TÜVNORD

Inspired by
Knowledge

Kundeninformation
„ISO/IEC 27001:2022“ – Umstellung

Wichtige Informationen zu Ihren bestehenden ISO 27001 Zertifizierungen

Sehr geehrter ISO 27001 Zertifizierungskunde,

wie Sie vermutlich bereits gehört haben, ist die ISO/IEC 27001 überarbeitet worden und als ISO/IEC 27001:2022 im Oktober 2022 erschienen.

Das „International Accreditation Forum“ (IAF) hat in dem IAF-Dokument IAF MD 26 vom 15.02.2023 eine dreijährige Übergangsfrist und einige Übergangsvorkehrungen festgelegt. Das bedeutet, dass nach dem Ablauf der Umstellungsphase jede Zertifizierung nach ISO 27001 ausschließlich auf der neuen Ausgabe basieren darf und alle Zertifikate nach der alten Ausgabe ungültig werden – ungeachtet der Angaben zum Ablaufdatum im Zertifikat.

Die Deutsche Akkreditierungsstelle (DAkkS) hat am 01.01.2023 eine Umstellungsanleitung für Akkreditierungen im Bereich ISO/IEC 27001:2022 veröffentlicht. Die Information der zertifizierten Kunden über die Übergangsregelung für die Zertifizierung nach ISO/IEC 27001:2022 ist eine der dort festgelegten Pflichten.

Anmerkung
Die in diesem Schreiben für die ISO/IEC 27001:2013 getroffenen Aussagen gelten analog auch für die deutsche Übersetzung der ISO/IEC 27001:2013, den Standard DIN EN ISO/IEC 27001:2017.

TÜV NORD CERT hat einen Antrag auf Erweiterung und Umstellung der Akkreditierung auf die neue Ausgabe des Standards gestellt.

Fortsetzung der ISO 27001 Zertifizierung mit der neuen Ausgabe der Norm

Bitte beachten Sie folgende von der IAF festgelegten allgemeinen Bedingungen: Wenn sie nicht vorher umgestellt sind, werden alle bestehenden ISO/IEC 27001:2013-Zertifikate am 31.10.2025 ungültig.

Jedes Audit zur Erstzertifizierung und Rezertifizierung, das ab dem 01.05.2024 beginnt, muss nach der neuen Version ISO/IEC 27001:2022 durchgeführt werden. Startpunkt ist der erste Tag des Audits vor Ort (Audit Stufe 1).

Alle Zertifizierungsentscheidungen zum Übergang einer bestehenden ISO/IEC 27001:2013 Zertifizierung müssen spätestens am 31.10.2025 abgeschlossen sein. Anderenfalls muss eine neue vollständige Erstzertifizierung durchgeführt werden.

Umstellungsaudits müssen eine zusätzliche Auditdauer vor Ort beinhalten. Diese Zusatzdauer ist ein einzelnes Ereignis und gilt ausschließlich für das Umstellungsaudit.

Die Kosten für diese Zusatzzeit werden wir den zertifizierten Kunden in Rechnung stellen.

Die Umstellung kann in Rezertifizierungsaudits, in Überwachungsaudits oder in einem „Audit aus besonderem Anlass“ (Sonderaudits) durchgeführt werden.

Audits entsprechend der neuen Ausgabe der ISO 27001 dürfen nur durch Auditteams durchgeführt werden, die zu den neuen Anforderungen geschult wurden und für den neuen Standard berufen sind.

Maßnahmen der Organisationen, die eine Umstellung ihrer Zertifizierung nach ISO 27001 anstreben

Für jede Organisation ist das Ausmaß der notwendigen Änderungen abhängig von der Reife und Wirksamkeit des aktuellen Informationssicherheitsmanagementsystems (ISMS), von Organisationsstrukturen sowie von Abläufen, Prozessen und Verfahren zu ermitteln. Daher wird dringend empfohlen, eine Einfluss- oder Gap-Analyse durchzuführen, um Auswirkungen auf Ressourcen und Fristen festzustellen.

Einer Organisation, die ein ISMS auf der Basis der ISO/IEC 27001:2013 betreibt, werden folgende Maßnahmen empfohlen:

- Ermittlung organisatorischer Lücken, die behandelt werden müssen, um neue Anforderungen erfüllen zu können.
- Erstellung eines Umstellungsplans.
- Angemessene Schulung und Bewusstseinsbildung aller Parteien, die Einfluss auf die Wirksamkeit der Organisation haben.
- Anpassung des bestehenden ISMS, um die geänderten Anforderungen zu erfüllen und Nachweise über die Wirksamkeit vorzulegen.

Bitte beachten Sie, dass ein vollständiges internes Audit und eine Bewertung des Managementsystems nach der neuen Ausgabe ISO/IEC 27001:2022 im Umstellungsaudit nachgewiesen werden müssen.

Kalkulationsregeln für die Zusatzdauer

In den Umstellungsanforderungen des IAF und der DAkkS ist in Kapitel 4.2 des IAF-Dokuments IAF MD 26:2022 eine Vorschrift zur zusätzlich erforderlichen Auditzeit in Umstellungsaudits enthalten. Wir haben uns dafür entschieden, diesen Ansatz zu übernehmen und bzgl. der vorliegenden Auditart (Single-Site-Audit bzw. Multisite-Audit) zu modifizieren.

Dies führt zu folgendem Ergebnis für den Zusatzaufwand (als Vor-Ort-Zeit):

	SINGLE-SITE-AUDIT	MULTISITE-AUDIT
Umstellung in einem Rezertifizierungsaudit	0,5 Manntage Zusatzaufwand	0,5 Manntage Zusatzaufwand für die Zentrale und 0,125 Manntage Zusatzaufwand pro Standort in der Stichprobe
Umstellung in einem regulären Überwachungsaudit	1 Manntag Zusatzaufwand	1 Manntag Zusatzaufwand für die Zentrale und 0,125 Manntage Zusatzaufwand pro Standort in der Stichprobe
Umstellung in einem Audit aus besonderem Anlass	1 Manntag Zusatzaufwand	1 Manntag Zusatzaufwand für die Zentrale und 0,125 Manntage Zusatzaufwand pro Standort in der Stichprobe

Anmerkung
Falls die Umstellung in einem Audit aus besonderem Anlass durchgeführt wird, dann muss dieses zusätzlich zum Überwachungsaudit mit dem hier beschriebenen Zusatzaufwand kalkuliert werden – das wäre eine aufwändigere Lösung.

Ein vollständiges Audit für eine Erstzertifizierung (Stufe 1 und 2) für ISO/IEC 27001:2022 erfordert keinen Zusatzaufwand für eine Umstellung und kann jedes andere Umstellungsaudit ersetzen.

Unter besonderen Umständen kann es erforderlich sein, diesen Ansatz anzupassen. Falls ein Transfer von einer Zertifizierungsstelle zu einer anderen beabsichtigt ist, muss der Transfer der Zertifizierung gemäß ISO/IEC 27001:2013 vollständig abgeschlossen sein, bevor die Planung eines Umstellungsaudits (wie oben beschrieben) fortgesetzt werden darf.

Nach einer Umstellung in einem Audit aus besonderem Anlass, im Überwachungsaudit oder im Rezertifizierungsaudit wird ein neues Zertifikat ausgestellt. Dieses trägt dasselbe Ablaufdatum wie das vorherige Zertifikat nach ISO/IEC 27001:2013. Eine neue volle dreijährige Zertifizierungsperiode darf nur nach einem Rezertifizierungsaudit gewährt werden.

Zusammenfassung
Um eine erfolgreiche Zertifizierung eines ISMS nach ISO 27001 fortsetzen zu können, ist es notwendig, das System entsprechend dem aktualisierten Standard anzupassen. Das kostet Arbeit, Zeit und Geld – aber es dient der Resilienz gegen unberechtigte Einflüsse.

Wir freuen uns auf die Fortsetzung der Zusammenarbeit mit Ihnen.

Kontakt

Dr. Karsten Grans

TÜV NORD CERT
Am TÜV 1
45307 Essen

T 0800 245-7457
F 0511 9986 69-1900

kgrans@tuev-nord.de
tuev-nord-cert.de

24-0553-03/23