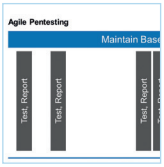
ISACA Switzerland Chapter

Nr. 04 | Dezember 2021 | www.isaca.ch

NEWSLETTER



Penetrationtests
Wie kann man erfolgreich Penetrationtests in einem agilen Software-Entwicklungsumfeld einbauen. **Seite 61**

CGEIT
Vertrauen ist gut – Kontrolle ist besser. Wie CGEIT hilft eine robuste IT Governance zu definieren. **Seite 63**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 65**

Penetrationstests für agile Software im Wochentakt. Geht das?

Von Cyrill Brunschwiler

Die agilen Softwareentwicklungsmodelle sind zum defacto Standard geworden, werden an einschlägigen Hochschulen gelehrt und in der Praxis nach Möglichkeiten umgesetzt. Wer Software nicht mit agilen Prozessen entwickelt, liegt auf den Brettern und ist bereits angezählt. So scheint es zumindest.

Folglich ist es nicht die Frage, ob Penetrationstests im agilen Umfeld machbar sind, sondern ob wir es schaffen, effektive Kontrollen in die neuen, hippen, rapiden Vorgehensweisen zu integrieren.

Viele Features, viele Bugs

Mit klassischen Softwareentwicklungsprozessen wie Wasserfall oder Rational Unified Process (RUP) müssen Penetrationstester jeweils mehr Zeit investieren, um die zahlreichen Änderungen zu verstehen und zu durchleuchten.

Und das führte dann schlimmstenfalls zu einer erneuten Runde im Entwicklungsprozess, um die Fehler auszumerzen. Also zu einer weiteren Verzögerung bevor die neuen Funktionalitäten den Kunden endlich erreichen.

Agile For The Win

Die agilen Methoden verfolgen das primäre Ziel, dass der Endbenutzer möglichst bald einen unmittelbaren Nutzen verzeichnen kann. So werden je nach Umsetzung des Prozesses innert zwei bis vier Wochen neue Funktionalitäten zur Verfügung gestellt. Zu diesem Zweck werden die Arbeiten in kleine Aufgaben geteilt, nach Wunsch des Kunden priorisiert und dann im genannten Zyklus entwickelt und in der Produktion eingebaut. Ein solcher Turnus wird typischerweise als Sprint bezeichnet.

Der Vorteil liegt auf der Hand: Der Kunde ist stetig involviert und kann so die Prioritäten gemäss seinen Anforderungen justieren und auch auf kurzfristige Veränderungen im Markt, relativ rasch reagieren.

Vertrauen ist gut, Kontrolle ist besser

«Veränderung» und «Sicherheit» haben seit jeher eine schwierige Beziehung und so stellt sich die Frage, ob, wie, wo und wann wir in den sehr kurzen Projektzyklen sinnvolle Kontrollen einbauen können, um eben auch die Sicherheit der Software und der damit bearbeiteten Daten gewährleisten zu können.

Heilung durch Selbsterkenntnis

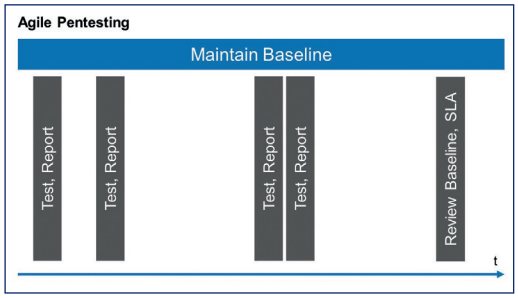
Im Zwei-Wochen-Takt einen Penetrationstest durchzuführen, da sind wir uns einig, ist weder effizient noch finanzierbar.

«Security ist ein Prozess», hören wir die Evangelisten unserer Branche sagen. Leider sind wir selbst sehr schlecht darin, einen Service anzubieten, der jederzeit ein aktuelles Attest abgeben könnte. Wir führen Standortbestimmungen und Zertifizierungen durch. Die Resultate sind eine Momentaufnahme, die binnen Tagen oder Wochen mindestens teilweise hinfällig werden.

Ein echter On-Demand Service wäre eine Hotline für den Entwickler, zu dem Zeitpunkt verfügbar, wo die Expertise benötigt wird.

Braucht es noch Reports?

Die Softwareentwicklung wird mit Werkzeugen unterstützt. Tickets werden durch Workflows geschoben und diese notifizieren die involvierten Teammitglieder über den Fortschritt einzelner Arbeitspakete. Es wäre logisch, dass die Resultate eines Tests auch in eben solche Tickets einfliessen würden.



Ist also ein Bericht noch zeitgemäss? Für einen Quartalsrapport oder ein Jahresbericht zu Handen der Geschäftsleitung. Vielleicht. Vielleicht auch in Form eines Statements für Endkunden. Aber die Entwickler werden wenig Freude an einem traditionellen Report haben, da er schlicht nicht in ihre Gewohnheiten passt.

Dennoch ist es für einen unabhängigen Tester sehr schwierig, eine Schwachstelle einem einzigen Ticket zuzuordnen. Manchmal entstehen Schwachstellen in Konstellation mehrerer Neuerungen oder erst in Konstellation mit der Installation in der produktiven Umgebung. Es braucht also jemanden, der hier die Brücke schlägt.

Abenteuer ist nur schlechte Planung

Den richtigen Zeitpunkt für einen Test zu finden, ist bei agilen Vorgehensweisen mit definierten Release Terminen, keine grosse Sache. Wenn ein Team aber nach einem rollenden Konzept wie beispielsweise Kanban arbeitet, dann wird kontinuierlich released. Insofern muss der Tester viel Flexibilität an den Tag legen.

Ein Team, welches auf Abruf arbeitet, könnte die spontanen Anfragen bearbeiten. Die Dauer der Arbeiten könnte im Vorfeld anhand der geplanten Features geschätzt und reserviert werden.

Reduce to the Max

Es bedarf einer Triage, welche Features wirklich sicherheitsrelevant sein könnten und es braucht eine Erklärung, wie die Features verwendet werden sollten. Dazu gehört auch zu definieren, was die notwendigen Privilegien beziehungsweise Vorbedingungen dafür sind, bekannte Fehlverhalten und Success Cases.

Es würde sich also anbieten, dass im Projektteam eine Person für die Erklärung der Features zuständig ist, die Dokumentation aktuell gehalten wird und idealerweise der Tester nicht dauernd wechselt, weil sonst viel Vorwissen über den Rest der Anwendung und die Geschäftsziele nicht in die Angriffsszenarien des Penetrationstest einfliessen.

Vorbereitungen ist alles

Es ist wichtig, solide Grundvoraussetzungen für die Tests zu schaffen. Dazu gehört, dass der Tester versteht, wie die finale Produktionsumgebung aussieht. Darüber hinaus wird definiert wie man Zugriff auf das Ticketing, die Dokumentation oder sogar den Quellcode bekommt. Es wird ein Set von Testbenutzern benötigt. Zudem braucht es gültige Testdaten und oftmals auch die eine oder andere Ausnahme, um einen Test effizient durchführen zu können. Dazu gehören beispielsweise auch iOS oder Android Apps, die für das Testing optimiert sind.

Aus den Gesprächen mit verschiedenen Firmen, die agile Modelle verfolgen, lässt sich ableiten, dass die Ausprägung und Maturität der Arbeitsweisen enorm variiert. So ist es oft der Fall, dass die automatische Erstellung einer voll funktionsfähigen Testumgebungen inklusive Abfüllung mit guten Testdaten, selten umgesetzt ist.

Reality Check

Automatisierung ist einer der Schlüssel zu sicherer Software. Das heisst, es werden automatisch Testumgebungen erstellt und abgefüllt. Zudem wird mit Scannern für den Quellcode und für grundlegende Funktionalitäten gearbeitet. Damit erreicht man eine Basisabdeckung und gewinnt so Zeit, kritischere Features über mehrere Sprints zu sammeln und dann in einem Lauf testen zu lassen.

Ausbildung ist ein anderer wichtiger Aspekt im Bereich der Softwareentwicklung. Konkret ist hier die Spezialisierung eines Team-Mitglieds auf Software- und Infrastruktursicherheit anzustreben. Der sogenannte Security Champion ist Ansprechpartner für das Team, trägt die Verantwortung für die Sicherheit der entwickelten Komponenten und sammelt bzw. koordiniert Penetrationstests mit externen Stellen. Er ist auch dafür zuständig, die Erkenntnisse aus den Tests zu beurteilen und allfällige Gegenmassnahmen zu koordinieren.

Fazit

Die Bedingung für eine erfolgreiche Umsetzung von Penetrationstests bei jedem Softwarerelease ist, dass kaum Aufwand für die Vorbereitung und Abstimmung entsteht. Das bedeutet im Umkehrschluss, dass eine Organisation einen überdurchschnittlichen Grad an Automatisierung an den Tag legen muss. Dies ist nach meiner Erfahrung noch eher selten der Fall und dadurch kippt das Gewicht vom Penetrationstest zum Vorbereitungsaufwand und die Tests werden unwirtschaftlich.

Zudem birgt die isolierte Analyse einzelner Neuerungen die Gefahr, dass Schwachstellen, verursacht durch das Gesamtkonstrukt der Software oder der Infrastruktur, nicht erkannt werden.

Folglich rate ich in den meisten Fällen noch davon ab, manuelle Penetrationstests an jeden Releasetermin eines agilen Projektes zu koppeln.

Ergo, Stand heute, sind die meisten Firmen nach wie vor mit vierteljährlichen oder halbjährlichen «Managed Pentest» eindeutig besser bedient.

DER AUTOR

Cyrill Brunschwiler ist seit über 20 Jahren in der Rolle des Hackers unterwegs. Er hat in seinen Anfängen Cyber Training Ranges entwickelt sowie Rätsel für hacking-lab.com erstellt. Seit 2005 hat er unzählige Projekte mit unabhängiger Expertise in den Bereichen Penetration Testing, Red Teaming, Incident Response und digitale Forensik, durchgeführt. Cyrill ist seit 2014 Geschäftsführer der Compass Security Schweiz AG. Er hält einen MSc in Information Security und Assurance von der Royal Holloway Universität in London und ist Lehrbeauftragter an der Ostschweizer Fachhochschule OST.

Vertrauen ist gut – Kontrolle ist besser (C GEIT)!

Von Peter R. Bitterli

Dieser altbekannte und im vorhergehenden, lesenswerten Artikel von Cyrill Brunnschwiler verwendete Leitsatz lässt sich auf viele Bereiche anwenden – wohl alle Lesenden haben diesbezüglich schon ihre eigenen Erfahrungen gemacht. Der Begriff «Kontrolle» wird hier im Sinne einer qualitätssichernden Handlung durch eine unabhängige zweite Person verwendet.

Gut nachvollziehbar kommt der Autor zum Schluss, dass «agile» Penetrationstests als Kontrolle in agilen Prozessen nur dann wirklich gut funktionieren, wenn die agilen Softwareentwicklungsprozesse auf einem sehr hohen Maturitätsniveau abgewickelt werden. Da dies nicht immer der Fall ist, schlägt der Autor vor, bei den «klassischen» viertel- oder halbjährlichen Pentests zu verbleiben. Etwas plakativ formuliert heisst das, dass in diesem Anwendungsfall nur 2–4 Mal pro Jahr eine Überprüfung aus Optik der Sicherheit vorgenommen wird.

Wem dies schon etwas selten (nicht seltsam!) vorkommt, sei an die (finanzrelevanten) Internen Kontrollsysteme (IKS) erinnert. Diese werden häufig auf Stufe Unternehmensführung definiert und im Rahmen eines eher schlanken Self Assessment-Prozesses typischerweise 1 Mal pro Jahr überprüft. Die Überlegung dahinter ist, dass es ausreicht, einmal jährlich das Vorhandensein und Funktionieren bestimmter Schlüsselkontrollen durch die Kontrollverantwortlichen bestätigen zu lassen. Im Rahmen der gesetzlich vorgeschriebenen Abschlussprüfung (Finanzprüfung) wird dieses IKS auch noch durch den Abschlussprüfer bestätigt. Man suggeriert damit, dass Verwaltungsrat (wo vorhanden) und/oder Geschäftsleitung das Unternehmen sorgfältig und eng überwachen und bezeichnet das dann noch grosszügig als wirksames GRC (Governance Risk Compliance).

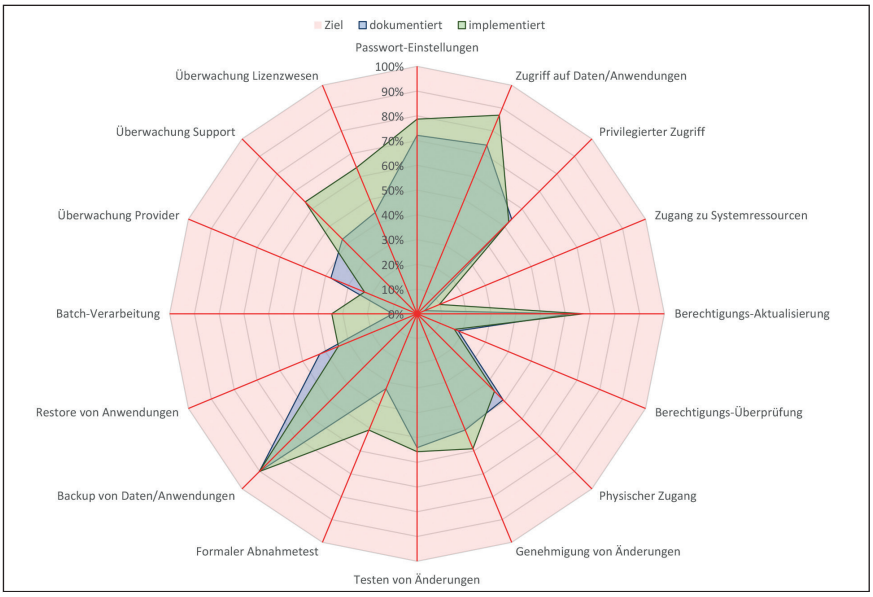
Wer sich mit der Finanzprüfung etwas auskennt, weiss, dass es sich dabei nur um eine Prüfung der sogenannten Design Effectiveness des IKS handelt (richtige Kontrolle am richtigen Ort) und nicht um eine Prüfung der Wirksamkeit über die gesamte Beobachtungsperiode. Einmal pro Jahr relativ oberflächlich hinschauen, ob einigermassen sinnvolle Kontrollen definiert sind, hat wohl wenig Wirkung auf die zugrundeliegenden Prozesse. Zudem wird schnell einmal klar, dass in diesem formal bestätigten IKS ausschliesslich die finanzrelevanten Kernsysteme abgedeckt werden.

Es fehlt mir hier der Platz, um noch weiter auszuholen. Aber aus meiner Optik hat das mit Governance eher wenig zu tun.

Das nachfolgende Beispiel soll dies noch kurz beleuchten: Eine Untersuchung der BDO bei 155 KMU hat ergeben, dass bei den im Rahmen der Finanzprüfung untersuchten «generellen IT-Kontrollen» ein Grossteil der Kontrollen weder ausreichend dokumentiert noch nachvollziehbar implementiert wurde.

Governance heisst: «to influence or control the way something happens or is done»; das heisst «beeinflussen oder im engeren Sinn überwachen, wie etwas gemacht wird». Einmal pro Jahr oberflächlich hinschauen, ob irgendwelche Kontrollen existieren, hat wohl kaum eine positive Wirkung auf die wirklich gelebten Prozesse und damit die freiwillig aber meist unwissend eingegangenen Risiken.

«Enterprise Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprises's resources are used responsibly.» Diese Definition von CIMA oder ähnliche Definitionen von OECD führen aus, dass Governance sicherstellen muss, dass die Unternehmensziele durch Priorisierung, Entscheidungsfindung und Überwachung von Leistung, Compliance und



Lesehilfe: Insgesamt wurden bei 155 Unternehmen je 16 IT-Kontrollen als Teil des finanzrelevanten IKS dahingehend überprüft, ob die Kontrollhandlung dokumentiert und ob sie im Alltag umgesetzt ist. Bei den Unternehmen geschieht dies sehr unterschiedlich gut je nach Art der IT-Kontrolle (und natürlich auch in Abhängigkeit vom Unternehmen).

Die Grafik zeigt auf, dass z.B. der «Zugang zu Systemressourcen» recht gut implementiert aber eher schlecht dokumentiert ist. Der «Restore von Anwendungen» ist bei den meisten Unternehmen weder gut dokumentiert noch gut implementiert.

Fortschritt im Vergleich zum Plan erreicht werden.

Etwas anders formuliert heisst das: Die in den Geschäfts- und IT-Prozessen integrierten Kontrollen stellen die vollständige, richtige, zeitgerechte, … Verarbeitung sicher. Dass diese Kontrollen am richtigen Ort implementiert und ausreichend wirksam betrieben werden, ist die Aufgabe des Managements (Führungskräfte auf allen Stufen) resp. der verschiedenen Managementsysteme wie IKS, Qualitätssicherung, Risikomanagement, Sicherheitsmanagement, Personalführung usw. Governance bedeutet jetzt, dass die vorhandenen Managementsysteme dahingehend gesteuert und überwacht werden, dass sie ihre Ziele tatsächlich erreichen. Einmal pro Jahr oberflächlich auf ein paar Finanzkontrollen schauen, reicht demnach ebenso wenig wie einmal pro Jahr ein paar Fragen zu den aktuellen Risiken zu stellen. Governance bedeutet, sich echt darum zu kümmern, dass etwas Vorbestimmtes wirklich und wirksam getan wird und mit diesen Tätigkeiten die definierten Ziele auch erreicht werden.

Was sonst noch alles zu (IT) Governance gehört, kann man den Standardwerken von ISACA wie dem aktuellen COBIT-Framework (gratis bei www.isaca.org herunterladbar) oder dem CGEIT Review Manual entnehmen. Wer es wirklich verstehen möchte, besucht den CGEIT-Vertiefungskurs, der ein grundlegendes Verständnis zum Thema Governance vermittelt sowie auf die internationale Zertifikatsprüfung vorbereitet und auch im Jahr 2022 wieder von unseren akkreditierten Ausbildungspartnern angeboten wird.

In der Schweiz bietet ISACA-CH bereits seit 2009 eine berufsbegleitende Aus- und Weiterbildung für IT-Governance an (CGEIT = Certified in Governance of Enterprise). Informieren Sie sich bei www.isaca.ch über das CGEIT-Berufsbild und die entsprechenden offiziellen CGEIT-Kurse des ISACA Switzerland Chapter.

DER AUTOR

Peter R. Bitterli,
CISA, CISM, CGEIT, CRISC, CDPSE

Rückblick ISACA/IIAS Konferenz vom 25. Oktober 2021

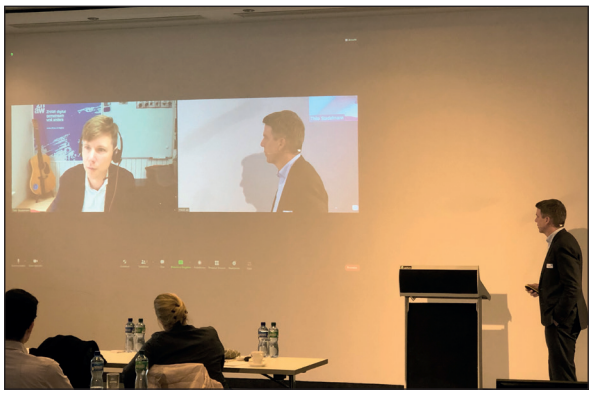
ISACA/IIAS Fachtagung zum Thema «Remote Audit – Prüfen aus der Ferne»

Am 25. Oktober 2021 besuchten 33 Teilnehmerinnen und Teilnehmer, Referentinnen und Referenten die alljährliche Fachtagung des ISACA Switzerland Chapters und des IIA Switzerland im Hotel Courtyard by Marriot in Zürich-Oerlikon. Coronabedingt wurde die Tagung als hybrider Anlass durchgeführt, so dass weitere 22 Teilnehmende die Tagung online verfolgen konnten. Mit neun monatiger Verspätung und nach zwei Verschiebungen waren alle gespannt auf das topaktuelle Thema «Remote Audit».

Die Tagung spannte einen weiten Bogen über das Thema Remote Audit. Den Sieben Referentinnen und Referenten gelang es den Teilnehmenden einen breiten Ein- und Ausblick zum Remote Audit selbst, aber auch zu Themen wie Homeoffice und Datenschutz und Sicherheit zu geben.

Den Anfang machte **Barbara Widmer,** Datenschutzstellen Kt. BS, zu datenschutzrechtlichen Risiken und Haftungsfragen rund um Videokonferenzen und dem Arbeiten im Homeoffice. **Volker Dohr,** Rechtsanwalt und Dozent an der ZHAW, beschäftige sich in seinem Referat mit der Frage von Fiktion und Wahrheit und wie kognitive Täuschungen das Prüfurteil beeinflussen, sowie wie wir uns vor diesen Einflüssen schützen können. **Luka Zupan,** Partner bei KPMG Schweiz, zeigte die Auswirkungen der Pandemie auf die Arbeit des Internen Audits auf. Sein Fazit war: Es konnten jederzeit Prüfungen durchgeführt werden, aber der risikoorientierte Ansatz hat während der Pandemie gelitten. Dies muss jetzt wieder korrigiert werden.

Nach der Mittagspause nahm uns **Angelica Bienz,** Audit&Risk GmbH, mit in ihre Überlegungen und Erfahrungen zur Frage, inwieweit die Pandemie für das Audit ein Stresstest war. Sie kam zum Schluss, dass die Auditoren den Stresstest insgesamt gut bestanden und ihre Arbeitsweise rasch der neuen Realität angepasst haben. **Aleksej Shaban,** Swisscows AG, erläutert in seinem Referat die Sicherheitsrisiken der Remotearbeit und worauf zu achten ist, damit man diese Risiken im Griff behält. Nach einer Erfrischungspause beschäftigte sich **Patrick Freudiger,** Admomentum AG, mit dem Thema «Führungsverhalten in disruptiven Zeiten» und zeigte auf, welches Führungsverhalten auch unter schwierigen Bedingungen zielführend ist. Zum Abschluss gab **Serdar Günal Rütsche,** Leiter der Abteilung Cybercrime der KaPo Zürich, einen Einblick in die Welt der Cyberrisken und in die Arbeit der Polizei bei deren Bekämpfung.



Der Abschluss dieses spannenden und lehrreichen Tages bildet dann ein Apéro Riche mit ausgedehntem Networking.

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 detaillierten Ausschreibungen aktualisieren wir laufend auf unserer Webseite www.isaca.ch. Bitte beachten Sie dort auch die aktuellen Hinweise zum Ort der Veranstaltung (Online oder lokal).

ISACA-TRAINING

Datum	Hauptthema – Kurstitel
20-23.12.2021	CISA 4-day exam preparation course (Module 2) (E/F)
20-22.12.2021	CISM 3-day exam preparation course (Module 2) (E/F)
20-22.12.2021	CGEIT 3-day exam preparation course (Module 2) (E/F)
20-22.12.2021	CRISC 3-day exam preparation course (Module 2) (E/F)
20-21.12.2021	COBIT 2019 - 2-day course
www.actagis.ch	
28.-30.03.2022	CCAK - Certificate of Cloud Auditing Knowledge (D) 3 Tage
25.-27.07.2022	CCAK - Certificate of Cloud Auditing Knowledge (D) 3 Tage
31.01.-01.02.2022	COBIT 2019 Foundation (D) 2 Tage
06.-07.07.2022	COBIT 2019 Foundation (D) 2 Tage
19.-20.04.2022	CSX Cybersecurity Fundamentals (D) 2 Tage
www.glenfis.ch	
Start Vorbereitung 01.03.2022 Präsenzunterricht im Juni 2022 Prüfungstrainigs Sept/Okt. 2022	CISA, CISM, CGEIT, CRISC, CDPSE: Selbststudium mit ausführlichen Unterlagen ab 01. März; 9-11 Tage; modularer Unterricht im Zeitraum 06.06.–01.07.; Prüfungsvorbereitungstraining im Herbst September Oktober
23.-24.03.2022	COBIT 2019 (sehr umfangreicher Kursinhalt)
www.itacs.ch	

IMPRESSUM ISACA NEWS

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Sekretariat ISACA Switzerland Chapter, c/o BDO AG, Biberiststrasse 16, 4501 Solothurn
Erscheinungsweise: 4× 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