03/2014

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Gewinnspiel
Freikarten zur IT-Trends
(siehe Rückseite)

Überarbeitete ISO 27001 setzt neue Schwerpunkte: Risikobetrachtung und Lieferantenüberwachung

Wer sich systematisch mit der Informationssicherheit beschäftigen möchte, kommt an der ISO 27001 nicht vorbei. Bei der letztjährigen Überarbeitung dieser Norm hat sich zwar auf den ersten Blick viel geändert, aber bei genauerem Hinsehen sind nur wenige gravierende Änderungen festzustellen. Insbesondere sind hier eine ausführlichere Auseinandersetzung mit der Risikobetrachtung zu nennen wie auch umfangreichere Anforderungen an die Überwachung von Dienstleistern/Lieferanten.

Der gesamte Aspekt des Risikomanagements wird in der neuen Version der Norm deutlich hervorgehoben und an verschiedenen Stellen in den einzelnen Phasen betrachtet. Hierbei ist eine Übernahme von Regelungen aus anderen Normen erfolgt, auf die bisher lediglich referenziert wurde. Nach Feststellung der UIMC ist es Realität, dass in vielen Unternehmen ein umfassendes Risikomanagementsystem noch nicht existiert. Deshalb werden häufig gerade im Umfeld der Informationssicherheit erste Erfahrungen mit dem Umgang mit Risiken gesammelt. Auch wenn die Norm nicht detailliert genug ist, um „kochrezeptartig" Hilfe für die Einführung und den Umgang mit einem Risikomanagement-System zu bieten, gibt sie doch gute Anregungen hierzu.

Nicht nur aufgrund der gesetzlichen und den Normenanforderungen der ISO 27001 zur Lieferantenbewertung sollten Dienstleister, die auf vertrauliche Daten des Unternehmens zugreifen können, regelmäßig kontrolliert werden. Wie auch bei internen Audits kann ein solches Vorgehen zu einer Verbesserung der internen Prozesse, aber auch zu einer höheren Umsetzungstreue von vereinbarten Leistungen führen. Selbst bei einer aufgrund von langjährigen Erfahrungen geprägter vertrauensvoller Zusammenarbeit sollte eine solche Auditierung vorgenommen werden. Dies wird nun dadurch unterstrichen, als dass in der neuen Norm ISO 27001:2013 die Lieferantenbewertung ein eigenes Kapitel erhält.

Da bei vielen Unternehmen eine Tendenz zum Outsourcing besteht, ist die exponierte Stellung und Ausweitung der Lieferantenbewertung in der novellierten ISO-Norm nach Erfahrungen der UIMCert nur konsequent. Wenn intern ein Informationssicherheits-Managementsystem (ISMS) aufgebaut wurde, geschäftskritische Dienste aber durch einen externen Lieferanten (Rechenzentrumsbetreiber, IT-Systemhaus, Software-Wartung o. ä.) betreut werden, könnten – ohne eine umfassende und gewissenhafte Auditierung des Dienstleisters – interne Prozesse und Maßnahmen „ausgehebelt" werden, die zur Sicherstellung der Informationssicherheit etabliert wurden.

Die Anpassung der Norm hat insbesondere für jene Unternehmen eine Bedeutung, die bereits nach ISO 27001 zertifiziert sind oder dies derzeit vorbereiten. So können ab dem 1. Oktober 2014 Erst- und Re-Zertifizierungen nur noch gemäß ISO 27001:2013 vorgenommen werden; Überwachungsaudits nach ISO 27001:2005 bei bestehenden Zertifikaten sind noch bis September 2015 möglich. Somit muss eine Umstellung auf die ISO 27001:2013 bis 1. Oktober 2015 stattfinden, weil dann die alte Norm ungültig wird.

Doch nicht nur zertifizierte, sondern losgelöst von der ISO sollten auch jene Unternehmen, die ein ISMS aufgebaut haben, und auch jene Institutionen, die kritische Datenverarbeitungen an einen Dienstleister ausgelagert haben, eine strukturierte Dienstleister-Auditierung vornehmen. Hierbei sollte der IT-Sicherheitsbeauftragte (CISO) und/oder Datenschutzbeauftragte (DSB) eine zentrale Rolle einnehmen; sofern vorhanden, auch die Revision. Ein Audit-Konzept dient dabei nicht nur der Erfüllung etwaiger Norm- oder Gesetzesanforderungen, sondern strukturiert das eigene Vorgehen, was zu einem Qualitätsgewinn führt.

Auf der anderen Seite ist eine ISO-Zertifizierung auch für den Dienstleister selbst von Nutzen. So kann durch das Vorlegen eines solchen Zertifikats gegenüber dem Auftraggeber ein sicheres ISMS dokumentiert und somit einen Großteil der Dienstleister-Audits im eigenen Hause vermieden werden. Der Auftraggeber kann somit u. U. auch Anforderungen der Lieferantenbewertung gemäß ISO 27001:2013 ohne eigene Auditierung erfüllen, was im Übrigen auch für die Datenschutzanforderungen im Rahmen der Auftragsdatenverarbeitung gelten kann.

Die UIMCert als akkreditierte Stelle für die Zertifizierung nach ISO 27001 informiert hierüber ausführlich über die aktuelle Norm und die Änderungen in dem UIMCollege-Seminar „Auditierung und Zertifizierung gemäß ISO 27001". Hierbei können auch pragmatische Herangehensweisen bei der Lieferanten-Bewertung diskutiert werden.

Mehr Pressemitteilungen finden Sie hier: www.UIMC.de/communication

Schon gewusst?

Ab sofort gilt eine neue ISO 27001:2013 als neue Basis für die Zertifizierung. Gegenüber der 8 Jahre alten Norm sind verschiedene inhaltliche Änderungen vorgenommen werden, die bei der IT-Sicherheits-Organisation nun berücksichtigt werden müssen. Es gelten Übergangsfristen für die Umstellung.

Die ISO 27001 ist eine Best-Practice-Norm zum Aufbau eines Informationssicherheits-Managementsystems. Mehr finden Sie hierzu unter

ISO27001.UIMCert.de

Haben Sie Fragen?
UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (02 02) 2 65 74 - 0
Fax: (02 02) 2 65 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

Stets auf dem Laufenden sein?
www.UIMC.de/Communication

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Vertrauen ist gut, Passworte sind besser

Natürlich kann man seinen Kollegen vertrauen, doch beim Zugriff auf Programme und Daten sind geheime Passworte wichtig. Dies hat nichts mit Misstrauen zu tun, sondern vielmehr damit, dass

- mit einem Passwort geschützte Zugänge unterschiedlichen Berechtigungen verknüpft sind (**mögliche Folge:** unberechtigter Zugriff und Vertraulichkeitsverlust).
- manche Gesetze eine personenbezogene Protokollierung fordern, die bei Zugriff durch Kollegen dann inkorrekt sind (**mögliche Folge:** Rechtsverstoß/Compliance-Problem).
- alle Aktivitäten protokolliert werden und niemand (also auch nicht die Kollegen) vor Fehlern gefeit ist (**mögliche Folge:** Rechtfertigung von Fehlern, die sie nicht begangen haben).

Folgende Tipps sollten Sie im dienstlichen, aber auch im privaten Umfeld beachten:

1. Passworte zwingend **geheim halten** und nicht notieren. Wenn dies erforderlich sein sollte, fragen Sie Ihre IT nach sicheren Lösungen!
2. Nutzen Sie **komplexe Passworte.** Komplex ist ein langes Passwort, welches aus Groß- und Kleinbuchstaben, aus Sonderzeichen (z. B. #!§$) und Zahlen besteht. Bauen Sie sich „Eselbrücken" zum besseren Merken (Sätze, Erlebnisse o. ä.).
3. Nutzen Sie **nicht überall das gleiche Passwort.** Sonst probiert der (erfolgreiche) „Angreifer", ob es auch bei anderen Accounts funktioniert (ggf. sind sogar Hinweise im „geknackten" E-Mail-Account: z. B. Newsletter von Einkaufsportalen).
4. **Denken Sie nicht,** dass Sie nicht wichtig genug sind. Viele Kriminelle greifen willkürlich an... und Ihr Geld ist denen wichtig genug!

Mehr Tipps finden Sie in der nächsten Ausgabe vom UIMCommunic@tion-Info-Brief oder erfahren Sie bei Ihrem Ansprechpartner!

Auszug aus bisher erschienenen Hinweisen/Tipps:
„Sichere Nutzung von E-Mails" (09/2013)
„Umgang mit sozialen Medien" (08 & 02/2013)
„Smartphone-Funktionen sicher nutzen" (07/2013)

Zertifizierung/Auditierung

Innerhalb des UIMCollege-Seminars „Auditierung und Zertifizierung gemäß ISO/IEC 27001" werden die Struktur und die Inhalts der Norm ISO/IEC 27001 vermittelt. Hierbei können auch Vorgehensweise der Auditierung und normgemäßen Zertifizierungsvorbereitung und Erfüllung relevanter Anforderungen diskutiert werden. Natürlich wird hierbei schon die Novelle (ISO/IEC 27001:2013) berücksichtigt. Es besteht Zeit, mit dem Refenten zu diskutieren!

28.04.2014, Wuppertal

Save the Date!

Am Rande der diesjährigen IT-Trends „Sicherheit" werden wir am **14.05.2014** über das Thema „Vertrauen ist gut, Kontrolle ist besser" im Hinblick auf das Outsourcing informieren.

Unter allen UIMCommunication-Abonnenten, die eine Mail an communication@uimc.de mit dem Betreff „Freikarte" bis zum 30.04.2014 gesendet haben, verlosen wir eine Freikarte im Wert von EUR 50,00.

Gewinnspiel*

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

☐ Überarbeitete ISO 27001 setzt neue Schwerpunkte: Risikobetrachtung und Lieferantenüberwachung

☐ Novellierung der Best-Practice-Norm ISO 27001:2013

Unser Tipp: Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu! Mir ist bekannt, dass ich der künftigen Zusendung jederzeit formlos per E-Mail an communication@uimc.de widersprechen kann.

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 265 74 - 19 oder formlos per Mail an communication@uimc.de

*) Teilnahmebedingungen: Die Teilnahme ist kostenlos und unabhängig von dem Erwerb von Waren oder Dienstleistungen. Ebenfalls werden die Gewinnchancen nicht durch etwaige Leistungen der Teilnehmer beeinflusst. Voraussetzung ist eine Abonnierung des UIMCommunic@tion-Info-Briefs zum Zeitpunkt des Einsendeschlusses.