Information Systems Audit and Control Association

News Letter

Nr. 66, November 2003

Thema Zertifizierungen

Switzerland Chapter
Germany Chapter
Austria Chapter

© 14.11.2003

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o Monika Josi
Novartis Animal Health
Global Information Technology
WRO-1032.1.90
4002 Basel

Redaktion:
Max F. Bretscher
KPMG Fides Peat
Badenerstrasse 172
8026 Zürich

Satz und Gestaltung:
WissensTransfer
Francesca Lüscher Baglioni,
8235 Lohn, SH

Jeder Nachdruck, auch auszugsweise, sowie Vervielfältigungen oder sonstige Verwertung von Texten oder Abbildungen aus dem *NewsLetter* nur mit schriftlicher Genehmigung des Herausgebers unter voller Quellenangabe.

Abo-Preis:
Mitglieder gratis
Abonnemente und Einzelnummern auf Anfrage

Inserate:
1 Seite CHF 400.–
1/2 Seite CHF 240.–
1/4 Seite CHF 160.–

Erscheint 5 Mal jährlich
Auflage: 1050 Exemplare

Nächste Ausgabe (Thema: Customer Relationship Management): Februar 2004, Redaktionsschluss: 12. Januar 2004

Inhaltsverzeichnis

Editorial 4

Zertifizierungen – Vertrauen dank der Informationssicherheits-Zertifizierung British Standard BS7799-2 (ISO 17799) 5

Zertifizierungen – Vom Wert eines Zertifikates 10

Zertifizierungen – Die Fachmitteilung Nr. 9: Software-Zertifizierung 12

Zertifizierungen – Qualitätszertifizierung für KMU – Sinn oder Unsinn? 13

Zertifizierungen – Ein Überblick gängiger Berufsexamen 16

Zertifizierungen – Webtrust$^{SM/TM}$ – Zertifizierung für Zertifizierungsstellen 17

Zertifizierungen – Qualitätszertifizierung (SIO 9000) 20

Buch des Monats – Risiken einer IT-Abteilung bewirtschaften 23

The ISACA Crossword Puzzle 24

Express Line 26

DACH-News 28

Veranstaltungen 30

Germany Chapter 32

Austria Chapter 33

Switzerland Chapter 34

Editorial

Gäste, die bei mir zuhause zum ersten Mal auf die Toilette müssen, kommen oft schmunzelnd heraus. Warum? Dort hängen nämlich sämtliche Diplome und Zertifikate meiner Familie: Das First Certificate meiner Tochter, eine Bestätigung des Bestehens des Hundertkilometermarsches meines Sohnes, das Bachelor-Diplom meiner Ehefrau, ja sogar mein Diplom als CDPA (ein Titel, der gar nicht mehr gebraucht werden darf, weil er zu nahe am CPA war und flugs durch den CISA ersetzt wurde) usw. Im Total über zwanzig solcher Helgen.

Weit gefehlt, dass ich die Diplome und Zertifikate gering schätzte: Schliesslich geht jedermann durchschnittlich ein- bis zweimal täglich aufs Klo. Wenn er vergessen hat, eine Zeitung mitzunehmen, hat er dabei bei mir die Möglichkeit, die Leistungsausweise der Familie in aller Musse zu betrachten. Was er daraus schliesst, ist wohl insbesondere (diesem Ort angemessen) seine Privatsache.

Was sind Zertifikate wirklich wert? Diese Frage hat sich das Redaktionsteam gestellt, als es das Schwerpunktthema dieser Nummer des *NewsLetters* bestimmte. Die wenigsten Zertifikate zeigen eine Qualifikation auf (Ausnahmen, wie mein lic., auf dem *cum laude* prangt, sind rar). Doch auch diese Benotungen sind lediglich eine Bestätigung einer Momentaufnahme. In Berufskreisen hörte ich schon oft den Kommentar: „Wichtig ist, dass Du das Diplom hast. Mit welchen Noten Du es erworben hast, interessiert später niemanden mehr.“ Ist dies so? In dieser Nummer werden verschiedene „Zertifikate“ vorgestellt. Sie alle nehmen in Anspruch, in der einen oder andern Form einen Wert aufzuweisen.

Da die Halbwertszeit des Wissens in der heutigen Zeit immer kürzer wird, nimmt auch die Aussagefähigkeit eines solchen Zertifikats allerdings schnell ab. Aus diesem Grund verlangen viele „Titel“ heute den Nachweis der Weiterbildung auf dem Gebiet des „Zertifikats“, wenn es die Gültigkeit behalten soll. Und das Einhalten dieser Forderung, so meine ich, ist mehr wert, als das Zertifikat selbst.

Wie auch immer: Der Inhaber eines Zertifikates wird stolz sein. Er darf dies, weil er zumindest im Zeitpunkt des Erwerbs einen geforderten Leistungsausweis erbracht hat. Viele Leute hängen ihre Zertifikate denn auch an prominentere Stellen als ich. Der Zahnarzt ins Wartezimmer, der Restaurateur neben das Tagesmenü in der Garderobe, der Revisor ins Sitzungszimmer, usw.

Lassen Sie, liebe Leserin, lieber Leser, sich durch die Lektüre über Sinn, Zweck und Aussagefähigkeit der diversen Zertifikate informieren. Vielleicht werden Sie ermuntert, das eine oder andere Diplom zu erwerben oder durch Ihren Arbeitgeber erwerben zu lassen. Andererseits sind Sie sicher besser in der Lage, den Wert einer solchen Bestätigung einzuschätzen, wenn Sie mehr über Entstehung und Inhalt wissen.

Max F. Bretscher

Zertifizierung

Vertrauen dank der Informations-sicherheits-Zertifizierung British Standard BS7799-2 (ISO 17799)

Informationssicherheit ist heute als wichtiger und unterstützender Faktor hinter vielen e-business-Lösungen geworden. Während durch die Externalisierung von Anwendungen und Prozessen bereits erhöhter Sicherheitsbedarf besteht, sind es auch die Kunden und Partner des Unternehmens, welche von ihm die Umsetzung nötiger Sicherheitsmassnahmen fordern. Der Schutz von Daten, Integrität und die Verfügbarkeit der Systeme sind im e-business-Zeitalter damit zu einer unternehmensübergreifenden Herausforderung geworden. Eine umfassende Sicherheitslösung besteht aus einer Kombination von Technologie, Regeln, Verfahren und dem Schulungsprozess der Mitarbeiter. Durch eine Zertifizierung nach dem British Standard BS7799-2 des Informations-Sicherheits-Management-Systems (ISMS) eines Unternehmens kann diese Anforderung umgesetzt werden.

Nutzen und entscheidende Erfolgsfaktoren einer BS7799-2 Zertifizierung für Ihre Unternehmung

Die Erfahrung hat gezeigt, dass die folgenden Faktoren oft entscheidend für die erfolgreiche Implementierung von Informationssicherheit innerhalb einer Organisation sind:

- Sicherheitspolitik, -ziele und -aktivitäten als Ausdruck der Geschäftsziele;
- Implementierung von Sicherheit in Übereinstimmung mit der Organisationskultur;
- Offenkundige Unterstützung und Engagement seitens der Geschäftsführung;
- Einheitliche Vorgehensweise für den Einsatz eines hohen Sicherheitsstandards mit einem möglichst optimalen Kosten-Nutzen-Verhältnis;
- Eingehende Kenntnis der Sicherheitsanforderungen, der Risikoanalyse und des Risikomanagements;
- International anerkanntes Zertifikat im Bereich Informationssicherheit gegenüber dem Kunden und dem Markt ohne interne Gegebenheiten aufdecken zu müssen;
- Sicherheitsrahmenwerk für Vertraulichkeit, Integrität, Zuverlässigkeit, Verfügbarkeit, Datenschutz, Führung, Genauigkeit, Benutzbarkeit und Transparenz;
- Effektives Marketing von Sicherheit gegenüber allen Managern und Mitarbeitern;
- Umfassendes und ausgewogenes Masssystem zur Leistungsbeurteilung beim Informationssicherheitsmanagement (Effektivität, Effizienz);
- Verteilung von Sicherheits-Richtlinien über Informationssicherheitspolitik und Normen an alle Angestellte und Auftragnehmer.

Eine Zertifizierung kann die Informationen sicherer machen, aber nicht alle Unternehmens-risiken ausschliessen

An der Tatsache, dass es keine hundertprozentige Sicherheit geben kann, vermag auch eine Zertifizierung des Informations-Sicherheits-Management-Systems (ISMS) nicht zu rütteln. Es kann behauptet werden, dass die Informationssicherheit eines Unternehmens nach der Zertifizierung besser ist als zuvor, doch das Umgehen mit den Risiken ist weiterhin Chefsache und muss von der Geschäftsleitung getragen werden. Dass Verbesserungspotential liegt in der Vorbereitung auf die Prüfung und in den Verbesserungsmassnahmen nach der Prüfung und nicht in der Prüfung selbst.

Es ist deshalb ein verbreiteter und auch sinnvoller Ansatz, das Informations-Sicherheits-Management-Systems (ISMS) eines Unternehmens auf der Grundlage der Norm 17799 der International Organization for Standardization (ISO) aufzubauen. Fehlen einem Unternehmen die dafür erforderlichen Spezialisten, können dazu externe Fachleuten beigezogen werden. Kann der Aufbau intern geleistet werden, ist zumindest eine Zweitbeurteilung durch einen Externen zu empfehlen. Lässt das Unternehmen danach noch eine Zertifizierung vornehmen, entstehen zwar

zusätzliche Kosten; das Sicherheitsniveau wird auf diesem Weg nicht mehr verändert. Die zusätzlichen Kosten für eine Zertifizierung können deshalb nicht ohne weiteres mit einer Verbesserung des Sicherheitsniveaus rechtfertigt werden.

Eine Zertifizierung kann für ein Unternehmen sinnvoll sein, wenn das Zertifikat und auch die zertifizierende Stelle vertrauenswürdig sind. Hier besteht durchaus die Gefahr, dass der Wert einer Zertifizierung generell gefährdet werden könnte, wenn allzu viele Anbieter mit Zertifikaten und Gütesiegeln auf den Markt drängen, deren Qualität nur schwer oder gar nicht überprüft werden kann.

Das Vertrauen in ein Zertifikat leidet auch dann, wenn es zu sehr als Marketinginstrument eingesetzt wird und wenn Zweifel darüber bestehen, ob die Prüfung tatsächlich in einer Art und Weise durchgeführt wird, die geeignet ist, den mit der Prüfung verbundenen Anspruch einzulösen. Die Zertifizierung nach ISO 9000ff beispielsweise ist solchen Kritiken ausgesetzt.

Weshalb eine Sicherheits-Zertifizierung sinnvoll sein kann

Folgende Gründe können für eine Zertifizierung des Informations-Sicherheits-Management-Systems (ISMS) eines Unternehmens nach BS7799-2 vorgebracht werden:

Selbstverpflichtung
Für den Einzelnen, wie auch für Unternehmen erhöht sich die Chance, dass Ziele zuverlässiger erreicht werden, wenn zusätzlich zur Selbstverpflichtung eine Überprüfung der Zielerreichung durch Dritte erfolgt. Genau so wie für ein Individuum die nahende Prüfung zum Lernen motiviert, sorgt die Zertifizierung im Unternehmen für den Druck, mit dem sich die Informationssicherheit in der Prioritätenliste der einzelnen Mitarbeiter nach oben schieben lässt.

Organhaftung
Verwaltungsrat und Geschäftsleitung eines Unternehmens, die kein effektives Informations-Sicherheitsmanagement initiiert haben, können im Schadenfall im Rahmen der Organhaftung zur Rechenschaft gezogen werden. Sicher können die genannten Organe einer Gesellschaft ihre Verantwortung auch über andere Massnahmen als über eine Zertifizierung des Informations-Risikomanagements wahrnehmen. Üblicherweise dienen Informations-Sicherheitsstrategien und -Konzepte unter anderem auch als Beleg dafür, dass die Verantwortung für die Sicherheit der Informationen erkannt und ordnungsgemäss delegiert wurde. Das Zertifikat unabhängiger Sachverständiger unterstützt dieses Vorgehen, indem es der Unternehmensleitung nicht nur attestiert, dass sie selbst ihre Verantwortung erkannt hat, sondern auch, dass die Mitarbeiter an welche die Verantwortung delegiert wurde, diese auch wahrgenommen haben.

Leistungsausweis
Wie können die Mitarbeiter, die der Geschäftsleitung gegenüber für das Informations-Sicherheitsmanagement verantwortlich sind, nachweisen, dass sie ihre Aufgaben erfüllt haben? Ein Assessment durch unabhängige Fachleute gibt Aufschluss darüber, wie es um das Informations-Sicherheits-Management-Systems des Unternehmens steht. Für den Fall einer positiven Beurteilung ist das Zertifikat auch ein Leistungsausweis für die verantwortlichen Mitarbeiter des Unternehmens. Die Vertrauenswürdigkeit eines BS 7799-2 Zertifikates wird wohl von den meisten Geschäftsleitungen als vertrauenswürdiger angesehen, als die Resultate eines Assessments, die möglicherweise in einer für sie unverständlichen Sprache niedergeschrieben wurden.

Die Zertifizierung als Instrument der internen Kommunikation

Der grösste Nutzen einer Zertifizierung liegt möglicherweise darin, dass sie als Anlass genommen werden kann, sowohl innerhalb wie auch ausserhalb über die Wichtigkeit des Informations-Sicherheitsmanagements für das Unternehmen zu informieren. Handelt es sich um ein als vertrauenswürdig anerkanntes Zertifikat, erhöht sich dadurch die Glaubwürdigkeit des Bekenntnisses der Geschäftsleitung zur Informationssicherheit.

Der Erfolg des Informations-Sicherheitsmanagements ist davon abhängig, dass sich die Mitarbeiter aller Stufen bewusst sind, für welche Aspekte der Informationssicherheit sie persönlich verantwortlich sind und, dass sie wissen, wie sie ihre Verantwortung wahrnehmen können. Im Arbeitsalltag kommt der Informationssicherheit in der Regel eine untergeordnete Bedeutung zu. Die

dringender erscheinenden operativen Aufgaben werden prioritär angegangen. Um die Sicherheit kümmert man sich, wenn noch Zeit dafür bleibt. Hier kann der von einer Zertifizierung ausgehende Zeitdruck die Kultur des Unternehmens beeinflussen. Informationssicherheit rückt dadurch in der Prioritätenliste nach oben. Wenn es der Unternehmensleitung zudem gelingt, den Mitarbeitern zu vermitteln, dass die Vorbereitung auf die Zertifizierung als gemeinsame Anstrengung aller Mitarbeiter zur Erreichung eines für den Unternehmenserfolg wichtigen Ziels ist, kann die erfolgreiche Zertifizierung zu einem kollektiven Erfolgserlebnis werden. Erachtet hingegen die Unternehmensleitung selbst die Zertifizierung als lästige Pflichtübung, werden es auch die Mitarbeiter tun.

Um ein nachhaltiges Aufrücken der Informationssicherheit in der Werteordnung des Unternehmens zu bewirken, darf es bei der Zertifizierung nicht bei einem einmaligen Effort bleiben. Dadurch, dass die Zertifizierung regelmässig erneuert werden muss, liefert sie aber auch den äusseren Anlass, um das Thema ständig aktuell zu halten.

Die Zertifizierung als Instrument der externen Kommunikation

Die Zertifizierung kann unter bestimmten Voraussetzungen das Unternehmen darin unterstützen, gegen aussen auf die Vertrauenswürdigkeit seiner Informationsbearbeitung hinzuweisen. Geschäftspartnern und Kunden sollen Belege dafür geliefert werden, dass sie es mit einem vertrauenswürdigen Unternehmen zu tun haben.

Vertrauenswürdig zu sein reicht jedoch nicht aus, um das Vertrauen von Geschäftspartnern und Kunden zu gewinnen. Diese müssen das Unternehmen aus ihrer eigenen Perspektive als vertrauenswürdig erkennen können. Ein wesentlicher Faktor dafür ist der gute Ruf des Unternehmens selbst. Ein Zertifikat kann hier unterstützend wirken. Voraussetzung dafür ist allerdings, dass das Zielpublikum das Zertifikat als Indiz für Vertrauenswürdigkeit anerkennt. Das wiederum ist abhängig davon, ob dem Zielpublikum Sinn und Zweck des Zertifikats hinreichend bekannt ist und es davon überzeugt ist, dass das Zertifikat mit dem Nachweis eines hohen Sicherheitsniveaus errungen wird und nicht bloss gekauft wurde. Deshalb kommt auch dem Vertrauen des Zielpublikums in die zertifizierende Instanz und die Behörde welche diese Instanz überwacht, eine erhebliche Bedeutung zu.

Unternehmen, die bei Ihren Geschäftspartnern und Kunden bereits ein hohes Vertrauen geniessen, werden dies durch eine Zertifizierung kaum erheblich steigern können. Unternehmen hingegen, die ihre Vertrauenswürdigkeit verstärkt kommunizieren möchten oder in einem Markt noch wenig bekannt sind, können unter den genannten Voraussetzungen von einer Zertifizierung profitieren.

Vorbereitung auf die Zertifizierung

Damit ein Unternehmen eine Zertifizierung nach BS7799-2 erfolgreich bestehen kann, sollte das Informations-Sicherheitsmanagement

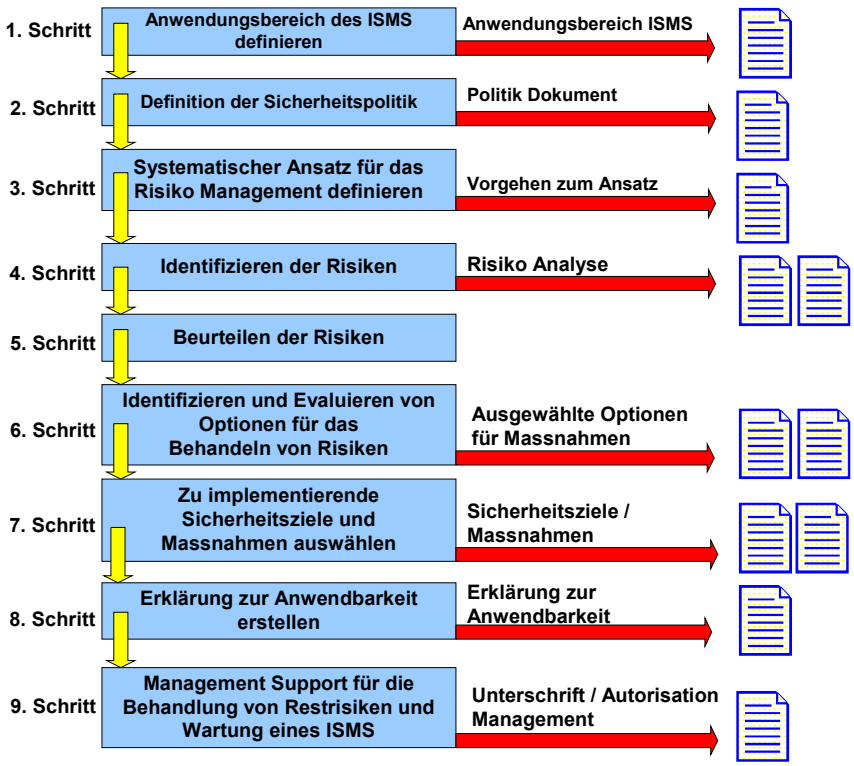


Bild 1: Risiko und Assessment Management Prozess nach BS7799-2 (ISO 17799)

bereits anhand der in dem Standard gemachten Empfehlungen aufgebaut werden. Der Standard sieht dafür ein Vorgehen in folgenden sechs Schritten vor:

1. Schritt
Der Anwendungsbereich des Managementsystems für Informationssicherheit ist zu bestimmen. Die Grenzen hinsichtlich der Merkmale der Organisation, ihres Standortes, ihrer Werte und ihrer Technologie sind festzulegen.

2. Schritt
Die Informationssicherheitspolitik ist zu definieren. Dabei soll von der Geschäftsführung ein Dokument zur Informationssicherheitspolitik genehmigt werden, welches die Unternehmung veröffentlicht und nach Bedarf an alle Mitarbeiter verteilt.

3. Schritt
Ein für die Unternehmung angemessener Ansatz bzw. Prozess für das Risiko-Management ist zu definieren. Dabei sind die Ziele für die Identifikation von Geschäftsinformation, rechtliche Aspekte und Richtlinien innerhalb der Unternehmung zu berücksichtigen. Somit werden auch Kriterien für die Akzeptanz von Risiken und der Level eines Sicherheitsrisikos definiert.

4. Schritt
Die Identifikation der Werte innerhalb des definierten ISMS-Anwendungsbereichs werden mit den Verantwortlichen (Prozess Owner) definiert. Zusätzlich sind die Gefahren, Verwundbarkeiten und Auswirkungen auf bestimmte Kernelemente unter Berücksichtigung der Vertraulichkeit, Integrität und Verfügbarkeit zu identifizieren.

5. Schritt
Die zu verwaltenden Risikobereiche sind auf der Basis der Informationssicherheitspolitik der Organisation und des erforderlichen Grades zur Gewährleistung der Sicherheit zu beurteilen.

6. Schritt
Es sind Optionen für die Behandlung von Risiken zu evaluieren. Bei der Entwicklung von Optionen ist zu berücksichtigen, dass der Prozess der kostenmässig vertretbaren Identifizierung, Beschränkung und Minimierung bzw. Elimination von Sicherheitsrisiken, die Informationssysteme beeinträchtigen können.

7. Schritt
Es sind selektive Sicherheitskontrollziele im ISMS einzubauen, welche die Risiko-Behandlung in der Unternehmung unterstützen.

8. Schritt
Für die umzusetzenden Sicherheitskontrollziele ist eine Anwendbarkeitserklärung zu erstellen, die Massnahmen und Aktionen für die bestimmten Sicherheitskontrollziele beschreibt. Die Anwendbarkeitserklärung soll vom Management unterschrieben und falls nötig periodisch aktualisiert werden.

9. Schritt
Ein Management-Unterstützungsprozess soll aufrecht gehalten werden. Das Management muss die Restrisiken der Unternehmung kennen und es muss die umgesetzten Sicherheitskontrollziele mit Ressourcen und Budget unterstützen.

Ablauf einer BS7799-2 Zertifizierung

Beim erstmaligen Audit prüft die Zertifizierstelle, ob das Informationssicherheits-Managementsystem (ISMS) der Unternehmung die Vor-

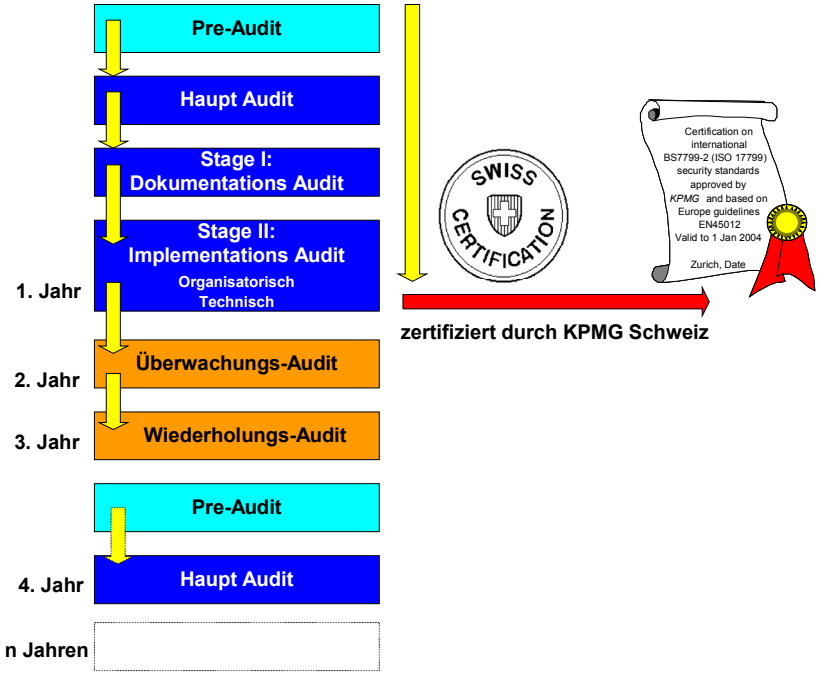


Bild 2: Zeitlicher Ablauf einer BS7799-2 (ISO 17799) Zertifizierung

aussetzungen für eine Zertifizierung nach British Standard BS7799-2 erfüllt. Insbesondere wird geprüft, ob die Unternehmung vom ISMS-Geltungsbereich keine Elemente ihres Betriebs ausschliesst, die notwendigerweise dazu gehören.

Im Pre-Audit werden die zwingenden Kontrollziele des BS7799-2 geprüft und zusätzlich die Grundlage zum ISMS analysiert. Auch die versicherungstechnischen Fragen und finanziellen Aspekte werden bereits im Pre-Audit auf Richtigkeit geprüft.

Das Haupt-Audit umfasst die Durchsicht und Begutachtung der relevanten Dokumentation (Dokumentations-Audit, Phase I), die Befragung der verantwortlichen Personen (Implementations-Audit, Phase II organisatorisch), die Beobachtung und die stichprobenweise Prüfung der Kontrollverfahren. Des Weiteren werden im Haupt-Audit (Implementations-Audit, Phase II, technisch) auch die technischen Sicherheitskonfigurationen auf dem Niveau Netzwerk, Betriebssysteme, Datenbanken und Applikation kontrolliert.

Nach einem Jahr wird ein Überwachungs-Audit für den zu zertifizierenden Prozess durchgeführt, dabei werden die Management-Kontrollen sowie weitere präventive, detektive und korrektive Massnahmen geprüft.

Nach zwei Jahren sollen durch ein Wiederholungs-Audit die Kontrollverfahren der zu zertifizierenden Prozesse ergänzend einem detaillierten Audit unterzogen werden, dabei soll das vollständige ISMS in Bezug auf Änderungen im Betrieb kontrolliert werden und sicherstellen, ob das ISMS gesamthaft wirksam geblieben ist.

Ein erfolgreiches Audit wird mit einem international anerkannten Zertifikat basierend auf dem British Standard BS7799-2 bescheinigt, dass nach dem offiziellen Europäischen Vertrag (EA Mulilateral Agreement Signatories EA-1/08, European Standard EN 45012 accreditation to certification body guidelines and ISO/IEC 62) weltweit seine Gültigkeit hat. Dieses BS7799-2-Zertifikat bescheinigt, dass die Unternehmung ihre Sicherheitskontrollziele umfassend berücksichtigt und implementiert hat und Sicherheitsmechanismen gemäss ISO 17799 Standard konform umgesetzt hat.

Fazit

Aufgrund der zunehmenden Bedeutung der Informatik in Banken, Versicherungen, Industrie und Verwaltung ist der Informationssicherheit und den eingesetzten Systemen hoher Stellenwert einzuräumen. Dies bedingt den Schutz der Infrastruktur gegen äussere Einflüsse. Heute hat man die Möglichkeit, mit den Massnahmen und notwendigen Kontrollzielen des British Standards BS7799-2 ein sicheres Informations-Sicherheits-Management-System (ISMS) aufzubauen. Der British Standard BS7799-2 ist eine adäquate Methode und kann mit Hilfe von diszipliniertem Fachpersonal und Benutzern eine hohe Sicherheit in der Unternehmung gewähren. Der Leitfaden BS7799-2 als Sicherheitsrahmen kann als Ausgangspunkt für die Entwicklung eines organisatorischen und technischen ISMS zu nutzen sein. Darüber hinaus kann mit einer Zertifizierung BS7799-2 die Konformität zu sämtlichen Kontrollzielen und Massnahmen im Bereich Informationssicherheit verhelfen, diese umzusetzen und dem Management sowie dem Kunden das nötige Vertrauen schenken.

Reto P. Grubenmann, IRM KPMG Zürich

EN 45012
Quality management system for accredited enterprises

ISO/ICE Guide 62
General requirements for accreditation bodies

EA Guidelines EA-7/03
Europäischen Richtlinie für den Prozessablauf

ISO 10011-1
Leitfaden für das Audit von Qualitätssicherungssystemen, Teil 1: Audit

ISO 10011-2
Leitfaden für das Audit von Qualitätssicherungs-systemen, Teil 2: Qualifikationskriterien für Qualitätsauditoren

BS7799-2 (ISO 17799)
Zertifizierte, Leitende Auditoren BS7799-2 durch das British Standard Institut in England.

Bild 3: Qualitäts-Management System der KPMG und METAS-SAS für akkreditierte Unternehmen

Zertifizierung

Vom Wert eines Zertifikates

Mein Unverständnis über das Verhalten der verantwortlichen Vorgesetzten

"Leider muss ich Ihnen, infolge eines negativen Unternehmensentscheides, die Teilnahme an der CISA-Ausbildung absagen"

Während wir in den letzten Vorbereitungen zum diesjährigen CISA-Kurs stecken, erreicht uns eine Hiobsbotschaft nach der anderen. Bei einzelnen Mails rinnen die Tränen aus dem Bildschirm und ich muss einen Kurzschluss meines geliebten Powerbook befürchten.

Ein Blick über den Bildschirmrand hinaus bestätigt mir, dass derzeit ein extremes Ungleichgewicht im Markt herrscht. Um die wenigen Personen, welche anscheinend noch über ein Ausbildungsbudget verfügen, kämpfen verschiedene Anbieter bis aufs Messer. Einige haben bereits die Waffen gestreckt oder befinden sich in Nachlass-Stundung (z.B. Digicomp).

Bis vor kurzem konnten wenigstens die Anbieter von Nachdiplomkursen resp. Kurse mit anerkanntem Zertifikatsabschluss ihre Klassen einigermassen füllen. In der letzten Zeit sind aber weitere neue Zertifikate aufgetaucht – jetzt ist es wohl bald dem letzten Personalchef klar, dass nicht alle dieser Zertifikate das Papier wert sind, auf dem sie gedruckt sind. Ein "Certified … … … " ist bei manchen Unternehmen geradezu in Verruf geraten. Wie soll man da die Spreu vom Weizen trennen?

"Zu meinem grossen Bedauern wurde mir der bereits bewilligte Kurs wieder gestrichen"

Die ganze Ausbildungssituation wird noch dadurch verschärft, dass heute jede und jeder Kurse anbietet. Ich bin an sich stolz auf unsere Handels- und Gewerbefreiheit, beobachte aber diese Entwicklung mit Sorge. Einige (Beratungs-)Unternehmen scheinen ihren Mitarbeitern eine neue Beschäftigungstherapie angeordnet zu haben: "Wir haben gerade keine Aufträge. Macht doch mal einen Kurs oder so!" Dieser Trend führt zu zwei gegenteiligen Entwicklungen: Auf der einen Seite gibt es Kurse zu teils unverschämten Preisen, wo im methodisch/didaktischen Bereich unbedarfte Laien mehrtägige Ausbildungen durchführen. Deren Kursteilnehmer sind oft dermassen enttäuscht, dass aufgrund des schlechten Feedback ganzen Abteilungen die Kurse generell gestrichen werden nach dem Motto: "*ein* Kurs schlecht, *alle* Kurse schlecht". Auf der anderen Seite gibt es hervorragend zusammengestellte Kurse von Top-Spezialisten. Da man damit die manchmal herumsitzenden Berater beschäftigen möchte, werden solche Kurse teilweise zu absoluten Spottpreisen oder sogar gratis angeboten. Diese Quersubventionierung führt aber dazu, dass realistisch kalkulierende Kursanbieter weiter unter Druck geraten und früher oder später vom Markt verschwinden.

Die Qualität eines Kurses scheint anscheinend in vielen Fällen keine Korrelation mehr zum Kurspreis aufzuweisen. Zertifikats-Abschlüsse geraten in Verruf, weil erstens einige wirklich kurrligen Zertifikate vorhanden sind und andererseits an sich anerkannte Zertifikate bei mehreren Anbietern in unterschiedlichsten Qualitätsstandards angeboten werden. Und die zur Qualitätssicherung vorgesehene Zertifizierung derjenigen Schulen, welche solche Zertifikats-Kurse anbieten, führt primär einmal zu einer weiteren Verteuerung für seriöse Anbieter.

"Aus Gründen der Gleichbehandlung darf ich Ihren Kurs nicht besuchen, obwohl ich sowohl für das Kursgeld, wie auch für die Zeit selber aufkommen möchte"

Am gestrigen "After-hour" Seminar in Zürich (für Mitglieder von ISACA-CH gratis) wurde von einem Teilnehmer erwähnt, dass angesichts der zahlreichen Entlassungen derzeit grundsätzlich keine Kurse mehr für die Mitarbeiter bewilligt werden. Auf den ersten Blick scheint dieser Entscheid vernünftig zu sein – warum soll man einzelnen Mitarbeitern Kursgeld oder Arbeitszeit gewähren, während andere Mitarbeiter auf die Strasse gestellt werden? Dieser Entscheid eines Personalverantwortlichen oder Linienchefs ist aber trotzdem katastrophal, führt dies doch sofort zu einer (weiteren) Verschlechterung des

Arbeitsklimas (mit allen negativen Folgen wie Arbeitsverweigerung oder kriminellen und anderen unerwünschten Machenschaften) und mittelfristig zu weniger kompetenten und damit auch weniger effizienten Mitarbeitern. Und während die Bosse sich nach wie vor an den Fringe-Benefits laben, dürsten ihre Mitarbeiter nach Wissen, Ausbildung und letztlich auch Anerkennung.

"Wir werden auch dieses Jahr den CISA-Kurs wieder für Arbeitslose bewilligen"

In dieser traurigen Situation gibt es von einer unerwarteten Seite einen Lichtblick. Seit mehreren Jahren wird der Besuch des CISA-Kurses von den Arbeitslosenämtern in den verschiedenen Kantonen unterstützt. Von den 39 Teilnehmern im Kurs 2003 waren deren fünf bei Kursbeginn arbeitslos; ihre Kurskosten wurden zu einem grossen Teil (teils vollständig) übernommen – wobei wir damals Arbeitslosen einen Rabatt von 20% gewährten. Die RAV-Spezialisten mit ihrem grossen Marktüberblick sind anscheinend der Ansicht (und das zu Recht!), dass das CISA-Zertifikat (und auch der CISA-Kurs) die Vermittlungsfähigkeit von Arbeitslosen so stark verbessert, dass sich die grosse finanzielle Investition lohnt. Auch dieses Jahr sind knapp 10% der eingeschriebenen Kursteilnehmer arbeitslos – und werden vom ISACA Switzerland Chapter mit bis zu Fr. 500.– pro Kopf unterstützt. Die RAV-Ansicht wird durch eine vor zwei Jahren durchgeführte Umfrage bestätigt: 71% der befragten CISA gaben an, dass dieses Zertifikat ihre Berufskarriere gefördert hat.

31 000 Personen haben bis heute das CISA-Zertifikat erworben und bereits etwa 1 000 das neue CISM-Zertifikat. Das zeigt doch ziemlich deutlich die Bedeutung der beiden Zertifikate. Auch in der Schweiz haben wir bereits 250 "aktive" CISA und rund 15 CISM. Während in der Schweiz in der Informatikrevision von Unternehmen wie Banken und Versicherungen der CISA-Kurs oder mindestens das CISA-Zertifikat grundsätzlich etabliert ist (mit den oben genannten Einschränkungen), sind CISA im Sicherheitsbereich anteilmässig noch etwas untervertreten. Zwar kommen seit einigen Jahren deutlich mehr als 50% der Kursteilnehmer aus Sicherheitsfunktionen, doch ist die Konkurrenz der Zertifikate im Sicherheitsumfeld recht gross: Neben dem IT-Governance orientierten CISA ("to be in control") und dem technisch versierten CISSP gibt es verschiedene andere anerkannte "Zertifikate" in Form von Nachdiplomkursen/-studien.

"Dieses Jahr haben wir kein Budget. Bitte merken Sie mich für den nächsten CISM-Kurs im 2004/05 vor"

Lassen Sie mich diesen *NewsLetter*-Beitrag noch mit einer (weiteren) persönliche Note abschliessen. Ich bin überzeugt, dass ein CISA-, CISM- oder auch CISSP-Zertifikat eine Aussage über die Befähigung eines Mitarbeiters machen kann. Diese Ansicht teilten auch mehr als 75% aller befragten ISACA-Mitglieder in einer Umfrage vor zwei Jahren. Eine Untersuchung von Foote Partners zeigte sogar auf, dass von 24 000 befragten Personen in 39 technischen Berufen die CISA den höchsten Bonus erhielten – mit 10% deutlich mehr als alle anderen Zertifikate (mehr dazu auf der Homepage von ISACA). Mehr Geld bekommt man aber in der Regel für mehr Leistung und nicht einfach für einen Titel oder ein Zertifikat.

Interessiert an einem Zertifikat wie CISA, CISM, CISSP, CNSP oder SANS/GIAC? Gibt es einen anerkannten Kurs dafür? Schauen Sie sich Ihren Kursanbieter sehr genau an: Was bietet er? Was alles ist inklusive? Hatten seine Kursteilnehmer in der Vergangenheit Erfolg? Vermittelt er Fachwissen oder nur ein Prüfungstraining? Sprechen Sie mit den Teilnehmern früherer Kurse und dann mit ihrer Chefin oder ihrem Chef.

P.S.
Wie so oft, trage ich auch beim Schreiben dieses *NewsLetter*-Beitrages mehrere Hüte gleichzeitig: Als Ausbildungsverantwortlicher des ISACA Switzerland Chapter liegen mir die ISACA-Zertifikate etwas näher als andere. Als Anbieter der offiziellen CISA- und CISM-Kurse in der Schweiz verfolge ich natürlich auch wirtschaftliche (Eigen-)Interessen. Und als Berufsmann mit unterdessen 20 Jahren Erfahrung auf dem Buckel bin ich der Ansicht, dass jede gezielte, seriöse und fachbezogene Ausbildung wichtiger ist, als ein allenfalls erworbenes Zertifikat – wobei eine Kombination dieser beiden Aspekte natürlich nicht zu übertreffen ist.

P.P.S.
Die kursiv gesetzten Textstellen sind Zitate aus Mails oder Telefonaten

der vergangenen Wochen und sind leider typisch.

Peter R. Bitterli, CISA und bald auch CISM

Zertifizierungen

Die Fachmitteilung Nr. 9: Software-Zertrifizierung

Es war im Jahr 1979, als ich den ersten Auftrag erhielt, der in Richtung Software-Zertifizierung zielte.

Ein Programmierer in Genf hatte eine Software erstellt, die er für das Führen einer Finanzbuchhaltung auf den damals noch in den Kinderschuhen steckenden PCs geeignet hielt. Als Verkäufer für die Firma *Atari* kam es als selbstverständlich, dass er seine Software auf dieser Hardwareplattform erstellt hatte. Von mir bzw. meinem damaligen Arbeitgeber erhoffte er sich, durch ein Gütesiegel ein zusätzliches Verkaufsargument zu erwerben. Nach wenigen Handgriffen erkannte ich, dass das Programm wenig zur Unterstützung einer Führung nach Ordnungsmässigkeitskriterien beitrug. So war es mir mit Leichtigkeit möglich, einseitige Buchungen in das System und später dieses zum Absturz zu bringen. Als ich den Programmierer mit meinen Erkenntnissen konfrontierte, war er empört: „Mais vous avez corrompu les fichiers!“ Als ich ihn darauf hinwies, dass eben eine Gebrauchsanweisung fehle und ich mich als „unschuldiger“ Anwender benommen hätte, wollte er nichts mehr von mir wissen. Infolge seines absehbaren Konkurses schrieb ich das Honorar in den Himmel.

Somit entging ich glücklicherweise der Fussangel, eine Zertifizierung von mir gegeben zu haben, welche mir später wohl sehr viel Bauchschmerzen bereitet haben könnte.

Der damalige Fachstab für Informatik der Kammer nahm die Thematik 1984 wieder auf, weil von verschiedener Seite der Ruf nach Gütesiegeln für Software laut geworden war. Nicht nur Softwarehersteller, sondern insbesondere konventionelle Revisoren, waren daran interessiert, solche „Bestätigungen“ zu erhalten. Sie versprachen sich wohl dabei, die ihnen unheimlich erscheinende EDV-Revision umgehen und die damit zusammenhängende Verantwortung an den Zertifikatersteller abschieben zu können.

Somit befasste sich der Fachstab mit der Thematik. Zuerst stand eine Stellungnahme im „Treuhänder“ zur Diskussion, doch schliesslich rang man sich dazu durch, eine Fachmitteilung zu verfassen. Diese and eine Norm erinnernde Publikation sollte den konventionellen Revisoren aufzeigen, unter welchen Umständen sie sich auf das richtige Funktionieren einer Software verlassen könnten. Wo zuerst lediglich Produkte bezüglich Finanzbuchhaltung im Vordergrund standen, zeigte sich bald, dass die Aussagen für Software irgendwelcher Provenienz und Anwendung Gültigkeit besitzen müssten.

Was ebenfalls sehr schnell erkannt wurde, ist die Tatsache, dass eine Gewährleistung bezüglich Richtigkeit der Buchhaltung praktisch ausgeschlossen bleiben muss. Die richtigen Handhabung des Instrumentes ist durch eine Beschreibung oder Vorschrift zu leiten, und die richtige Eingabe der variablen Daten kann erst recht nicht beurteilt werden. Wo zuerst relativ grosse Euphorie bezüglich der Software-Zertifizierung geherrscht hatte, zeigte es sich, dass immer mehr Einschränkungen notwendig wurden, um den Missbrauch eines erstellten Zertifikats zu verhindern.

Im Jahr 1988 entstand damit die Fachmitteilung Nr. 9, welche sich über das Ziel der Zertifizierung, insbesondere die Verarbeitungsregeln, die Interne Kontrolle, die Dokumentation, die Ausgabe und Aufbewahrung (damals noch auf die alten Art. 92/3 OR abgestützt) sowie die Nachprüfbarkeit (Prüfpfad) äussert. Wichtige Hinweise waren darüber verfasst, was die Fachmitteilung regelt und was sie nicht regelt. Darin wurden die Grenzen schonungslos aufgezeigt.

Sowohl Softwarehersteller als auch Revisoren sahen ihre Erwartungen nicht erfüllt, und es fragte sich, ob die Fachmitteilung eine Totgeburt war.

Die rasante Entwicklung der Informatik brachte es nämlich mit sich, dass die Produkte in schnellem Wechsel immer wieder auf den neuesten Stand gebracht wurden, und damit ein Zertifikat wegen der Versionsbeschränkung wertlos wurde. Der Aufwand für eine Neuzertifizierung war für viele Hersteller neben der Tatsache, dass das Zertifikat bei seiner (endlichen) Erstellung bereits überholt war, einfach zu hoch.

Der konventionelle Revisor musste einsehen, dass die Umgebung, in welcher eine zertifizierte Software eingesetzt wurde, vielfach wichtiger war, als die Software selbst. Immerhin kann der Fachstab als bemerkenswerte Leistung in diesem Zusammenhang in Anspruch nehmen, sowohl Anwender als auch Revisoren für die Notwendigkeit der Verfahrenprüfungen einschliesslich Software sensibilisiert zu haben.

Max F. Bretscher

Zertifizierungen

Qualitätszertifizerungen für KMU – Sinn oder Unsinn?

Jede Zertifizierung ist aufwendig. Warum sollte sich ein kleines Unternehmen dem Stress und den Kosten eines solchen Vorganges aussetzen? Nicht jedes Unternehmen hat mit einer Qualitätszertifizierung wirklich gewonnen. Welches sind also die Kriterien, welche einen Entscheid für und wider erleichtern sollen?

Ich kann mich sehr genau an die Diskussionen erinnern, welche wir vor vier Jahren in der Geschäftsleitung geführt haben. Es ging damals um die Frage, ob wir nebst allen sicherheitstechnischen und fachlichen Zertifikaten nun auch noch ISO-Qualitätsmanagement einführen sollten. Unsere Firma beschäftigte zum damaligen Zeitpunkt ca. 10 Mitarbeiter. Eine Firmengrösse, welche sich den Luxus unnötiger Belastungen nicht leisten kann und will. Niemand hat bestritten, dass die Zertifizierung unter dem ISO-9001 Standard eine nette Sache wäre, aber die Meinungen bezüglich des zu erwartenden Nutzens waren sehr kontrovers. Die verschiedenen Argumente, welche zu unserem Entscheid führten sollen folgend kurz erläutert werden:

1. QA-Zertifikate statt Referenzen?

Zertifikate reduzieren im Umgang zwischen Fremden das maximal mögliche Enttäuschungspotential. Der Versuch zu standardisieren und den definierten Standard langfristig zu kontrollieren und durchzusetzen, gibt eine nicht zu unterschätzende Sicherheit. Wir finden heute überall Zertifikate in den unterschiedlichsten Formen. Ein Kind, welches am Sonntag nachmittag nach einem Big Mac schreit, will eine exakt definierte Leistung. Zweifellos verfügt *MacDonalds* weltweit nicht nur über alle externen QA-Zertifikate, sondern darüber hinaus auch über ein

berühmtes internes QA-Management. Das heisst aber nicht, dass der Bratwurststand um die Ecke oder dessen Kunde automatisch im Nachteil wäre, wenn dort offizielle Zertifizierungen fehlen.
Aus der vereinfachten KMU-Betrachtung lässt sich sagen, dass eine Zertifizierung sinnvoll oder notwendig ist, wenn

- berufsrechtliche Anforderungen dies erfordern,
- zwischen dem Kunden und dem KMU keine längere Beziehung besteht,
- die durch eine Zertifizierung optimierten Geschäftsprozesse die Kosten senken,
- der Marketingeffekt einer Zertifizierung den Umsatz oder die Marge steigert.

Es ist also sehr angebracht, sich vor allem über den Nutzen jeder Zertifizierung genau im Klaren zu sein. Fehlt der langfristige wirtschaftliche Nutzen, wird sich kein QA-Management halten können. Nach erfolgter Erosion der Qualitätsprozesse wird bald auf eine Erneuerung des Zertifikates verzichtet und das ISO-Label verschwindet mit schlechten Gefühlen und fantasievollen Ausreden von der Bildfläche. Was ist besser? Ein gutes Drei-Stern-Hotel, das seine Sache immer gut gemacht hat oder ein ehemaliges Vier-Stern-Hotel, dem der vierte Stern abhanden gekommen ist?

Bei grossen Unternehmen sehe ich den Sinn von Zertifikaten und QA-Management-Prozessen als unbestritten. Bei KMU bin ich hingegen sehr skeptisch. Unsere Firma ist als KMU dauernd im Kontakt mit grossen Kunden. Wir haben von etwa 100 Kunden nur einen, der weniger Mitarbeiter beschäftigt als wir. Wir müssen aufpassen, dass wir uns im täglichen Umgang mit grossen Kunden nicht am Schluss auch für gross halten. Was zählt, ist einzig und allein, einen guten Job zu machen und als KMU dafür zu sorgen, dass jeder Kunde zur aktiven Referenz unserer Leistungen wird. Wenn ich als Kunde entscheiden muss zwischen der Top-Garage mit den Top-Auszeichnungen und den Top-Preisen und dem von meinem besten Freund empfohlenen Kleinbetrieb mit garantierter Chefbetreuung und Preisen ohne Schnickschnack. Für wen würde ich mich entscheiden? Gute Referenzen sind immer noch erstes Ziel eines KMU. Wenn auch noch tolle Zertifikate dazukommen, umso besser.

2. Wie wichtig sind QA-Zertifikate für KMU-Kunden?

Erinnern Sie sich noch an die ISO-Euphorie vor 10–15 Jahren. Keine Firma ohne ISO9000-Zertifizierung werde zukünftig noch öffentliche Aufträge erhalten und die Wirtschaft müsse sich dieser Praxis sehr bald angeschlossen haben. Heute wissen wir, dass sich diese Prophezeiungen nicht erfüllt haben. Ein KMU wird von seinem Kunden nach viel persönlicheren Kriterien beurteilt. Normalerweise steht der Firmeninhaber für sein Unternehmen. Seine Ausbildung, Erfahrung und Persönlichkeit transportieren das Vertrauen, welches bei grösseren Firmen nicht mehr an einzelnen Menschen festgemacht werden kann. Ob ein ISO-Zertifikat im Büro oder Besprechungszimmer hängt, ist für die Auftragsbücher eher zweitrangig. Gerade die Treuhandbranche lebt ja von langfristigen persönlichen Beziehungen und Vertrauen. Viele der Leser dieses Beitrages kommen aus der Treuhand- und Auditoren-Szene. Wann wurden Sie, ob zertifiziert oder nicht, zum letzten Mal von Ihren Kunden zu diesem Thema befragt? Der Kunde hat andere Prioritäten. Er ist interessiert an guten Resultaten, einer guten persönlichen Beziehung und vor allem vorteilhaften Preisen. Ist es nicht so, dass wir einem fachgeprüften (auch ein Zertifikat) Handwerksmeister mehr QA-Management in seinem Betrieb zutrauen, als dem Jahresaudit einer Zertifizierungsfirma?

3. Kosten einer QA-Zertifizierung?

Eine vollständige ISO9000-Zertifizierung kostet Zeit, Geld, Nerven und schafft einiges an Unruhe. Da beim KMU das Projekt ISO9000 nicht einfach an eine interne Fachgruppe delegiert werden kann, bleibt die meiste Arbeit beim Chef hängen. Bei der laufenden Belastung des Alltagsgeschäftes ist eine ISO9000-Zertifizierung ohne Unterstützung eines Coachs kaum zu machen. Auch diese Kosten müssen eingerechnet werden. Sind die Geschäftsprozesse dann QA-konform beschrieben und dokumentiert, müssen sie auch so gelebt werden. Auch das kostet. Jedes Jahr erfolgt dann eine Nachprüfung, um festzustellen, ob der KMU den ISO-Stempel nach wie vor verdient. Wieder Kosten, Zeit und Nerven. Es wäre für jedes Unternehmen spannend, sein QA-Zerti-

fikat nach Vollkostenrechnung zu bewerten und dem wirtschaftlichen Nutzen gegenüberzustellen.

4. Warum haben wir ISO9000 eingeführt?

Nach langen internen Diskussionen haben wir uns 1999 entschlossen, unser kleines Unternehmen ISO9001 zertifizieren zu lassen. Unsere Begeisterung war damals schon sehr verhalten und wir haben uns keine grossen Illusionen über den zu erwartenden wirtschaftlichen Effekt dieser Massnahme gemacht. Die Realität hat uns dann auch nicht enttäuscht. In den vergangenen vier Jahren hat mich ein einziger bestehender Kunde nach unserem Zertifikat gefragt. Kein neuer Kunde hat je angerufen und unsere Leistungen bestellt, weil er von dieser tollen QA-zertifizierten Firma gehört habe. Mir geht es da übrigens genauso. Bei der Auswahl von KMU-Lieferanten ist ISO9000 für unsere Selektion kein Thema. Der Kontakt zum qualitätsverantwortlichen Chef ist einfach zu direkt. Der wichtigste QA-Prozess bleibt der Griff zum Telefon und in kürzester Zeit ist das Problem behoben. Wenn nicht, gibt es tausende von anderen Firmen, die gerne in die Bresche springen würden. Wettbewerb ersetzt bei erfolgreichen KMU eigentlich jede QA-Zertifierung.

Warum wir unsere Firma zertifiziert haben, ist immer noch nicht beantwortet. Ausschlaggebend war die Gelegenheit. Wir haben einen externen Berater und Coach hinzugezogen, um uns für den Entscheid eine externe Sicht zu gönnen. Dieser hat uns darauf Lust gemacht, es den Grossen zu zeigen. Wir hatten einfach Spass daran, uns bezüglich Qualitätsinsignien auf gleiche Augenhöhe wie unsere grossen Kunden zu begeben. Natürlich hätte es uns noch mehr Spass gemacht, wenn diese sich für unsere Leistung ein wenig interessiert hätten. Haben sie aber nicht. Da, wie bereits vorerwähnt, Kosten und Aufwand sich jedes Jahr wiederholen, musste ein neuer interner Sponsor gefunden werden. Bei uns heisst der Wachstum. Unser Unternehmen ist seit 1994 in der Schweiz aktiv. Dort kennt aufgrund der staatlichen Kleinheit sowieso jeder jeden. Seit einem Jahr expandiert unser Markt schnell im EU-Raum und ab 2004 laufen bei uns globale Projekte und Initiativen. Auf einmal füllen sich die Aktenordner voller beschriebener Arbeitsprozesse mit Leben und die Firma besitzt glücklicherweise einen zentralen Qualitätsstamm, der je nach Bedarf neue Zweige und Blätter aufnehmen kann und diese mit wachstumswichtiger Struktur und Qualität versorgt. Nach Jahren der Zweifel ist unser QA-Management heute innerhalb der Firma absolut unumstritten.

Christoph A. Oschwald

Der Autor ist Mitgründer und CEO der schweizerischen SIAG Secure Infostore AG mit Sitz in Aesch-Basel und Zürich. Die SIAG betreibt ein sicheres Logistikzentrum für industrielle Aktenarchivierung und zwei hochsichere, unterirdische Datencenter im schweizerischen Alpenmassiv. Dort werden geschäftskritische Daten internationaler Kunden elektronisch, vollautomatisch und mehrfach verschlüsselt gesichert um bei Datenverlust schnell wieder zur Verfügung zu stehen. SIAG verfügt über Business-Continuity-Prozesse, welche gerade mittleren und kleineren Firmen hochwertige, aber bezahlbare, Datensicherheit ermöglichen.
Infos unter www.siag.ch
Kontakt christoph.oschwald@siag.ch

Zertifizierungen

Ein Überblick gängiger Berufsexamen

Mit der Einführung des Examens zum Certified Information Security Manager (CISM) stellt sich wieder einmal die Frage nach vorhandenen, teilweise konkurrierenden, Examen auf den Gebieten der IT-Sicherheit sowie der IT-Revision. Hierzu soll ein kurzer Überblick gegeben werden, der keinen Anspruch auf Vollständigkeit erhebt.

ISACA hat bereits 1978 mit dem Examen zum Certified Information Systems Auditor (CISA) ein professionelles und mittlerweile weltweit anerkanntes Berufsexamen für interne und externe IT-Prüfer ins Leben gerufen. Ein in Großbritannien angebotenes Examen im Bereich der IT-Prüfung ist die Qualification in Computer Auditing (QiCA), das vom Institut of Internal Auditors UK and Ireland (IIA UK: www.iia.org.uk) als eine high-level Qualifikation für interne IT-Prüfer angeboten wird. Dieses Examen wird allerdings ausschließlich in Großbritannien ausgerichtet und hat nicht die internationale Bekanntheit, die das CISA-Examen auszeichnet. In Deutschland gibt es kein vergleichbares nationales Examen. Somit ist der CISA auf seinem Gebiet bis heute das einzige derartige weltweit anerkannte Berufsexamen für interne und externe IT-Prüfer geblieben.

Bei den Zertifizierungen im Bereich der IT-Sicherheit sind grundsätzlich die produktspezifischen von den nicht produktspezifischen Zertifizierungen zu unterscheiden. Unter letzteren sind auch die hier im Fokus stehenden Berufsexamen wiederzufinden.

Produktspezifische Zertifizierungen haben in der Regel ein oder mehrere Produkte aus technischer Sicht der IT-Sicherheit zur Grundlage. Als typischer Vertreter solcher Zertifizierungen gilt bspw. die Zertifizierung zum Microsoft Certified Systems Engineer (MCSE) von Microsoft.

Ein bekanntes Berufsexamen im Bereich der IT-Sicherheit ist bereits seit vielen Jahren das Examen zum Certified Information Systems Security Professional (CISSP) des International Information Systems Security Certifications Consortium, Inc ((ISC)^2: www.isc2.org). Ein weiteres unbekannteres Examen des ISC^2 ist der Systems Security Certified Practioner (SSCP). Neu hinzugekommen ist in diesem Jahr das Examen zum CISM der ISACA, das basierend auf vorhandenen Kenntnissen, wie sie bspw. im CISSP Examen vermittelt werden, in Richtung Management von Sicherheit in Informationssystemen weiterbilden soll. Die vorgenannten Examen vermitteln ein breites Wissensspektrum zur IT-Sicherheit bzw. zum Management in diesem Bereich, sind aber nicht gebunden an spezielle Systeme, sondern befähigen den Teilnehmer unterschiedliche Systeme und Ansätze in kürzester Zeit verstehen und bewerten sowie entsprechende Maßnahmen treffen zu können. Schnittmenge zwischen den aufgeführten Examen sind aufgrund der ähnlichen Ansätze und Gebiete vorhanden.

Neben den bereits erwähnten anerkannten Berufsexamen, die durch nicht kommerzielle Berufsverbände angeboten werden sowie den speziellen produktabhängigen technischen Zertifizierungen gibt es weitere kommerzielle Anbieter, die für die Teilnahme an einem Seminar zur IT-Revision oder IT-Sicherheit ein entsprechendes Zertifikat mit einem wohlklingenden Titel ausstellen. Diese Zertifikate sind allerdings hinsichtlich der vermittelten Inhalte kritisch zu prüfen und von ihrem Bekanntheitsgrad nicht zu vergleichen mit einem der genannten Berufsexamen.

Ingo Struckmeyer, CISA, CIA

Zertifizierungen

Webtrust$^{SM/TM}$ – Zertifizierung für Zertifizierungsstellen

New York, 1. Mai 2001. Die Institute amerikanischer und kanadischer Wirtschaftsprüfer AICPA und CICA kündigen an, dass der Softwarehersteller Microsoft die Webtrust$^{SM/TM}$-Zertifizierung oder äquivalente Massnahmen zur Auflage für alle Zertifizierungsstellen macht, die ihr Wurzelzertifikat durch Microsoft-Software verteilen möchten. Diese Massnahme wird zum wesentlichen Bestandteil einer grossangelegten Sicherheitsinitiative des Softwareherstellers, der erkannt hat, dass sich der Mangel an Vertrauen in Internet und Internetdienste zu einem wirtschaftlichen „Show-Stopper" entwickeln kann. Und tatsächlich: Wie soll ein gewöhnlicher Verbraucher beurteilen, ob ein Internetanbieter die notwendigen organisatorischen, physischen und technischen Vorkehrungen trifft, um seine Internetdienste und Kundendaten zu schützen?

Web-Siegel

Im Internet-Umfeld erfordert es Gütesiegel, anhand derer ein Anwender bzw. Verbraucher auf Anhieb erkennen kann, ob eine Dienstleistung definierte Standards zur Qualität und Sicherheit einhält und dies durch einen anerkannten unabhängigen Prüfer regelmässig kontrolliert wird. Das Webtrust$^{SM/TM}$-Programm ist eines von diversen Programmen, das die Prüfung, Zertifizierung und regelmässige Re-Zertifizierung von Webdiensten bzgl. definierter Sicherheitsziele hat. Geprüft werden die Gebiete Datenschutz, Sicherheit, Transaktionsintegrität, Verfügbarkeit, Vertraulichkeit und Nicht-Abstreitbarkeit. Das Webtrust$^{SM/TM}$-Siegel dient als leicht erkennbares Zeichen für die Qualifikation eines Internetanbieters nach den Webtrust$^{SM/TM}$-Vorgaben.

Der Teufel im Detail

Bei der Diskussion um die Sicherheit von Internetdiensten und elektronischen Geschäftsprozessen wird gerne ein Aspekt ignoriert, der anfangs als technisches Detail wenig wichtig erscheint: Das Schlüsselmanagement. Doch gerade dieser Aspekt hat es in sich! Denn die Sicherheit nahezu aller Massnahmen zur Sicherung elektronischer Geschäftsprozesse steht und fällt mit der vertrauenswürdigen Erzeugung, Verteilung und Verwaltung elektronischer Schlüssel. Da dieser Aspekt so fundamental wichtig ist, hat Webtrust genau hierfür das spezielle Programm „Webtrust$^{SM/TM}$ für Zertifizierungsstellen" geschaffen. Ziel des Programms ist es, die Vertrauenswürdigkeit von Zertifizierungsstellen auf ein definiertes hohes Niveau zu bringen. Die Basis dafür ist die Prüfung von Zertifizierungsstellen nach einem öffentlichen international anerkannten Standard durch unabhängige akkreditierte Parteien. Eben weil „Webtrust$^{SM/TM}$ für Zertifizierungsstellen" die für die Internetsicherheit dringenden Anforderungen erfüllt, hat sich Microsoft entschlossen, diesen Standard zu adoptieren.

Zertifizierungsstellen

Eine Zertifizierungsstelle (Certification Authority) ist die wichtigste Komponente in einer speziellen Infrastruktur zu sicherem Schlüsselmanagement und sichere Schlüsselanwendung, der Public-Key Infrastruktur (PKI). Über PKI gibt es zahlreiche Publikationen, so dass wir nur kurz einige Grundfunktionen rekapitulieren wollen.

Eine PKI ermöglicht es jedem Internetteilnehmer, die Identität eines anderen Internetteilnehmers und das Vertrauen in diesen automatisch überprüfen zu können. Dazu bedient sich die PKI der Verfahren der Public-Key-Kryptographie. Dabei erhält jeder Teilnehmer ein Schlüsselpaar bestehend aus einem geheimen Schlüssel (Private-Key) und einem öffentlichen Schlüssel (Public-Key). Um sicher zu stellen, dass ein Schlüsselpaar zu einem bestimmten Benutzer gehört, bedarf es einer Zertifizierungsstelle, welche die Identität eines Schlüsselbesitzer und die eindeutige Zuordnung eines Schlüssels zum Besitzer überprüft. Die Zertifizierungsstelle bestätigt die Korrektheit der Prüfung durch ein digitales Zertifikat. Dabei handelt es sich um ein kleines Datenpaket, welches u.a. den Namen der Zertifizierungsstelle, den Namen des Schlüsselbesitzers, den Public-Key,

Gültigkeitsdauer usw. enthält. Das Datenpaket wird durch eine digitale Unterschrift der Zertifizierungsstelle kryptographisch gekapselt. Die Zertifizierungsstelle kann als Behörde zur Ausstellung von elektronischen Ausweisen (digitale Zertifikate) aufgefasst werden.

Darum hohe Sicherheitsanforderungen

Public-Key-Schlüsselpaare bzw. digitale Zertifikate dienen häufig zur Realisierung der Kontrollelemente für elektronische Geschäftsprozesse wie digitale Signaturen, Zeitstempel, Notardienste etc. Die Zertifizierungsstellen werden hin und wieder treffend als Trust-Broker bezeichnet, denn durch sie ist es letztendlich möglich, eine Vertrauensbeziehung zwischen Parteien zu etablieren, die sich a priori nicht kennen. Sicherlich gehört noch mehr zu einer Vertrauensbeziehung als eine Zertifizierungsstelle. Doch ist klar, dass elektronische Geschäftsprozesse, die PKI verwenden, eine vertrauenswürdige Zertifizierungsstelle als notwendige Bedingung haben. Denn sollte die Zertifizierungsstelle nicht vertrauenswürdig sein, da z.B. die Prozesse nicht professionell durchgeführt werden oder die technische Sicherheit ungenügend ist, können alle darauf basierenden Anwendungen auch nicht vertrauenswürdig sein.

Webtrust$^{SM/TM}$ für Zertifizierungsstellen

Der Standard „AICPA/CICA Webtrust$^{SM/TM}$ Program for Certification Authorities“ (Version 1.0) bedient sich der bestehenden Standards

- RFC2527: PKI Certificate Policy and Certification Practices Statement
- ANSI X9.79: PKI Practices and Policy Framework
- BS7799: Environmental Information Security

In der Umsetzung hat dies den gravierenden Vorteil, dass die meisten der Webtrust$^{SM/TM}$-Anforderungen aufgrund der Popularität von BS7799 (bzw. ISO 17799) bereits bekannt oder gar in IT-Umgebungen schon implementiert sind. Wer also ein BS7799-konformes IT-Umfeld besitzt, könnte bei der Zertifizierung seiner Zertifizierungsstelle darauf aufsetzen und so Kosten einsparen.

Die Zertifizierung beinhaltet die drei Grundprüfbereiche:

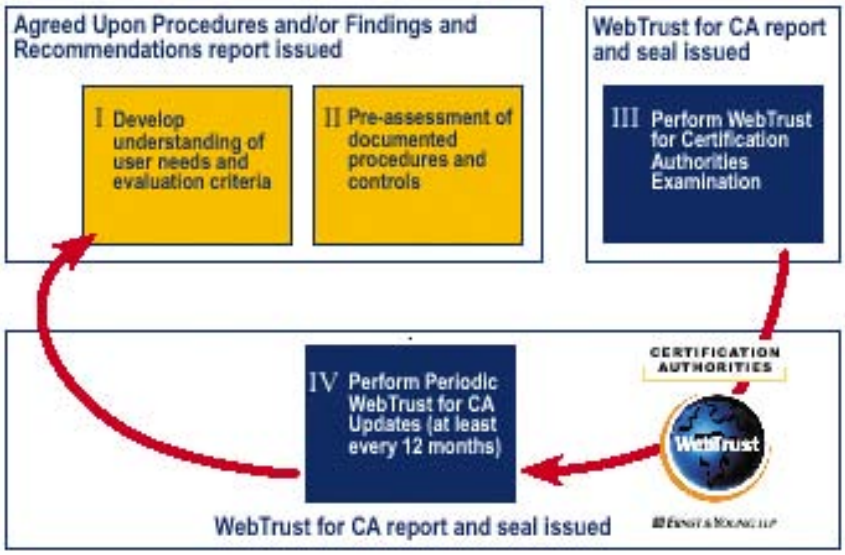
1. CA Business Practices Disclosures
2. CA Service Integrity
3. CA Environmental Controls

Im ersten Bereich wird geprüft, ob die Zertifizierungsstelle seine Praktiken, Prozeduren und relevante Informationen in der nötigen Weise gegenüber dem Verbraucher publiziert. Der zweite Bereich behandelt die Integrität aller kritischen PKI-Prozeduren rund um den Lebenszyklus von Schlüsseln, Zertifikaten, Sicherheitstoken (sofern eingesetzt), spezieller Sicherheitshardware usw. Der dritte Bereich beinhaltet die Prüfbereiche zum allgemeinen Management der Informationssicherheit gemäss BS7799, d.h. Policy- und Sicherheits-Management, Asset-Klassifikation und -Management, Zugriffskontrolle, Personalsicherheit, operationelle Sicherheit, physische Sicherheit, Systementwicklung und -änderung, Business-Continuity-Planning, Compliance, Journaling und Audit.

Die Webtrust$^{SM/TM}$-Zertifizierung

Die Webtrust$^{SM/TM}$-Zertifizierung ist ein Prozess, der in vier Schritten stattfindet und zwei Blickwinkel bzw. Rollen erfordert: die Webtrust$^{SM/TM}$-Advisor- und die Webtrust$^{SM/TM}$-Auditor-Rolle. Der Webtrust$^{SM/TM}$-Advisor unterstützt die Zertifizierungsstelle bei der zielgerechten Hinführung zum Webtrust$^{SM/TM}$-Standard, d.h. zur Erfüllung der Webtrust$^{SM/TM}$-Anforderungen in den drei Grundprüfbereichen. Dies geschieht durch eine Bestandesaufnahme und Gap-Analyse sowie einer schrittweise Schliessung der Gaps. Die Vorgehensweisen unterscheiden sich je nachdem, ob eine Zertifizierungsstelle neu aufgebaut wird, oder ob sie bereits existiert und das Vertrauensniveau auf Webtrust$^{SM/TM}$-Niveau angehoben werden soll.

Wenn die Zertifizierungsstelle mit ihren Praktiken an das Webtrust$^{SM/TM}$-Rahmenwerk angepasst ist, kann der Webtrust$^{SM/TM}$-Audit erfolgen. Dabei werden vom Auditor die Übereinstimmung der von der Zertifizierungsstelle spezifizierten Praktiken mit deren Umsetzung und die Übereinstimmung mit den Webtrust$^{SM/TM}$-Anforderungen überprüft. Mit der Erfüllung des Audit erhält die Zertifizierungsstelle das Webtrust$^{SM/TM}$-Siegel auf ihrer Webpage als leicht sichtbares Zeichen der Qualifikation.



Graphik 1: Ablauf einer Webtrust$^{SM/TM}$-Zertifizierung (Siegel unten rechts)

Die Zertifizierungsstelle wird alljährlich einer Re-Zertifizierung unterzogen, um die Wirksamkeit der Kontrollen im Laufe der Zeit zu prüfen und die ordnungsgemässe Behandlung von Veränderungen sicherzustellen. Im Fall einer festgestellten Nichteinhaltung der Webtrust$^{SM/TM}$-Anforderungen kann das Webtrust$^{SM/TM}$-Siegel revoziert werden. Durch Anklicken des Siegels und einen damit gekoppelten technischen Sicherheitsmechanismus wird der Gültigkeitsstatus des Siegels für den Verbraucher erkennbar.

Stolperstein "Key Creation Ceremony"

Kann sich jede Zertifizierungsstelle einer Webtrust$^{SM/TM}$-Zertifizierung unterziehen? Prinzipiell ist das möglich. Doch es kann leicht zu unüberwindbaren Problemen kommen, wenn z.B. einer Zertifizierungsstelle nicht nachweisen kann, dass der eigene Schlüssel, der sogenannte Root-Key, sicher erzeugt wurde und seither sicher aufbewahrt ist. Den Vorgang des korrekten und vertrauenswürdigen Aufsetzens der Zertifizierungssoftware und -hardware und der Schlüsselerzeugung wird als „Key Creation Ceremony" bezeichnet. Man mag schmunzeln, doch dieser Vorgang verläuft tatsächlich wie ein offizieller Akt, an dem auch eine qualifizierte, autorisierte und unabhängige Prüfinstanz teilnimmt und jeden einzelnen Schritt beobachtet und beglaubigt. Aus diesem Grund ist jeder Zertifizierungsstelle zu empfehlen, die Key-Creation-Ceremony und Root-Key-Aufbewahrung in jedem Fall nach Webtrust$^{SM/TM}$-Anforderungen durchzuführen, um ein späteres Nachsehen zu vermeiden.

Standards mit Abweichungen

Zertifizierungsstellen können sich sowohl durch Geschäftsmodelle als auch PKI-Architektuen unterscheiden. Entsprechend kann es zu unterschiedlichen Auslegungen zur Erfüllung des Webtrust$^{SM/TM}$-Standards kommen. Im Rahmen des ersten Webtrust$^{SM/TM}$-Audits, den Ernst & Young in der Schweiz vorgenommen hat, galt es die Wurzel-Zertifizierungsstelle in einer hierarchischen PKI zu zertifizieren. Dabei tauchten spezifische Fragen auf, die mit dem Geschick des Advisors gelöst werden konnten. Ein Beispiel: Müssen in einer hierarchischen PKI neben der Wurzel-Zertifizierungsstelle auch alle untergeordneten Zertifizierungsstellen zertifiziert werden? Falls ja, so wäre dies u.U. sehr teuer. Falls nein, ergeben sich womöglich Probleme mit der Vererbung von Vertrauensbeziehungen. Das Finden einer Antwort kann leicht lange Diskussionen heraufbeschwören. Die Lösung steckt in der Orientierung am Geschäftsmodell der jeweiligen Zertifizierungsstelle und lässt letztendlich beide Möglichkeiten zu.

Webtrust$^{SM/TM}$ Status Quo

Das Webtrust$^{SM/TM}$-Siegel hat unter der e-business- und PKI-Frustration in den letzten zwei Jahren gelitten. Dennoch nimmt die Zahl der Zertifizierungsstellen, die sich nach dem Standard zertifizieren lassen, stetig zu. Die Organisationen, welche das Siegel erlangt haben, können unter [1] verfolgt werden, die Teilnehmer am Microsoft Root CA Programm hingegen unter [2]. Ernst & Young hat mittlerweile etwa zehn Webtrust$^{SM/TM}$-Audits weltweit durchgeführt.

Es ist anzunehmen, dass die Webtrust$^{SM/TM}$-Zertifizierung aufgrund der wachsenden Popularität des BS7799-Standards und infolge der Microsoft-Initiative weiter an Bedeutung gewinnen wird. Viele

Unternehmen wissen noch zu wenig über Webtrust[SM/TM] und sind sich daher auch nicht der möglichen Synergien mit anderen Zertifizierungen, z.B. nach BS7799, bewusst. Vielen ist auch nicht bewusst, dass man eine Zertifizierung nach Webtrust[SM/TM] zunächst auf eine reine Wurzel-Zertifizierungsstelle beschränken kann. Hierdurch kann man Kosten einsparen, und dennoch einen wichtigen Schritt zur Sicherung elektronischer Geschäftsprozesse gehen.

[1] www.webtrust.org/abtseals.htm
[2] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/rootcertprog.asp

Dr. Stephan Teiwes, Ernst & Young AG, Zürich

Michael Burkhardt, Ernst & Young AG, München

Zertifizierung

Qualitätszertifizierung (ISO-9000)

Immer häufiger begegnet man in Werbeunterlagen, in Verbindung mit Firmennamen, sogar auf Anschriften auf Firmenautos, dem Logo „SQS“. Bei näherer Betrachtung fällt auch das Wort Zertifizierung in der einen oder andern Form im umschliessenden Ring des Logos auf. Was hat es damit auf sich? Was bedeutet SQS?

Am Beispiel von ISO-9001:2000 sei illustriert, welche Merkmale das Siegel aufweist, und welche Anforderungen erfüllt sein müssen, um es zu erlangen. SQS bedeutet übrigens *Schweizerische Vereinigung für Qualitäts- und Management-Systeme* (Dienstleistungspalette siehe Box).

Historischer Rückblick

Im Jahr 1987 führten diverse nationale Normen zu einer Erstausgabe ISO 9001ff mit dem Schwergewicht auf Nachweissicherheit. 1994 erfuhren diese Vorgaben eine erste sanfte Revision, um im Jahr 2000 eine umfassende Neugestaltung der ganzen Normenreihe zu erfahren. Heute arbeiten über 800 000 Anwender (-firmen) mit diesen Messlatten, wobei über 560 000 zertifiziert sind.

Ziel der Zertifizierung

Einmal mehr kann behauptet werden, „der Weg ist das Ziel“. Im Vordergrund steht demnach die Kundenorientierung, ein Prozessmanagement und insbesondere eine *ständige Verbesserung*. In einem ersten Schritt (vgl. Darstellung) sollen Vorlagen und Dokumentationen erarbeitet werden, die ein Messen der Qualität erst ermöglichen. Vielfach geht eine erste Überprüfung der Organisation ins Land, ein sogenannter Audit. Dabei werden Schwachstellen aufgedeckt und Forderungen aufgestellt, wie diese zu beheben sind. Hat der Zertifizierungswillige die Normen theoretisch erfüllt, erhält er eine erste Bescheinigung, ein Zertifikat. Von aussen betrachtet ist damit noch wenig erreicht, hat sich die Organisation doch erst Vorgaben geschaffen, an welche sie sich halten will. Ob sie dies auch tut, ist noch offen. Der nächste Schritt soll diese zutage bringen. Nach einer gewissen Zeit (normalerweise drei Jahre) nach der Zertifizierung soll die Prüfung erfolgen, ob die erstellten Normen auch eingehalten werden (Assessment bzw. Rezertifizierung). Ob damit letztlich auch die aus den zertifizierten Prozessen hervorgehenden Produkte bzw. Dienstleistungen qualitätsmässig einwandfrei sind, kann zwar nicht garantiert werden, doch sollten alle Voraussetzungen dafür erfüllt sein.

Die acht Managementgrundsätze

- Kundenorientierung: Jetzige und künftige Forderungen erkennen und erfüllen
- Führung: Schaffen einer geeigneten Unternehmensstruktur
- MitarbeiterInnen: Einbeziehen aller MitarbeiterInnen und ihrer Fähigkeiten zum Nutzen der Organisation
- Prozessorientierung: Lenken zusammengehöriger Mittel und Tätigkeiten in Prozesse
- Systemorientierung: Erkennen und Lenken des Prozessnetzwerks und ihrer gegenseitigen Abhängigkeiten
- Verbesserung: Wahrnehmen der permanenten Aufgabe der Organisation
- Sachlichkeit: Entscheiden auf der Basis von logischer und/oder intuitiver Analysen
- Lieferantenbeziehungen: Sicherstellen eines gegenseitigen Nutzens

Eckpunkte

Der Aufbau eines bewussten Managementsystems ist ein *strategischer Entscheid* der Unternehmensleitung. Irgend ein Managementsystem existiert zwar immer, aber verdient es wirklich das Attribut „systematisch“? Und wird es bewusst, ja sogar kontrollierbar, gelebt?!

Das Unternehmen soll dazu gebracht werden, eine Konformität und hohe Qualität der Produkte bzw. Dienstleistungen ständig sicherzustellen. Daraus folgt, dass alle Aktivitäten letztlich auf Kundenforderungen zur *Kundenzufriedenheit* eingebunden sind. Die Vorgaben sind für alle Grössen von Unternehmungen und Organisationen ausgelegt und sind grundsätzlich für jedes Produkt und jede Dienstleistung anwendbar. Kreative und künstlerische Tätigkeiten (Entwicklung und Design) mögen hier Ausnahmen sein.

Die allgemeinen Forderungen an ein zu zertifizierendes System setzen eine (nicht immer klare) Definition der Unternehmensprozesse und deren Vernetzung mit Wechselwirkungen voraus. Kriterien zum eigentlichen Management sind zu erarbeiten, die ein Messen der Leistung erlauben. Daneben sind die notwendigen Ressourcen und Informationen stets bereitzuhalten, damit Betrieb und Steuerung fortlaufend gewährleistet sind. Das Erarbeiten von Dokumentationen ist unerlässlich und unter Umständen drängen sich auch Begradigungen an Prozessen und Abläufen auf. Jeder Prüfer weiss, dass er für seine Tätigkeit eine Prüfspur braucht. Deshalb ist einerseits eine klare Vorgabe in einem Management-Handbuch festzuhalten, andererseits müssen Aufzeichnungen die *Nachweissicherheit* gewährleisten.

Die Leitung hat sich zur Führung gemäss den erarbeiten Vorgaben zu verpflichten (neudeutsch: „Commitment“). Leitfigur ist immer der Kunde. Dies ist der primäre Schwerpunkt der Unternehmenspolitik, der Prozesse, des Einsatzes der MitarbeiterInnen, der Kommunikation im Unternehmen und nach aussen, der gesamten Organisation des Unternehmens. Es wäre vermessen, der Unternehmensleitung die Verantwortung für jedes Detail zu überbinden. Deshalb ist das Bestimmen der *Prozesseigner* wichtig. Damit sie im Sinne des Managementsystems arbeiten können und ihre Tätigkeit kontrollierbar wird, ist die Dokumentation in Manualform unabdingbar.

Angebotspalette der SQS

- Zertifizierung von Qualitätsmanagement-Systemen gemäss der ISO-9000er-Reihe
- Zertifizierung von Umwelt-Management-Systemen gemäss ISO-14000er-Reihe, BS 7750 und Begutachtung nach EMAS-Richtlinie
- Zertifizierung im Fachgebiet Medizinaltechnik gemäss EN-46000er-Reihe
- Zertifizierung im Fachgebiet Schweisstechnik gemäss EN 729
- Zertifizierung von Qualitäts- und Management-Systemen gemäss Branchenvorschriften (z.B. QS 9000)
- Vermittlung und Realisierung von Konformitätsbewertungen und der CE-Kennzeichnung
- Konformitätsbescheinigungen gemäss Schweizer Recht
- Auskünfte über Produktevorschriften und Normen (EWR-Service)
- Assessment nach EQA-Modell
- Auditierung gemäss Kundenauftrag (z.B. VDA, QS 9000, usw.)

Die Verpflichtung zur laufenden Verbesserung setzt voraus, dass die Qualität der Produkte bzw. Dienstleistungen, aber auch der Prozesse, laufend gemessen wird. Korrekturen, Ursachenanalyse und Massnahmen zum Verhindern von Fehlleistungen müssen zur Routine werden.

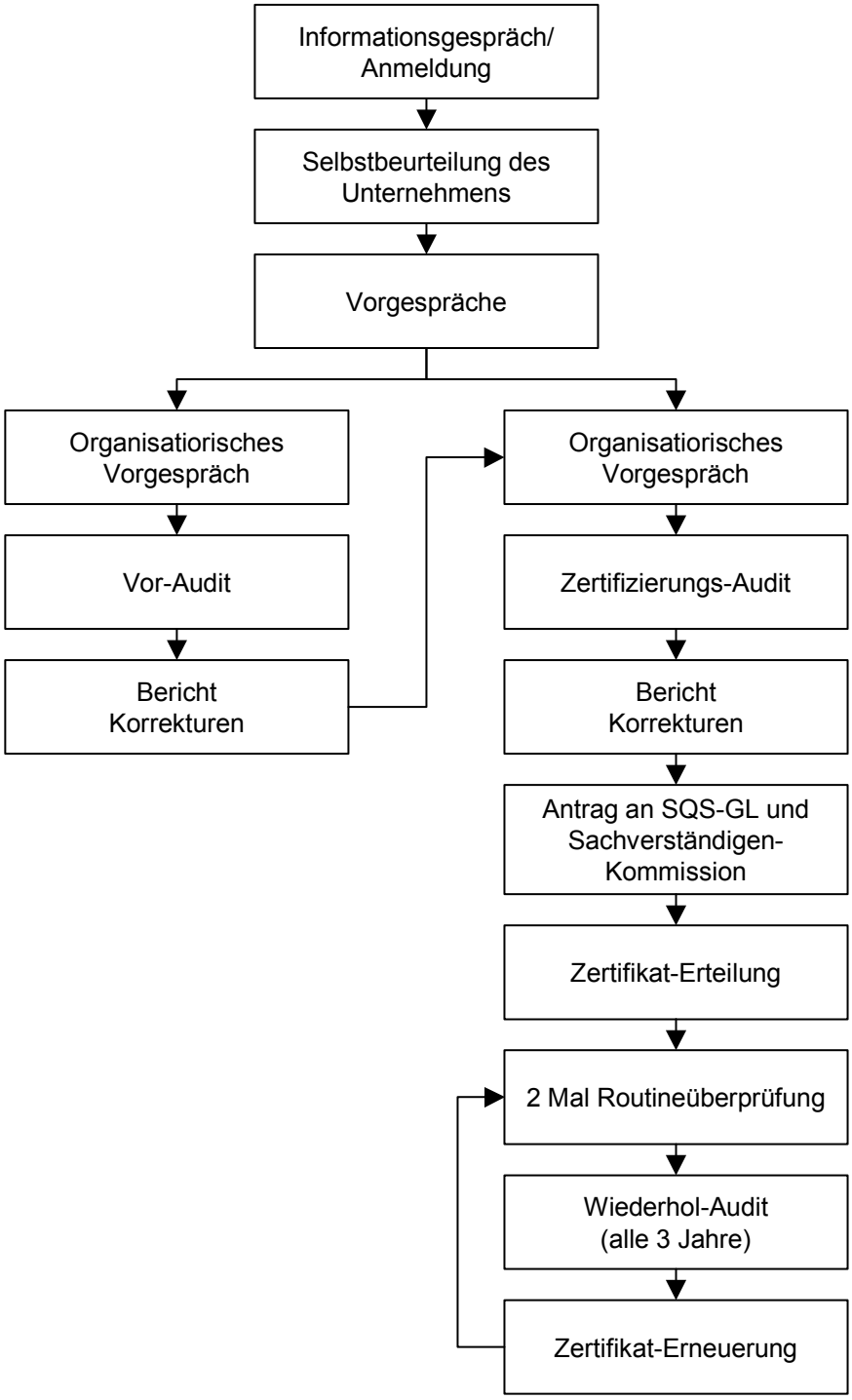
Ein wichtiges Element ist die *Ausbildung*. Sie darf nicht nur einmal „abgetan“ werden, sondern muss *laufend* erfolgen.

Schlussbemerkung

Aus einer gewissen Distanz betrachtet, erscheint das Zertifizierungswesen aufwendig, teuer und unter Umständen gar umständlich. Aber Qualität hat sich noch nie „von selbst“ eingestellt und fordert eben ihren Preis. Wenn der Anwender den Grundsatz der Kundenorientierung hoch hält, wird der Kunde die Leistung auch anerkennen und den entsprechenden Preis bezahlen. Ein Geschäft ist letztlich nur eines, wenn alle Beteiligten davon profitieren: *Die Win-Win-Situation.*

Abstrahiert aus Unterlagen der SQS durch Max F. Bretscher

Der Zertifizierungsablauf



Buch des Monats

Risiken einer IT-Abteilung bewirtschaften

Ausgangslage

Aus meiner 20jährigen Praxis als IT-Auditor bei der Rentenanstalt/Swiss Life habe ich meine Erfahrungen im Bereich IT-Riskmanagement in Form eines Lehrmittels für die Informatik Berufsbildung Schweiz (i-ch) zusammengefasst (www.compendio.ch).

Dass ein IT-Projekt oder eine ganze IT-Abteilung in ein Krise gerät, ist in der heutigen Zeit keine Ausnahme. In solchen Situationen ist zielorientiertes und schnelles Handeln gefragt, denn einiges kann auf dem Spiel stehen: Die Treue der Kunden, der Ruf des Unternehmens, die Einhaltung des IT-Budgets und die gesetzlichen Vorschriften sowie vieles mehr.

Im angekündigten Lehrmittel wird auf die Prävention und die praktische Vorgehensweise zur Bewirtschaftung von IT-Risiken eingegangen.

Aus dem Inhalt

Das Lehrbuch besteht aus sechs Teilen u.a. mit folgenden Inhalten: Externe und interne Rahmenbedingungen, COSO und COBIT-Kontrollmodelle, Grundbegriffe, Zweck und Nutzen des Risikomanagements, Aufbau einer Risikomanagement-Organisation und Kernprozesse, Leitplanken einer Risikopolitik und Risikostrategie, Methoden der Risikoanalyse und Risikobewältigung, Tools zur Unterstützung des Risikomanagements, Vorgaben zur Information, Kommunikation und Monitoring, Einsatz einer Balanced Scorecard für das IT-Riskmanagement.

Der Anhang beinhaltet u.a. eine Gesamtzusammenfassung, über 40 Antworten zu den Repetitionsfragen, einen Überblick über das COBIT-Kontrollmodell, ein Glossar und ein Stichwortverzeichnis.

Ziel und Zweck

Das IT-Governance-Prinzip soll sicherstellen, dass die IT-Risiken im Sinne der Unternehmensziele bewirtschaftet werden. Ein unternehmensweites Risikomanagement gehört deshalb zu den grundlegenden Voraussetzungen für eine zweckmässige und wirksame Unternehmensführung.

Der Aufbau des Lehrmittels gibt einen guten Überblick, wie die Risiken einer IT-Abteilung sowohl von Grossunternehmen als auch von KMU systematisch bewirtschaftet werden können. Dazu gehören nicht nur der Aufbau einer zweckmässigen Risikomanagement-Organisation, sondern auch effiziente Kernprozesse und eine effektive Überwachung des Risikomanagement-Systems, um die IT-Ressourcen zielgerichtet zu nutzen.

Anwendbarkeit und Nutzen

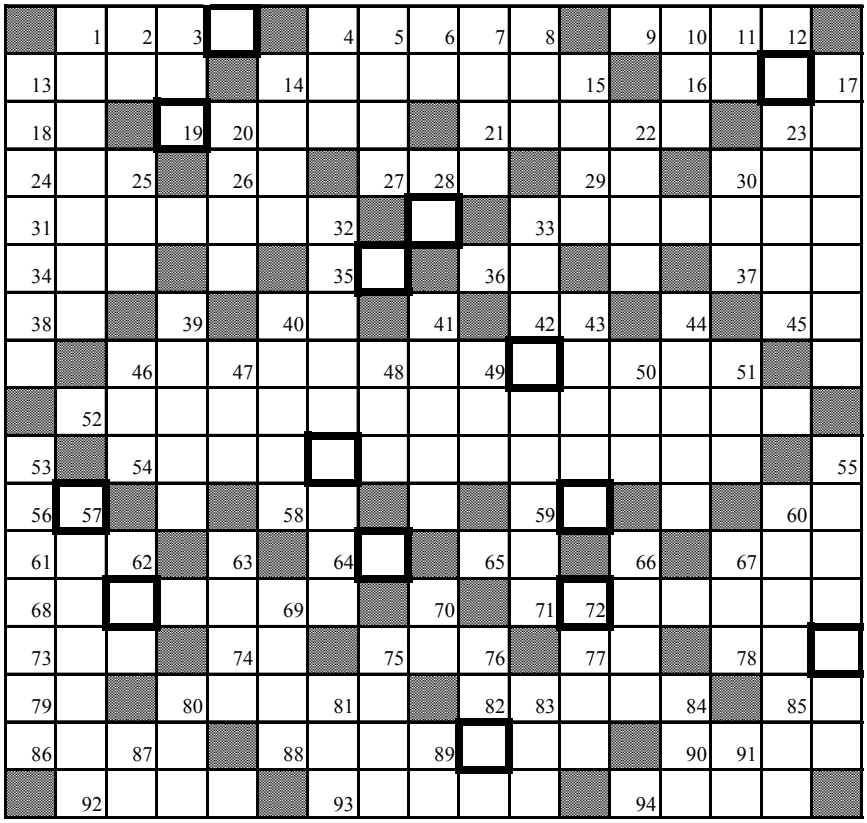
Dieses Lehrmittel orientiert sich an der Modulidentifikation und den Handlungszielen „Risiken einer IT-Abteilung bewirtschaften“ der i-ch. Zahlreiche Methoden und Techniken, die auf international anerkannten Standards beruhen, werden anhand von Beispielen und Grafiken veranschaulicht, um den Transfer theoretischer Erläuterungen in die Praxis zu erleichtern.

Das Lehrbuch richtet sich einerseits an Auszubildende, welche sich auf das eidgenössische Diplom vorbereiten und anderseits an Praktiker, welche sich auf strategischer und operativer Ebene mit der Bewirtschaftung von IT-Risiken befassen. Darüber hinaus kann es als nützlicher Leitfaden für die Einführung eines Risikomanagement-Systems und für die konsequente Überwachung von IT-Risiken eingesetzt werden.

Bruno Wiederkehr

The ISACA Crossword Puzzle 5/03

Dieses Rätsel ist auf deutsch und hat mit dem Schwerpunktthema dieser Nummer zu tun. Autor ist der Redaktor. Lösungen, Kommentare und Reklamationen sind an ihn zu richten.



Waagrecht: 1 Adelstitel; 4 Pferdeleine; **9 so ist jemand, der jeder Zertifizierung glaubt;** 13 Farbe; 14 Vogelart; 16 Quarzprodukt; 18 pers Fürwort; 19 engl Gesangsensemble; 21 Alpenpass; 23 Schiffsgewichteinheit (Abk); 24 Wendebefehl; 26 span Artikel; 27 Windrichtung; 29 oben angeführt; **30 zertifiziert den CIA (Abk); 31 Zertifikat; 33 „Zertifizierungsstelle" der Seligen und Heiligen;** 34 Getränk (engl); 35 Trademark (Abk); 36 Flussname aus der Innerschweiz; 37 durchfliesst Pforzheim; 38 noch ein Fluss, diesmal zur Donau; 40 internationales Südost; 41 Rekrutenschule; 45 zur Erinnerung; **46 dokumentarisch bestätigen; 52 einschränkende Voraussetzung; 54 Normen;** 56 der Ausserirdische; 58 die Hälfte eines Ballettröckchens; 59 zweite Stufe der italienischen Tonleiter; 60 Boxerbegriff; 61 nennt sich heutzutage Idée Suisse; 64 halber Reissverschluss aus Mendrisio; 65 AZ aus der schweizerischen Hauptstadt; 67 schweizerisches Flächenmass; 68 einem Bergeinschnitt gleich; **71 ob das Zertifikat dies tut, muss sich weisen;** 73 Laban verkuppelte sie zuerst; 74 frz Verneinungsteil; 75 an der Corrida zu hören; 77 natürlicher Logarithmus; 78 Zinn (engl); 79 kurzes Obergeschoss; 80 Vermächtnis; 82 nobler Begleiter; 85 frz rückbezügliches Fürwort; 86 gibt in den Psalmen den Takt an; 88 Karibikinsel; 90 glatt; 92 Pferd; 93 engl Nasen; 94 Bruchstück.

Senkrecht: 1 bedauern; 2 kurzer Rundlauf; 3 Alphabet; 4 so viele Wochen hatte wohl auch das römische Jahr; 5 der Andere (span); 6 ohne Trumpf im Bridge; 7 Schadstoff; 8 ein Vorläufer des Euro; 10 türkischer Titel; 11 it Artikel; 12 Begriff aus der Statistik; 13 gut herausgekommen; 14 Einzelgesänge; 15 im Innern verwirrte römische Stunde; 17 Löcher herauspressen; 20 Landarmee; 22 Bauernhütte; 25 europ Weltraumbehörde; 28 AZ aus der Nordschweiz; 30 Eisenhowers Spitzname; 32 Wehreinrichtung bei Burgen; 33 Spielarten ausprobieren; 39 Heidibetreuer (Mz); 40 folgte früher im Militär auf „Achtung"; 41 Kreaturen; 43 Mähgerät; 44 nicht billig; 46 slawischer Herrschertitel; 47 Racing Motor Club; 48 so könnte Freiburg abgekürzt werden; 49 zur Dienstordnung; 50 inmitten vom Burgsee; 51 drei gleiche Konsonanten; **53 ob man so befriedigt ist nach der Zertifizierung, ist fraglich; 55 beherrschen;** 57 Stütze; 60 Kinderspielzeug; 62 geschäftsleitender Ausschuss; 63 Gebiet; 66 Schlachtort Napoleons; 67 dem Doktor fehlt das „r"; 69 Rettungsflugwacht; 70 Orientierungslauf; 72 deutscher Mädchenkurzname; 75 deutscher Königsname; 76 Ackergerät; 80 span Artikel; 81 engl Prinzessin; 83 fertig; 84 Berliner Verneinung; 87 it Artikel; 89 Informationssystem; 91 „doppelte" Vorsilbe.

Die Lösung liegt in den markierten Feldern. Dieses Wort ist auf einer Postkarte zu senden an M.F. Bretscher, Oberrenggstrasse 8, 8135 Langnau a/A. Lösungen werden auch entgegengenommen unter der e-mail-Adresse mbretscher@kpmg.com.
Einsendeschluss ist der 12. Januar 2004.

Solution Crossword Puzzle 4/03: *Treasurer*

Across: 1 monograph; 7 voucher; 14 our; 15 II; 16 banner; 17 oar; 19 ut; 20 *titles*; 23 do; 24 raid; 25 type; 26 *teller*; 27 torre; 28 Edam; 30 spot; 32 emit; 33 lr; 34 rope; 36 antlers; 37 Hi; 38 Ji(had), 39 aced; 40 est; 42 lone; 44 event; 46 Diesel: 49 rr; 51 sex; 52 semi; 53 MO(nday); 54 Mex(ico); 55 peers; 57 TR; 58 *stock exchange*; 60 SE; 61 stink; 62 NEH; 63 r(everen)d; 64 *gain*; 66 RPE; 68 NE; 69 etseqq; 70 aries; 71 salt; 73 yes; 74 urge; 75 re; 76 yard; 78 pendule; 81 user; 83 AM; 84 eoli(thic); 85 eats; 87 slab; 89 gents; 91 Stuart; 92 item; 94 inos (Sony); 95 Po; 96 *shares*; 98 En; 99 OTR; 100 bedi(g)ht; 102 el; 103 bad; 104 Midwest; 105 transfers.

Down: 1 mouse; 2out; 3 nr; 4 grip; 5 ail; 6 pieton; 7 vallee; 8 on; 9 undress; 10 CEO; 11 HR; 12 roar; 13 *order*; 18 airline; 20 tympanist; 21 tes; 22 *settlement*; 24 rot; 25 tao; 27 tic; 29 driver; 31 paddock; 35 (s)ect; 37 Hoss (Cartwright); 38 jesters; 41 *trend*; 43 *expense*; 45 (g)em; 47 sexes; 48 exchequers; 50 Reg; 53 money; 55 parquet; 56 regresses; 59 tin; 60 sierra; 61 Sela; 65 AI; 67 *payment*; 69 -ese: 70 AGU; 72 trets; 77 DOS; 79 naught; 80 lather; 82 elm; 83 *agios*; 86 Sir; 88 *bonds*; 90 norm; 93 teas; 95 pew; 97 ala; 98 ear; 100 b(e)d; 101 is; 103 be.

Watson: Of the alphabet, the letter "Z" is missing in the solution.

Es wurden weniger als 5 Lösungen eingesandt und die Watson-Eigenheit wurde von niemandem entdeckt. Somit befinden sich $US 150.– im Jackpot!

In der Karibik, da lebte einst ein schrecklich bösartiger Pirat,
Er hatte für die Seefahrer Enterungen an der Reihe parat.
Er teerte, federte und holte Kiel,
und tat sonstiges Böses noch viel.
Das Seegericht kümmerte ihn nicht, denn er hatte ein Zertifikat.

An auditor was awaiting the results of the exams quite petrified;
When asked what her status was, she hesitated and finally lied.
When receiving the letter, her heart rather sunk.
She was sure that she did nothing but flunk.
She was wrong: The Institute had her very happily certified.

Express Line

A Word from the Chair

It is once again renewal season at ISACA. I am pleased to announce that this year all members have the opportunity to renew their membership online through ISACA's new web site. Members should have received their unique user ID and password by mail. Otherwise, members can have their access information e-mailed to them by using the New User functionality link on the ISACA home page.

Please be reminded that as of 1 September, we are accepting membership applications only for 2004. October is an excellent time for recruiting new members, since those joining on or after 1 September receive membership through the end of December 2004 (with the balance of 2003 being complimentary). Members who have not renewed for 2003 must pay a US $30 fee to reactivate their membership.

Howard Nicholson
Chair, Membership Board

Bookstore Update

CISA Study Materials

■ The CISA Review Manual 2004 is updated extensively each year to reflect current and changing industry principles and practices. It includes a thorough explanation of the structure and content of the examination, offer tips on how to develop a study plan and provides guidance and coverage of technical matter outlined in the process and content areas of the exam. Review questions are provided at the end of each chapter. (Available: October 2003)

■ The CISA Review Questions, Answers & Explanations Manual 2003, consists of 500 multiple-choice study questions arranged in the same proportion as the CISA job analysis. Many of these items appeared in the 2001 and 2002 editions of the CISA Review Questions, Answers and Explanations Manual, but have been re-written to provide further clarity and account for changes in the exam and/or changes in practice. This publication is ideal for use in conjunction with the CISA Review Manual 2004. (Currently available)

■ CISA Review Questions, Answers & Explanations Manual Supplement is developed each year by ISACA. The 2003 and 2004 supplements each include 100 sample questions, answers and explanations for the candidates to use in preparation for the CISA exam and have been created using a similar process as is used for actual exam items. (2003 Supplement: Currently available; 2004 Supplement: November 2003)

■ CISA Review Questions, Answers & Explanations CD-ROM 2004 consists of the 700 questions, answers and explanations included in the CISA Review Questions, Answers & Explanations Manual 2003 and the 2003 and 2004 editions of the CISA Review Questions, Answers & Explanations Manual Supplement. With this product, CISA candidates can identify strengths and weaknesses by taking various length random sample exams and breaking the results down by area. (Available: December 2003)

CISM Study Materials

The CISM Review Manual 2004 is updated extensively each year and is designed to assist individuals in preparing for the CISM exam and for individuals who wish to learn more about the role and responsibility of an information security manager. The manual features detailed descriptions of the tasks performed by information security managers, and the knowledge required to manage, design and oversee an enterprise's information security program. The CISM Review Manual 2004 also provides

■ definitions, practical examples and sample questions to facilitate the learning process. (Available: January 2004)

■ The CISM Review Questions, Answers & Explanations Manual 2004, consists of 100 multiple-choice study questions arranged in the same proportion as the CISM job practice analysis. The questions include the answers and detailed explanations for the candidates to use in preparation for the CISM exam. This publication is ideal to use in conjunction with the CISM Review Manual 2004. (Available: January 2004)

Look for descriptions and ordering information on our web site at www.isaca.org/bookstore, or in the

Information Systems Control Journal, or contact the bookstore at +1.847.253.1545, ext. 401, or bookstore@isaca.org.

Standards Update

Standards Guidance

The ISACA Standards Board has undertaken an extensive review project to:

- Examine the robustness of existing ISACA IS Auditing Standards and Guidelines
- Revise, expand and add additional IS Auditing Standards and Guidelines to address areas not covered by the existing Standards and Guidelines
- Codify the revised IS Auditing Standards and Guidelines
- Address the role of COBIT in IS Auditing Standards and Guidelines

The current IS Auditing Standards are available on the ISACA web site, in 12 languages, at www.isaca.org/standards.
A comprehensive standards PDF document containing all of the standards, guidelines and procedures is also available at www.isaca.org/standards.

Education Update

New COBIT Implementation Course Available

A new COBIT implementation course has been developed and is available as part of ISACA's Professional Seminar Series (PSS). This course is intended for individuals responsible for, or involved in, IT governance. Chapters interested in bringing this course to their area should contact Robert Bergquist at +1.847.253.1545, ext. 473, or *rbergquist@isaca.org.*

CISM Grandfathering

The CISM grandfathering period is available only through 31 December 2003, so please encourage all experienced information security managers to act now.

The number of information security professionals applying for CISM certification under the grandfathering provision continues to increase each day. In turn, the CISM designation continues to grow in stature, influence and size, as information security managers join their peers and colleagues who hold the CISM designation.

CISA Update

CISA Recognition

Despite downward pressure on pay for information technology skills and certification, a recent report by Foote Partners LLC indicates that premium pay for professionals holding the Certified Information Systems Auditor (CISA) certification increased by 25 percent during the past 12 months.

The Foote Partners report confirms the value of earning a CISA designation. The 25 percent increase was the largest reported among the 57 certifications surveyed. In fact, according to the survey, overall, premium bonus pay for the certifications surveyed fell by nearly 6 percent over the past 12 months. CISA is among the exceptions.

The Foote Partners LLC findings are published in the *Quarterly Hot Technical Skills and Certifications Pay Index*. Additional information can be found at www.footepartners.com.

DACH-News

CH:

EUROCACS 2004 in der Schweiz

Reservieren Sie die Daten 21.–24. März 2004 in Zürich.

News aus den Interessengruppen

IG Government IT-Audit

Neu!

Michel Huissoud, CISA, CIA
Eidg. Finanzkontrolle/
Contrôle fédéral des finances
Monbijoustr. 45
3003 Bern
Tel. +41 31 323 10 35
Fax. +41 31 323 11 00
Michel.Huissoud@efk.admin.ch

Geschlossene Gesellschaft der Bundes- und Kantons-IT-Prüfer.

IG Computer Forensics

Paul Wang
PricewaterhouseCoopers
Avenue Giuseppe-Motta 50
1211 Geneva 2
Tel. +41 22 748 5601
Fax. +41 22 748 5354
Mobile: +41 79 220 5407
Paul.Wang@ch.pwc.com

L'objectif de ce groupe de discussion lié aux « Computer Forensics », est de fournir un forum d'intérêt et d'information sur les méthodologies et les outils de ce qu'on appelle communément en français « Assistance informatico-légale » Ce forum offre la possibilité de partager des idées, des technologies, des outils et certainement aussi des notions juridiques de ce domaine en constante évolution. Ce groupe de discussion abordera également des discussions techniques et procédurales sur les prérequis en matière de recherche de preuves informatiques. Même si les participants doivent être familiers avec la recherche, l'acquisition et l'analyse de preuves informatiques, tous les intéressés de tout niveau de connaissance sont les bienvenus.

IG Einführung von IT Governance

Leitung a.i.:
Jean-Pierre Brenn
Zürcher Kantonalbank, RII
Neue Hard 9
8010 Zürich
Tel. +41 1 292 82 84
Fax. +41 292 86 05
jean-pierre.brenn.kb.ch

Letzte Sitzung: Kick-off Sitzung am Freitag, 31. Oktober 2003, bei Ernst & Young AG, Zürich

Urs Fischer stellte in einem interessanten Einführungsreferat den Stand der Entwicklung innerhalb ISACA dar. Die Interessenten haben die möglichen Inhalte der IG diskutiert und die nächste Sitzung geplant.

Bis zur nächsten Sitzung wird der Entwurf des IT Governance Implementation Guide studiert. Ziel ist, eine deutsche Zusammenfassung und Präsentation für die Entscheidungsträger zu erstellen.

Nächste Sitzung: Donnerstag, 15. Januar 2004, 09.00 – ca. 16.00 Uhr, Ernst & Young AG, Bleicherweg 21, 8022 Zürich, Sitzungszimmer Sydney/Tokyo
Traktanden:
1. Diskussion Implementation Guide
2. Festlegen weiteres Vorgehen
3. Wahl IG-Leiter
4. Beantwortung von Fragen durch Urs Fischer (Nachmittag)

Anmeldung bis 12. Januar 2004 an Rolf Merz (+41 58 286 6679 oder rolf.merz@ey.com.ch

IG e-business

Leitung a.i.:
Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
rolf.merz@eycom.ch

IG Romandie

Vacant : touts personnes intéressées à participer ou animer un groupe de travail ou tous ceux qui aimeraient proposer un thème de réflexion peuvent s'annoncer auprès de M. Paul Wang.
paul.wang@ch.pwcglobal.com

IG Outsourcing/Insourcing

Ueli Engler
KPMG Fides Peat
Badenerstrasse 172
8004 Zürich
Tel. +41 1 249 26 16
uengler@kpmg.com

Nächste Sitzung: Offen. Interessenten melden sich bei Ueli Engler.

Geplant sind *Gespräche* zum Thema „Grounding" eines IT Service Providers mit ausgewählten Gesprächspartnern aus den Bereichen Legal, Service Provider, Industrie und Financial Services.

IG MIS/EIS/DWH

Leitung:
Daniel Oser
Ernst & Young AG
Badenerstrasse 47
Postfach 5272
8022 Zürich
Tel. +41 58 286 34 39
Fax. +41 58 286 32 76
daniel.oser@eycom.ch

Letzte Sitzung: Die letzte Sitzung fand am 15. Oktober 2003 bei Ernst & Young am Bleicherweg statt.

Folgende Teilnehmer waren anwesend:
Michael Clemens, UBS AG
Reinhart Höllstin, BKW FMB Energie AG
Michael Maes, Berata AG
Daniel Oser, Ernst & Young AG
Herbert Stauffer, Berata AG

Weitere Mitglieder sind stets herzlich willkommen!

Folgende Themen wurden besprochen:

- Referenzmodell Data Load: Das Feedback von Axel Mönkeberg von SwissRe zum Referenzmodell wurde im Detail besprochen. Als nächster Schritt ist die Überarbeitung gewisser Teile des Modells sowie ein Treffen mit Herrn Mönkeberg geplant. An dieser Stelle sei für sein Feedback gedankt.
- Risk Matrix: Die Risk Matrix wird nach Bereinigung des Referenzmodells überarbeitet und neu verabschiedet.
- Publikation Ergebnisse: Die Risk Matrix soll zusammen mit dem Data Load Modell, dem Glossar und der Literaturliste nach oben genannter Überarbeitung durch ISACA CH auf deren Homepage öffentlich zugänglich gemacht werden.
- Weiteres Vorgehen: Aus Zeitmangel konnten die Fact Sheets noch nicht besprochen werden. Einige waren auch noch nicht fertig erstellt. Deshalb werden folgende Fact Sheets für das nächste Mal vorbereitet und dann besprochen:

Projekt Management und Projekt Abwicklung, Datenschutz und sonstige Regulatoren, Change and Configuration Management, Berechtigungen, Disaster Recovery Planning

Nächste Sitzung: t.b.d bei E&Y, Bleicherweg 5. Stock
Für Informationen wenden Sie sich bitte an Daniel Oser.

IG SAP R/3

Monika E. Galli Mead
Eidg. Finanzkontrolle
Monbijourstrasse 51a
3003 Bern
Tel. +41 31 324 9495
Fax. +41 31 323 1101
monika.galli@efk.admin.ch

Letzte Sitzung: Donnerstag, 14. November 2002, bei PWC, Zürich
Traktanden:

- ACL/Berechtigungen wie prüfen (Hr. Appl., SNB)
- Qualitätsprüfungskonzept im SAP (Hr. B. Bolli, CCSAP BAIT)
- Im SAP das Risk Assessment Tool RAT einsetzen (Hr. A. Hilsbos, PWC)
- Neues vom Jahresmeeting SAP-AK's (H.J. Stritter, EDV-Audit-Consult)
- Übertragung von SAP Walldorf (M. Galli)
- SAP und AIS AUDITool News, Erfahrungen und Tipps (alle)

Die für 21. Mai 2003 geplante Sitzung ist ausgefallen und wird auf 13. November 2003 verschoben.

Nächste Sitzung: Donnerstag, 13. November 2003, 10.00 Uhr, PwC, Stampfenbachstrasse 73, 8035 Zürich, Sitzungszimmer J

Traktanden:

- Begrüssung
- Vorstellung des Implementierungs-Review Tool „TeamMate" (Frau F. Seheri, PwC)
- Enterprise oder die neue Architektur der SAP (Herr Ch. Winzer, BIT)
- Neues Berechtigungskonzept BV (Frau M. Galli)
- Java und ABAP (Herr X, BIT)
- Neues aus der Arbeitsgruppe SAP-Security (FGSec SAP) (Frau M. Galli)
- Erfahrungen und News (alle)

Veranstaltungen

CISA Vertiefungskurs	9. Dezember 2003 – 24./25. Mai 2004 Zürich, 17 Tage, ISACA CH/ITACS Trainings AG
Network Security Conference	17.–19. November 2003 Milano, 3 Tage, ISACA INTL
Windows 2003 Server-Sicherheit	20./21. November 2003 Bern, 2 Tage, Infosec
Federated Identity Management (After Hour Seminar)	26. November 2003 Zürich, ISACA CH
Mobile & Wireless Security	24.–27. November 2003 Dublin, 4 Tage, MIS
IT-Sicherheitberater, Intensivkurs	1.–5. Dezember 2003 Bern, 5 Tage, Infosec
Fraud Week	8.–12. Dezember 2003 London, 5 Tage, MIS
Forensic Investigation – Beweismittelsicherung	26.–28. Januar 2004 Zürich, 3 Tage, ISACA CH/adverum ag/CMC
Securing and Auditing Windows 2000 Server	13.–16. Januar 2004 London, 4 Tage, MIS
Hacking Your Network DMZ	29.–30. Januar 2004 London, 2 Tage, MIS

Kontaktadressen Veranstalter

Der *NewsLetter* empfiehlt folgende Veranstalter (weitere Kurse und Unterlagen direkt anfordern):

AFAI
Tel. +33 1 55 62 12 22
afai@afai.asso.fr
www.afai.asso.fr

advanced technology seminars
Grundgasse 13
CH-9500 Wil
Tel. +41 71 911 99 15
Fax. +41 71 911 99 16
Maurer@inf.ethz.ch

Stiftung für Datenschutz und Informationssicherheit
Dr. Beat Rudin
Kirschgartenstrasse 7
Postfach
CH-4010 Basel
Tel. +41 61 270 17 70
Fax +41 61 270 17 71
beat.rudin@privacy-security.ch
www.privacy-security.ch

e-tec Security
PO Box 54
Wilmslow Chesire SK9 6FU
United Kingdom
info@a-tecsecurity.com

Euroform Deutschland GmbH
Hans-Günther-Sohl-Strasse 7
D-40235 Düsseldorf
Tel. +49 211 96 86 300
Fax. +49 211 96 86 509
info@euroforum.com

Hochschule für Technik Rapperswil
Institut für Internet Technologien und Anwendungen
Oberseestrasse 10
8640 Rapperwil
Tel. +41 55 222 41 11
Fax. +41 55 222 44 00
office@hsr.ch

IIR-Akademie
Ohmstr. 59
D-60468 Frankfurt/Main
Tel. +49 69 7137 69-0
Fax. +49 69 7137 69-69
iir.academie@iir-ev.de

InfoGuard AG
Feldstrasse 1
CH-6300 Zug
Tel. +41 41 749 19 00
Fax +41 41 749 19 10
www.infosec.com

Integralis GmbH
Gutenbergstr. 1
D-85737 Ismaning
Tel. +49 89 94573 447
Fax +49 89 94573 199 fx
schulung@integralis.de

ISACA CH
Kurssekretariat
c/o. Bitterli Consulting AG
Konradstr. 1
8005 Zürich
Tel. +41 1 440 33 60
Fax. +41 1 440 33 61
kurse@isaca.ch

ISACA USA
3701 Algonquin Rd #1010
USA_Rolling Meadows IL 60008
Tel. +1 847 253 15 45
Fax. +1 847 253 14 43
www.isaca.org

Marcus Evans
Weteringschans 109
1017 SB, Amsterdam
The Netherlands
Tel. +31 20 531 28 13
Fax. +31 20 428 96 24
www.marcusevansnl.com

MIS Training Institute
Nestor House
Playhouse Yard P.O. Box 21
GB-London EC4V 5EX
Tel. +44 171 779 8944
Fax. +44 171 779 8293
www.misti.com

MediaSec AG
Tägernstrasse 1
8127 Forch/Zürich
Tel. +41 1 360 70 70
Fax. +41 1 360 77 77
it@mediasec.ch

Secorvo Security Consulting GmbH
Secorvo College
Albert-Nestler-Strasse 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455
info@secorvo.de
www.secorvo.de

Treuhand-Kammer
Jungholzstrasse 43
Postfach
CH-8050 Zürich
Tel. +41 1 305 38 60
Fax. + 41 1 305 38 61

ZfU Zentrum für Unternehmensführung AG
Im Park 4
CH-8800 Thalwil
Tel. +41 1 720 88 88
Fax. +41 720 08 88
info@zfu.c

Germany Chapter

Vereinsadressen

Geschäftsstelle
ISACA e.V., German Chapter
Eichenstr. 7
D-46535 Dinslaken
Tel. +49 2064 733191
Fax. +49 2064 733192
isaca.dinslaken@t-online.de

Präsidentin
Karin Thelemann
Ernst & Young AG
Wirtschaftsprüfungsgesellschaft
Mergenthalerallee 10–12
65760 Eschborn/Frankfurt am Main
Tel. +49 6196 99626 488
Fax. +49 6196 99626 449
karin.thelemann@de.ey.com

Konferenzen
Markus Gaulke
Marie-Curie-Str. 30
D-60439 Frankfurt
Tel. +49 69 9587 2313
Fax. +49 69 9587 192313
MarkusGaulke@kpmg.com

Mitgliederverwaltung und Kassenwart
Norbert Gröning
PwC Deutsche Revision AG
Friedrich-List-Str. 20
D-45128 Essen
Tel. +49 201 438 0
Fax. +49 201 438 1000
Norbert.Groening@
de.pwcglobal.com

Public Relations
Heinrich Geis
Deutsche Börse AG
Neue Börsenstrasse 1
D-60487 Frankfurt
Tel. +49 692 101 5149
Fax. +49 692 101 4396
heinrich.geis@deutsche-boerse.com

Arbeitskreise und Facharbeit
Bernd Wojtyna
WLSGV-Prüfungsstelle
Regina-Portmann-Strasse 1
D-48159 Münster/Westfalen
Tel. +49 251 288 4253 oder
+49 251 210 4539
bernd_wojtyna@gmx.net

Publikationen
Ingo Struckmeyer
comdirect private finance AG
Pascalkehre 15
25451 Quickborn
Tel. +49 4106 704 2336
Fax. +49 4106 704 2301
ingo.struckmeyer@pf.comdirect.de

CISA-Koordinator
Michael M. Schneider
Deloitte & Touche
Schumannstraße 27
60325 Frankfurt am Main
Tel. +49-69 75606 121
Fax. +49-69 75695 84448
michaelschneider@deloitte.de

Austria Chapter

Vereinsadressen

Vorsitzender (Präsident)
Ing. Mag. Dr. Michael Schirmbrand, CIA, WP, StB
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 211 70-2831
michael.schirmbrand@at.eyi.com

Stellvertretender Vorsitzender I (Vizepräsident I)
Dipl.-Ing. Maria-Theresia Stadler,
Österreichische Kontrollbank Aktiengesellschaft
Strauchgasse 1–3
1010 Wien
Tel: +43 1 531 27-857
maria-theresia.stadler@oekb.co.at

Stellvertretender Vorsitzender II (Vizepräsident II)
Mag. Josef Renner, StB
GRT Price Waterhouse
Prinz-Eugen-Straße 72
1040 Wien
Tel: +43 1 50188-0

Sekretär
Mag. Gunther Reimoser, CISA
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 21170-4113
gunther.reimoser@at.eyi.com

Kassier
Mag. Helmut Zodl
IBM Österreich
Obere Donaustraße 95
1020 Wien
Tel: +43 1 21145-0
helmut_zodl@at.ibm.com

CISA-Koordinator
Mag. Maria Rieder
Münze Österreich AG
Am Heumarkt 1
1010 Wien
Tel: +43 1 71715-0
maria.rieder@aon.at

Public Relations/Newsletter-Koordination
Rolf von Rössing
MA, D.E.s.s, CBCP, MBCI
Europa Treuhand Ernst & Young
Praterstraße 23
1020 Wien
Tel: +43 1 211 70-2812
dk@cos-ag.de

E-Mail ISACA Austria Chapter:
office@isaca.at
Homepage ISACA Austria Chapter:
www.isaca.at

Switzerland Chapter

Vereinsadressen

Präsidentin
Daniela S. Gschwend
Swiss Re
Mythenquai 50/60
8022 Zürich
Tel. +41 43 285 69 36
Fax. +41 43 285 33 69
daniela_gschwend@swissre.com

Vizepräsident
Michel Huissoud, CISA, CIA
Eidg. Finanzkontrolle/
Contrôle fédéral des finances
Monbijoustr. 45
3003 Bern
Tel. +41 31 323 10 35
Fax. +41 31 323 11 00
Michel.Huissoud@efk.admin.ch

Kassier
Pierre A. Ecoeur, CISA
Thurgauer Kantonalbank
Bankplatz 1
8570 Weinfelden
Tel. +41 71 626 64 61
Fax. +41 71 626 63 60
pierre-alain.ecoeur@tkb.ch

Ausbildung/Kurssekretariat
Peter R. Bitterli, CISA
Bitterli Consulting AG
Konradstr. 1
8005 Zürich
Tel. +41 1 440 33 60
Fax. +41 1 440 33 61
prb@bitterli-consulting.ch

CISA/CISM-Koordinator
Thomas Bucher
Ernst & Young AG
Postfach
8022 Zürich
Tel. +41 58 286 42 90
Fax. +41 58 286 40 14
thomas.bucher@eycom.ch

Sekretär
c/o Präsidentin

Information & Kommunikation
Monika Josi
Novartis Animal Health
Global Information Technology
WRO-1032.1.90
4022 Basel
Tel. +41 61 697 72 41
Fax. +41 61 697 78 44
monika.josi@ah.novartis.com
Adressmutationen bitte hier melden.

Koordinator Interessengruppen
Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
Rolf.Merz@eycom.ch

Représentant Suisse Romande
Paul Wang
PricewaterhouseCoopers
Avenue Giuseppe Motta 50
1211 Genève 2
Tel. +41 22 748 56 01
Fax. +41 22 748 53 54
paul.wang@ch.pwcglobal.com

Marketing
Bruno Wiederkehr
Rigistrasse 3
CH-8703 Erlenbach
bru.wiederkehr@bluewin.ch

Homepage ISACA Switzerland Chapter: www.isaca.ch