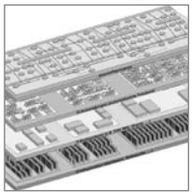
ISACA®
Trust in, and value from, information systems
Switzerland Chapter
Nr. 04 | Dezember 2013 | www.isaca.ch
NEWSLETTER

3-Way-Match
Das Abstimmverfahren mit Potential für Prozessverbesserungen.
Seite 65



IT General Controls
Das Vorgehensmodell IT-Risikoanalyse hilft in der Beurteilung von generellen IT-Kontrollen.
Seite 67

ISACA-Training
Aktuelle Aus- und Weiterbildungs möglichkeiten für Mitglieder und Nicht-Mitglieder
Seite 69

3-Way-Match – Wissen was dahintersteckt

Nur die Wirksamkeit der Kontrollen in einem Einkaufsprozess zu prüfen, erfüllt zwar einen wichtigen Zweck, decken aber nur teilweise die Ansprüche der Verantwortlichen ab. 3-Way-Matching ist eine dieser Kontrollen, die auch das Potential für Prozessverbesserungen hat.

Von Roland Giger

Ein Risiko im Einkaufsprozess besteht darin, dass die ursprüngliche Bestellung sowohl in der Menge und den Preisen nicht mehr der dazugehörigen Lieferung und Rechnung entspricht. Sowohl tiefere als auch höhere Liefermengen und Preise können negative Folgen haben. Tiefere Liefermengen führen z.B. dazu, dass interne Produktionsprozesse nicht mit den erforderlichen Mengen versorgt werden und somit ein Produktionsengpass entsteht. Nicht gerechtfertigte höhere Preise in der Rechnung, die nicht mit dem vereinbarten Preis in der Bestellung übereinstimmen, führen zu nicht vorgesehenen Kosten. Diese nicht abschliessende Aufzählung zeigt den Bedarf für risikomindernde Kontrollen bei der Abstimmung zwischen Bestellung, Wareneingang und Rechnung. Das Prinzip, welches dahinter steckt, wird als sogenanntes «3-Way-Match-Prinzip» bezeichnet.

Mit diesem Beitrag erläutere ich Ihnen dieses Abstimmverfahren («Matching») allgemein und wie es konkret am Beispiel von SAP umgesetzt wird, worauf Sie bei einem Audit achten sollten und welche Möglichkeiten für Prozessverbesserungen vorhanden sind.

3-Way-Match – Das Prinzip

Mengen und Werte auf der Bestellung müssen identisch sein mit der Lieferung sowie mit der Rechnung. Gibt es Abweichungen, sollten diese nur dann zugelassen werden, wenn bestimmte Bedingungen erfüllt sind. Diese Ausgangslage ist als Rahmenbedingung für den ganzen Einkaufsprozess einzuhalten. Im ganzen Ablauf gibt und soll es aber auch genügend Spielraum geben, um den Prozess nicht unnötig zu blockieren oder zu verlangsamen. Aus diesem Grund gibt es verschiedene Möglichkeiten zur Abstimmung. Nachfolgendes Bild zeigt Ihnen 3 Möglichkeiten, die bei der Prüfung der Mengen und Werte im Einkaufsprozess angewendet werden. Jedes dieser Verfahren deckt Risiken ab, welche sich mit der Erweiterung des Abstimmschrittes entsprechend reduzieren.

Welches dieser 3 Verfahren unter welchen Bedingungen im Einkaufsprozess anzuwenden ist, sollte festgelegt sein. Für einfache Beschaffungen kann 2-Way-Match durchaus ausreichend sein. Bei Waren, die höchsten Ansprüchen genügen müssen, ist ein 4-Way-Match angebracht. Hinweisen möchte ich, dass mit Liefermenge nicht ausschliesslich eine physische Ware gemeint sein muss. Auch bei Dienstleistungen kann und sollte eine Abstimmung der Liefermenge (z.B. in Form eines Arbeitsrapports) durchgeführt werden.

Umgesetzt werden kann die Abstimmung manuell oder automatisiert. Wie dies in SAP vollständig automatisiert wird, erläutere ich Ihnen nachfolgend.

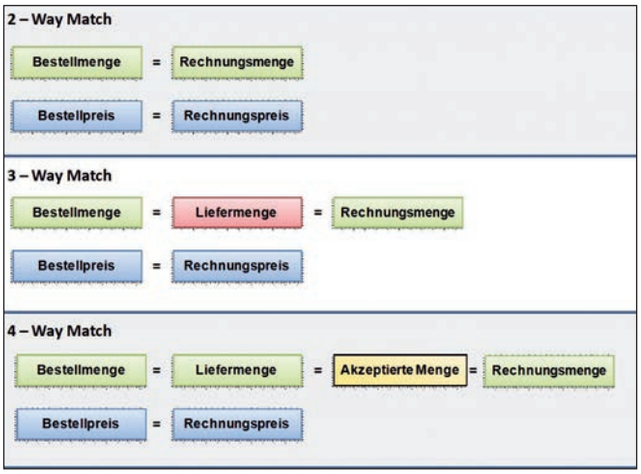


Abb 1: Abstimmverfahren im Einkaufsprozess

Verglichen werden nur die Bestellung und die Rechnung.
Verbleibendes Risiko: Nicht gelieferte, zu viel oder zu wenig gelieferte, unvollständig bzw. mangelhaft gelieferte Ware.

Zusätzlich wird auch die gelieferte Menge verglichen, damit das Risiko aus 2-Way-Match eliminiert wird.
Verbleibendes Risiko: Die Qualität der Ware kann mangelhaft sein.

Das 3-Way-Match-Verfahren wird ergänzt mit der Qualitätsprüfung der Ware.

3-Way-Match mit SAP

Eine Bestellung und Lieferung in SAP abzuwickeln, erfordert das SAP-Modul Materialwirtschaft. Die Rechnung sollte natürlich auch mit diesem Modul erfasst werden, könnte aber auch direkt in der Finanzbuchhaltung erfolgen. Der Einkaufsprozess mit dem SAP-Modul Materialwirtschaft vergleicht nicht automatisch die Mengen und Werte der Bestellung, Lieferung und Rechnung. Um dieses Verfahren zu ermöglichen, gibt es in SAP keine technische Einstellung, die sich wie ein Schalter betätigen liesse. Erst das Zusammenwirken verschiedener Faktoren bewirkt diesen Effekt und erfordert es, dass zuerst der gesamte Prozessablauf festgelegt werden muss.

Die erste einzurichtende Kontrolle ist, dass eine verbindliche Verknüpfung der Bestellung, Lieferung und Rechnung vorliegt. Dies erreicht man damit, dass die Lieferung und Rechnung mit einem Bezug zur Bestellung erfasst werden muss. Wie ermöglicht man dies in SAP?

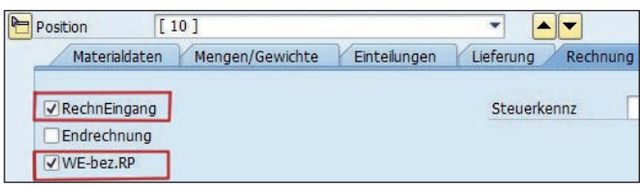


Abb 2: Kennzeichen in einer SAP-Bestellung

Setzt man in der Bestellung das Kennzeichen «WE-bez.RP» (Wareneingangsbezogene Rechnungsprüfung), erzwingt man, dass eine Rechnung nicht ohne vorherige Buchung der Lieferung möglich ist. Gleichzeitig wird damit auch verhindert, dass höhere Rechnungsmengen als die gelieferte Menge verbucht werden können. Ebenfalls gesetzt werden muss das Rechnungseingangskennzeichen. Dieses legt fest, dass zur Bestellung auch eine Rechnung folgen wird. Abbildung 2 zeigt, wie diese beiden Kennzeichen in einer SAP-Bestellung aussehen.

Bei der Erfassung der Lieferung und bei der Erfassung der Rechnung sind dann die dafür vorgesehenen SAP-Transaktionen zu verwenden. Die Buchung der Lieferung (Transaktion MIGO) muss dabei mit einem Bezug zur Bestellung erfolgen und der Rechnungseingang (Transaktion MIRO) mit einem Bezug zur Bestellung/Lieferung. Ob eine Bestellung so abgewickelt wurde, lässt sich in der Bestellung dadurch erkennen, dass auf der jeweiligen Bestellposition unter «Bestellentwicklung» sowohl die Buchung der Lieferung wie auch der Rechnung erscheint.

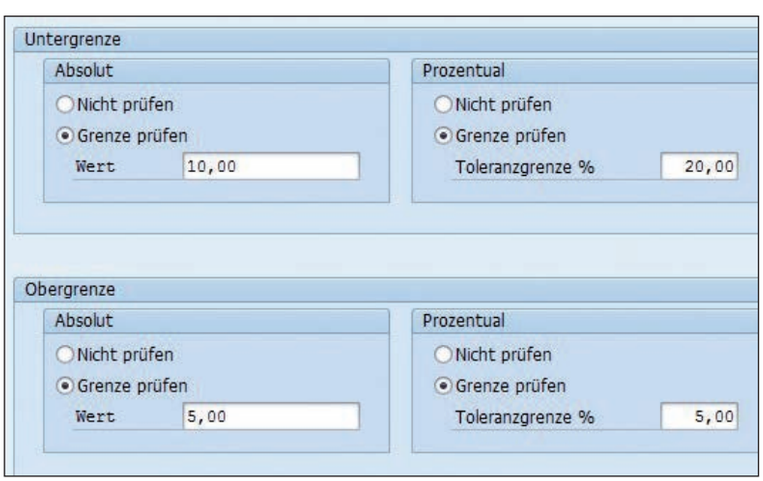


Abb 3: Toleranzkriterien

Tolerant sein

Die Verknüpfung alleine reicht nicht aus, da ja noch die Abstimmung der Mengen und Preise von der Bestellung bis zur Rechnung abgesichert werden soll. Erst dadurch ist korrekterweise die Rechnung in Ordnung und kann zur Zahlung freigegeben werden. Gibt es eine Differenz bei der Menge oder den Preisen, dann ist die Rechnung zur Zahlung zu sperren. Nun macht es aber keinen Sinn, wenn im normalen Geschäftsablauf vorkommende Differenzen vollständig ausgeschlossen werden und somit zu unnötigem Bereinigungsaufwand oder Verzögerungen führen. Zu diesem Zweck sind in SAP verschiedene Toleranzkriterien möglich, die entweder mit einem absoluten Betrag oder relativen Prozentsatz eine Ober- bzw. Untergrenze zulassen. Alle Toleranzkriterien lassen sich wie auf Abbildung 3 abgebildet definieren und ermöglichen für verschiedenste Situationen eine grösstmögliche Flexibilität, welche ausgenutzt, aber auch im internen Kontrollsystem definiert sein sollte.

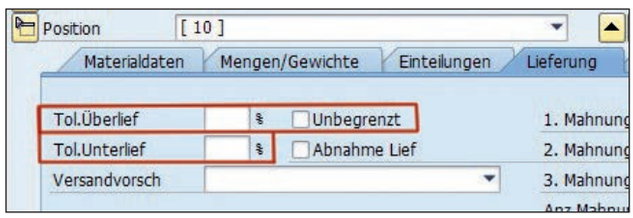


Abb 4: Parameter einer SAP-Bestellung

Ist die Prüfung der Unter- oder Obergrenze eingeschaltet, bewirkt diese Kontrolle, dass nur diejenigen Rechnungen zur Zahlung freigegeben werden, die innerhalb dieser Toleranzgrenzen liegen. Rechnungen ausserhalb der Toleranz werden zwar gebucht, aber ein Sperrcode verhindert die automatische Zahlung.

Für die Prüfung der Liefer- und Bestellmenge ist festzulegen, wie mit Unter- und Überlieferungen vorzugehen ist. Unterlieferungen sind grundsätzlich zugelassen und werden als Teillieferung interpretiert. Es ist möglich, eine prozentuale Unterlieferungstoleranz anzugeben. Das Gegenstück, die Überlieferung, ist standardmässig nicht zugelassen. Wenn dies erlaubt sein soll, dann ist dies explizit durch eine prozentuale Toleranzangabe oder als unbegrenzte Überlieferung zu definieren. Abbildung 4 zeigt, wie diese Parameter in der Bestellung zu erkennen sind.

3-Way umgehen

Die gesamte Kontrolle kann umgangen werden, wenn beispielsweise die Rechnung ohne Bestellbezug oder direkt auf Sachkonten gebucht wird. Wenn offene Bestellungen mit Mengen-/Preisdifferenzen einfach den Status abgeschlossen erhalten und die Differenz ausgebucht wird. Kritisch zu beurteilen ist auch, wie der Ablauf zur Freigabe der gesperrten Rechnungen ist. Eine rasche Nachbearbeitung ist hier angebracht. Sie sollte aber nicht ohne Kontrolle erfolgen, da damit alle vorherigen Kontrollen hinfällig werden, welche zur Sperrung führten.

3-Way beschleunigen

Eine Doppelunterschrift auf der Rechnung, bevor die Zahlung erfolgt, ist eine der häufigsten Kontrollen im Einkaufsprozess. Mit einem wirksamen und automatisierten Abstimmverfahren kann diese Kontrolle reduziert werden. Wenn die Bestellung mittels Doppelunterschrift genehmigt wurde und ein 2-Way-Match mit Toleranzprüfung im System durchgeführt wird, dann ist eine Unterschrift auf der Rechnung ausreichend. Diese Unterschrift bestätigt die materielle Lieferung. Bei einem 3-Way-Match kann auch auf diese Unterschrift verzichtet werden, weil in diesem Fall ja die bewilligte Bestellung mit der Lieferung und Rechnung übereinstimmt. SAP ermöglicht auch, dass direkt nach der Lieferung die Rechnung automatisch erzeugt wird. Dadurch können keine Rechnungssperren mehr auftreten und der Prozess wird effizienter. Den Ablauf blockieren kann die Tatsache, dass für dringend benötigtes Material keine Bestellung erfasst wurde, sondern telefonisch bestellt wird. In diesem Fall kann SAP so eingerichtet werden, dass mit der Buchung der Lieferung automatisch eine Bestellung angelegt wird und so nicht auf das 3-Way-Match verzichtet werden muss.

Fazit

Das Prinzip des 3-Way-Match ist nicht abhängig davon, ob SAP eingesetzt wird oder ein anderes Produkt. Die erwähnten Beispiele veranschaulichen das Prinzip und können ohne weiteres für die Prüfung des Einkaufsprozesses allgemein verwendet werden. 3-Way-Match – Sie wissen nun was dahinter steckt für Ihren nächsten Audit.

CHECKLISTE:

- Werden Bestellung, Lieferung und Rechnung miteinander verknüpft?
- Wie sehen die Kontrollen zur Sicherstellung der korrekten Mengen und Preise über den gesamten Einkaufsprozess aus?
- Sind für Abweichungen von Mengen und Preisen die Toleranzen festgelegt und entsprechen den Firmenrichtlinien?
- Unter welchen Bedingungen werden Rechnungen zur Zahlung gesperrt?
- Wie ist die Freigabe gesperrter Rechnungen geregelt?
- Werden offene Bestellungen, Lieferungen und ausstehende Rechnungen überwacht?
- Werden die Konten mit Differenzbuchungen ordnungsmässig geführt, überwacht und korrekt bereinigt?
- Werden Lieferungen ohne Bestellbezug direkt in den Warenbestand erfasst?
- Wenn Rechnungen vor der Lieferung eintreffen, wie wird dann deren Richtigkeit bestätigt?
- Könnte die Doppelunterschrift bei der Rechnungsprüfung reduziert werden, weil 2-Way-Match oder 3-Way-Match ausreichend ist?
- Werden Rechnungen automatisch erzeugt nach der Lieferung?

DER AUTOR

Roland Giger, Inhaber der Giger Consulting GmbH, Bern (www.giger-consulting.com) Eidg. Dipl. Wirtschaftsinformatiker, CISA, CRISC, mehrjährige IT-Erfahrung, davon mehr als 10 Jahre in der SAP-Beratung und 7 Jahre als leitender Revisor.

IT General Controls im Zeitalter Cloud Computing

Die rasante Verbreitung mobiler Endgeräte, welche dauerhaft mit der Wolke verbunden sind, stellt neue Anforderungen an die zugrundeliegende Informationstechnologie. Das «Vorgehensmodell IT-Risikoanalyse» bietet im KMU-Umfeld eine praxistaugliche Lösung, um die Herausforderungen systematisch zu beurteilen.

Von Aldo Dubacher, CISA, Engagement Manager bei Mattig-Suter und Partner

In kaum einem Unternehmen sind IT-unterstützte Geschäftsprozesse mehr wegzudenken. Airlines, Autovermietungen und Hotels werden bald nur noch über das Internet oder über Apps von Mobilgeräten gebucht. E-Commerce nimmt sogar in der Bekleidungsbranche Einzug, dank den Apps auf mobilen Geräten. Die Informationstechnologie beeinflusst massgeblich die Weiterentwicklung von Geschäftsmodellen erfolgreicher Unternehmen. IT-unterstützte Geschäftsprozesse erfordern deshalb ein solides Fundament an IT-Infrastukturen, welche professionell betrieben werden und in welchen Kontrollen etabliert sind, um den IT Risiken zu entgegnen.

Die Durchdringung neuer Technologien in verschiedenen Lebensbereichen der Gesellschaft führt unweigerlich zu einem enormen Bedeutungsgewinn der Informationstechnologie. Mit dieser Entwicklung öffnen sich neue Chancen, aber auch nicht zu negierende Risiken (Identity Theft als ein Stichwort und eine Vielzahl weiterer Ausprägungen).

«Vorgehensmodell IT-Risikoanalyse» als Assessment Tool

Das «Vorgehensmodell IT-Risikoanalyse» als Arbeitshilfe für KMU-Prüfer der Schweizer Treuhand-Kammer und der ISACA Switzerland bewährt sich als standardisierter Framework für die Beurteilung von generellen IT-Kontrollen (ITGC) in KMU-Unternehmen.[1] Mit dieser Assessment-Methodik werden in zwei Phasen anhand von 16 generellen und 90 detaillierteren Fragen alle wesentlichen Aspekte der Informationstechnologie in ihrer gesamten Breite ausgeleuchtet. Mit diesem Assessment-Tool wird ermöglicht, mit vertretbarem zeitlichem Aufwand die IT-Aspekte in verschiedenen Dimensionen zu beurteilen, ohne dass sich die Methodik in den Details der IT verirrt.

Wegen dem Bedeutungsgewinn der Informationstechnologie stellen die generellen IT-Kontrollen ein wesentliches Element des internen Kontrollsystems (IKS) von Unternehmen dar. Die Schweizer Prüfungsstandards sehen deshalb im Standard PS 890 (IKS Existenzbestätigung) die jährliche Prüfung der generellen IT-Kontrollen vor. Eigene Beobachtungen führten vor Augen, dass bei konventionellen KMU-Betrieben der Betrieb der IT-Infrastruktur in den letzten Jahren einen stabilen Reifegrad erreicht hat und sich deshalb die ITGC - im Gegensatz zu Anwendungskontrollen in sich laufend verändernden Geschäftsprozessen - weniger rasch verändern. Bei der Weiterentwicklung der PS 890 ist deshalb zu prüfen, ob es nicht sachgerecht wäre, die Prüfung der prozessbasierten Anwendungskontrollen anstelle der jährlichen Überprüfung der generellen IT-Kontrollen stärker zu priorisieren.

Die Stärken und somit die Vorteile der genannten IT-Risikoanalyse bestehen im beherrschbaren Umfang des Arbeitstools. Der Kriterienkatalog zur ITGC-Beurteilung überbordet nicht, weshalb dieses Instrument in KMU-Unternehmen gewinnbringend eingesetzt werden kann, welche der ordentlichen Revision unterstehen. Der für die Abwicklung erforderliche Zeitbedarf kann in einer ordentlichen Revision integriert werden und die dafür erforderlichen Prüfungskosten im KMU-Umfeld bleiben vertretbar. Der standardisierte Kriterienkatalog und die Ausprägungen in Form eines Capability Maturity Model (CMM) ermöglichen qualitative Erkenntnisse quantitative auszuwerten, so dass beurteilte Unternehmen mit Einschränkungen untereinander verglichen werden können.[2]

ITGC im Kontext der aktuellen technologischen Entwicklung

Die frappante Entwicklung der Informationstechnologie führt zu einer fundamentalen Veränderung. Die Absatzzahlen von intelligenten Smartphones und Tablets beschleunigen die Entwicklung von immer wieder neuen Dienstleistungen, welche nicht nur die Unternehmenswelt verändern sondern auch in den privaten Alltag jedes einzelnen eindringen.

Nur die Transformation des Mainframe-Computing in das Zeitalter des Personal Computing (Client-Server Architekturen) der 1980er Jahre ist mit der gegenwärtigen Veränderung zum Cloud Computing des 21. Jahrhunderts vergleichbar. Beide technologischen Transformationen wurden durch Entwicklungssprünge in der Netzwerk-Kapazitäten, in der Verkleinerung der Hardware (vom Grossraumcomputer über den Desktop Computer zum handlichen Smartphone) und der Weiterentwicklung der Software hinzu web-basierten Applikationen (Apps) überhaupt erst ermöglicht. Nicht ohne Grund stellte sich die EuroCACS / ISRM Conference Mitte September in London unter den Leitsatz «New Era – New Edge», um der gegenwärtigen Entwicklung Rechnung zu tragen und Antworten auf drängende IT-Fragen zu finden.

Unberührt von der Veränderung bleibt die Bedeutung des Fundaments der IT-Infrastruktur. Die aufgezeigte technologische Entwicklung beeinflusst die 7 x 24 Stunden Gesellschaft

massgeblich. Die Konsumenten sind in real-time Online und verlangen ungeduldig eine rasche, nahe zu hundertprozentige Verfügbarkeit der IT-Services in ihren Apps auf ihren Smartphones. Diese Entwicklung spricht sogar für einen Bedeutungsgewinn der zu Grunde liegenden IT-Infrastrukturen und die darin integrierten generellen IT-Kontrollen.

Aus der aufgezeigten Entwicklung lässt sich ableiten, dass die IT-Risikobeurteilung für KMU-Unternehmen um Aspekte des neuen IT-Zeitalters zu ergänzen ist. Nicht mehr Antiviren-Probleme dominieren die Schlagzeilen. Auch KMU-Unternehmen sind von der BYOD-Debatte und Fragen der Mobile und Cloud Security betroffen. Die aktuell laufende technologische Veränderung ist definitiv keine kurzfristige Modeerscheinung.

[1] Der Autor des Fachartikels hat die Methodik bei rund zehn KMU-Firmen in den Branchen Hotellerie, Spezialitätenchemie, Detail- und Grosshandel und bei einer Pensionskasse, welche zwischen 30 und 250 Mitarbeitern beschäftigen, seit 2010 eingesetzt.

[2] Abbildung aus «Vorgehensmodell IT-Risikoanalyse: Arbeitshilfe für KMU-Prüfer»; Fachstab für Informatik der Treuhand-Kammer; Seite 14

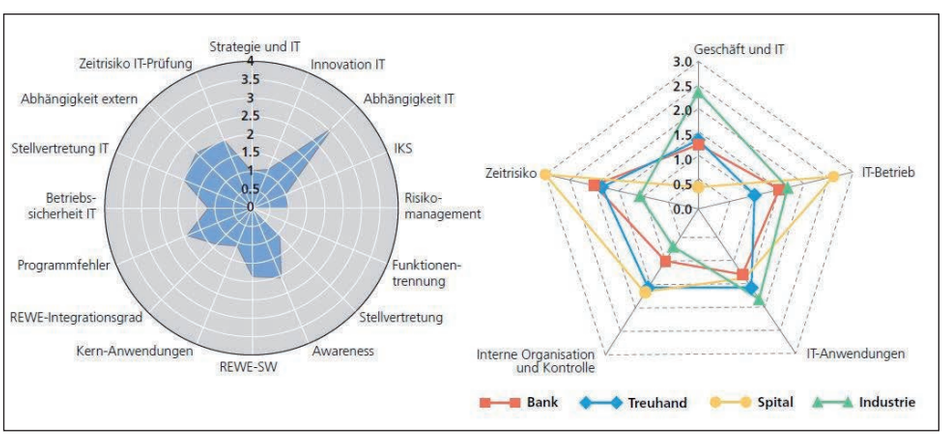


Illustration der Auswertungsmöglichkeiten anhand Vorgehensmodell IT-Risikoanalyse

DER AUTOR

Aldo Dubacher, CISA, ist als Engagement Manager bei der Mattig-Suter und Partner tätig und dort für den Bereich der Wirtschaftsprüfung unter besonderer Berücksichtigung der IT-Revision zuständig.
aldo.dubacher@mattig.ch; www.mattig.ch

Informationen des Verbands

CISA – der faszinierende Beruf als IT-Prüfer

Die Welt der Informationstechnologie (IT) unterliegt einem (teilweise extrem) raschen Wandel – das weiss heute wohl jedes Kind. Wahrscheinlich für jedes IT-Berufsbild (z.B. Software-Entwickler) ist eine permanente Aus- und Weiterbildung daher unabdingbar. Für den IT-Prüfer, der ausnahmslos jedes IT-Thema auch revidieren können muss, gilt dies in deutlich erhöhtem Masse: er muss ja letztendlich jedes IT-Thema – und damit die Summe aller IT-Themen – effizient und hochgradig kompetent prüfen können.

Die hohen Anforderungen an die Fachkompetenz des IT-Prüfers gelten auch für die eher nicht-technischen «Management-Themen», also für Fragestellungen aus der Personalführung oder dem Projektmanagement – darüber hinaus vermehrt auch für die unterschiedlichsten Governance-Aspekte.

Eine gute Basis für eine breite Ausbildung für (IT-) Sicherheitsspezialisten oder (IT-) Prüfer auf Führungs- und Managementstufe sind unsere CISA-Vertiefungskurse, welche wir seit über 20 Jahren mit grossem Erfolg (und immer wieder angepasst an aktuelle Anforderungen und Gegebenheiten) anbieten: Die berufsbegleitende, fünfmonatige Ausbildung bereitet mit 15 Tagen Präsenzunterricht, ausführlichen und klar strukturierten Unterlagen (und Hausaufgaben!) auf die Tätigkeit im Beruf sowie auf die internationale CISA-Prüfung vor.

Der nächste CISA-Kurs startet am 8. Januar 2014 – mit einem «freiwilligen» Einführungstag am 13. Dezember 2013. Für sehr erfahrene Berufspraktiker bieten wir auch ein sehr kompaktes Prüfungstraining an, das am 31.3. startet. Auch im Herbst gibt es wieder zwei entsprechende Kurse.

Melden Sie sich baldmöglichst an! Informieren Sie sich auf unserer Website www.isaca.ch

WEITERE INFORMATIONEN

Weitere Details zum CISA-Zertifikat und zur entsprechenden Ausbildung finden Sie auf: www.isaca.ch

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
13.12.2013	VK 14|1	**Int. Zertifikatskurse CISA, CISM, CGEIT und CRISC Einführungstag**
10.01.2014	GOV-CH	**IT-Governance 2014|1 - ISACA Zertifikat**
10.01.2014	GOV-KK	**Governance – für IT, Security und Risikomanagement**
28.01.2014	AHS	**AHS Januar**
03.02.2014	AUD-CH	**IT-Audit 2014|1 - ISACA Zertifikat**
03./04.2.2014	AUD-KK	**Standards und Verfahren der (IT-) Revision**
06.02.2014	IRM-CH	**IT-Risikomanagement 2014|1 - ISACA Zertifikat**
06.02.2014	ISM-CH	**Informationssicherheits-Management 2014|1 - ISACA Zertifikat**
06.02.2014	RM-KK	**Risikomanagement-Methoden wirksam anwenden**
07.02.2014	PER-KK	**Effizientes Messen von Leistungs- und Risiko-Indikatoren**
27./28.02.14	PVS-RW	**Wie vermeidet der Prüfer im Sicherheitsumfeld, dass er selber zum Risiko wird?**
03.03.2014	STR-KK	**Strategische Ausrichtung von Geschäft (Business) und Informatik (IT)**
www.itacs.ch		
17.-19.03.14	COB-FD	**ISACA COBIT 5 Foundation Zertifikat von ISACA**
www.glenfis.ch		

IMPRESSUM ISACA NEWS

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Kurssekretariat, c/o ITACS Training AG, Stampfenbachstr. 40, 8006 Zürich
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