wichtige Frage ist die Festlegung der «richtigen» Risikomanagementmethode: Soll es AS/NZS 4360:2004, ONR 4900x, ISO31000 oder vielleicht die praktisch identische Norm ISO27005 sein, vielleicht das sehr hilfreiche Risk IT oder eventuell die absolut interessante Neuerscheinung COBIT 5 for Risk? Für wirklich grosse resp. börsenkotierte Unternehmen gibt es wahrscheinlich keinen Weg vorbei an COSO ERM, das sich – obwohl z.B. in der Informatik de facto unbrauchbar – als de facto Standard etabliert hat.

Fragen über Fragen – haben Sie noch immer das Gefühl, dass Ihr Unternehmen dieses Thema wirklich im Griff hat? Dann lassen Sie mich noch einen letzten Einwand aus der Praxis einbringen: Nehmen wir einmal an, Ihr Unternehmen betreibt ein nahezu perfektes Risikomanagement und hat auch die Organisation themenbezogen gruppiert (siehe Abb. 2): Wie kombinieren Sie die so unterschiedliche Betrachtung des Enterprise Risk Management (Zitat: «Ich fokussiere mich einzig auf die Top-10 Liste der operationellen Risiken») mit den Hunderten wenn nicht Tausenden von einzelnen Risiken z.B. im Bereich der IT- und Informationssicherheit oder den applikatorischen Risiken und Kontrollen innerhalb der verschiedenen Geschäftsanwendungen?

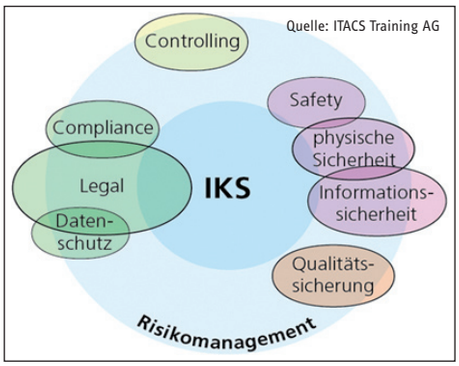


Abb. 2: Gruppierung ähnlicher Themen innerhalb eines übergeordneten Risikomanagement.

Nun – jeder Narr kann eine Frage stellen, auf die selbst der weiseste Mensch keine Antwort hat. Ich suche hier jedoch keinesfalls die perfekte Antwort sondern einfach die Erkenntnis der Leser, dass sie sich einmal etwas mehr mit diesem Thema auseinander setzen sollten. Wer das systematisch und im Rahmen einer internationalen Zertifikatsausbildung einmal tun möchte, der sei hier auf das Angebot des ISACA Switzerland Chapter hingewiesen (siehe Kasten), das einen berufsbegleitenden Kurs zu IKS und Risikomanagement anbietet, der auf die internationale CRISC-Prüfung vorbereitet.

Peter R. Bitterli

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 des Verbandes

Das neue CRISC-Zertifikat

Das neue CRISC-Zertifikat (CRISC =Certified in Risk Management and Internal Control) deckt 39 verschiedene Aufgaben in fünf übergeordneten Themenbereichen ab: Es geht einerseits um die Identifikation, Einschätzung und Bewertung von Risiken sowie um deren Management und Überwachung. Anderseits geht es um Design und Implementation von IT-Kontrollen sowie deren Überwachung und Unterhalt. In dieser Kombination deckt das neue CRISC-Berufsbild und die entsprechende Zertifizierung ein offensichtliches Markt-Bedürfnis ab.

Der berufsbegleitende CRISC-Kurs des ISACA Switzerland Chapter (13 Kurstage verteilt über 4-5 Monate) richtet sich an alle Personen, die sich mit unterschiedlichsten Risikomanagementfragen und Frameworks oder mit dem Design, der Implementation, der Überwachung und Wartung von Sicherheitsmassnahmen und anderen Kontrollen beschäftigen – also Risikomanager und Sicherheitsbeauftragte innerhalb und ausserhalb der IT, Compliance-Officer, IKS-Verantwortliche, erfahrene Informatikrevisoren, IT-Anwendungsentwickler oder Projektcontroller. Der nächste Kurs startet anfangs Juli; ein Einstieg ist bis Mitte August möglich.

CRISC™ Certified in Risk and Information Systems Control™ An ISACA® Certification

WEITERE INFORMATIONEN

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

Herzliche Gratulation zum Platz 1!

Eine der zahlreichen Angebote unseres Vereins sind die qualitativ hochstehenden Ausbildungsmöglichkeiten, wie z.B. die nationalen und internationalen Seminare und Fachkonferenzen, welche vom Dachverband oder dem Switzerland Chapter – teilweise zusammen mit anderen Organisationen - durchgeführt werden.

Speziell zu erwähnen sind die Veranstaltungen, welche für unsere Mitglieder gratis sind: neben den zahlreichen über das Internet zugänglichen Referate mit Online-Chat sind es auch die monatlichen After Hours Seminare in Zürich (in unregelmässigen Abständen auch in Bern oder Genf), welche wertvolle Praxiserfahrungen vermitteln und ein intensives Networking ermöglichen.

Stolz sind wir als Verein auf die seit 1992 durchgeführten Zertifikatskurse, welche auf die internationalen Zertifikate CISA, CISM, CGEIT und CRISC vorbereiten (siehe auch Kasten zu CRISC). Unsere Teilnehmer schneiden an den international standardisierten Prüfungen immer wieder hervorragend ab und haben bereits drei Mal Podestplätze belegt.

Ganz besonders freut uns die Leistung von Bruno Blumenthal (siehe Bild), der an der CISM-Prüfung im Dezember 2012 unter 2454 Teilnehmern der ersten Platz belegte – herzliche Gratulation.

Der Vorstand
ISACA Switzerland Chapter

Bruno Blumenthal

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
1.-2.7.13	ERM-UF (E)	**Risk Management Workshop featuring ISACA's Risk IT Framework and Guidance** Implementing an effective enterprise-wide risk management
3.7.13	COB-KK	**Einführung in COBIT 5**
4.-5.7.13	LAB-FI	**Forensic Investigation**
8.-9.7.13	APR-BJ	**High-Level Analyse von Projektrisiken** Kritische Projekte auf Ihre Risiken analysieren
12.7.13	CISA-VK 13|2	**CISA-Vertiefungskurs 2013|2**
12.7.13	CISM-VK 13|2	**CISM-Vertiefungskurs 2013|2**
12.7.13	CGEIT-VK 13|2	**CGEIT-Vertiefungskurs 2013|2**
12.7.13	CRISC-VK 13|2	**CRISC-Vertiefungskurs 2013|2**
16.8.13	GOV-KK	**IT-Governance -** erfolgreiche Einführung eines entsprechendes Frameworks
26.-27.8.13	LAB-IPS	**iPhone & iPad Security**
3.-4.9.13	LAB-WAB	**Web Application Security: Basics**
5.-6.9.13	LAB-WAA	**Web Application Security: Advanced**
www.isaca.ch		
17.-19.6.13	COB-FD	**ISACA COBIT 5 Foundation Zertifikat**
29.-31.7.13	COB-FD	**ISACA COBIT 5 Foundation Zertifikat**
23.9.-25.9.13	COB-FD	**ISACA COBIT 5 Foundation Zertifikat**
www.glenfis.ch		