Trust in, and value from, information systems

Switzerland Chapter

Nr. 03 | September 2015 | www.isaca.ch

NEWSLETTER

**After Hours Seminare**
Relaunch der After Hours Seminare in Zürich und Bern. **Seite 99**

**Information Governance**
Information Governance ist – den Kühlschrank im Griff zu haben. **Seite 100**

**ISACA-Training**
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 103**

# Relaunch ISACA After Hours Seminare

Das ISACA Switzerland Chapter organisiert seit 2003 unter dem Titel «ISACA After Hours Seminare» (kurz AHS) zirka einstündige Vorträge zu aktuellen Themen. Die zur Vorabendzeit stattfindenden Anlässe erfreuen sich seit über zehn Jahren grosser Beliebtheit. Thematisch decken die AHS die Haupttätigkeitsgebiete der ISACA, Information Governance, Information Riskmanagement, Information Audit and Assurance sowie Information Security ab.

Von Thomas Streckeisen

Nach einem Unterbruch im 2014 konnten die AHS am 3. Februar 2015 wieder neu lanciert werden. Sie finden vorerst sechs Mal jährlich, jeweils am ersten Dienstag der «geraden» Monate statt. Neu ist, dass die Referate im April und Oktober in Bern stattfinden. Dies um den Kolleginnen und Kollegen aus der Region Bern und Westschweiz eine regelmässige Teilnahme an den AHS zu vereinfachen. Die übrigen Referate finden wie gewohnt in Zürich statt.

Die Teilnahme an den AHS ist für alle Interessierten offen, aus organisatorischen Gründen ist eine Anmeldung erforderlich. Die Ausschreibung erfolgt jeweils spätestens zwei Wochen vor dem Anlass in den offiziellen Publikationsorganen des ISACA Switzerland Chapter: Im Internet (www.isaca.ch) und den per eMail versandten eNews (Informationen für die Mitglieder). Alle Termine des laufenden Jahres sind unter www.isaca.ch/after-hours.html ersichtlich.

Der Start in die Neuauflage der AHS verlief sehr erfreulich. So konnten wir im Februar und Juni in Zürich je zwischen 40 und 50 interessierte Teilnehmer begrüssen. In Bern fanden rund 20 Personen Zeit die AHS zu besuchen.

Am 3. Februar 2015 durften wir uns von Dr. Bruce Nikkel über Trends und Veränderungen im Bereich der Cyber-Kriminalität informieren lassen. Mit dem auf Englisch gehaltenen Referat ist uns der Einstand gelungen. Auf das Referat folgte eine intensive und angeregte Diskussion mit dem Referenten, die dann beim obligaten Apéro fortgesetzt wurde. Das Networking ist ein unverzichtbares Element der AHS und dauert oft bis in die frühen Abendstunden.

Die Fortsetzung fand am 14. April 2015 in Bern mit einem spannenden Einblick in die Arbeit des Nachrichtendienstes des Bundes statt. Herr Philipp Kronig zeigte uns das Spannungsfeld in der Arbeit des Nachrichtendienstes zwischen

Freiheit und Sicherheit auf. Am 2. Juni 2015 führte uns Herr Dr. Peter W. Pfefferli vom Forensischen Institut Zürich in die Welt der modernen Kriminaltechnik ein. In seinem Referat gelang es Herrn Pfefferli auf eindrückliche und verständliche Art und Weise die Arbeit der Forensiker in der Realität Zürichs darzulegen und gleichzeitig immer wieder die Brücken zur Fiktion der CSI-TV-Serien und zur Arbeit der IT Prüfer zu schlagen.

In den kommenden Referate werden folgende Themen behandelt: Cyber Resilience – wie mache ich mein Unternehmen fit für die Zukunft am 18. August 2015 in Zürich, Information Governance am 6. Oktober 2015 in Bern und PCI-DDS Credit Card Payment Security Standards am 1. Dezember 2015 in Zürich. Der Vorstand des ISACA Switzerland Chapters freut sich auf eine rege Teilnahme.

Falls Sie Interesse haben selbst ein Referat in diesem Rahmen zu halten oder Ideen für spannende Themen einbringen können, freut sich der Vorstand über Ihren Input. Einfach eine Mail an ahs@isaca.ch senden.

## DER AUTOR

Thomas Streckeisen, CISA, ist im Vorstand des ISACA Switzerland Chapters verantwortlich für die Koordination der After Hours Seminare. Er ist seit über 20 Jahren in verschiedenen Funktionen im landwirtschaftlichen Genossenschaftswesen tätig. Seit 2006 ist er für die internen IT Prüfungen der fenaco Genossenschaft verantwortlich.

# Information Governance – Grundvoraussetzung für die Digitalisierung

Digitalisierung ist für Organisationen nur dann erfolgreich, wenn Information aktiv gesteuert wird. Information Governance geht über das heutige IT-Management hinaus und verlangt nach neuen Kompetenzen.

Von Dr. iur. Bruno Wildhaber, CIP / CISA / CGEIT / CISM

Was haben unsere Daten mit einem WG-Kühlschrank gemein?

Beginnen wir mit einem Vergleich, nämlich dem Kühlschrank einer WG:

- Niemand weiss, was drin ist
- Niemand fühlt sich für dessen Pflege zuständig
- Niemand weiss, ob die Esswaren noch geniessbar sind
- Niemand weiss, ob derjenige, dem die Esswaren gehören, überhaupt noch in der WG wohnt
- Niemand weiss wie lange die Esswaren schon im Kühlschrank sind
- Niemand getraut sich, Esswaren wegzuwerfen

Dummerweise verfügen jedoch die meisten Unternehmen nicht nur über einen Kühlschrank, sondern im übertragenen Sinn über eine Hundertschaft von Kühlschränken, deren Standort sie meist nicht einmal kennen. Der Kühlschrank steht hier als Synonym für eine der wichtigsten Unternehmensressourcen unserer Zeit – unseren Informationen (in Form von Daten).

Landauf – landab wird die Digitalisierung als wichtigstes Mittel für den Erfolg der Unternehmen gepredigt. Dabei geht vergessen, dass der wichtigste Rohstoff, nämlich die Daten, meist in einem bemitleidenswerten Zustand sind. Social Media Protagonisten predigen die Dringlichkeit, sich endlich in die Welt der digitalen Unverbindlichkeit zu begeben. Solche Initiativen nützen den Unternehmen jedoch

nur dann, wenn die neu gewonnenen Daten tatsächlich auch genutzt werden können.

Unseren Daten geht's folglich meist wie dem Gemüse im WG-Kühlschrank: Sie werden mehr schlecht als recht betreut und keiner kümmert sich um sie. Ausser wenn der Hunger überhand nimmt, dann erinnert man sich an diesen wichtigsten Rohstoff. Doch dann wird oftmals die Frage zu spät gestellt: Wie geniessbar sind eigentlich unsere Daten?

## Information als Strategischer Erfolgsfaktor

Der Umgang mit der Ressource Information bedarf der Einbettung in die Strategie des Unternehmens. Die Zeiten sind vorbei, wo man das Bearbeiten der Daten der IT-Abteilung überlassen konnte. Wir reden ja heute bewusst nicht mehr von Daten, sondern vor allem von Information. Doch gute Information gewinnen wir nur dann, wenn unsere Basis, d.h. die Daten, verlässlich und aktuell sind. Nebst dem Gewinn von Marktanteilen durch die Nutzung solcher Informationen werden unsere Unternehmen je länger je mehr auch vom Gesetzgeber unter regulatorischen Druck gesetzt. Obwohl die Pflicht zur Aufbewahrung der Geschäftskorrespondenz im Schweizerischen Handelsrecht seit dem 1.1.13 wegfällt, heisst dies noch lange nicht, dass man auf diese Daten verzichten kann! Man muss keine Bank sein, um zu wissen, dass verschiedenste Stellen mittlerweile Informationen aus den Unternehmen benötigen und diese auch konsequent einfordern. Die Beweisführung mit elektronischen Daten ist zwar noch nicht alltäglich, doch es ist absehbar, dass in wenigen Jahren auch die Gerichte vollumfänglich auf den elektronischen Schatz der Unternehmen zugreifen wollen.

## Old IT meets Social Media

Verwaltungsräte tun deshalb gut daran, sich im Rahmen ihrer Tätigkeit nicht nur um die «sexy» Social Media Agenda zu kümmern. Sie sollten sich generell darum kümmern, wie reif das Unternehmen im Umgang mit Information ist. Wer hat noch die Übersicht bzw. Kontrolle wenn im Unternehmen jede Mitarbeiterin innert kürzester Zeit einen eigenen Server aufsetzen oder eine eigene Applikation mieten kann? Wer kontrolliert, dass Ihre wertvollen Kundendaten nicht in ihrem CRM sondern in einer x-beliebigen Cloud gehostet werden? Und ja, der Serverstandort Schweiz garantiert keine Sicherheit, denn kein Datendieb wird sich die Mühe nehmen, einen klassischen Einbruch in einen Datensafe zu versuchen – da gibt es wesentlich erfolgversprechendere Mittel.

Wir verfügen mittlerweile über einige Erfahrung im Archivieren von Daten aus traditionellen Applikationen. Schon schwieriger wird der Umgang mit E-Mails. Nur ein Teil der Unternehmen verfügt heute bereits über eine abgestimmte E-Mail Strategie, die sowohl den Anforderungen der Aufbewahrung, der Beweissicherung aber auch dem Datenschutz Rechnung trägt.

## Was ist Information Governance?

Information Governance ist eine Führungsaufgabe, welche analog der Corporate Governance funktionieren sollte. Der Umgang mit Information muss stufenge-

**Ihr Kühlschrank = Ihre Daten?**

recht adressiert werden, indem die jeweiligen Verantwortlichen klare Aufgaben und Zielvorgaben erhalten. Dies beginnt beim VR und setzt sich bis auf die operative Ebene fort. Das Instrumentarium basiert auf verschiedenen Methoden und Frameworks, von der Unternehmensstrategie bis zur Informationssicherheit oder anderen Spezialdisziplinen. Als wichtige Grundlage der Information Governance dient u.a. eine Daten (Informations) – Landkarte welche die Grundlage sowohl für die werterzeugenden wie auch risikobasierten Aktivitäten enthält. Die Informationslandkarte zeigt, wo Informationen gehalten und wie sie genutzt werden. Es handelt sich dabei um eine Kombination von betrieblicher und IT-architektonischer Sicht, die in den Unternehmen meist nicht vorhanden ist.

## Wie ergänzen sich IT und Information Governance?

Information Governance bewegt sich viel näher am Geschäft und der Unternehmensstrategie und muss per se nichts mit IT zu tun haben. Auch Unternehmen, welche keine eigene IT betreiben, benötigen Information Governance als Führungsdisziplin. Andererseits basiert eine gute Information Governance in einem Unternehmen mit klassischer IT auf einer soliden IT-Governance. Art und Umfang der Information Governance sind vor allem strategieabhängig und deshalb nicht generell beschreibbar.

Wir haben in unserem neuen Leitfaden IG (Buchtipp) eine Methode beschrieben, wie man Information Governance Frameworks aufbauen kann. Die MATRIO® Methode zielt darauf ab, sowohl einen kurzfristigen Nutzen zu erzielen wie auch die Langfristigkeit nicht aus dem Auge zu verlieren.

## Wie bringt man Ordnung in den Kühlschrank?

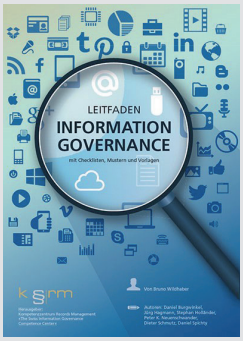
Zuerst ist es notwendig, dass sie die Bedeutung der Ressource der Information in Ihrem Unternehmen bewerten. Handelt es sich dabei um eine grundlegende Ressource für ihre zentralen Geschäftsmodelle, dann wird es unumgänglich sein, dass sie das Thema zur Chefsache machen. Dies beginnt bei der Aufnahme des Agendapunktes IG im Verwaltungsrat und sollte bei der Strategieentwicklung auf Geschäftsleitungsebene fortgeführt werden. In Organisationen geht es in erster Linie darum, die zentralen Wertschöpfungsketten zu identifizieren und zu analysieren, welche Daten wie verwendet und eingesetzt werden. Es ist manchmal erstaunlich, wie viele Medienbrüche in den Unternehmen noch existieren. Identifizieren Sie die wichtigsten Pain Points und überlegen Sie wie Sie kurzfristige Lösungen erzielen können. Oftmals reicht es, organisatorische Massnahmen zu treffen. Es gibt wichtige Themen, die Sie nicht ignorieren sollten (wir nennen sie «Red Flags»), dazu gehört z.B. der Umgang mit Stammdaten oder die geschäftsorientierte Klassifizierung der Information. Auch eine wichtige Rolle spielt der rechtliche Rahmen: Ist die Organisation nur in der Schweiz tätig oder müssen internationale Abhängigkeiten berücksichtigt werden (z.B. bezüglich Aufbewahrungsfristen)? Diese «Red Flags» sollten bei der Erarbeitung der IG identifiziert und beobachtet werden.

So wie man den Kühlschrank nicht nur mit technischen Mitteln im Griff hat, so muss auch für die Information Governance ein vielfältiges Instrumentarium eingesetzt werden. Organisatorische Massnahmen, Technik und Recht müssen sich zu einem sinnvollen Ganzen finden, wobei die Zielsetzung letztlich immer von oben kommen muss. Trotzdem dürfen solche Vorhaben den guten Willen und die Initiative von unten nicht ignorieren. Wenn jemand den Kühlschrank aufräumen will, dann soll er das tun dürfen, ohne dass es dazu eine zwanzigseitige Policy braucht! Information Governance ist eine Initiative im Interesse aller Beteiligten, denn der richtige Umgang mit Information wird in Zukunft über das Schicksal von Unternehmen entscheiden.

Information Governance ist – den Kühlschrank im Griff zu haben!

## INFORMATION GOVERNANCE – EIN LEITFADEN FÜR DIE PRAXIS

Eine Gruppe von erfahrenen Praktikern um Bruno Wildhaber hat einen Leitfaden erstellt, welcher die Grundlagen der Information Governance, deren Bedeutung und v.a. auch deren Umsetzung ausführlich beschreibt. Nebst den rechtlichen Grundlagen enthält der Leitfaden Case Studies aus verschiedenen Branchen. Ebenfalls enthalten eine neue Methode zur einfachen Entwicklung von Governance Modellen (MATRIO®) sowie eine umfassende Methodenübersicht und deren Bewertung. Wer sich mit dem Thema auseinandersetzen möchte, findet Information zu vielen Aspekten der Information Governance. Das Buch richtet sich sowohl an Verwaltungsgräte wie auch und Geschäftsleitungsmitglieder sowie Compliance-Experten und Projektleiter sowie die Revision. Das Buch wird durch eine Community Plattform ergänzt (www.informationgovernance.ch).




**ISBN:** 3-9524430-0-2 Erhältlich im Buchhandel; in Kürze auch als eBook bei Amazon.
**Herausgeberin:** Kompetenzzentrum Records Management, Zollikon, 2015, www.informationgovernance.ch

## ZUM AUTOR:

Bruno Wildhaber ist freier Berater und Geschäftsführer des Kompetenzzentrums Records Management und blickt auf eine langjährige Praxis in der IT Industrie zurück. Interdisziplinarität ist seine Kernkompetenz, als ehemaliger Präsident der ISACA Schweiz ist es ihm ein Anliegen, die unternehmerische Sichtweise auch in Compliance orientierten Initiativen hervorzubringen.

Das KRM berät Unternehmen bei der Umsetzung von Information Governance und Records Management Initiativen.

Informationen des Verbands

# Informationssicherheit und Information Governance

Während ich diesen kurzen Beitrag schreibe, herrschen seit Tagen Temperaturen über 30 Grad – zu heiss, um zu denken, und zu heiss, um zu arbeiten. Darum wäre jetzt so ein Kühlschrank nicht nur eine mutige Verknüpfung zum Artikel von Bruno Wildhaber sondern eine echte Erleichterung. Und dank seiner Vernetzung würde er nicht nur die Getränke nachbestellen sondern könnte gleich noch eine Verbindung zu Kühlschränken mit anderen CISOs herstellen, die alle ähnliche Probleme zu lösen haben wie ich.

Eine Vernetzung findet auch statt in unseren CISM-Vertiefungskursen – Sicherheitsbeauftragte und andere Fachspezialisten aus unterschiedlichsten Umgebungen arbeiten gemeinsam an den oft ziemlich schwierigen Gruppenarbeiten, lösen eine Foto-Fallstudie oder ärgern sich über die ach so komischen Multiple-Choice Fragen, so wie sie an den internationalen CISM-Prüfungen auftauchen.

Im CISM Review Manual werden die verschiedenen Aktivitäten eines Sicherheitsbeauftragten klar beschrieben: Die wichtigsten Grundlagen sind im ersten Domain des CISM-Berufsbildes zusammengefasst: «Governance der Informationssicherheit». Wie auch im erwähnten Artikel erläutert, geht es hier um die Strategie, um ein geordnetes Framework, um klare Vorgaben und Richtlinien, um die Verpflichtung der Führungskräfte oder zum Beispiel um Rollen und Verantwortlichkeiten. Analog enthalten die anderen drei Kapitel die wichtigsten Kenntnisse zum Risikomanagement, zur Entwicklung eines Informationssicherheits-Programmes oder zum eigentlichen Sicherheits-Ereignismanagement.

Wer mehr über das spannende Berufsbild erfahren möchte, kann sich einerseits durch das CISM Review Manual quälen. Besser ist es definitiv im CISM-Kurs des ISACA Switzerland Chapter – unser Vertiefungskurs beginnt jeweils im Februar mit einem strukturierten Selbststudium. Danach folgt im heissen Juni/Juli der Präsenzunterricht in Zürich. Im doch wieder etwas kühleren Herbst findet dann das auch separat buchbare CISM-Prüfungstraining statt, gefolgt von einer weiteren individuellen Vorbereitung mit einem elektronischen Fragekatalog auf die internationale Zertifikatsprüfung anfangs Dezember – dann braucht es den Kühlschrank höchstens noch wegen seiner Vernetzung.

Der durch ITACS Training AG im Auftrag des ISACA Switzerland Chapter durchgeführte Kurs vermittelt und vertieft theoretisches wie praktisches Fachwissen im breiten Feld von Risikomanagement und internen Kontrollen, bereitet aber auch intensiv auf die von ISACA organisierte CISM-Prüfung vor. Weitere Details zum CISM-Zertifikat und zur entsprechenden Ausbildung finden Sie auf www.isaca.ch

## ISACA-TRAINING

| Datum | Code | Hauptthema – Kurstitel |
|---|---|---|
| **www.isaca.ch** | | |
| 01.10. – 03.10.2015 | CGEIT-PV2 | CGEIT Prüfungsvorbereitung 2015 |
| 08.10. – 10.10.2015 | CRISC-PV-2 | CRISC Prüfungsvorbereitung 2015 |
| 14.10. – 17.10.2015 | CISA-PV-2 | CISA Prüfungsvorbereitung 2015 |
| 22.10. – 24.10.2015 | CISM-PV-2 | CISM Prüfungsvorbereitung 2015 |
| **www.glenfis.ch** | | |
| 14.9. – 16.9.2015 | P-COA3 | COBIT 5 Assessor |
| 28.9. – 30.9.2015 | P-COF3 | COBIT5 Foundation |
| 12.10. – 14.10.2015 | P-CGEIT4 | CGEIT Prüfungsvorbereitung |
| **www.ardantic.ch** | | |
| 26. – 30.10.2015 | | CISA – Module 2 – 5 jours |
| 3. – 6.11.2015 | | CISM – Module 2 – 4 jours |


## IMPRESSUM ISACA NEWS

ISACA

**Herausgeber, Redaktion:** ISACA Switzerland Chapter
**Adresse:** Sekretariat ISACA Switzerland Chapter, c/o BDO AG, Biberiststrasse 16, 4501 Solothurn
**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