ISACA Newsletter SEPTEMBER 2009

ISACA 20 JAHRE ANS ANNI
Serving IT Governance Professionals
Switzerland Chapter

newsletter

After Hours Seminar

Zürich • Dienstag, 29.9.2009 • 16:40 – 17:40
IT Governance im Zusammenspiel mit dem IT Audit
* Vergleich von bekannten IT Governance Frameworks
* Rolle des IT Audits in der IT Governance
* Zusammenspiel des IT Audits und der IT Governance
* Prüfung der IT Governance durch das IT Audit
* Beispiel des Zusammenspiels bei der AXA Winterthur

Fokus

Records Management
Wieso das Bewältigen der Informationsflut beim Vernichten beginnt

➜ Mehr auf Seite 2

Inside

Risiken der Informatik bewirtschaften ➜ Mehr auf Seite 3

ISACA-Kurse und -Veranstaltungen

Die aktuellsten Veranstaltungs- und Kursdaten ➜ Seite 4

Neue, interessante Konditionen und Rabatte für Kurs-Teilnehmende derselben Firma: Der 2. Teilnehmer erhält 30% Rabatt; alle weiteren 50%

Impressum

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

Redaktionsschluss:
5. Oktober 2009

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

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

Editorial

Durant les dernières semaines, des entretiens ont été menés avec les membres de la Direction de l'ISACA Suisse et les responsables des groupes d'intérêt existants afin de définir leur futur et leur place au sein de notre association.

En ce basant sur ces discussions, la Direction de l'ISACA Suisse a défini les objectifs suivants:
- Obtenir une vue d'ensemble des activités effectuées par les groupes d'intérêt;
- Mettre à jour et améliorer le format ainsi que le contenu des pages Internet concernant les divers groupes d'intérêt;
- Faciliter le partage d'information entre les responsables des groupes d'intérêt, les membres, la Direction de notre association ainsi que les non-membres ;
- Soutenir dans leur démarche les membres de l'ISACA ayant la volonté de créer un groupe d'intérêt sur un thème d'actualité.

A ce jour, cinq groupes d'intérêt ont vu le jour concernant des sujets très divers comme la gouvernance informatique, le logiciel SAP, Computer Forensic ou la plateforme bancaire AVALOQ.

Il est prévu dans les prochaines semaines, avec l'aide des responsables des groupes d'intérêt, de mettre à jour notre site Internet avec une information beaucoup plus détaillée afin que nos membres puissent comprendre les thèmes généraux, mais surtout afin de susciter l'intérêt d'autres membres à participer à un groupe d'intérêt.

Les informations que nous mettrons à disposition de nos membres sur notre site Internet sont les suivantes ; le responsable du groupe d'intérêt, l'objectif dudit groupe, le nombre de participants et les participants cibles, les prochaines dates des réunions ainsi que les thèmes qui seront discutés. Des liens vers des articles et toute autre information intéressante pour la communauté de l'ISACA Suisse devront également être disponibles. Cette information sera mise-à-jour régulièrement sur notre site Internet afin d'offrir à nos membres une vue la plus actualisée possible des activités de nos groupes.

De plus, nous encourageons nos membres qui aimeraient créer un groupe d'intérêt concernant un sujet ayant trait à l'audit, ou la sécurité informatique à s'annoncer afin de discuter des possibilités de soutien offertes par notre association.

Nous espérons que l'atteinte des objectifs fixés par notre Direction permettra aux groupes d'intérêt de trouver un nouvel écho dans notre communauté, d'apporter une valeur ajoutée pour nos membres ainsi que d'accroitre la visibilité de l'ISACA Suisse.

Yan Borboën

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

ISACA 20 JAHRE ANS ANNI
Serving IT Governance Professionals
Switzerland Chapter

Fokus

Records Management

Wieso das Bewältigen der Informationsflut beim Vernichten beginnt

Autor: Dr. Bruno Wildhaber

Die zunehmende Bedeutung der elektronischen Dokumentenbearbeitung und die Virtualisierung verschiedenster Geschäftsprozesse haben in den letzten Jahren dazu geführt, dass sich viele Unternehmen dem Thema **Dokumenten-/Informationsmanagement** (**IM**) spätestens jetzt umfassend stellen müssen. Die in den letzten Jahren entstandenen informationstechnischen Fachdomänen **Dokumentenmanagement**, Content-Management oder umfassend **«Enterprise Content Management»** (ECM) bieten den Kunden eine Vielfalt an Angeboten zur Bewältigung dieser Herausforderung. Die Frage ist nur: In welchem Mass sind die Unternehmen in der Lage, Marktangebote zu verarbeiten, bzw. welche Voraussetzungen müssen gegeben sein, damit sich technische Lösungen auch entsprechend nutzbringend einsetzen lassen?

Auf Grund der Datenzunahme ist davon auszugehen, dass Unternehmen zukünftig nicht in der Lage sein werden, alle Daten zu speichern, weil die Zunahme der Dateigrössen den verfügbaren Speicher mehr als kompensiert – oder anders gesagt, **Vernichten** gehört in Zukunft zu den **Kernkompetenzen** im Rahmen des Information Managements!

Die zentrale Herausforderung liegt darin, dass die Daten im Unternehmen meist in sogenannten «Stovepipes» (**Silos**) angelegt sind. Der Zugriff erfolgt meist applikationsbezogen und nicht nutzenorientiert (**Applikationsdatensicht**). Der Zugriff auf einen aufschlussreichen Informationsbestand (**Horizontale Informationssicht**) ist deshalb oftmals nicht möglich:

Abb.: Vertikale (Applikationsdatensicht) vs. horizontale Informationssicht

Records Management (RM) befasst sich mit der Behandlung und Verarbeitung von kritischen Geschäftsinformationen. Im Vordergrund steht das Ziel, die rechtlichen und betrieblichen Anforderungen möglichst wirtschaftlich erfüllen zu können. Die Fokussierung auf den Themenbereich Records Management bedeutet nichts anderes, als dass die Verwaltung von geschäftskritischen Daten unter rechtlichen und ökonomischen Gesichtspunkten integriert betrachtet wird.

Sind die Daten aus unterschiedlichen Quellen einmal erfasst, dann müssen sie **klassiert** werden, ein Datenbestand ohne Klassierung ist wie eine Sondermülldeponie ohne Inventar – eine tickende Zeitbombe. Oder anders gesagt: Die **Vernichtung** der Datenbestände ist nur dann möglich, wenn bereits zu Beginn des Lebenszyklusses die entsprechende Organisation aufgebaut wurde, **nachträgliches Organisieren ist unmöglich**. Deshalb scheitern auch sogenannt «chaotische» Speichersysteme, auch mit der stärksten **Search-Engine** ist es unmöglich, kontextbezogene Daten, die vielleicht 10 oder noch mehr Jahre früher entstanden sind, vollständig und lückenlos zu identifizieren. Dies ist aber z.B. eine zentrale Anforderung, wenn es darum geht, Daten für Gerichtsfälle herauszugeben (**Edition**). Die Qualität eines RM Systems misst sich deshalb über die Fähigkeit, bestimmte Daten innerhalb einer vordefinierten Zeit zu finden (**Suchen & Finden**).

Wo Licht ist, ist auch Schatten: Durch die horizontale Erschliessung der Daten werden plötzlich **Datenschutzfragen** aktuell, an welche vorher niemand gedacht hatte. Daten können damit zur Bedrohung für das Unternehmen und seine Stakeholder werden. Daten nach Ablauf der Aufbewahrungsfristen zu vernichten, ist damit ein zentrales Anliegen des Records Managements.

Zur Identifikation der aufbewahrungspflichtigen Daten braucht es mehr als rechtliche Vorschriften. Obwohl RM ein zentrales Element zur Erreichung

➜ Fortsetzung auf Seite 3

Inside

Risiken der Informatik bewirtschaften

Neuerscheinung der 2. Auflage lieferbar

Mit der weltweiten Finanzkrise fordern Gesetzgeber ein professionelles Risiko- und Kontroll-Verhalten. Aufgrund der regulativen Bestimmungen wurden die «Best-Practices»-Standards laufend angepasst und teilweise in die Unternehmen integriert. In diesem Lehrmittel wurden diese Neuerungen für das Geschäfts- und IT-Umfeld im Hinblick auf den Aufbau eines unternehmensweiten Risikomanagement-Systems sowie dessen praktischen Umsetzung berücksichtigt.

Die Kurzbeschreibung, das vollständige Inhaltsverzeichnis und 33 Graphiken (PDF) sind unter der Hompage www.compendio.ch via Fachbücher/Suchen mit Eingabe Namen des Autors, Bruno Wiederkehr, ersichtlich.

Ein unternehmensweites Risikomanagement gehört zu den grundlegenden Voraussetzungen für eine zweckmässige und wirtschaftliche Unternehmensführung nach dem Governance-Prinzip. Demzufolge empfehlen die Autoren allen am Risikomanagement-Prozess Beteiligten dieses Lehrmittel.

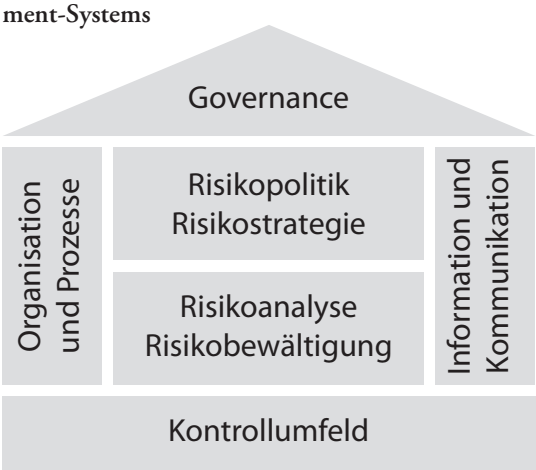
Autoren: Bruno Wiederkehr und Johannes Scheuring
Compendio Bildungsmedien AG, 8050 Zürich

Zielgruppe: Aus- und Weiterbildung, Erwachsenenbildung, Selbststudium, von der Praxis für die Praxis

Bestellung: www.compendio.ch • Telefon: +41 1 368 21 11
Mail: postfach@compendio.ch • Telefax: +41 1 368 21 70

Erscheinungsjahr 2003 • 2. Auflagen 2009
ISBN 978-3-7155-9416-3 • Preis CHF 39.90

Kernprozesse eines umfassenden Risikomanagement-Systems



Aktualisierung:
Es wurden verschiedene Anpassungen und Ergänzungen vorgenommen, die wegen gesetzlicher Änderungen im OR, DSG, URG, FMG und UWG sowie wegen Änderungen am CobiT-Framework notwendig waren. Namentlich wurden folgende Inhalte des bisherigen Lehrmittels aktualisiert:

- Nützliche Literatur zum Thema
- Kapitel 1.4 Schweizer Regulative
- Kapitel 2.2 Internes Kontrollsystem (IKS)
- Kapitel 2.3 Kontrollmodelle
- Kapitel 8 Risikobewältigung
- Anhang: CobiT-Kontrollmodell im Überblick
- Glossar und Stichwortverzeichnis

Fortsetzung "Records Management"

der **Compliance**-Vorgaben darstellt, geht der Nutzen für das Unternehmen weit darüber hinaus. Die Records-Management-Aktivitäten sollen nicht nur den rechtlichen Vorgaben folgen, sondern es muss eine Umsetzung angestrebt werden, die sich an den Grundsätzen der IT - Governance orientiert. Dies bedeutet eine Abkehr von der rein rechtlichen Orientierung zu einer mehr betriebswirtschaftlichen, beziehungsweise **strategischen Orientierung** des Records Management.

Wildhaber Consulting und das Kompetenzzentrum Records Management führen am 11. November 2009 die 3. Records Management Konferenz in Volketswil bei Zürich durch.

ISACA-Mitglieder profitieren von einem reduzierten Konferenzbeitrag in der Höhe von CHF 490.- (anstelle 550.-).

Weiterführende Information und die Anmeldung: www.wildhaber.com/konferenz/prog_rm2009.pdf

Code für ISACA Mitglieder:
ISACRM09 (im Anmeldeformular anzugeben)
Als weiterführende Literatur empfehlen wir:
Praxisleitfaden Records Management
J. Beglinger, B. Lehmann, P. Neuenschwander, B. Wildhaber
2. Auflage, Zürich 2008, ISBN 978-3-033-01801-3

ISACA-Kurse und -Veranstaltungen

Diese Übersicht enthält die aktuellsten Veranstaltungs- und Kursdaten. Details: ➜ www.isaca.ch

29.9.09	➜ **ISACA After Hours Seminar** • ➜ **sekretariat@isaca.ch**
20.10.09	➜ **Design und Prüfung von anwendungsabhängigen Kontrollen (IKS)** Wirtschaftliches Design und wirksame Überprüfung von anwendungsabhängigen Kontrollen; ein praxisorientierter Vorgehensansatz
28.10.–29.10.09	➜ **Networking & Penetration Testing** • Security Labor-Kurs mit Compass Security
30.10.09	➜ **Wireless Security – Bypassing the Firewall** • Security Labor-Kurs mit Compass Security
2.–3.11.09	➜ **Web Applications: Basics** • Security Labor-Kurs mit Compass Security
4.–5.11.09	➜ **Web 2.0: Web Applications: Advanced** • Security Labor-Kurs mit Compass Security
5.–18.11.09	➜ **CISM-Prüfungsvorbereitungskurs 2009|2** Die gezielte Vorbereitung auf die internationale CISM-Prüfung
6.11.09	➜ **SBC – Terminal Server Security** • Security Labor-Kurs mit Compass Security
10.–11.11.09	➜ **Windows Forensics – Spurensuche** • Security Labor-Kurs mit Compass Security
12.–13.11.09	➜ **Malware Analysis – Reverse Engineering** • Security Labor-Kurs mit Compass Security
16.11.09	➜ **Einführung in Enterprise Risk Management • (Kompaktkurs)** Sicherheit durch proaktive Handhabung der Risiken
20.11.09	➜ **ISMS gemäss ISO 27001/2 implementieren und verbessern (Kompaktkurs)** Ein ISMS in 30 effizienten Schritten implementieren oder verbessern
23.–24.11.09	➜ **Risikomanagement im Projektumfeld** Rasche Identifikation, Bewertung und Management typischer Projektrisiken
25.–27.11.09	➜ **Projektmanagement für IT-Sicherheitsfachkräfte und IT-Revisoren** Erwerben Sie sich das notwendige Rüstzeug, um Softwareentwicklungsprojekte optimal zu begleiten und zu prüfen
30.11.–2.12.09	➜ **Avaloq-Reporterstellung für Revisoren/Sicherheitsbeauftragte** Effiziente Erstellung von verlässlichen Reports aus dem Avaloq Banking System
30.11.09	➜ **Einführung in das Interne Kontrollsystem (IKS-Kompaktkurs)** Konzeption, Betrieb und Prüfung des IKS

Weitere Kurs- und Veranstaltungsanbieter

➜ **www.grb-romand.ch**	**Quatrième séance de travail; «Comment bien intégrer l'audit des processus informatiques selon CobiT dans une démarche d'audit ?»** En collaboration acec l'ISACA Romande	**1.10.2009** Fédération des Entreprises Ro-
➜ **www.csnc.ch**	**Hacking-Lab • Compass Event; «Löchrig wie ein Schweizer Käse?"** ISACA-Mitgliedern erhalten 20% Rabatt (CHF 200.- statt CHF 250.-).	**15.10.2009** Aula der FH Rapperswil
➜ **www.wildhaber.com**	**3. Records Management Konferenz** ISACA Mitglieder profitieren von einem reduzierten Konferenzbeitrag	**11.11.2009** Volketswil
➜ **www.isss.ch**	**12. ISSS Berner Tagung für Informationssicherheit «ICT Risk Management: Aufwand und Nutzen»** ISACA-Mitgliedern erhalten CHF 90.– Rabatt	**26.11.2009** Hotel Bellevue Bern