Trust in, and value from, information systems

Nr. 04 | Dezember 2016 | www.isaca.ch

Switzerland Chapter NEWSLETTER

Business- und IT-Audit
Gemeinsame Konferenz von SVIR und ISACA im Januar 2017 in Zürich: «Cybersecurity – Ein Fall für Revisoren?» Seite 63

ISACA-Training
ISACA Zertifizierungen und aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder Seite 66

After Hours Seminare
Der regelmässige Treffpunkt für Fachspezialisten zu Governance, Risk, Security und Audit. Seite 67

Umfassende Risikobetrachtung durch Business- und IT-Audit

Eine umfassende Risikobetrachtung der ganzen Unternehmung kann gefördert werden durch verbesserte Zusammenarbeit und Kommunikation zwischen Business- und IT-Audit. Im Januar 2017 findet eine gemeinsame Konferenz von SVIR und ISACA statt.

Von Olga Valek und Peter Marti

In den letzten Jahren hat sich die Informatik in den meisten Firmen und Branchen von einer technischen Backoffice-Dienstleistung zu einem treibenden und kritischen Träger der Business Prozesse entwickelt. Die Verzahnung zwischen den Businessprozessen und der Informatik hat sich so stark intensiviert, dass jedes technische Husten in der Informatik sich oft unmittelbar mit Schüttelanfällen im Business bemerkbar macht. Ein Stillstand der Informatik könnte gar Krisen auslösen und das Überleben der Unternehmung in Frage stellen. Daher ist es konsequent und nachvollziehbar, dass Risikobetrachtungen vermehrt unternehmensweit erfolgen und neben den wertschöpfenden Business-Prozessen auch die unterstützenden Prozesse und Systeme der Informatik adäquat mitberücksichtigt werden.

In grösseren Organisationen wird das unternehmensinterne Audit häufig in zwei dedizierten Units aufgebaut: als Business- wie auch als IT-Audit. Beide Teams haben einen entsprechenden Fokus und Expertise, aber auch ihre Grenzen. Das IT-Audit versteht sich zwar in den technischen Prozessen und Systemen souverän zu bewegen. Das Business-Audit hat seinerseits eine hohe Kompetenz der Geschäftsabläufe und Wertschöpfungskette. Aber Beiden ist die Expertise des anderen Teams verwehrt.

Darum ist es umso wichtiger, dass die beiden Einheiten einen aktiven

Informationsaustausch leben, sich über den eigenen Gartenzaun hinauslehnen und sensibilisiert sind für Wechselwirkung zwischen den IT und Business Prozessen:

- Welche Business-Prozesse werden mit welchen IT-Applikationen umgesetzt?
- In welchen IT-Systemen sind hochsensible Geschäftsinformationen gespeichert?
- Wie sind die Abhängigkeiten wischen IT- und Business-Controls?
- Wie sieht die Beziehung einer Business-Rolle zu den darunter liegenden Applikations-User aus?

Integrated Audit

Unter dem Begriff ‚Integrated Audit' werden verschiedene Formen der Zusammenarbeit dieser beiden Audit-Units diskutiert und wie die unterschiedlichen Risk-Frameworks miteinander in Bezug gesetzt werden können (zB Mapping zwischen dem COSO-Würfel und dem COBIT-Modell). Letztendlich bleibt aber die Wichtigkeit einer aktiv gelebten Kommunikation zwischen IT-Audit und Business-Audit. Damit wird die Sensibilisierung zum anderen Audit-Team gestärkt. Konkrete Informationen zur vertieften Analyse können bei Bedarf weiter gereicht oder bei gemeinsam geplanten Audits die Risikobeurteilung wesentlich erhöht werden.

Auditverbände in der Schweiz

In der Schweiz werden Business- und IT-Audit von zwei unterschiedlichen Verbänden gefördert und unterstützt: SVIR (Schweizerischer Verband für Revision) und ISACA (Information Systems Audit and Control Association). Diese beiden Verbände sorgen gemäss ihrem Kernauftrag dafür, dass das Business- wie auch IT-Audit in der Schweiz thematisiert, optimal gestärkt und aktiv mit Schulungen gefördert wird.

SVIR - ISACA Konferenz

Nach einer Ruhepause von fast zwei Jahren laden SVIR und ISACA wieder zu einer gemeinsamen Konferenz in Zürich ein.

EINLADUNG

ISACA I SVIR Fachtagung

19. Januar 2017 in Zürich

«Cybersecurity – ein Fall für Revisoren?»

Chancen der Digitalisierung – das Flüstern der Dinge
Thomas Ribi, NZZ

Strategy and implication of regulation and digital
Dr. Daniel Diemers, PwC Strategyand (Switzerland) GmbH

Echtzeitkampf gegen Hacker
Dr. Lukas Ruf, Consecom AG

Prüfung von Cyber Security Readiness
Dr. Peter Weiss, Swiss Re

Aufbau einer Infrastruktur zur Sicherstellung von Cybersecurity bei Swissgrid
Reto Amsler, Swissgrid AG

IT-Grundschutz versus Cybersecurity
Luc Pelfini, BDO

Versicherbarkeit von Cyberrisiken
Dr. Carin Gantenbein, Zurich Insurance Group

Bitte melden Sie sich direkt auf www.isaca.ch bis spätestens am 20.Dezember 2016 an. Die Teilnehmerzahl ist beschränkt.

Switzerland "Wir fördern Good Corporate Governance."

IIA in der Schweiz

Cyber Risks stellen nicht nur ein Schlagwort der aktuellen Zeit dar, sondern gehören in der Kategorie der technologischen Risiken gemäss dem WEF-Report 2016 zu den grössten globalen Risiken. Als Schweizer Vertretung (Schweizerischer Verband für Interne Revision – **SVIR** resp. **IIA Switzerland)** des internationalen Dachverbandes Institute of Internal Auditors **(IIA)** mit Sitz in Florida, USA sind wir generell daran interessiert, dass alle Unternehmen resp. Organisationen, privat sowie öffentlich, in der Schweiz und in Liechtenstein alle Arten von Risiken ganzheitlich überwachen und ein wirksames Risk Management aufweisen, welches regelmässig vom Internal Audit überprüft wird. Die Gründung des IIA geht auf das Jahr 1941 zurück und zählt etwa 190'000 Mitglieder aus 170 Ländern. Der SVIR wurde 1980 gegründet

und zählt rund 2500 Mitglieder aus sämtlichen Branchen.

Die SVIR-Mitglieder resp. Internen Revisoren arbeiten primär mit dem vom IIA erlassenen Standardwerk IPPF (Internationale Standards der Berufspraxis). Das Internal Audit ist sehr oft diejenige Stelle in Unternehmen und Organisationen, welches bezüglich Risiken und deren Management den grössten Überblick hat und deshalb via Verwaltungsrat resp. Audit Committee einen substanziellen Beitrag zur Erhaltung/Erhöhung des Unternehmenswertes leisten kann. Dies stärkt den Berufsstand des Internal Audit und führt zu einer besseren **Corporate Governance.**

Direkt unterstützen wir Interne Revisoren resp. deren Abteilungen durch entsprechende Aus- und Weiterbildungen (zu aktuellen Themen) sowie Zertifizierungen **(CIA, CCSA, CFSA, CGAP, CRMA),** beurteilen deren Tätigkeit durch **External Quality Assessments** und vermitteln ihnen Zugang zu **Fachdokumentationen** sowie entsprechendem **(internationalen) Netzwerk.** Die jährliche nationale **SVIR-Konferenz** ist in der Regel die grösste Plattform für den vielfältigen Austausch. Am 21./22. September 2017 findet an ihrer Stelle erstmals die entsprechende **Europäische Konferenz der Internen Revisoren (ECIIA)** in der Schweiz, in Basel statt.

ISACA

Die **Information Systems Audit and Control Association** (ISACA) ist eine weltweite Verbindung von Fachleuten, die sich mit Sicherheit, Kontrolle, Revision und Management von Informationssystemen befassen; sie wurde bereits 1969 gegründet. Die Dachorganisation hat über 200 Chapter in ca. 80 Ländern – mit insgesamt rund 140'000 Mitgliedern aus 180 Ländern. Heute ist ISACA zusammen mit dem IT Governance Institute der Knowledge-Provider für IT Enterprise Governance, Information Systems Audit, Information Security und IT Risk Management. Die ISACA setzt sich in professioneller Art mit allen Entwicklungen in diesen Themenbereichen auseinander, organisiert globale Konferenzen und macht ihre diesbezüglichen Erkenntnisse interessierten Kreisen weltweit zugänglich. Zu den bekanntesten Produkten gehören die international anerkannten Frameworks COBIT®, Val IT™ und Risk IT – und seit ein paar Jahren auch auf «Cybersecurity» spezialisierte Standards.

ISACA Trust in, and value from, information systems Switzerland Chapter

Governance, Sicherheit und Audit von Informationssystemen

Das **ISACA Switzerland Chapter** wurde 1988 als Verein gegründet. Es richtet sich ebenso an Vertreter der internen und externen Revision wie an Spezialisten, welche sich mit Fragen der Informationssicherheit und der Qualitätskontrolle beschäftigen. Die rund 1›500 Mitglieder kommen aus den verschiedensten Bereichen, vom Rechnungswesen über die Beratung, die Revision bis hin zur Informationstechnologie – sowie aus verschiedensten Hierarchiestufen der Unternehmen.

Neben verschiedensten Schulungen als Vorbereitung auf die globalen Zertifikatsprüfungen **CISA, CISM, CGEIT** und **CRISC** (und neu auch **CSX)** organisiert das ISACA Switzerland Chapter seit 2003 unter dem Titel «ISACA After Hours Seminare» (AHS) zirka einstündige Vorträge zu aktuellen Themen. Thematisch decken die AHS die Haupttätigkeitsgebiete der ISACA, IT Enterprise Governance, IS Audit, Information Security und Riskmanagement ab.

DIE AUTOREN

Dr. Olga Valek, lic. oec. HSG, CIA befasst sich seit über 20 Jahren in verschiedenen internationalen Funktionen mit den Themen Internal Audit, Risk Management, Corporate Governance sowie dem ganzheitlichen Management. Nun ist sie beim SVIR für die fachliche Weiterentwicklung und Quality Assurance zuständig.

Peter Marti, CISA, im Vorstand des ISACA Switzerland Chapters. Seit 18 Jahren in der Informatik in verschiedensten operativen und strategischen Funktionen. Heute interner IT-Auditor bei der Bank Julius Baer.

IMPRESSUM ISACA NEWS

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

Aus- und Weiterbildung

ISACA Zertifizierungen – global anerkannte und preisgekrönte Zertifizierungen bei unseren Ausbildungspartnern (siehe unten für Kursdaten und -orte):

CISA – Certified Information Systems Auditor – ist für Spezialisten im Bereich IS (Information System) Audit, Kontrollsysteme und Sicherheit gemacht. Mit über 125'000 weltweiten Zertifizierungen seit Entstehung, sind davon heute 2'800 zertifizierte Personen als CEO, CFO oder äquivalente C-Level Positionen tätig.

CISM – Certified Information Security Manager – ist für Manager im Bereich Informationssicherheit gestaltet. Mit über 32'000 weltweiten Zertifizierungen seit Entstehung, sind davon heute 7'500 zertifizierte Personen als Security Director oder -Manager tätig. 3'500 zertifizierte Personen arbeiten als IT Director oder -Manager.

CGEIT – Certified in the Governance of Enterprise IT – ist für Spezialisten in IT Governance konzipiert. Mit über 7'000 weltweiten Zertifizierungen seit Entstehung, sind davon heute 1'400 zertifizierte Personen als IT Director, -Manager oder Consultant tätig.

CRISC – Certified in Risk and Information Systems Control – ist für Spezialisten für Risiko-Kontrollen und Informationsrisiko-Management vorgesehen. Mit über 20'000 weltweiten Zertifizierungen seit Entstehung, sind davon heute 2'400 zertifzierte Personen als CEO, CFO, CISO, CIO oder äquivalente C-Level Positionen tätig.

Neben den bekannten vier Zertifizierungen gibt es neu auch die Möglichkeit, praktische Prüfungen und entsprechende Zertifizierungen im Bereich Cyber-Security zu erlangen. ISACA hat dazu **«Cybersecurity Nexus»** lanciert, um neben der CISM Zertifizierung entsprechend praktische Weiterbildungen anzubieten.

ISACA-TRAINING

Datum	Hauptthema – Kurstitel
1.2.*; 12.-29.06.2017	CISA Vertiefungskurs, garantierte Durchführung: 10 Tage
11.-14.10.2017	CISA Repetitionsblock / Prüfungstraining: 4 Tage
1.2.*; 12.-29.06.2017	CISM Vertiefungskurs, garantierte Durchführung: 10 Tage
19.-21.10.2017	CISM Repetitionsblock / Prüfungstraining: 3 Tage
1.2.*; 12.-29.06.2017	CRISC Vertiefungskurs, garantierte Durchführung: 9 Tage
05.-07.10.2017	CRISC Repetitionsblock / Prüfungstraining: 3 Tage
1.2.*; 12.-29.06.2017	CGEIT Vertiefungskurs: 9 Tage
28.-30.09.2017	Repetitionsblock / Prüfungstraining CGEIT: 3 Tage
www.itacs.ch / * Strukturiertes Selbststudium; Selbststudium ab 01.02.2017	
14.-17.03.2017	CISA 4-day exam preparation course (Module 2) (E/F)
02.-05.05.2017	CISA 4-day exam preparation course (Module 2) (E/F)
22.-24.03.2017	CISM 3-day exam preparation course (Module 2) (E/F)
10.-12.05.2017	CISM 3-day exam preparation course (Module 2) (E/F)
29.-31.03.2017	CGEIT 3-day exam preparation course (Module 2) (E/F)
17.-19.05.2017	CGEIT 3-day exam preparation course (Module 2) (E/F)
29.-31.03.2017	CRISC 3-day exam preparation course (Module 2) (E/F)
17.-19.05.2017	CRISC 3-day exam preparation course (Module 2) (E/F)
www.actagis.ch	
03.-05.04.2017 und 08.05.2017*	CGEIT, 3 Tage Prüfungsvorbereitung P-CGEIT4
20.-22.03.2017	COBIT5 Foundation, 3 Tage, P-COF3
17.-19.07.2017	COBIT5 Foundation, 3 Tage, P-COF4
03.-05.04.2017	COBIT5 Implementation, 3 Tage, P-COI3
18.-20.04.2017	COBIT5 Assessor, 3 Tage, P-COA3
22.-24.05.2017	Implementation of NIST Cybersecurity Framework with COBIT5, 3 days, P-CON3
16.-18.01.2017	Cybersecurity Fundamentals on the basis of NIST, 3 days, P-CSFU3
10.-12.04.2017	Cybersecurity Fundamentals on the basis of NIST, 3 days, P-CSFU4
www.glenfis.ch / * Vorbereitung Juni-Prüfung 2017	

Informationen des Verbands

ISACA After Hours Seminare

Reservieren Sie sich die nächsten Termine: Die After Hours Seminar des ISACA Switzerland Chapters sind ein beliebter Treffpunkt für Fachspezialisten aus den Bereichen Information Governance, Information Risk Management, Information Security und Information Audit/Assurance. Rund 40 bis 50 Personen besuchen regelmässig diese Anlässe um sich über aktuelle Themen zu informieren und Kontakte zu pflegen. Die nächsten Termine und Themen sind:

7. Februar 2017, 16:40 Uhr in Zürich

Thema: Management Systeme: Handhabung vereinfachen und Wirkung steigern

Modelle bilden die Strukturen der Organisation ab: die Aufbauorganisation, die Funktionen und Skillprofile, die Prozesse und deren Rollen. Management Systeme verwenden diese Modelle, um die angestrebte Wirklichkeit nach Innen und Aussen vermittelbar wie auch überprüfbar zu gestalten. Um die Nützlichkeit der verwendeten Modelle zu verbessern kommt dem konsistenten Aufbau und der konsistenten Verknüpfung aller relevanten Modelle untereinander ein hoher Stellenwert zu. Im Vortrag wird eine Methode vorgestellt, mit der diese Konsistenz gesichert und gleichzeitig die Komplexität des Gesamtmodells reduziert werden. Es wird dargestellt, wie die mentalen Modelle der Mitarbeiter in Übereinstimmung mit den offiziellen Modellen gebracht werden können und wie Architekturmängel der Organisation entdeckt und viele davon auf einfache Weise beseitigt werden können. Damit soll der Organisation ein Hilfsmittel an die Hand gegeben werden, mit dem Risiken einfacher erkannt und sowohl die ablauforientierte wie auch die schwachstellen- & schadensausmass-orientierte Überprüfung und Steuerung der Organisation wirtschaftlicher gestaltet werden können.

Referent: Walter Vogt, SOFCOM GmbH

Die weiteren Termine 2017

- 4. April 2017, 16.40 Uhr in Bern
- 6. Juni 2017, 16.40 Uhr in Zürich
- 15. August 2017, 16.40 Uhr in Zürich
- 3. Oktober 2017, 16.40 Uhr in Bern
- 5. Dezember 2017, 16.40 Uhr in Zürich

Die detaillierten Ausschreibungen aktualisieren wir laufend auf unserer Webseite

Informationen des Verbands

IT-Berufe mit Wachstumspotential

Wie im Lead-Artikel aufgezeigt, hat sich die Informatik in den letzten Jahren zu einer immer kritischer werdenden Komponente von (fast) sämtlichen Geschäftsprozessen entwickelt. Im privaten Bereich wird dieser Trend noch fast überholt von der zunehmenden Vernetzung von allem (Internet of Things). Ob wir den selbständig bestellenden Kühlschrank als Spinnidee oder unnötigen Luxus abtun, ändert nichts: längst sind solche Gadgets in vielen privaten Bereichen installiert. Apple hat in seine Fernsteuerung des Heimbereichs rund 100 grosse Anbieter integriert, was den Trend zu bestätigen scheint.

Wie hinlänglich bekannt ist, haben wir derzeit einen immensen Bedarf an Informatikern, welche sich um Entwicklung, Beschaffung und Betrieb von Informatik-(Komponenten) kümmern müssen. Zur Analyse, Steuerung oder Überwachung all dieser Tätigkeiten benötigen wir weitere IT- und Informationssicherheits-Spezialisten für die sogenannte 2nd Line of Defense: IT-Governance, IT-Controlling, Projektcontrolling, Risikomanagement, IT- oder Informationssicherheitsmanagement usw. Alle diese Funktionen sind häufig personell unterdotiert – einerseits weil die Verantwortlichen Personen in Geschäftsleitung usw. nicht erkannt haben, wie wichtig diese Aufgaben sind, andererseits auch, weil der Markt ziemlich ausgetrocknet ist. Für die sogenannte 3rd Line of Defense, die IT-Revision, wird es zunehmend schwierig, qualifizierte Fachkräfte zu finden. Für diesen wohl interessantesten Job im Informatikumfeld benötigt eine Kandidatin oder ein Kandidat Fachwissen aus allen anderen IT-Berufsbildern: Der IT-Prüfer (IT-Revisor) überprüft die gesamte Breite von der physischen Sicherheit von Rechenzentren über die Sicherheit von Netzwerken, Betriebssystemen und Datenbanken, die Ordnungsmässigkeit von Anwendungen bis hin zu strategischen Themen wie IT-Governance, Controlling oder Risikomanagement.

Wagen Sie daher den Sprung in einen weiteren Karriereschritt!

Für Personen, welche in der IT-Revision arbeiten (wollen), aber auch für die anderen Berufsspezialisten bietet das ISACA Switzerland Chapter seit 1992 eine seriöse Aus- und Weiterbildung in der Form von umfassenden Vertiefungskursen an, welche den Teilnehmern sowohl die notwendigen theoretischen Grundlagen (grösstenteils im Rahmen eines strukturierten Selbststudiums ab 1. Februar 2017) als auch die bewährte Berufspraxis (grösstenteils im Präsenzunterricht im Juni/Juli) vermitteln. Ausführliche und klar strukturierte Unterlagen mit Fachbüchern, Skript und Fallstudien dienen nicht nur zur Vorbereitung auf die internationale Zertifikatsprüfung sondern auch als Nachschlagewerk im Berufsalltag.

Für Personen, welche sich (ausschliesslich) auf eine der internationalen Zertifikatsprüfungen vorbereiten wollen, gibt es verschiedene Anbieter mit kompakten Prüfungsvorbereitungkursen.

Sehen Sie dazu die Liste der Zertifikate und Kurse auf Seite 66 oder erkundigen Sie sich auf unserer Website www.isaca.ch