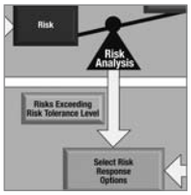
ISACA®
Trust in, and value from, information systems
Switzerland Chapter
Nr. 03 | September 2011 | www.isaca.ch
NEWSLETTER



ISO27001-Zertifizierung
Dass diese Zertifizierung gleichbedeutend sei mit einer hohen Sicherheit, entspricht nicht immer der Realität. **Seite 73**

CISM
Ein Personenzertifikat für Informationssicherheitsmanagement weit über ISO27000 hinaus **Seite 77**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 77**

Zertifizierte Sicherheit – Illusion oder Wirklichkeit?

Oft wird die Ansicht vertreten, dass eine ISO27001-Zertifizierung gleichbedeutend sei mit einer hohen Sicherheit. Leider entspricht dies nicht immer der Realität, was der nachfolgende Artikel beleuchtet.

Von Peter R. Bitterli, Bitterli Consulting AG

ISO27000er-Familie

Die ISO27000er-Familie besteht aus insgesamt 16 Normen, von denen nur ISO27001 und ISO27002 in einem breiteren Umfeld bekannt und für die Zertifizierung direkt relevant sind.

Die Norm ISO/IEC 27001

In ISO/IEC 27001 wird ein Informationssicherheitsmanagementsystem (ISMS) analog einem ISO9000-Qualitätsmanagementsystem beschrieben. Die Norm erschien erstmals 1998 als British Standard BS7799-2 und fordert ein prozessorientiertes Vorgehen zum Aufbau und Betrieb eines ISMS, das aus den vier zyklischen Phasen «Planen», «Umsetzen», «Überwachen» und «Verbessern» besteht – im Englischen mit «Plan – Do – Check – Act» bezeichnet.

Ein ISMS soll gemäss ISO27001:

- sicherstellen, dass adäquate Massnahmen getroffen werden, um die Informations-Werte angemessen zu schützen;
- dem Management Gewissheit geben, dass die Geschäftsrisiken bezüglich Informationssicherheit kontrolliert werden;
- eine Basis darstellen für Unternehmen, die eine effektive Sicherheitsorganisation betreiben wollen;
- bei Kunden, Handelspartnern und anderen betroffenen Parteien Vertrauen schaffen.

ISO27001 regelt im Detail den Geltungsbereich eines ISMS, die Formulierung einer Informationssicherheitspolitik, die systematische Risikoeinschätzung, die Inventarisierung sämtlicher Werte («Assets»), die Reduktion der Bedrohungen dieser Assets auf ein festgelegtes Risikoniveau, die formale Akzeptanz sämtlicher Restrisiken, die Durchführung von internen Sicherheitsaudits, und, und … und. Wenn man die Norm wirklich genau anschaut, sind es insgesamt über 160 verschiedene Anforderungen an die Aufbau- und Ablauforganisation eines ISMS.

Die Norm ISO/IEC 27002

ISO27002 ist die ursprünglich erste Norm in der Serie; sie erschien 1995 als British Standard BS7799 und enthält eine Sammlung allgemein anerkannter Sicherheitsmassnahmen, welche grundsätzlich und für alle Unternehmen gültig sind (sogenannte «Grundschutzmassnahmen») – leider in einem unterschiedlichen Detaillierungsgrad und teilweise redundant zu Elementen aus ISO27001 oder ISO27005.

Auch hier steckt der Teufel im Detail: Die insgesamt 133 Sicherheitsmassnahmen entpuppen sich bei wirklich genauem Hinschauen als Meta-Massnahmen (Themenpakete); insgesamt enthält ISO27002 demnach weit über

1200 Einzel-Massnahmen – eine kaum überschaubare Menge!

Andere zugehörige Normen

Von den insgesamt 16 Normen der ISO27000er-Familie sind für ein Unternehmen, das sich ernsthaft um ein wirksames ISMS kümmern möchte, noch die folgenden «interessant»:

- ISO27005 enthält die Beschreibung eines unternehmensweiten Frameworks für Informationssicherheits-Risikomanagement (2006 erstmals unter BS7799-3 veröffentlicht) und ist ähnlich zu ISO31000 aufgebaut. Da die systematische Identifikation, Bewertung und Behandlung von Risiken eine zentrale Komponente eines ISMS darstellt, ist diese Norm für die Umsetzung von ISO27001 wichtig aber freiwillig.
- ISO27004 enthält Angaben, wie Metriken für die Wirksamkeit von Informationssicherheitsmassnahmen z.B. im Rahmen eines ISMS entwickelt und gemessen werden können. Diese Norm enthält primär die entsprechende Theorie – ist dank der systematischen Herleitung, der klaren Sprache und letztlich der 17 detaillierten Beispiele auch für die Praktiker ein zentrales Hilfsmittel.

Was ist eine Zertifizierung?

Eine Zertifizierung ist das Ergebnis einer – durch eine formal akkreditierte Zertifizierungsstelle durchgeführten – unabhängigen Beurteilung, ob das Managementsystem eines Unternehmens die spezifischen Anforderungen einer bestimmten Norm erfüllt. Bei ISO27001 sind dies vor allem die folgenden Punkte:

Scope

Eine zentrale Aussage gemäss ISO27001 ist die formale Festlegung des Geltungsbereichs des ISMS («Scope») in Bezug auf die Charakteristika der Geschäftstätigkeit, des Unternehmens, seines Standortes, der Informationswerte und der eingesetzten Technologien.

Am einfachsten ist die Festlegung des Scope auf das gesamte Unternehmen. Unter Umständen sinnvoll ist der Ausschluss bestimmter Bereiche («alles ausser ...») oder die explizite Aufführung der abgedeckten Bereiche (z.B. «alle Unternehmensstandorte in der Schweiz»). Sinnvoll abgegrenzt wird z.B. nach Unternehmenseinheiten gemäss dem Organigramm des Unternehmens, nach Geschäftsprozessen oder auch nach Produkten, obwohl letzteres in der Praxis manchmal etwas schwierig ist.

Statement of Applicability

Sollten auf Grund des Charakters eines Unternehmens und seiner Geschäftstätigkeit eine oder mehrere der 133 Sicherheitsanforderungen aus dem Katalog ISO27002 nicht anwendbar sein, können sie in einer formalen Deklaration («Statement of Applicability») ausgeschlossen werden – z.B. wenn intern keinerlei Software-Entwicklung durchgeführt wird, schliesst man die entsprechenden Sicherheitsmassnahmen (Themen) aus.

Solche Ausschlüsse sind jedoch nur unter bestimmten Bedingungen zulässig: Ausschlüsse dürfen die Fähigkeit des Unternehmens nicht beeinträchtigen, die aufgrund ihrer Tätigkeit oder der rechtlichen Anforderungen notwendige Informationssicherheit bereitzustellen. Im Weiteren müssen Ausschlüsse begründet werden. Zudem muss der Nachweis erbracht werden, dass die mit Ausschlüssen verbundenen Risiken von den dafür verantwortlichen Personen ordnungsgemäss akzeptiert wurden.

ISMS-SCOPE

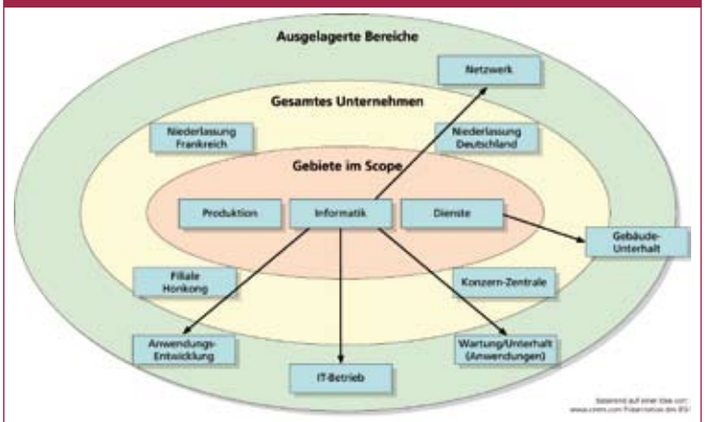


Abbildung 1: Abgrenzung des Geltungsbereichs des ISMS

Weitere, zwingend zu erstellende ISMS-Dokumente

Neben der formalen Festlegung von «Scope» und «Statement of Applicability» gibt es weitere ISMS-Dokumenten, welche als Einzeldokument oder als Teil eines übergeordneten Gesamtdokumentes vorhanden sein müssen. Dies sind unter anderem:

- Die ISMS-Politik umfasst die übergeordneten Ziele sowie die Stossrichtung für sämtliche Aktivitäten im Zusammenhang mit der Informationssicherheit und berücksichtigt die gesetzlichen, regulatorischen wie auch die unternehmensspezifischen Anforderungen an Informationssicherheit. Die ISMS-Politik muss auch die Ausrichtung des ISMS auf das unternehmensweite Risikomanagement sowie die Kriterien für die Risikobewertung erläutern. Als zentrales ISMS-Dokument muss die Politik von der Geschäftsleitung formal bewilligt sein. Die ISMS-Politik ist einem allenfalls vorhandenen Informationssicherheitskonzept übergeordnet.
- Beschreibungen des Prozesses für die Identifikation, Bewertung, Beurteilung und Behandlung von Risiken, sämtlicher implementierter Sicherheitsmassnahmen und anderer wesentlicher Kernelemente des ISMS

Wie läuft ein Zertifizierungsaudit ab?

Das Vorgehen für Zertifizierungsaudits ist in Dokumenten beschrieben, welche primär für die Zertifizierer und nicht für das zu zertifizierende Unternehmen von Bedeutung sind: ISO/IEC 17021 («Requirements for bodies providing audit and certification of management systems») sowie ISO/IEC 27006 («Requirements for bodies providing audit and certification of information security management systems»).

Vorbereitende Dokumentenprüfung

Typischerweise führt der Zertifizierer als erstes einen «Vor-Audit» durch, der im Wesentlichen aus einer systematischen Durchsicht der formalen ISMS-Dokumentation besteht. Zusätzlich zu den bereits erwähnten Dokumenten umfasst dies in aller Regel auch die Durchsicht des Risikoberichtes, also eines Kataloges sämtlicher (erkannten) Risiken des Unternehmens mit ihrer Bewertung und Behandlung. Ein Vor-Audit findet meist in den Räumlichkeiten des Zertifizierers und ohne aktive Beteiligung des zu zertifizierenden Unternehmens statt.

Zertifizierungs-Audit

Sind aufgrund des Vor-Audits keine wesentlichen Lücken in der formalen Dokumentation des ISMS erkennbar, führt der Zertifizierer den eigentlichen Zertifizierungs-Audit durch. Dabei geht es darum, die Einhaltung der unternehmensinternen Richtlinien, die Erreichung der unternehmensspezifischen Sicherheitsziele sowie die Einhaltung der implementierten Sicherheitsverfahren und -prozesse zu bestätigen. Zudem muss verifiziert werden, ob das Unternehmen ein ISMS konform zu ISO27001 implementiert hat und alle Sicherheitsanforderungen gemäss ISO27002 abdeckt. Zertifizierungs-Audits finden zum grössten Teil rein Interview-basiert statt, fallweise ergänzt mit weiteren Prüfungshandlungen des Auditors.

Aufrechterhaltungs-Audit

Periodisch und genügend häufig (in der Regel einmal jährlich) sollten kleinere Überwachungs-Audits und normalerweise alle drei Jahre umfassende Re-Zertifizierungs-Audits stattfinden.

Kritische Fragen bei Zertifikaten

Wer hat die Zertifizierung durchgeführt?

Aufgrund internationaler Verträge kann jedes – in irgendeinem Vertragsland für ISO27001-Zertifizierungen – akkreditierte Unternehmen in sämtlichen dieser Länder eine gültige Zertifizierung durchführen. Dies führt zwangsläufig zu kulturbedingten Unterschieden in der Breite und Tiefe der Durchführung. Die niedrigeren Kostenstrukturen der ausländischen Zertifizierer führen aufgrund des oft grossen wirtschaftlichen Drucks der Auftraggeber auch in der Schweiz zu einem gewissen Verdrängungskampf. Da der Name des Zertifizierers auf dem Zertifikat ersichtlich ist, werden aus Reputationsgründen aber in der Regel regional tätige Zertifizierer gewählt.

Was genau steht im «Scope»?

Für Aussenstehende ebenfalls leicht erkennbar ist der auf dem Zertifikat aufgedruckte Scope. Jedoch sind die verwendeten Bezeichnungen nicht immer sehr aussagekräftig: «Ganzes Unternehmen» ist klar, allenfalls auch «Ganzes Unternehmen mit Ausnahme des Bereichs Entwicklung» – aber was genau heisst z.B. «Kredit Beratungs-Komponente», «neues Medium E-Mail» oder «Data Warehouse»? Hier müssten interessierte Dritte (z.B. potentielle Geschäftspartner) weitere Erläuterungen vom zertifizierten Unternehmen einfordern – ein manchmal schwieriges Unterfangen.

Was wurde im «Statement of Applicability» ausgeschlossen?

Als potentieller Partner eines ISO27001-zertifizierten Unternehmens würde es mich interessieren, ob dieses bestimmte Sicherheitsmassnahmen im Rahmen des ISMS wirklich abdeckt oder ob für mich zentrale Sicherheitsthemen im «Statement of Applicability (SoA)» ausgeschlossen wurden. Das SoA ist aber nicht öffentlich und wird auch auf Anfrage nur ungern ausgehändigt – vor allem nicht mit allen zugehörigen Risikoüberlegungen, warum die ausgeschlossenen Sicherheitsmassnahmen denn nicht notwendig seien.

Warum hat das Unternehmen die Zertifizierung veranlasst?

Eine wichtige Frage – für deren Diskussion an dieser Stelle der Platz leider nicht ausreicht – ist, warum ein Unternehmen eine ISO27001-Zertifizierung durchführen lässt: Ist es aus Marketing-Überlegungen oder wegen dem Bestreben, ein bereits hervorragendes ISMS durch eine unabhängige Stelle bestätigen zu lassen? Manchmal wird auch von Geschäftspartnern (wie z.B. in der Automobilindustrie) grosser Druck ausgeübt, ein Zertifikat vorweisen zu können.

Illusion und Realität

PDCA-Modell suggeriert Kreislauf

ISO27001 wird als perfektes Managementsystem angepriesen, das sich im Rahmen eines Lebenzyklus' systematisch um alle Informationssicherheitsrisiken kümmert. In Tat und Wahrheit wird der PDCA-Prozessansatz einzig in der Einleitung im Abschnitt 0.2 auf einer halben Seite kurz beschrieben – im gesamten restlichen Dokument ist dieser Lebenszyklus nur ansatzweise und in den anderen 15 Normen der 27000er-Serie gar nicht erkennbar. Entsprechend wird dieser Kreislauf auch höchst unterschiedlich in die konkrete Praxis umgesetzt.

Abgrenzung zu verwandten Sicherheitsbereichen

Die 27000er-Normen kümmern sich um Informationssicherheit und grenzen diese in keiner Art und Weise zur IT-Sicherheit ab. Nur indirekt erkennbar ist die Tatsache, dass IT-Sicherheit als Untermenge der Informations-Sicherheit verstanden wird; so sind rund die Hälfte der 133 Sicherheitsmassnahmen aus ISO27002 technischer Natur. In der Praxis bestehen vor allem in grösseren Unternehmen oft zwei getrennte Organisationsbereiche: eine «Fachstelle für Informationssicherheit» und eine zweite – oft in der Informatik versteckte – «Fachstelle für IT-Sicherheit». Eine klare Abgrenzung ihrer Aufgaben, Kompetenzen und Verantwortlichkeiten wäre in der Praxis auf jeden Fall notwendig; die Normen enthalten aber keine diesbezüglichen Vorgaben.

Inhaltlich kümmern sich auch andere Stellen um Themen, welche gemäss ISO27001/2 im Rahmen des ISMS abgedeckt sind. Dies führt in der Praxis immer wieder zu widersprüchlichen oder fehlenden Sicherheitsmassnahmen:

- Wer ist z.B. dafür verantwortlich, dass die im neuen Datenschutzgesetz im Land einer Tochtergesellschaft aufgeführte Pflicht der Verschlüsselung sämtlicher Festplatten (!) auch auf dem Radar des ISMS auftaucht – der zentrale oder der lokale Rechtsdienst, der lokale IT-Verantwortliche oder die ISMS-Fachstelle?
- Wer ist verantwortlich, dass die Vertraulichkeitsvereinbarung nicht nur von neu angestellten Mitarbeitenden sondern auch von allen Temporärarbeitskräften und Drittfirmen-Mitarbeitern unterschrieben wird – der Personaldienst, die Einkaufsabteilung oder die ISMS-Fachstelle?
- Wer setzt die (unbeliebte) Schreibtisch-Aufräumpflicht («Clear desk policy») im Unternehmen durch – die «Fachstelle Physische Sicherheit» oder die «ISMS-Fachstelle»? Und wird sie gemäss der Verpflichtung der Norm überhaupt implementiert?

Integration in Enterprise Risk Management

In der Praxis bestehen oft grosse Unsicherheiten hinsichtlich der Integration des Risikomanagements als Teil des ISMS in ein unternehmensweites Risikomanagement (ERM). Wer kümmert sich darum – und sind z.B. die Kriterien für die Risikobewertung und Risikoakzeptanz einheitlich definiert?

Und was machen wir mit der Tatsache, dass wir auf dem ISMS-Radar (eigentlich) Hunderte von Informationssicherheitsrisiken haben und dann auf dem Radar des ERM vielleicht nur noch ein einziges Stellvertreter-Risiko für das gesamte ISMS?

ISMS-PROZESSE

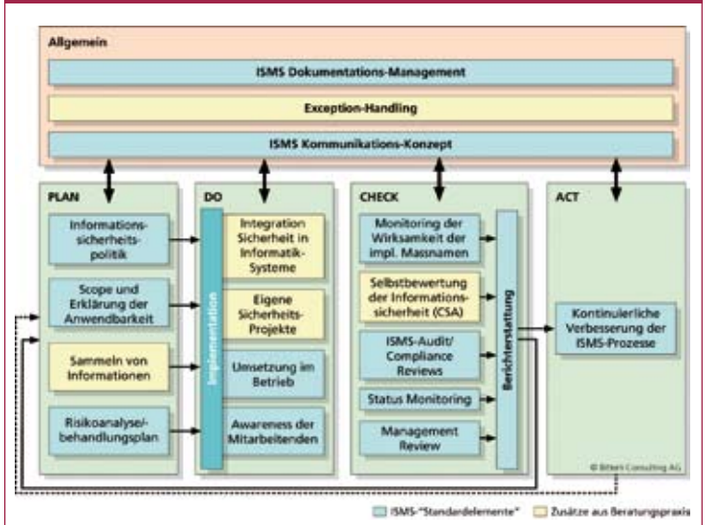


Abbildung 2: Typische Gestaltung der ISMS-Prozesse

Inventarisierung und Ownership

Eigentlich steht in ISO27001, dass sämtliche «Assets» (alles, was für das Unternehmen einen Wert darstellt), also z.B. alle Anwendungen, IT-Systeme, Daten usw. in einem Inventar aufgeführt und einem klaren Owner zugewiesen sein müssten. In der Praxis gilt das «Ownership-Prinzip» aber als ein Unding, das in dieser Form nicht umsetzbar sei und daher auch häufig nicht umgesetzt wird. Damit unterbleibt in der Regel aber auch die geforderte Untersuchung sämtlicher Assets nach den sie betreffenden Risiken.

Messung der Wirksamkeit der Sicherheitsmassnahmen

Als Teil des ISMS müsste gemäss ISO27001 für alle Sicherheitsmassnahmen festgehalten werden, wie deren Wirksamkeit genau gemessen und überwacht werden soll. Zudem müsste auch die Wirksamkeit des ISMS selbst gemessen werden. Das aber ist alles andere als einfach und wird von vielen Unternehmen wegen des vermeintlich hohen Aufwands nicht konsequent gemacht – auch wenn die noch wenig bekannte Norm ISO27004 sehr hilfreich wäre.

Umgang mit Outsourcing

Ein besonders schwieriges Unterfangen ist der Umgang mit ausgelagerten Teilbereichen. Meist wird das jeweilige Thema im «Statement of Applicability» einfach ausgeschlossen: Typischerweise finden wir solche Ausschlüsse für Themen wie «Softwareentwicklung» oder «IT-Betrieb». Macht das aber wirklich Sinn?

- Auch bei einer ausgelagerten Softwareentwicklung müssten z.B. die anwendungsspezifischen Sicherheitsanforderungen spezifiziert werden, damit diese im Rahmen der Softwareentwicklung berücksichtigt werden. Analog müsste bei der Abnahme der extern entwickelten Software auch die Erfüllung der ursprünglichen Sicherheitsanforderungen verifiziert werden. Das Thema wurde aber im ISMS ausgeschlossen – ist das so richtig?
- Analog das ebenfalls häufig ausgeschlossene Thema «IT-Betrieb». Wenn einem IT-Provider z.B. kritische Geschäftsanwendungen zum Betrieb übergeben werden, wird damit in aller Regel auch die Überwachung des Betriebs ausgelagert. Wie wird dann die Wirksamkeit der ausgelagerten Sicherheitsmassnahmen beim Provider gemessen?

Die 27000er-Normen sind hinsichtlich Outsourcing nicht sehr hilfreich. Die konkrete Ausgestaltung eines trotz Outsourcing auch in diesen Bereichen wirksamen ISMS verlangt viel Erfahrung und eine gehörige Portion Einsatzwille auf beiden Seiten. Auch der Zertifizierer ist gefordert, muss er doch die Risikoüberlegungen des Unternehmens zu diesen Ausschlüssen im «Statement of Applicability» nachvollziehen, beurteilen und letztlich akzeptieren. Und gemäss FINMA-Rundschreiben 2008/7 «Outsourcing Banken» müsste eigentlich das IKS des Providers (in diesem Fall das ISMS) zwingend in das IKS einer Bank integriert werden – ein Ausschluss wäre dann eigentlich gar nicht möglich!

ISMS-Audits im Vergleich zu «eigentlichen» Prüfungen

Viele Zertifizierungsaudits werden mit einem erstaunlich bescheidenen Budget durchgeführt: 1–2 Tage für den Vor-Audit zur Überprüfung der ISMS-Dokumentation; 1–2 Tage mit meist 2 Auditoren für den eigentlichen Zertifizierungs-Audit; alles zusammen und inklusive Bericht oft nur 4–7 Tage. Wie viel Gewissheit über die Wirksamkeit eines ISMS kann in so kurzer Zeit erworben werden? Wie viel Zeit benötigt man für ein wirklich detailliertes Studium der gesamten ISMS-Dokumentation und für die notwendigen Erhebungen, um eine fundiertere Aussage zur Wirksamkeit des ISMS zu machen?

Stellenwert eines ISO27001-Zertifikats

Stellenwert aus Abschlussprüfer-Optik

Börsenkotierte Unternehmen unterstehen immer neuen Rechnungslegungstandards sowie oft auch zusätzlichen Anforderungen der jeweiligen Börsenplätze. Sie müssen z.B. alle wesentlichen Outsourcing-Aktivitäten nach nationalen oder internationalen Prüfstandards (z.B. ISAE 3402, dem Nachfolger von SAS70) durch speziell zugelassene Revisionsunternehmen untersuchen und bestätigen lassen.

Die gesetzlichen und regulatorischen Anforderungen an solche Revisionsunternehmen unterscheiden sich sehr stark von den Anforderungen an ISO27001-Zertifizierer; ein ISO27001-Zertifikat z.B. eines IT-Providers hat in diesem Kontext daher nur eine sehr eingeschränkte Bedeutung. In diesen Fällen sinnvoll wäre die Zertifizierung des Providers durch ein Unternehmen, das einerseits als ISO27001-Zertifizierer akkreditiert ist und andererseits auch über die entsprechende Zulassung der Revisionsaufsichtsbehörde verfügt. Die gleichzeitige Berücksichtigung der unterschiedlichen Revisions-/Audit-Standards und Zulassungsbedingungen erhöht aber auch die Komplexität und Dauer der Zertifizierungs-Audits.

Stellenwert aus Sicht des zertifizierten Unternehmens

Verwaltungsrat und Geschäftsleitung können mit einer ISO27001-Zertifizierung sowohl innerhalb des Unternehmens als auch gegenüber Kunden und Geschäftspartnern demonstrieren, welche Bedeutung sie der Informationssicherheit zumessen. Um jedoch eine hohe Gewissheit über die Wirksamkeit des implementierten ISMS zu erlangen, sind nach unserer Erfahrung vertiefte Security Reviews wesentlich besser geeignet.

Stellenwert aus Sicht eines Geschäftspartners

Eine ISO27001-Zertifizierung bietet noch keine Gewissheit, dass angemessene und wirklich effektive Prozesse beim zertifizierten Unternehmen implementiert sind. Die Möglichkeit von nicht öffentlich erkennbaren Ausschlüssen sowie die manchmal sehr kurze Dauer eines Zertifizierungs-Audits lassen zu viel Interpretationsspielraum.

Schlussfolgerung

Zusammenfassend kann gesagt werden, dass

- mit den effektiv 160 Anforderungen von ISO27001 grundsätzlich eine sehr nützliche Vorlage besteht für den Aufbau und Betrieb eines wirksamen ISMS;
- der Katalog der 133 Grundschutzmassnahmen von ISO27002 eine gute erste Basis für Sicherheitsmassnahmen darstellt;
- die Implementierung eines wirksamen ISMS ein echtes und lang anhaltendes Bekenntnis der Geschäftsleitung bedingt;
- ein ISO27001-Zertifikat weder zwingend eine hohe Sicherheit bedeutet noch dass ein Unternehmen ohne ISO27001-Zertifikat seine Informationssicherheit nicht im Griff hat.

DER AUTOR

Peter R. Bitterli, dipl. math. ETH, CISA, CISM, CGEIT; Bitterli Consulting AG, Zürich

- Gründungsmitglied und Vorstandsmitglied des ISACA Switzerland Chapter
- Mitglied des Fachstabs für Informatik der Schweizerischen Treuhandkammer
- von der Schweizerischen Akkreditierungsstelle SAS (SECO) beauftragter Fachexperte für die ISO27001-Zertifizierung
- seit bald 30 Jahren in den Gebieten IT-Revision, IT-Security, IT-Risikomanagement und IT-Governance als Prüfer und Berater unterwegs

Information des Verbandes

CISM - Zertifikat für Informationssicherheit

Im Bereich IT- resp. Informationssicherheit gibt es verschiedene Personen-Zertifizierungen; so z.B. ISO27001 Lead Auditor, CISSP sowie das von ISACA getragene Zertifikat CISM (Certified Information Security Manager). Während der Titel «ISO27001 Lead Auditor» mit einer 3–5tägigen Ausbildung und einer relativ einfachen Prüfung erworben werden kann, basieren sowohl CISSP wie auch CISM auf einer Kombination von Prüfung und qualifizierter Berufspraxis.

Das seit 2003 angebotene CISM-Zertifikat deckt insgesamt 45 (!) verschiedene Aufgaben in fünf Themenbereichen ab: Governance der Informationssicherheit (Aufbau- und Ablauforganisation), Informations-Risikomanagement, Entwicklung eines Programms für Informationssicherheit, Management dieses Programms sowie Response Management. Dabei umfasst der Begriff «Sicherheitsprogramm» sämtliche Aktivitäten einer Sicherheitsorganisation, insbesondere auch alle Projekte zur Entwicklung und Verbesserung der Sicherheit (also z.B. Identity Management Systems, Data Loss Prevention, usw.) sowie die Überwachung und Anpassung sämtlicher aktuell laufenden Sicherheitsmassnahmen. Vergleicht man das CISM-Berufsbild mit den Inhalten von ISO27000, so deckt letzteres keine 15% der Tätigkeiten eines CISM ab.

Bereits haben über 15,500 Personen das CISM-Zertifikat erworben, wofür eine vierstündige Prüfung zu bestehen ist sowie fünf Jahre qualifizierte Fachpraxis nachzuweisen sind. Bestimmte Abschlüsse und Titel können mit bis zu max. zwei Jahren angerechnet werden (z.B. CISSP, SANS Global Information Assurance Certification GIAC, Microsoft Certified Systems Engineer MCSE, CompTIA Security+, Disaster Recovery Institute Certified Business Continuity Professional CBCP).

Das ISACA Switzerland Chapter führt zwei Mal jährlich einen berufsbegleitenden Kurs (14 Kurstage verteilt über jeweils 4–5 Monate) durch. Dieser richtet sich an alle Personen, die unternehmensweit oder auch in Teilbereichen für das Management der IT-/Informationssicherheit verantwortlich sind oder eine Schnittstellen-Funktion bekleiden – also Sicherheitsbeauftragte, Risikomanager, Verantwortliche für Business Continuity usw. Die Informatik ist zwar für die Informationssicherheit von Bedeutung, doch für einen CISM ein Faktor von vielen.

Der CISM-Kurs vermittelt und vertieft theoretisches wie praktisches Fachwissen im breiten Gebiet von Informationssicherheit, bereitet aber auch intensiv auf die von ISACA organisierte CISM-Prüfung vor.

WEITERE INFORMATIONEN

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

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
12.9.11	COB-IG	**ISACA Implementing Governance of Enterprisse IT Using COBIT**
13.-14.9.11	LAB-WAB	**Web Applications:** Basics
15.-16.9.11	LAB-WAA	**Web 2.0 – Web Applications:** Advanced
20.9.2011	OUT-KMU	**Risiken, Überwachung & Prüfung von Outsourcing-Providern** Bekommen Sie Ihr Outsourcing in Griff – speziell auch für KMUs
26.9.2011	ISMS-KK	**ISMS gemäss ISO 2700x implementieren und verbessern** Ein ISMS in 30 effizienten Schritten implementieren oder verbessern
3.10.2011	RIM-KK	**Risikoprüfungen und kontinuierliche Risikoüberwachungen** Wirksame Überwachung von Risiken
4.10.2011	IKS-KK	**Design, Betrieb, Überwachung & Unterhalt von Kontrollen** Effizientes Design & wirksame Überprüfung von anwendungsabhängigen Kontrollen
7.10.2011	JAVA-KK	**JAVA Enterprise für IT-Revisoren und IT-Sicherheitsbeauftragte** Professionelle Prüfung von Java-basierten Anwendungen
8.-10.11.11	AVA-REP	**Avaloq-Reporterstellung für Revisoren/Sicherheitsbeauftragte** Effiziente Erstellung von verlässlichen Reports aus dem Avaloq Banking System
17.-19.10.11	COB-FB	**ISACA COBIT 4.1 Foundation Zertifikat**
19.10.–15.11.11	CISA-PV	**CISA-Prüfungsvorbereitungskurs 2011|2** Kompakter Prüfungsvorbereitungskurs für erfahrene Kursteilnehmer; offizieller Kurs des ISACA Switzerland Chapter
20.-21.10.11	QM-IR	**Qualitätsmanagement in der Internen (IT-) Revision** Bringen Sie Ihre eigene Revisionstätigkeit auf ein ausreichendes Qualitätsniveau!
24.10.-16.11.11	CISM-PV	**CISM-Prüfungsvorbereitungskurs 2011|2** Kompakter Prüfungsvorbereitungskurs für erfahrene Kursteilnehmer; offizieller Kurs des ISACA Switzerland Chapter

Das gesamte Trainingsangebot mit näheren Informationen finden Sie online unter www.isaca.ch

IMPRESSUM ISACA NEWS

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Kurssekretariat, c/o ITACS Training AG, Stampfenbachstr. 40, 8006 Zürich
Erscheinungsweise: 4x jährlich in Swiss IT Magazine
Mitgliedschaft: Wir begrüssen alle, die Interesse an Audit, Governance und Sicherheit von Informationssystemen haben. Es ist nicht notwendig, dass Sie Sicherheitsspezialist oder Revisor sind, um bei uns Mitglied zu werden. Weitere Informationen finden Sie unter www.isaca.ch

Copyright: © Switzerland Chapter der ISACA