UIMCert: Überarbeitete ISO 27001 setzt neue Schwerpunkte: Risikobetrachtung und Lieferantenüberwachung

UIMCert: 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.

UIMCert GmbH
Dr. Jörn Voßbein
Moltkestraße 19
42115 Wuppertal
Tel.: (0202) 309 87 39
Fax: (0202) 309 87 49
E-Mail: certification@uimcert.de
Internet: www.uimc.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=559089" width="1" height="1">

Pressekontakt

UIMCert

42115 Wuppertal

certification@uimcert.de

Firmenkontakt

UIMCert

42115 Wuppertal

certification@uimcert.de

Die UIMCert GmbH ist eine Schwestergesellschaft der UIMC DR. VOSSBEIN GmbH & Co KG.Geschäftsführer der UIMCert ist Prof. Dr. Reinhard Voßbein.Die UIMCert gehört zu den führenden Unternehmen imBereich der IT-Sicherheits- und Datenschutzzertifizierung. Sie ist akkreditiert als Sachverständige Prüfstelle bei der TGA für ISO/IEC 27001 - BS 7799 und beim ULD für den Bereich Datenschutz Recht und Technik.Sie hat einen Fachbeirat, der die Geschäftsführungin wichtigen Fachfragen im Bereich IT-Sicherheit und ihrer Zertifizierung berät. Die UIMCert verfügt über qualifiziertesPersonal für die Begutachtung und Zertifizierung von IT-Sicherheitssystemen.