ISACA Newsletter MAI 2009

newsletter

ISACA 20 JAHRE ANS ANNI
Serving IT Governance Professionals
Switzerland Chapter

After Hours Seminar • Zürich

Zürich • Dienstag, 26. Mai 2009 • 16:40 – 17:40
Web 2.0: Hype or Threat?
Referent: Cyrill Brunschwiler ➜ **Weitere Informationen**

After Hours Seminar • Lausanne

Lausanne • Mercredi 27 mai 2009 • 14:00 – 17:15
Accès à l'information: rôles et responsabilités
➜ **Plus Informations**

Focus

Risk Management Process in PMBOK
➜ **Mehr auf Seite 4**

ISACA-Kurse und -Veranstaltungen

Die aktuellsten Veranstaltungs- und Kursdaten ➜ **Seite 6**

ISACA Switzerland Chapter • Jubiläumsveranstaltung
25. August 2009 • Zürich

Impressum

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

Redaktionsschluss
Nr. JUN|2009:
5. Juni 2009

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

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

Editorial

IT-Governance: bekannt und unbekannt

Wohl sämtliche unserer Mitglieder kennen den Begriff «IT-Governance» und haben von CobiT, dem Standard für IT-Governance, mindestens einmal gehört.

Erstaunlich wie erschreckend zugleich ist aber die Tatsache, dass viele Informatikleiter (CIO) den Begriff zwar kennen, aber selber gemäss eigenen Aussagen keine IT-Governance betreiben (23 von 25 Teilnehmern einer CIO-Konferenz im letzten Jahr). Damit beweisen sie vor allem, dass sie den Begriff «IT-Governance» nicht verstanden haben: die andere Alternative wäre nämlich noch viel erschreckender: dass sie als CIO ihre Informatik nicht im Griff haben – und dies möchte ich ihnen ja nicht unterstellen…

Was meines Erachtens IT-Governance vom früher gebräuchlichen Begriff IT-Management unterscheidet, ist die umfassende und aufeinander abgestimmte Steuerung der IT in den fünf Disziplinen strategische Ausrichtung der IT, Schaffen von IT-Werten, IT-Risikomanagement, Management der IT-Ressourcen und Management der IT-(Dienst)Leistung. Die Betonung liegt auf «umfassend und aufeinander abgestimmt». Auch wenn die oben aufgeführten fünf Schwerpunktgebiete von IT-Governance wohl in den meisten (grösseren) Unternehmen mehr oder weniger gut betrieben werden, sind sie in den seltensten Fällen konsequent aufeinander abgestimmt. Und wenn hinsichtlich Abstimmung und Koordination bereits Anstrengungen mit mehr oder weniger Erfolg geleistet wurden, so beschränkt sich dies in vielen Fällen auf die Erstellung von SLAs und Rahmenvereinbarungen – zugegebenermassen sehr wichtig, aber für sich isoliert betrachtet einfach nicht zielführend.

Was ich persönlich beim Aufbau unseres neuen CGEIT-Zertifikatkurses (Certified in the Governance of Enterprise IT) realisiert habe, sind vor allem die folgenden Punkte: Wie auch in anderen Bereichen ist die korrekte Definition und einheitliche Verwendung von Schlüsselbegriffen (wie Governance, Management, Führung, usw.) in einem Unternehmen von zentraler Bedeutung. Widersprüchliche Auslegungen führen ansonsten mindestens zu Missverständnissen und damit zu Leerläufen und erhöhten Kosten wenn nicht sogar zum Chaos. ➜ **Fortsetzung**

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

Exclusif en Suisse Romande ! A ne pas manquer.

Mercredi 27 mai 2009 • 14:00 – 17:15 • Hôtel Alpha Palmier • Lausanne

Accès à l'information: rôles et responsabilités

Public cible

Cet atelier d'une demi-journée s'adresse aux décideurs, propriétaires et détenteurs d'informations, aux responsables métiers et responsables de la gestion des systèmes d'information, risk managers et auditeurs internes ou externes, débutants ou confirmés. Il s'adresse également aux responsables informatiques et les spécialistes sécurité souhaitant mieux cerner l'impact risque sur les processus d'exploitation et de maintenance des systèmes d'information.

Objectifs

Les principaux objectifs de ce séminaire visent à

- Analyser les risques liés à l'accès à l'information
- Mettre en œuvre un système d'accès à l'information
- Auditer l'adéquation du système d'information et des processus implémentés, maîtrise les risques opérationnels
- Développer les contacts entres les spécialistes et auditeurs des systèmes d'information et de sécurité et les auditeurs non spécialisés

But de l'atelier

La gestion de l'accès à l'information tout au long de son cycle de vie ne peut être réduite à une simple opération exclusivement technique. Alors, pour mieux comprendre les tenants et les aboutissants de cette problématique, cet atelier abordera de manière pragmatique les trois volets de l'analyse des risques initiale, de la mise en œuvre des mesures de protection et finalement de l'audit relatifs au contrôle d'accès à l'information.

Quelle que soit sa forme ou son support, qu'elle soit commerciale, opérationnelle ou comptable, l'information est une ressource stratégique pour l'activité d'un organisme et nécessite à ce titre une protection appropriée. La maîtrise de l'accès à ce capital est donc un maillon essentiel du système de gestion de la sécurité de l'information et un garant du système de contrôle interne.

➜ **Plus informations**

Programme

14h00 • Mot de bienvenue

14h15 • L'analyse des risques

Animé par Monsieur Olivier Luxereau,
NetExpert SA

Comment appréhender les besoins de protection des informations au long de leur cycle de vie et apprécier les risques d'une manière méthodologique et pragmatique? Quels sont les principes de sécurité et les bonnes pratiques de protection à mettre en oeuvre et quelles sont les normes, lois et réglementations à respecter?

15h00 • Mise en œuvre d'une solution biométrique d'authentification forte pour l'accès aux données sensibles

Animé par Monsieur Sylvain Maret,
MARET Consulting

Retour d'expérience dans le cadre de la mise en œuvre d'un projet de gestion des identités au sein d'un établissement bancaire. Choix technologique? Difficultés rencontrées ? concept et design, mise en œuvre, formation, processus humain. Un Retour d'expérience pragmatique.

15h45 • La demi-heure de réseautage - Apéritif

16h15 • Maîtrise des risques opérationnels

Animé par Monsieur Anthony Walsh,
Deloitte Suisse

Aujourd'hui, l'acheminement des flux de données devient de plus en plus opaque et les concepts et rôles du propriétaire de données incompris.

En conséquence, les impacts d'une perte ou d'un vol de données sont mal mesurés et les responsabilités loin d'être établies. Les défis tel que réglementaires, de la vulnérabilité de l'environnement IT, et de continuité des services de manière intégrée, doivent être adressés sur une méthodologie établie et une compréhension approfondie des risques au sens large.

17h15 • Fin de l'événement

L'atelier du risque, de l'audit et de la sécurité

CLUSIS

ISACA 20 JAHRE ANS ANNI
Serving IT Governance Professionals
Switzerland Chapter

SVIR ASAI ASRI SIIA
SVIR Schweizerischer Verband für Interne Revision
ASAI Association suisse d'audit interne
ASRI Associazione svizzera di revisione interna
SIIA Swiss Institute of Internal Auditing

Editorial (Fortsetzung)

Die inneren Zusammenhänge der fünf IT-Governance Schwerpunktthemen (Focus Areas) bestehen auf allen Ebenen der Führung, Organisationsstrukturen und Prozessen; und sie müssen aktiv gemanagt werden. CobiT – gerade in den beiden Teilen «Val IT» sowie den «Control Practice Statements» – enthält eine unermessliche Fülle an hochgradig kompetenten Praktiken für IT-Governance in einem Detaillierungsgrad, wie er für die konkrete Umsetzung in die Praxis zweckdienlich ist. Es lohnt sich, diese Teile genauer anzuschauen!

Was sich besonders lohnt, ist sich systematisch mit der Thematik auseinanderzusetzen – unabhängig davon, ob man jetzt als (zukünftiger) IT-Manager in einer Führungsposition arbeitet (oder mindestens in diese Richtung schielt) oder als IT-Risikomanager, IT Service Management Spezialist oder etwa IT-Revisor. Neben einem Selbststudium z.B. der zahlreichen Unterlagen des IT Governance Institute (www.itgi.org) eignen sich insbesondere auch klar strukturierte Aus- und Weiterbildungen anerkannter Institutionen.

Ausbildung lohnt sich – packen wir's an!

Peter R. Bitterli, CISA, CISM
ISACA Switzerland Chapter
verantwortlich für Aus- und Weiterbildung ■

Stay Competitive – Stand Out

As an ISACA member, you can succeed in challenging times. ISACA has responded to the global economy with a new web section packed with resources: new CobiT® discounts, a free online eLibrary coming soon, an upgraded Career Centre with a huge number of job postings, easier access to FREE CPEs and convincing Return-On-Investment information to present to your employer to demonstrate the value of ISACA and ensure the success of your enterprise. Visit ➜ **www.isaca.org/standout** now to learn how ISACA can help you to stay competitive. ■

New ISACA Certification!

Urs Fischer will be chair of the task force who will be developing ISACA's new certification program aimed at serving IT professionals who identify and manage risks through proper IT controls and comply with regulations which impact IS. It has tentatively been named CISREM (Certified Information Systems Risk and Exposure Manager), but that may change as the credential is developed. It will take around 18 months to develop the program. Further information will follow when made available. ■

Focus

Risk Management Process in PMBOK

Author: Andres Maurer

Risk Management in a project differs slightly from operational risk management mainly due to the temporary nature of a project. PMBOK does not define new risk management methods and framework, instead it uses existing expert knowledge and concentrates only on the process.

As the project environment can be subjected to large changes, PMBOK has defined Risk Management as its own knowledge area. The Risk Management approach can be divided into 3 phases: Plan, Identify & Analyze, Monitoring & Controlling. These phases are defined by 6 processes.

11.1 Plan Risk Management	11.2 Identify Risks	11.3 Perform Qualitative Risk Analysis
Inputs • Project scope statement • Cost management plan • Schedule management plan • Communications management plan • Enterprise environmental factors • Organizational process assets **Tools** • Planning meetings and analysis **Outputs** • Risk management plan (Methodology, Roles & Responsibilities, Budgeting, Timing, Risk Categories, Risk Breakdown Structure, Stakeholders' Tolerances, etc.)	**Inputs** • Risk management plan • Activity cost estimates • Activity duration estimate • Scope baseline • Stakeholder register • Cost management plan • Schedule management plan • Quality management plan • Project documents • Enterprise environmental factors • Organizational process assets **Tools** • Documentation reviews • Information gathering techniques • Checklist analysis • Assumption analysis • Diagramming techniques • SWOT analysis • Expert judgement **Outputs** • Risk register	**Inputs** • Risk register • Risk management plan • Project scope statement • Organizational process assets **Tools** • Risk register • Risk management plan • Project scope statement • Organizational process assets • Risk probability and impact assessment • Probability and impact matrix • Risk data quality assessment • Risk categorization • Risk urgency assessment • Expert judgement **Outputs** • Risk register (updated)

11.4 Perform Quantitative Risk Analysis	11.5 Plan Risk Response	11.6 Monitor and Control Risks
Inputs • Risk register • Risk management plan • Cost management plan • Schedule management plan • Organizational process assets **Tools** • Data gathering and representation techniques • Quantitative risk analysis and modelling techniques • Expert judgement **Outputs** • Risk register (updated)	**Inputs** • Risk register • Risk management plan **Tools** • Strategies for negative risks or threats • Strategies for positive risks or opportunities • Contingent response strategies • Expert judgement **Outputs** • Risk register (updated) • Risk-related contract decisions • Project management plan (updated) • Project documents (updated)	**Inputs** • Risk register • Project management plan • Work performance information • Performance report **Tools** • Risk reassessment • Risk audits • Variance and trend analysis • Technical performance measurement • Reserve analysis • Status meetings **Outputs** Risk register (updated) • Organizational process assets (updated) • Change Requests • Project management plan (updated) • Project documents (updated)

Although PMBOK defines certain tools and methods, this is neither a complete list nor are they mandatory. This is a mere example listing, it is left up to expert judgement and hence the actual best practice in this subject matter. Therefore it is not forbidden to use existing risk management framework to manage project risks as well, this is considered under "Organizational process assets».

11.1 Plan Risk Management

This process describes how risk will be managed in the project. The resulting risk management plan uses inputs from other planning documents like project scope statement, time management plan, cost management plan and communications management plan as well as considering organization and environmental factors. Besides the risk categories, a risk breakdown structure may also be created if the project complexity and size mandates it.

11.2 Identify Risks

Once the risk management plan is defined, the next step is to identify the possible risks. This is done through by analyzing the project documentation, typical risk analysis methods as well as using the expert judgement of the stakeholders.

11.3 Perform Qualitative Risk Analysis

Creating a risk register is only the beginning, the next step is to analyze the risks qualitatively so that the risks can be prioritized. This is done mainly by assessing risk probability and impact, but also the urgency and other factors based on expert judgement.

11.4 Perform Quantitative Risk Analysis

Although PMBOK defines qualitative and quantitative analysis as separate steps, they can often done simultaneously. The goal of this process is to define a numerical value to the risk. This process may often be difficult and tedious to accomplish, therefore PMBOK states that only the risks with high priority need be quantified.

➜ Fortsetzung

Focus

Risk Management Process in PMBOK (Fortsetzung)

11.5 Plan Risk Response

Once the risks are identified and prioritized, the next step is to determine the risk owner as well as the response to risks themselves. PMBOK explicitly view risk as both negative (threats) and positive (opportunities). The response are categorized accordingly - (Avoid/Transfer/Mitigate/Accept) and (Exploit/Share/Enhance/Accept). Contingency responses may also defined if deemed necessary.

11.6 Monitor and Control Risks

Monitoring and controlling risks is an activity that is done continually within the Monitoring and controlling process group. This means that not only existing risks are monitored and reassessed, but also that potentially new risks are constantly being identified as soon as a change occurs.

Typical project risks are:

External Unpredictable
- Regulatory (unanticipated government intervention)
- Natural hazards
- Postulated events (vandalism, sabotage)
- Indirect events (environmental, social)
- Lack of completion

External Predictable
- Market risks
- Operational
- Environmental impacts
- Social impacts
- Currency fluctuation
- Inflation
- Taxation

Internal non-technical
- Management deficiencies
- Schedule overruns
- Cost overruns
- Cash flow
- Loss of potential

Technical
- Changes in technology
- Performance
- Design
- Size and/or complexity of project

Legal
- License
- Patent rights
- Contractual obligations
- Outsider Legal Actions
- Insider Legal Actions
- Force Majeure

Last but not least, PMBOK differentiates the reserves into 2 types: contingency reserves for “known unknowns» and management reserves for “unknown unknowns» (which is not part of the project budget).

At project closure, all project risks should be accounted for. The residual risks that are associated with operations will be handed over to the corresponding organizational entity.

References:

A guide to the project management body of knowledge PMBOK – 4th Edition,
Project Management Institute,
ISBN: 978-1-933890-51-7
Project and program risk management – A guide to managing project risks & opportunities,
R. Max Wideman (Editor), Project Management Institute,
ISBN 13: 978-1-880410-06-6

After Hours Seminar

Dienstag, 26. Mai 2009 • 16:40 – 17:40 • Zürich • Stampfenbachstrasse 40

Web 2.0: Hype or Threat? • Referent: Cyrill Brunschwiler

Anmeldung für Mitglieder ➜ sekretariat@isaca.ch

ISACA-Kurse und -Veranstaltungen

	IT Security Training Week (All Courses in English !)
8.–9.6.09	➜ **Introduction to Information Security** **(Days 1+2 of the IT Security Training Week)** Highly compact introduction to information security
10.6.09	➜ **Understanding and Securing the Wireless Network** **(Day 3 of the IT Security Training Week)** Effectively secure wireless networks
11.6.09	➜ **Using ISO27002 to Audit Mobile Technology** **(Day 4 of the IT Security Training Week)** Effectively audit mobile technology issues
1.6.09	➜ **Understanding and Auditing Windows Active Directory** **(Day 5 of the IT Security Training Week)** Effectively audit Windows Active Directory
17. – 19.6.09	➜ **ISACA CobiT 4.1 Foundation Certificate** • **Definitive Durchführung** • **Anmeldung noch möglich!** Offizieller ISACA-Zertifikatskurs mit international standardisiertem Curriculum
22. – 26.6.09	➜ **Hacking Defense Training** Wirksame Verteidigung von Hacking-Angriffen mit anspruchsvollen Fallstudien – wahlweise drei bis fünf intensive Tage (nur) für Fortgeschrittene!
29.6.09	➜ **IT-Risikomanagement wirksam umsetzen** (Kompaktkurs) Risikoanalysen für IT-Systeme, IT-Projekte und IT-Anwendungen; Kompaktkurs
1. – 3.7.09	➜ **Praxisgerechte Anwendung von ISO 27001 und ISO 27002** Ein Muss für Sicherheitsverantwortliche, Risikomanager und alle anderen, welche den Zwillingsstandard erfolgreich in ihrem Unternehmen umsetzen wollen – mit unzähligen Praxistipps
6.7. – 17.11.09	➜ **CISA-Vertiefungskurs 2009|2** • **Definitive Durchführung** • **➜ Jetzt anmelden!**
7.7. – 18.11.09	➜ **CISM-Vertiefungskurs 2009|2** • **Definitive Durchführung** • **➜ Jetzt anmelden!**
8.7. – 19.11.09	➜ **CGEIT-Vertiefungskurs 2009|2** Einführungstag: Mittwoch, 8. Juli 2009

Wo nichts anderes vermerkt, finden die Veranstaltungen/Kurse in den Schulungsräumlichkeiten von ITA-CS Training AG, Stampfenbachstrasse 40 (5 Geh-Minuten vom Hauptbahnhof), 8006 Zürich, statt.

Weitere Kurs- und Veranstaltungsanbieter

➜ **www.isss.ch**	**ISSS Security Lunch Zürich • ➜ Details und Anmeldung** «IT Bedrohungen 2009: Prognosen und Realität»	**27.5.2009** Zürich
➜ **www.treu-hand-kammer.ch**	**Kammer-Seminar: IT-Migration aus Sicht des Prüfers** **➜ Anmeldung noch möglich**	**16.6.2009** Hotel Bellevue Pallace Bern
➜ **www.isss.ch**	**ISSS Zürcher Tagung:** «Digital Rights Management (DRM): the good, the bad and the ugly?» ISACA-Mitglieder erhalten Fr. 50.00 Rabatt auf die Teilnahmegebühr	**17.6.2009** Widder Hotel Zürich
➜ **www.isss.ch**	**12. ISSS Berner Tagung für Informationssicherheit** **«ICT-Riskmanagement»**	**24.11.2009** Hotel Bellevue Pallace Bern