ISACA Newsletter JANUARI09

newsletter

ISACA
Serving IT Governance Professionals
Switzerland Chapter

After Hours Seminar

Zürich • Dienstag, 27.1.2009 • 16:40 – 17:40
Controlling user authorizations across the enterprise; how can auditors contribute? ➜ Mehr auf Seite 5

Focus

Sieben Gründe für den Einsatz von Governance, Risk und Compliance (GRC) Software ➜ Mehr auf Seite 2

Inside

IT Professional Outlook 2010 ➜ Mehr auf Seite 3

Neuauflage "Berufe der ICT" und "Salärumfrage 2008" ➜ Mehr auf Seite 4

ISACA-Kurse und -Veranstaltungen

Beachten Sie das neue Kusangebot auf ➜ www.itacs.ch

Die aktuellsten Veranstaltungs- und Kursdaten ➜ Seite 6

Editorial

Draussen ist es kalt, sehr kalt um genau zu sein. Der Winter hat mit Schnee und Eis die Schweiz fest im Griff. Da sollte es vielen besonders leicht fallen, einen kühlen Kopf zu bewahren und der Finanzkrise zu trotzen.

Äussere Einflüsse, Krisen oder unternehmensinterne Initiativen sind häufig die Auslöser für Veränderungen. Die Notwendigkeit von Veränderungen erkennen Unternehmen meist frühzeitig. Massnahmen werden aber oft nur dann ergriffen, wenn die Krise bereits Spuren im Unternehmen hinterlassen hat. Je deutlicher diese Spuren erkennbar sind, desto mehr Aspekte stehen auf dem Prüfstand. Restrukturierungsprojekte im Bereich Strategie, Organisation und Technologie stehen auf der Tagesordung.

Wie schon vor einem Jahr, als der Skandal um die Société Générale die Medien bestimmte, werden auch im Rahmen der Finanzkrise bessere Kontrollsysteme und Instrumente zur effektiveren Risikosteuerung gefordert.

Der Berufstand der IT-Revision wird sich folglich auch in 2009 jeder Menge neuer und spannender Herausforderungen stellen müssen.

Da trifft es sich gut, dass das ISACA Switzerland Chapter dieses Jahr am 25. August sein 20 jähriges Jubiläum feiert und Sie recht herzlich dazu einlädt. Über die Details zur Veranstaltung werden wir in den nächsten Ausgaben des Newsletters noch umfassend informieren. Bis dahin ist es dann auch hoffentlich nicht mehr so kalt.

Freundliche Grüsse
Michael Kuss

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o ITACS Training AG
Stampfenbachstrasse 40
8006 Zürich
kurse@isaca.ch

Redaktionsschluss:
Ausgabe Februar 2009:
5. Februar 2009

Redaktion:
Michael Kuss
Färberstrasse 27
8008 Zürich
mkuss@gmx.net

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

CISA 30 Certified Information Systems Auditor
CISM Certified Information Security Manager
CGEIT Certified in the Governance of Enterprise IT

Focus

Sieben Gründe für den Einsatz von Governance, Risk und Compliance (GRC) Software

Autor: Michael Kuss

Unternehmen wie Approva, Control Software International, Fox Technologies, Oracle oder SAP sind weltweit die bekanntesten Anbieter von GRC Software. Die neueste Generation der Software verspricht Echtzeit-Compliance und eine Minimierung von Risiken aus dem Einsatz von ERP- und Finanzbuchhaltungssystemen.

Echtzeit-Compliance bedeutet, dass beispielsweise Benutzer eines ERP-Systems durch GRC Software daran gehindert werden können, bestimmte Transaktionen im System auszuführen, sofern diese gegen definierte Regeln verstossen. Dabei werden Vorschriften und Richtlinien in das ERP oder Finanzsystem integriert, um dauerhafte Compliance zu gewährleisten.

GRC Software im Allgemeinen bringt eine ganze Reihe von Vorteilen mit sich, die nicht nur das Herz eines IT-Revisors höher schlagen lassen. Es lassen sich nicht nur strategische Geschäftsrisiken in Echtzeit überwachen, sondern auch Prozesse nachhaltig verbessern und Compliance Kosten langfristig stark reduzieren.

1. Verbessertes Risikomanagement: Risiken können innerhalb der Software definiert und ausgewählt werden sowie mit vordefinierten oder selbsterstellten Kontrollen verbunden werden. Es ist in Echtzeit erkennbar, in welchem Prozess oder in welcher Unternehmenseinheit gerade Risiken aufgrund nicht anforderungsgerechter Handhabung oder Konfiguration des Systems bestehen.

2. Überwachung der Funktionstrennung: Ein Regelkatalog zur Funktionstrennung wird innerhalb der Software definiert. Die Einhaltung der Funktionstrennung kann ebenfalls in Echtzeit abgefragt werden.

3. Kontrolle von Geschäftsprozessen: Das interne Kontrollsystem (IKS) kann durch die Integration von Standard- oder selbsterstellten Kontrollen automatisiert werden.

4. Einhaltung von Handelsvorschriften: Der weltweite Handel erfordert die Einhaltung zahlreicher Einfuhr- und Ausfuhrvorschriften, welche ebenfalls durch GRC Software adressiert werden können und das manuelle Ausfüllen von Formularen automatisiert.

5. Einhaltung von Datenschutz- und Sicherheitsrichtlinien: Hier geht es darum, vertrauliche Informationen vor unerlaubtem Zugriff und Manipulation zu schützen. Änderungen an der Konfiguration und den Sicherheitsparametern eines Systems führen zu automatisierten Eskalationsverfahren, sofern Verstösse vorliegen.

6. Überwachung gesetzlicher Vorgaben zum Umweltschutz: Mit Hilfe dieser Funktionalität kann durch vordefinierte Prozesse auf neue Gesetzesanforderungen wie zum Beispiel „Corporate Social Responsibility“ oder die europäische Chemikaliengesetzgebung (REACH) reagiert werden.

7. Produkt Compliance: Neben den gesetzlichen Anforderungen zum IKS können weitere Vorschriften und Standards (FDA, REACH, BASEL II, ISO 20000 etc.) durch Regelkataloge integriert werden. So warnt eine GRC Software beispielsweise bei Rezepturen, die zu Produkten führen, welche aufgrund ihrer Zusammensetzung in bestimmten Ländern nicht verkauft werden dürfen, da gesetzliche Bestimmungen nicht eingehalten werden.

Inside

IT Professional Outlook 2010

Autor: Bruno Wiederkehr

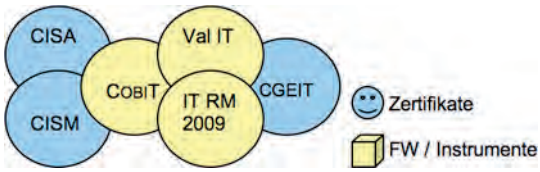
Mit Blick auf die zukünftige IT-Professionalität können aus der Gartner- und IDC-Studie folgende Aussagen entnommen werden:

- Die ideale Belegschaft ist auf Teamwork ausgerichtet mit nach aussen fokussiertem Kompetenzzentrum
- Steigender Bedarf an IT-Generalisten mit betriebswirtschaftlichem Verständnis
- Gute Zukunftsaussichten für System-Analysten und -Auditoren
- Zunahme der Kompetenzen im Bereich IT- und Informations-Sicherheit
- Wachsende Bedeutung der Compliance-Fähigkeit.

Daraus lässt sich ableiten, dass mit der Innovation im globalen Systemumfeld und der immer schnelleren Entwicklung in der Informations- und Kommunikations-Technologie die geforderten Fähigkeiten unverzichtbar sind, wenn man konkurrenzfähig bleiben will.

Umso grösser ist die Herausforderung in der gegenwärtigen Wirtschaftslage, welche den Einsatz von integrierten und effizienten Management-Instrumenten verlangt, wie z.B. ein effektives Risikomanagement in Abstimmung mit dem internen Kontrollsystem und dessen Einhaltung.

Dank der vorausschauenden Entwicklungen des IT Governance Institutes (ITGI) stehen sowohl international anerkannte Standards (CobiT Control Framework, ValIT Framework) als auch Ausbildungsmöglichkeiten und Zertifizierungen der ISACA zur Verfügung. Anfangs 2009 werden die bestehenden Standards durch das CobiT IT Risikomanagement-Framework (IT RM) als konsequente Weiterentwicklung ergänzt.



Anlässlich der AHS vom 25. November 2008 wurde auf die wesentlichen Inhalte des neuen CGEIT-Berufsbildes und die geplanten Zertifikatskurse in der Schweiz eingegangen und entsprechend diskutiert.

Aus der bereits erhaltenen Kursbroschüre können einerseits der Bedarf gegenüber den CISA- und CISM-Areas ausgewertet und andererseits die Auswahl in Bezug auf die geplanten CGEIT-Kurse im ersten Halbjahr (7 Kurstage ab 23.3.09) und im zweiten Halbjahr (13 Kurstage ab 8.07.09) getroffen werden. Die weltweit anerkannten Zertifikats-Prüfungen finden im Juni und Dezember 2009 statt. Seit der Ankündigung von CGEIT sind im ersten Jahr nach dem "Grandfathering"-Verfahren weltweit bereits über 1000 Personen zertifiziert worden. Dieses Verfahren wurde von ISACA bis 31. Dezember 2008 verlängert. Weitere Informationen zum CGEIT-Zertifikat sind unter ➜ **www.isaca.org/certification** ersichtlich.

Ausserdem unterstützt die ISACA mit "CobiT in Academia" den Wissenstransfer dieser Materie auf internationaler Ebene. Im Januar 2009 organisiert das ISACA Switzerland Chapter für die Verantwortlichen der Schweizer Bildungsinstitutionen (Uni, ETH, HF, FH etc.) den zweiten Erfahrungsaustausch zu diesem Thema.

Gerade in der zunehmend komplexeren Geschäftswelt ist es für Arbeitsgeber und -nehmer gleichermassen wichtig, über Know-how zu verfügen, damit neue Instrumente professionell und erfolgswirksam eingesetzt werden können. Um die Zukunftsperspektiven auszuloten und den Wissensvorsprung sicherstellen zu können, sollte diese Aus- und Weiterbildung rechtzeitig geplant werden.

Inside

Neuauflage "Berufe der ICT" und "Salärumfrage 2008"

Autor: Bruno Wiederkehr

Mit der Unterschrift von Bundesrätin Doris Leuthard und der Direktorin Dr. Ursula Renold (Bundesamt für Berufsbildung und Technologie) wurde im November 2008 die 7. stark überarbeitete Auflage "Berufe der ICT" (Informations- und Kommunikationstechnologie) angekündigt. Als Silber-Sponsor hat das ISACA Switzerland Chapter die Berufsbilder "ICT-Auditor und „ICT-Sicherheitsbeauftragter" wesentlich mitgeprägt. Ebenso wurden die Kernelemente von IT Governance mit CobiT als Integrator nebst weiteren "Best Practicies" u.a. ITIL, ISO, Six Sigma umfassend beschrieben. Mit Graphiken und Tabellen werden Zusammenhänge von Berufsbildern, Aufgaben, Kompetenzen, Ausbildungswegen bis hin zu Zertifikaten dargestellt.

Mit der neuen Ausgabe wird ein wertvoller Beitrag zur Strukturierung der sich in ständigem Wandel befindenden ICT Berufe geleistet. Die in regelmässigen Abständen erscheinende Publikation hat sich bereits in der Wirtschaft, bei den Personal- und Berufsberatern, Ausbildungsinstituten, Arbeitnehmern aber auch in der Revision (u.a. im Zusammenhang mit RACI-Chart) durchgesetzt.

Die aktualisierte Auflage überzeugt nebst der Präsentation der ICT-Berufsdefinitionen auch mit der darauf ausgerichteten Salärerhebung. Die Standardauswertung "Salärumfage 2008" kann auch via des unten aufgeführten Links bezogen werden.

Dank Mitwirkung der ISACA bei "Berufe der ICT"sind die Mitglieder berechtigt, ein persönliches Exemplar zum Sonderpreis von CHF 49.- zu beziehen. Das Buch konzentriert sich auf rund 40 relevante, teilweise neue Berufe der Informatik, Telekommunikation, Organisation/Betriebswirtschaft und Projektmanagement.

Weitere Informationen bezüglich Inhalt und Bezug sind unter ➜ **www.swissict.ch/shop/index.php** ersichtlich.

■

Lohnt sich IT-Governance auch für KMUs?

Im Rahmen einer Diplomarbeit am Institut für Informatik der Universität Zürich wird zurzeit untersucht, welche Aktivitäten der IT-Governance auch für KMU's sinnvoll und lohnenswert sind. Dazu soll mittels einer Befragung gezeigt werden, dass die Durchführung von bestimmten IT Governance Mechanismen auch bei KMU's zu Erfolgen beiträgt – und das Fehlen derselben zu Problemen und Misserfolgen führt.

Befinden Sie sich in einer Führungsposition eines schweizerischen Klein- oder Mittelbetriebes (insbesondere im Industriesektor) und sind Sie für die Führung der IT Ihres Unternehmens mitverantwortlich? Haben Sie Erfahrung in der Umsetzung von IT-Governance in Ihrem Betrieb?

Nehmen Sie an der Befragung teil und ermöglichen Sie damit ein aussagekräftiges Ergebnis dieser Arbeit! Weitere Angaben erhalten Sie per Email von c.landolt@access.uzh.ch oder finden Sie unter ➜ **http://www.ifi.uzh.ch/im/theses/diplomarbeit_itgovernance**

After Hours Seminar

Dienstag, 27.1.2009 • 16:40 – 17:40 • Zürich • Stampfenbachstrasse 40

Controlling user authorizations across the enterprise; how can auditors contribute?

Referent: Maarten Stultjens, in English

Access to information is generally seen as one of the most critical security leakages and from the end-user's perspective getting access is a frustrating process. Though everybody recognizes the problems as business problems, approaches are still driven by IT. How can we break out of this dilemma? What role can the auditor play?

- Organizations recognize the chaotic situation with regard to the user authorization administration
- For several reasons organizations want to improve authorization management: efficiency, control, compliance, business change
- Kuppinger Cole: "36% of all organizations are in the planning phase of role management implementations"
- The fussy and IT driven approach does not bring solutions nearer
- Gartner: "Identity management projects leave user authorizations hanging in the wind"
- Lessons can be learned from other administrations and processes
- Roles seem to be part of the answer, but there is a lot more to say
- How can organizations granularly re-gain control over user authorizations?
- Where can you start, what are realistic ambitions, how can you measure progress, how can you proceed?
- What is the role the auditor can play?
- Practical experiences will be shared based on BHOLD's 11 years support of European enterprises

Anmeldung für Mitglieder ➜ kurse@isaca.ch

by Bitterli Consulting
itacs training

Details und andere Kurse siehe unsere Homepage: ➜ www.itacs.ch

Avaloq-Einführung für IT-Revisoren/Sicherheitsbeauftragte
9.–13. März 2009
Avaloq verstehen als Grundlage für effiziente Prüfungen

Virus/Trojan/Backdoor Security Lab • 16.–18. März 2009
Kritische Betrachtung moderner Perimeterschutzmechanismen und deren Gefährdung durch mobile Technologien und aktuelle Malware

Von IT Governance bis IT Security Management – wirksamer Einsatz von CobiT 4.1 • 23.–25. Mätz 2009
Anwendung des internationalen Standards auf die wichtigsten Governance-Themen Security, Risk Management, Projekt Management, usw.

ITACS Training AG
Stampfenbachstr. 40
CH-8006 Zürich
Tel. +41 44 444 11 01
kurse@itacs.ch

ITACS Training ist der offizielle Ausbildungspartner des ISACA Switzerland Chapter **www.isaca.ch**

ISACA Serving IT Governance Professionals Switzerland Chapter

ISACA-Kurse und -Veranstaltungen

	Diese Übersicht enthält die aktuellsten Veranstaltungs- und Kursdaten. Details: ➜ www.isaca.ch
21.1.09 Manno (Lugano)	➜ **IT Governance, Outsourcing e Porfolio/Project Management**
27.1.09	➜ **ISACA After Hours Seminar** Controlling user authorizations across the enterprise; how can auditors contribute?
12.2.09 – 16.5.09 Genève	➜ **CISA Cours d'approfondissement 2009l1** Audit des systèmes d'information • Préparation à la certification internationale CISA
16.2.09 – 15.5.09 Genève	➜ **CISM Cours d'approfondissement 2009l1** Sécurité des systèmes d'information • Préparation à la certification internationale CISM
9.3.09 – 13.3.09	➜ **Avaloq-Einführung für IT-Revisoren/Sicherheitsbeauftragte** Bedienung des Avaloq Banking Systems. Vertiefung in Parametrisierung u.a. von Security-, Workflow- und Rule Engine
19.3.09 – 20.3.09	➜ **Leadership-Seminar für Revisoren und Sicherheitsbeauftragte** Verbesserung des persönlichen Kommunikationsverhaltens von Revisoren/Sicherheitsbeauftragten in kritischen Situationen
23.3.09 – 25.3.09	➜ **Von IT Governance bis IT Security Management – wirksamer Einsatz von CobiT 4.1** Praxisorientierte Anwendung von CobiT 4.1 für IT-Governance in ausgewählten Schwerpunktbereichen – mit dem Herausgeber des ersten deutschsprachigen CobiT-Buches
23.3.09 – 13.5.09	➜ **CGEIT Zertifikatskurs 09l1 (verkürzter Kurs für Prüfung im Juni 09)** Vertieftes theoretisches wie praktisches Fachwissen im breiten Feld von IT-Governance wie: strategische Ausrichtung, Wertschöpfung, Risikomanagement, Ressourcenmanagement und Leistungsmessung in der Informationstechnologie (IT). Intensive Vorbereitnug auf die von ISACA organisierte CGEIT-Prüfung.
26.–27.3.09	➜ **Prüfung und Berichterstattung bei Outsourcing-Providern** Standardisierte Prüfungen im Outsourcing-Umfeld – ein Kurs für Provider und deren Kunden (mit Provider-Gastreferat!)
30.3.09	➜ **ISMS gemäss ISO27001/2 implementieren und verbessern** Die wichtigsten Elemente eines ISMS kennen und in 30 klaren Schritten implementieren oder verbessern
	Wo nichts anderes vermerkt, finden die Veranstaltungen/Kurse in den Schulungsräumlichkeiten von ITACS Training AG, Stampfenbachstrasse 40 (5 Geh-Minuten vom Hauptbahnhof), 8006 Zürich, statt.

Weitere Kurs- und Veranstaltungsanbieter

➜ **RSSI 2009**	**RSSI 2009, Rencontre Suisse de la Sécurité Informatique** Membres ISACA bénéfices d'un tarif préférentiel	**17. 3. 2009** Four Seasons Hôtel des Bergues, Genève
➜ **www.vereon.ch/iks**	3. IKS Fachtagung Rabatt für ISACA-Mitglieder **Internes Kontrollsystem** Bewährtes aus dem Abschluss 2008 für das neue Geschäftsjahr	**24. + 25.3.2009** Hotel Courtyard by Marriott, Zürich Nord
➜ **www.hacking-lab.com**	**Swiss Cyber Storm** Security Event and Wargames	**18. + 19.4.2009** Aula Fachhochschule Rapperswil

IT Governance Institute