Neufassung der ISO 27001 vom Oktober 2013

Die neue ISO27001:2013 liegt bisher nur in englischer Sprache vor und ist in ihrem Hauptteil in wesentlichen Teilen neu formuliert worden. Dies gilt auch für den Anhang A mit den Controls, der zwar statt der bisherigen 133 Controls nunmehr nur 114 umfasst – jedoch sind nicht nur einige Controls entfallen, es hat auch Ergänzungen und Neuformulierungen gegeben.

Insgesamt ist die Neufassung besser strukturiert, einfacher lesbar und kürzer; weiterhin wurden Begrifflichkeiten präziser gefasst und Redundanzen vor allem im Anhang A beseitigt bzw. überarbeitet.

Was hat das zur Folge? Es kommt auf alle ISO27000-affinen Organisationen die Aufgabe zu, in naher Zukunft die neuen Normpunkte durchzugehen, mit dem alten Stand abzugleichen, Zuordnungen zu ändern und ggf. Änderungen bzw. Ergänzungen bei den Prozessen und Maßnahmen vorzunehmen. Letzteres wird allerdings nur in geringem Umfang erforderlich sein.

Wer sich bisher nach der älteren Fassung dieser Norm gerichtet hat, wird somit einiges an *formalem* Aufwand investieren müssen, um seine Compliance mit der neuen Fassung nachweisen zu können. Dies gilt vor allem für solche Organisationen, die sich in Bälde auditieren oder sogar re-zertifizieren lassen wollen.

Üblich ist eine Übergangsfrist von einem Jahr, d.h. grundsätzlich könnte man die ältere Fassung bis Oktober 2014 weiter verwenden – möglicherweise sogar länger, wenn man vom Erscheinungstermin einer deutschen Übersetzung (geplant für 2014) ausgeht.

Dies gibt andererseits genügend Zeit, die notwendigen Änderungen und Ergänzungen vor allem im Bereich der Dokumentation vorzunehmen:

1) Hierzu sollte man sich zunächst die aktuellen Fassungen der ISO 27000, ISO 27001 und ISO 27002 beschaffen.
2) Die Anforderungen der 27001 (Hauptteil und Anhang A) sind in entsprechende Compliance-Tabellen umsetzen.
3) Anschließend ordnet man entsprechende (Verweise auf) Dokumente, Maßnahmen, Begründungen etc. aus den älteren Tabellen den neuen Normpunkten zu – soweit dies inhaltlich geht.
4) Eventuell sind hierbei Änderungen und Ergänzungen vorzunehmen: Dies kann Verweise auf Dokumente, Maßnahmen, Begründungen betreffen, aber auch Angaben zur Erfüllung neuer bzw. geänderter Controls erfordern.
5) Soweit im Einzelfall bei den Schritten 3) und 4) Änderungen bzw. Ergänzungen vorgenommen worden sind, ist zu prüfen, ob diese bereits in der Realität umgesetzt worden sind oder ob dies entsprechend nachzuholen ist.

Mit diesem „kleinen“ Arbeitsprogramm wird man den Übergang zur neuen Normfassung erfolgreich gestalten können.

Im Dezember 2013

Heinrich Kersten

Jürgen Reuter

Klaus-Werner Schröder

http://www.springer.com/978-3-658-01723-1

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz

Der Weg zur Zertifizierung

Kersten, H.; Reuter, J.; Schröder, K.-W. - Kersten, H.; Wolfenstetter, K.-D. (Hrsg.)

2013, XIII, 377 S. 4 Abb., Softcover
ISBN: 978-3-658-01723-1