Bild: Pixabay

Bei den Standards sind die Gemeinsamkeiten der PDCA-Zyklus und betont die kontinuierliche Verbesserung, Risikomanagement und Führungsverantwortung

ISO 27013: Leitfaden für die Umsetzung

In vielen Unternehmen werden die IT-Prozesse nach ITIL umgesetzt. Da ITIL nur Personen zertifiziert, wurde die ISO 20000 entwickelt. Damit können Unternehmen ihre IT-Services zertifizieren und durch eine unabhängige Stelle prüfen lassen. Doch wie können diese mit der Informationssicherheit nach ISO 27001 in Verbindung gesetzt werden? Da hilft die ISO 27013.

Bevor wir uns mit der ISO 27013 beschäftigen können, ist es wichtig zu verstehen, was die ISO 20000 ist. Die ISO/IEC 20000-1 ist der international anerkannte Standard für Servicemanagement-System (SMS). Er definiert die Anforderungen für die Planung, Umsetzung, Überwachung und kontinuierliche Verbesserung von IT-Dienstleistungen. Das Hauptziel besteht darin, eine effektive und effiziente Bereitstellung von Dienstleistungen sicherzustellen, die den Anforderungen der Kunden und der Organisation entsprechen.

Die Norm ISO 20000-1 orientiert sich an den etablierten Best Practices der IT Infrastructure Library (ITIL) und ist insbesondere für IT-Dienstleister und interne IT-Bereiche relevant. Sie beinhaltet Prozesse wie Incident Management (Störungsmanagement), Changemanagement (Änderungsmanagement) und Service Level Management (Servicestufenmanagement), um eine erstklassige Servicequalität sicherzustellen.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

ISO 27013: Brücke zwischen Informationssicherheit und Servicemanagement

Die ISO/IEC 27013 ist ein Leitfaden für die integrierte Umsetzung von ISO 27001 (Informationssicherheitsmanagement) und ISO 20000-1 (Servicemanagement). Sie hilft Organisation en, Synergien zwischen diesen beiden Standards zu nutzen, um eine Doppelspurigkeit zu vermeiden und ein effizientes, ganzheitliches Managementsystem zu schaffen.

Warum ist die Integration wichtig?

Informationssicherheit und Servicemanagement sind eng miteinander verbunden. Ein effektives Servicemanagement kann ohne Berücksichtigung der Informationssicherheit nicht funktionieren und umgekehrt. Die ISO 27013 zeigt auf, wie Organisationen beide Standards harmonisch kombinieren können, um folgende Vorteile zu erzielen:

- Glaubwürdigkeit: Sichere und effektive Dienstleistungen stärken das Vertrauen von Kunden und Partnern.
- Kosteneffizienz: Gemeinsame Prozesse reduzieren den Implementierungs- und Wartungsaufwand.
- Zeitersparnis: Integrierte Prozesse verkürzen die Implementierungszeit.
- Verbesserte Kommunikation: Klare Strukturen fördern die Zusammenarbeit zwischen Teams.

Kerninhalte der ISO 27013 – Gemeinsamkeiten und Unterschiede

Die ISO 27013 hebt sowohl die Überschneidungen als auch die Unterschiede zwischen den beiden Standards hervor:

- Gemeinsamkeiten: Beide Standards folgen dem PDCA-Zyklus (Plan-Do-Check-Act) und betonen kontinuierliche Verbesserung, Risikomanagement und Führungsverantwortung.
- Unterschiede: Die ISO 27001 konzentriert sich auf den Schutz von Informationen (Vertraulichkeit, Integrität, Verfügbarkeit) während sich die ISO 20000-1 zielt auf die effektive Erbringung von IT-Services ab.

Ansätze für die integrierte Umsetzung

Die Norm beschreibt drei typische Umsetzungs-Szenarien:

1. Kein bestehendes Managementsystem: Hier empfiehlt die ISO 27013, je nach Geschäftsprioritäten mit einem der beiden Standards zu beginnen und schrittweise den anderen zu integrieren.
2. Bestehendes ISMS oder SMS: Organisationen sollten das vorhandene System erweitern, um die Anforderungen des anderen Standards zu erfüllen.
3. Getrennte Systeme: Hier gilt es, gemeinsame Elemente zu identifizieren und zu konsolidieren, während spezifische Anforderungen weiterhin separat behandelt werden. Dies wird als sehr aufwendig beschrieben.

Herausforderungen und Lösungen

Die ISO 27013 benennt potenzielle Herausforderungen, insgesamt 11 Punkte, bei der Integration und bietet Lösungsansätze. Nachfolgend die drei Hauptthemen:

- Risikomanagement: Die ISO 27001 fordert eine detaillierte Risikobewertung, während ISO 20000-1 Risiken im Kontext von Dienstleistungen betrachtet. Die Norm empfiehlt, einen gemeinsamen Risikomanagement-Ansatz zu entwickeln.
- Incident Management: Unterschiedliche Definitionen von «Vorfall» können zu Verwirrung führen. Die Norm schlägt klare Kriterien für die Klassifizierung von Vorfällen vor.
- Asset Management: Die Definition von «Assets» variiert zwischen den Standards. Hier hilft eine einheitliche Terminologie.

Potenzielle Gewinne

Die Integration beider Standards bietet zahlreiche Vorteile:

- Service Level Management: Berichte können sowohl Service- als auch Sicherheitskennzahlen umfassen.
- Verwaltung der Kapazitäten: Die beiden Normen fordern die Ermittlung und Bereitstellung notwendiger Ressourcen. Während ISO/IEC 20000-1 umfassende Anforderungen an das Kapazitätsmanagement formuliert – bezogen auf personelle, technische, informationelle und finanzielle Ressourcen – enthält ISO/IEC 27001 keine spezifischen Vorgaben dazu.
- Kontinuierliche Verbesserung: Gemeinsame Prozesse fördern eine ganzheitliche Optimierung.
- Drittanbieter-Management: Integrierte Ansätze vereinfachen das Management externer Lieferanten.
- Kontinuitäts- und Verfügbarkeitsmanagement: Die ISO/IEC 20000-1 deckt ausdrücklich zwei Bereiche ab, die für die Informationssicherheit von Interesse sind: Service Availability Management und Service Continuity Management.

Der informative (bedeutet verbindlich) Anhang A zeigt die Verbindung zwischen der ISO 27001 und ISO 20000, Klauseln 1 bis 10. Die Hauptunterschiede sind in den Kapiteln 6.1 und 8 zu finden. Das Kapitel 8 ist in der ISO 20000 sehr viel ausführlicher beschrieben.

Der ebenfalls informative Anhang B macht die Verknüpfung des Anhangs A der ISO 27001 und der ISO 20000 in den Kapitel 4 bis 10. Der informative Anhang C vergleicht die Begriffe und Definitionen der beiden Normen. Dies ist bei der Umsetzung sehr wichtig, da die Normen nicht immer genau das gleiche unter einem Begriff verstehen.

Hinweis: beide Normen wurden vor der Veröffentlichung der ISO 27001:2023 publiziert. Das Amendment 1 von Dezember 2024 zeigt daher die notwendigen Anpassungen auf.

Praktische Tipps für die Umsetzung

Die Norm beschreibt das folgende Vorgehen zur Integration der beiden Normen:

1. Start mit einer Gap-Analyse: Identifizieren Sie Überschneidungen und Lücken zwischen Ihrem ISMS und SMS.
2. Harmonisierung der Dokumentation: Nutzen Sie gemeinsame Dokumente für ähnliche Anforderungen, zum Beispiel für interne Audits oder Managementbewertungen.
3. Schulungen und Awareness: Sensibilisieren Sie Mitarbeiter für die Zusammenhänge zwischen Servicemanagement und Informationssicherheit.
4. Tool-Unterstützung: Integrierte Softwarelösungen können beide Standards unterstützen und die Umsetzung erleichtern.

Fazit

Die ISO 27013 ist ein wertvoller Leitfaden für Organisationen, die sowohl ISO 27001 als auch ISO 20000-1 implementieren möchten. Durch die Integration beider Standards können sie nicht nur Ressourcen sparen, sondern auch ein stärkeres, ganzheitliches Managementsystem aufbauen. Die Norm bietet klare Anleitungen, um gemeinsame Prozesse zu identifizieren, Herausforderungen zu meistern und die Vorteile beider Standards optimal zu nutzen.

Für Unternehmen, die bereits eines der beiden Systeme eingeführt haben, lohnt sich ebenfalls ein Blick auf die ISO 27013, um die Integration einer Norm in die andere zu planen. Und für diejenigen, die noch am Anfang stehen, bietet die Norm eine Roadmap, um von Beginn an ein harmonisches System zu schaffen.