Informationsblatt zur Umstellung auf ISO/IEC 27001:2022

IFU-CERT
DER ZERTIFIZIERUNGSPARTNER

KUNDEN-INFO

1 Kurze Zusammenfassung der Änderungen

- Die Strukturierung der Norm nach High Level Structure ist unverändert.
- In den einzelnen Kapiteln der Norm wurden teilweise redaktionelle aber auch viele wichtige kleine Anpassungen vorgenommen.
- Die Änderungen im Annex A sind grundlegend; die in Tabelle A.1 aufgeführten Informationssicherheitsmaßnahmen sind aus ISO/IEC 27002:2022 direkt abgeleitet und daran ausgerichtet.
- Die Maßnahmen (Controls) wurden aktualisiert und neu strukturiert. Die Controls sind in vier Kontroll-Typen unterteilt:
    - Organisational Controls
    - People Controls
    - Physical Controls
    - Technological Controls
- Einige Themenblöcke werden getrennt, auf der anderen Seite wurden bestehende Maßnahmen teilweise zusammengefasst.
- Elf (11) neue Maßnahmen wurden definiert, die Cloud-Sicherheit, Threat Intelligence und datenschutzverwandte Themen behandeln. Die Anzahl der Maßnahmen hat sich infolge der Neu-Strukturierung geändert.

2 Gültigkeit der Zertifikate

- Die Übergangsfrist für die Zertifikate endet am **31.10.2025.**
- Zertifikate, die infolge von Erst-Zertifizierungs- oder Re-Zertifizierungsaudits gem. DIN EN ISO/IEC 27001:2017 nach dem Zeitpunkt des Erscheinens der neuen Norm-Revision ausgestellt wurden, werden mit entsprechender kürzerer Gültigkeit, bis zum 31.10.2025, ausgestellt.
- Alle Zertifikate nach DIN EN ISO/IEC 27001:2017, auch solche, die ggf. während der Übergangsfrist für 3 Jahre ausgestellt wurden, verlieren nach diesem Datum ihre Gültigkeit.

3 Umstellungsaudits

- Die Umstellung der Zertifikate ist erst nach einem erfolgreichen Audit zur Prüfung der Umstellung des Systems auf ISO/IEC 27002:2022 möglich.
- Die Prüfung der Umstellung kann in einem Re-Zertifizierungsaudit, in einem Überwachungsaudit oder in einem separaten (außerordentlichen) Audit stattfinden.

- Das Umstellungsaudit besteht aus einem Stufe 1-Audit als Dokumentenprüfung offsite und einem Stufe 2-Audit vor Ort.
- Im Umstellungsaudit werden geprüft
  a.) die Vorbereitung der zertifizierten Kunden auf die Umstellung (Nachweise der Gap-Analyse, der Umstellungs- und Umsetzungsplanung, interne Verifizierung der Umsetzung im Rahmen eines internen Audits),
  b.) die nachweisbare Erfüllung aller Anforderungen der Norm ISO/IEC 27001:2022.
- Die Audittage vor Ort der Re-Zertifizierungsaudits mit Umstellung auf die neue Revision der Norm werden gemäß Umstellungsregeln um 10%, aber mindestens um 0,5 Audittag, erhöht. Die Audittage vor Ort der Überwachungsaudits mit Umstellung auf die neue Revision der Norm werden gemäß Umstellungsregeln um 20%, aber mindestens um 0,5 Audittag, erhöht.
- Die Aufwandskosten für die Revision der Zertifikate richten sich nach den gültigen bekannten Gebühren zur Änderung der Zertifikate.

4 Erstellung der Zertifikate gemäß ISO/IEC 27001:2022

Voraussetzungen für die Erstellung der Zertifikate, gemäß Umstellungsanleitung der DAkkS:

- Die Akkreditierung der Zertifizierungsstelle ist auf die aktuelle Norm umgestellt; die DAkkS plant spätestens bis zum 31.10.2023 alle Zertifizierungsstellen umgestellt zu haben;
- die DAkkS plant, die Akkreditierungsurkunden der Zertifizierungsstellen bei nächster Gelegenheit anzupassen, sobald die Norm ISO/IEC 27001:2022 als europäische Norm in deutscher Fassung (als DIN EN ISO/IEC) veröffentlicht wurde;
- das Audit zur Umstellung für den zertifizierten Kunden und die Entscheidungsprozesse der Zertifizierungsstelle sind erfolgreich abgeschlossen.

5 Weitere Informationen

Für weitere Informationen oder z.B. hinsichtlich Wünsche zur Planung von Umstellungsaudits oder bei Unklarheiten können die zertifizierten Kunden gerne direkt die IFU-CERT-Zertifizierungsstelle ansprechen.

KUNDEN-INFO