Deloitte.

ISO 27001/2:2013
Die Neuerungen auf einen Blick

Technologiekonzepte wie Software as a Service (SaaS), Cloud-Computing oder Bring Your Own Device (BYOD), eine Weltwirtschaft mit globalen Lieferketten über mehrere Ebenen und die verstärkte Nutzung sozialer Netzwerke führen dazu, dass sich immer mehr vertrauliche Informationen außerhalb der klassischen IT-Systeme befinden. Gleichzeitig steigen die Gefahren durch gezielte Cyber-Angriffe mit drohenden finanziellen Folgen und Reputationsverlust für die Unternehmen.

Diese rasanten Entwicklungen prägen die heutige Unternehmenskultur und stellen das Management vor neue Herausforderungen – wie können Informationen verschiedensten Ursprungs in verschiedensten Systemen effizient und effektiv geschützt werden?

Ein erster Blick auf die neue ISO 27001

Zuerst fällt auf, dass der Begriff „ISMS policy" durch den allgemeinen Terminus einer „information security policy" ersetzt wurde. Beim raschen Überfliegen der Kontrollen im Anhang A ist festzustellen, dass die Anzahl der Kontrollgruppen von 11 auf 14 erweitert, die Anzahl an Kontrollen insgesamt jedoch von 133 auf 113 reduziert wurde.

Ausgewählte Neuerungen im Überblick	
A.6.1.5: Informationssicherheit im Projektmanagement	Unabhängig von der Art des Projekts soll Informationssicherheit durch das Projektmanagement adressiert werden.
A.6.2.1: Mobile Geräte	Die Anforderungen an die Sicherheit mobiler Geräte werden deutlich geschärft und aufgewertet, sodass diese nun unter dem Oberkapitel „Organization of Information Security" anstelle von „Access Control" zu finden sind.
A.10: Kryptographie	Inhaltlich bzgl. Authentisierung leicht erweitert, haben sich die Anforderungen kaum geändert. Durch die Aufwertung als eigene Kontroll-Domäne erhält Kryptographie insgesamt jedoch mehr Gewicht.
A14.2: Sicherheit in Entwicklungs- und Unterstützungsprozessen	Regeln und Grundsätze zur Entwicklung sicherer Software und sicherer Systeme sind aufzustellen und umzusetzen. Ergänzende Kontrollen beinhalten das Entwickeln ausschließlich speziell gesicherter Entwicklungsumgebungen und die Durchführung gezielter Funktionstests der entwickelten Sicherheitsfunktionen.
A.15: Lieferanten-Beziehung	Der Schutz von Assets, auf die berechtigte Dritte Zugriff haben, wurde deutlich ausgeweitet. So ist eine übergreifende Supplier Security Policy zu erstellen und individuelle Vereinbarung sollen risikobasiert um Anforderungen an die Informations-und Kommunikationstechnologie erweitert werden.

Die Konzepte von „Dokumenten" (Absichtserklärungen) und „Aufzeichnungen" (Belegen) wurden unter dem Begriffe „dokumentierte Informationen" zusammengefasst und die Auflistung aller für ein ISMS notwendigen Dokumente (Abschnitt 4.3.1) ersatzlos gestrichen. Abhängig von Einflussfaktoren wie Unternehmensgröße, Prozesskomplexität und Kompetenz können Unternehmen selbst entscheiden, wie eine angemessene ISMS-Dokumentation aufgebaut ist. Entsprechende Kontrollen (Zugriff, Änderungen, Aufbewahrungsfristen etc.) der dokumentierten Informationen sind somit einheitlich für Dokumente und Aufzeichnungen anzuwenden.

Neben diesen ausgewählten inhaltlichen Änderungen, birgt die Neufassung wesentliche strukturelle und methodische Änderungen, die wir hier zusammenfassen:

Integrierte Managementsysteme

Als erste wesentliche Änderung ist herauszustellen, dass die Neuauflage der ISO/IEC 27001 konform zum Annex SL „Proposals for management system standards" der ISO/IEC Directive, Part 1 erstellt wurde. Alle überarbeiteten und neuen ISO-Standards zu Managementsystemen müssen konform zu diesem Proposal sein und einheitliche Strukturen und Begriffe anwenden. In Folge können verschiedene Managementsysteme einfacher integriert werden. Neben der neuen ISO/IEC 27001 gilt dies bereits für die ISO/IEC 22301 (Business Continuity Management) oder die ISO/IEC 20000-1 (IT Service Management). Weitere Standards werden zeitnah folgen, etwa die ISO 9001 (Quality Management) oder die ISO 14001 (Environmental Management Systems).

Zu beachten ist weiterhin, dass die Prozesse zur Risikobewertung und -behandlung an die Prinzipien und Empfehlungen der ISO 31000 (Risiko Management) angeglichen wurden und nicht mehr separat beschrieben werden.

Mehr Wahlfreiheit

Die zweite Fassung der ISO/IEC 27001 erlaubt Unternehmen deutlich mehr Wahlfreiheit bei der Implementierung eines Information Security Management Systems (ISMS). So können Unternehmen notwendige Kontrollen frei aus beliebigen Quellen wählen, solange diese für die gewählte Risikobehandlungsoption geeignet sind. Die Kontrollen im Anhang A und damit in der ISO/IEC 27002 sind nur noch als normative Referenz zu sehen. Im Statement of Applicability (SoA) ist jedoch explizit eine Begründung für alle ausgeschlossenen Kontrollen des Anhangs A zu formulieren.

Die Prozesse zu Aufbau, Implementierung, Betrieb, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung eines ISMS sind nicht mehr fest an das Plan Do Check Act (PDCA) Model gebunden. Die alte und bestehende zugrunde liegende Anforderung ist die der kontinuierlichen Weiterentwicklung des ISMS und PDCA ist lediglich ein möglicher Ansatz hierzu. Unternehmen steht es somit frei andere oder eigene Modelle anzuwenden, die ggf. besser zum individuellen Unternehmenskontext passen.

Aus Themen und Anforderungen werden Risiken und Chancen

In der ersten Fassung von 2005 wurde von einem „dokumentierten ISMS im Rahmen der allgemeinen Geschäftsrisiken der Organisation" gesprochen. Die aktuelle Fassung fordert hingegen, dass Unternehmen die internen und externen Themen bestimmen, die relevant für ihre Ziele sind und die ihre Fähigkeit zur Erreichung der beabsichtigten Ergebnisse des ISMS betreffen.[1] Zudem muss ein Verständnis der Erwartungen betroffener und interessierter Parteien wie typischerweise Stakeholder, Kunden, Partner oder Behörden, inklusive abgeleiteter rechtlicher und regulatorischer Anforderungen vorliegen. Abschließend müssen Schnittstellen und Abhängigkeiten der (Geschäfts-) Aktivitäten, durchgeführt durch die eigene oder andere Organisationen, berücksichtigt werden. Erst dann kann der Rahmen des ISMS festgelegt und dokumentiert werden.

Ausgehend von diesen Themen und Anforderungen gilt es, Risiken und Chancen abzuleiten, die behandelt werden müssen, sodass

- die beabsichtigten Ergebnisse des ISMS erreicht werden können,
- unbeabsichtigte Effekte vermieden oder reduziert werden und
- eine kontinuierliche Verbesserung sichergestellt werden kann.

Angepasst hat sich ebenso die Art zur Bewertung der Effektivität des ISMS. War diese in 2005 noch auf einzelne Kontrollen ausgelegt, gilt es nun, die Effektivität des gesamten Risikomanagements, basierend auf den Plänen zur Behandlung von Risiken und Chancen, zu bewerten. Die Neufassung ermöglicht durch die Anforderung kontinuierlicher Risikobewertungen auch eine schnellere Reaktion auf Veränderungen der Bedrohungslage. Die Effektivität eines ISMS soll somit kontinuierlich auf einem hohen Niveau gehalten werden.

[1] Dieses Vorgehen ist konform zum Entwicklung des Kontexts des Risikomanagements einer Organisation gem. ISO 31000, Abschnitt 5.3.

Was bedeutet die Neuerung für das Top-Management?

Die Kernaufgabe des „generischen" Managements innerhalb des ISMS war bisher u.a. die Etablierung einer ISMS Policy, entsprechender Rollen und Verantwortungen und die Sicherstellung, dass Ziele und Pläne des ISMS etabliert werden. In der Neuauflage wird dies weiter konkretisiert, indem gezielt das Top-Management der Organisation in die Pflicht genommen wird. Dieses muss nicht nur die oben genannte Aufgaben wahrnehmen, sondern auch die Konformität des ISMS mit den strategischen Zielen der Organisation und eine Integration der ISMS-Anforderungen in andere Unternehmensprozesse sicherstellen.

Hiermit spiegelt die ISO 27001 die geänderte Wahrnehmung von Information Security wider. Information Security ist nicht länger nur ein IT-Thema, sondern ebenso auf der Tagesordnung der Geschäftsführung, der Vorstände und Aufsichtsräte. Diese sollen der Information Security Organisation nicht nur formal vorstehen, sondern aktiv an der Gestaltung mitwirken.

Was ist nun zu tun?

Unternehmen, die bereits konform zu oder zertifiziert nach ISO/IEC 27001:2005 sind, sollten durch eine Gap-Analyse des alten zum neuen Standard für sie relevante Abweichungen identifizieren. Darauf aufbauend können konkrete Transformationspläne erarbeitet werden.

ISMS nach ISO/IEC 27001:2013 – Konformität zu anderen Managementsystemen und Flexibilität durch mehr Freiheit in der Ausgestaltung

Unternehmen, die bisher weder konform zur ISO/IEC 27001:2005 noch zertifiziert sind, bietet die Neuauflage einen einfachen Einstieg in das Thema Information Security Management. Durch die größere Flexibilität bei der Implementierung und die Konformität zu anderen Managementstandards können Synergien genutzt und Hürden beseitigt werden. Die Integration mit den strategischen Zielen der Organisation erlaubt die Etablierung von Business Cases, wodurch Sponsoren und notwendige Unterstützung innerhalb der Organisation einfach zu finden und sichergestellt werden können.

Ihr Ansprechpartner

Für mehr Informationen

Peter Wirnsperger
Partner
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Dr. Andreas Knäbchen
Partner
Tel: +49 (0)89 29036 8582
aknaebchen@deloitte.de

Dr. Carsten Schinschel
Partner
Tel: +49 (0)211 8772 3163
cschinschel@deloitte.de

Für weitere Informationen besuchen Sie unsere Website auf www.deloitte.com/de/cyber

Stand 12/2013