

Neue ISO 27001 und 27002

Umsetzung der Anforderungen der ISO 27001:2022 / 27002:2022

Auf ISO 27001 zertifizierte KRITIS Organisationen kommen umfangreiche Änderungen im Zusammenhang mit der Aktualisierung der ISO 27001 und der neuen ISO 27002 zu.

Neuerungen in der ISO 27001 / 27002

Die Norm hat eine neue Kapitelstruktur. Ihre Dokumentation muss daran angepasst werden. Statt der üblichen 14 Kapitel im Anhang sind es jetzt nur noch vier.

- ▶ Kapitel 5 Organisatorisch
- ▶ Kapitel 6 Personenbezogen
- ▶ Kapitel 7 Physisch
- ▶ Kapitel 8 Technologisch

Für Stadtwerke, Energieversorger und Stromerzeuger wird in der Übergangsfrist bis zur Veröffentlichung der umstrukturierten ISO 27019 auch ein Mapping notwendig. Darüber hinaus haben sich die Inhalte der einzelnen Kapitel geändert und in einigen Bereichen sind die Anforderungen wesentlich schärfer geworden.



Unterstützung in der Integration

Um die Einführung der neuen Maßnahmen zu erleichtern ohne den Betrieb des bestehenden ISMS einzuschränken, beraten wir Ihr Kernteam gerne. Mit uns finden Sie den Weg zu Ihrem zukunftsorientierten ISMS. Mit umfangreicher Erfahrung und tiefgehendem Know-How mit Praxisbezug begleiten wir Sie in der bestmöglichen Umsetzung der ISO 27002:2022 bis zur Rezertifizierung.

Wir bieten Ihnen:

- ✓ Tiefgehende Kenntnisse aus der System- und Netzwerksicherheit
- ✓ Umfangreiche Praxiserfahrung
- ✓ Einen gut strukturierten, detailorientierten Lösungsweg
- ✓ Aktuelles Wissen über Schwerpunkte in der Auditierung





Wichtige Anforderungen

► Bedrohungsaufklärung / Überwachung von Aktivitäten

Auch in der neuen ISO 27002 werden elementare Bestandteile eines Systems zur Angriffserkennung gefordert. Dazu gehört es, Informationen zu aktuellen Bedrohungen zu sammeln und auszuwerten. Außerdem müssen die Netzwerke, Systeme und Anwendungen auf anomales Verhalten überwachen und geeignete Maßnahmen ergriffen werden, um potenzielle Informationssicherheitsvorfälle zu erkennen.

Anhang A, Kapitel 5.7; 8.16

► Business-Continuity Management / BCM

Die Bereitschaft der Informations- und Kommunikationstechnologie (IKT) soll auf Grundlage von Zielen der Business-Continuity und IKT-Continuity geplant, implementiert, aufrechterhalten und getestet werden. Dazu gehört jetzt auch eine Business-Impact-Analyse.

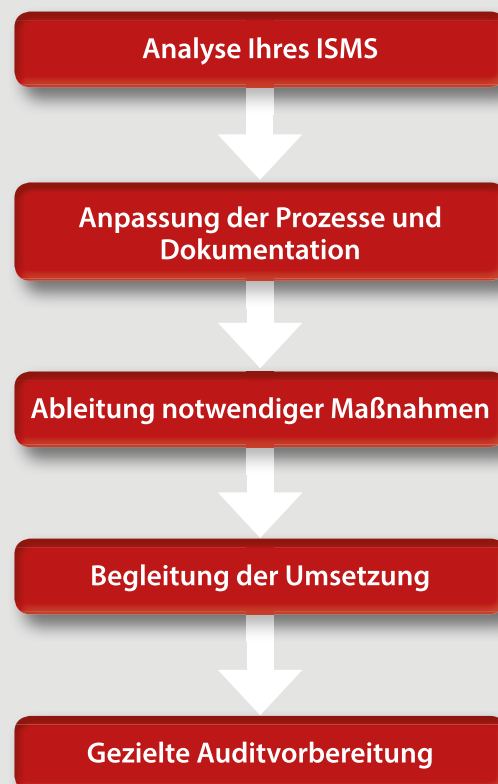
Anhang A, Kapitel 5.30.

► Konfigurationsmanagement (Configuration management)

Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken sollen erstellt, dokumentiert, implementiert, überwacht und überprüft werden.

Anhang A, Kapitel 8.9

GEMEINSAME VORGEHENSWEISE



Quellennachweis: AdobeStock, Picture Alliance, WVV GmbH, Stadtwerke München

www.ausecus.com



ausecus GmbH

Werner-von-Siemens-Straße 6
D-86159 Augsburg

Tel +49 821 207097-0
Fax +49 821 207097-99
E-Mail info@ausecus.com

