Änderungen ISO/IEC 27001 und ISO/IEC 27002

Die Norm ISO 27001 für das Informationssicherheitsmanagement wird derzeit zur DIN ISO/IEC 27001:2023 überarbeitet, während eine neue Version der Norm ISO/IEC 27002 im Februar dieses Jahres veröffentlicht wurde.

1. Was ist der Unterschied zwischen ISO/IEC 27001 und ISO/IEC 27002?

Unternehmen können weiterhin die ISO/IEC 27001-Zertifizierung für die Systemkonformität erhalten, aber nicht die ISO/IEC 27002.

Die Norm ISO/IEC 27001 bietet einen Rahmen für das Informationssicherheitsmanagement, während ISO/IEC 27002 Richtlinien für Informationssicherheitsmanagementpraktiken, einschließlich der Implementierung und Verwaltung von Kontrollen unter Berücksichtigung des Informationssicherheitsrisikos einer Organisation bietet.

2. Die neue Norm ISO/IEC 27001:2022 wird voraussichtlich folgende Änderungen mit sich bringen:

a) Die neue Norm umfasst 93 Kontrollen, die in 4 Bereiche unterteilt sind, vorher waren es 114 Kontrollen und 14 Bereiche.

b) Jede Kontrolle hat 5 Attribute:
   1. Kategorisierung: präventiv, detektivisch, korrigierend
   2. Merkmale der Informationssicherheit: Vertraulichkeit, Integrität, Verfügbarkeit (CIA)
   3. Cybersicherheitskonzepte: Identität, Schutz, Identifizierung, Reaktion, Wiederherstellung
   4. Operative Fähigkeit: Governance, Vermögensverwaltung, Informationssicherheit, Sicherheit der Humanressourcen, usw.
   5. Sicherheitsbereiche: Governance, Schutz, Widerstandsfähigkeit

c) Die neue Norm ISO/IEC 27001:2022 führt darüber hinaus neue Kontrollen ein, darunter:
   - Identitätsmanagement
   - Löschung von Informationen
   - Maskierung von Daten

Bild: Pixabay.com

Sobald die deutsche Version DIN EN ISO/IEC 27001:2022 (Anfang 2024) verfügbar ist, werden wir gemeinsam mit Ihnen das vorhandene Managementsystem an die neue Revision anpassen.

Für weitere Fragen rund um das QM-System, den Datenschutz und der IT-Sicherheit stehen wir Ihnen selbstverständlich jederzeit gerne zur Verfügung.

Kontaktieren Sie uns

EuroConsult Deutschland GmbH
Albertus-Magnus-Straße 2
D – 86836 Graben
Tel.: +49 8232 80988-0

info@euroconsult.de
www.euroconsult.de

EuroConsult
Unternehmensberatung

Übrigens:

Nutzen Sie E-Learning!

Unser Partner coseco GmbH bietet E-Learning-Kurse zu verschiedenen aktuellen Themen an, momentan ist der Kurs **„Phishing-Mails“** äußerst beliebt bei den Kunden.

Nach Bestehen erhalten alle Teilnehmenden ein Zertifikat. Sie können also nachweisen, dass Ihr Team für diese Betrugsmasche sensibilisiert wurde, um sie dadurch sicherer im Umgang damit zu machen.

Informieren Sie sich hier: https://dsms-online.com/informationssicherheit.html

© EuroConsult Deutschland GmbH | Juli 2025