Kundeninformation
„ISO/IEC 27006-1:2024“ – Umstellung

Wichtige Informationen zu Ihren bestehenden ISO 27001 Zertifizierungen!

Sehr geehrter ISO 27001 Zertifizierungskunde,

wie Sie vermutlich bereits gehört haben, ist die ISO 27006 überarbeitet worden und als ISO/IEC 27006-1:2024 im März 2024 erschienen. Dieser Standard legt die Regeln für Audits und Zertifizierungen von Managementsystemen fest, die auf der ISO 27001 basieren.

Das International Accreditation Forum (IAF) hat in dem IAF-Dokument „IAF MD 29 - TRANSITION REQUIREMENTS FOR ISO/IEC 27006-1:2024“ vom 21.05.2024 (IAF_MD_29_27006-1_Transition_21052024.pdf) eine zweijährige Übergangsfrist und einige Übergangsvorkehrungen festgelegt. Das bedeutet, dass nach dem Ablauf der Umstellungsphase am 31.03.2026 jede Zertifizierung nach ISO 27001 ausschließlich auf der neuen Ausgabe der ISO 27006 basieren muss.

Die Deutsche Akkreditierungsstelle (DAkkS) hat am 07.08.2024 Umstellungsregeln in Form der Meldung „DAkkS ermöglicht Umstellung auf Norm ISO/IEC 27006-1:2024“ (DAkkS ermöglicht Umstellung auf Norm ISO/IEC 27006-1:2024 - DAkkS - Deutsche Akkreditierungsstelle) veröffentlicht. Diese bezieht sich im Wesentlichen auf das oben erwähnte IAF-Dokument „IAF MD 29“. Die Information der zertifizierten Kunden über den Übergangsprozess und weitere Einzelheiten ist eine der dort festgelegten Pflichten für die Konformitätsbewertungsstellen.

Anmerkung
Die deutsche Version der ISO/IEC 27006-1:2024, die DIN EN ISO/IEC 27006-1:2024, wurde im August 2024 veröffentlicht – der Inhalt beider Versionen ist äquivalent, und die in diesem Schreiben für die ISO/IEC 27006-1:2024 getroffenen Aussagen gelten analog auch für die deutsche Version.

Zudem gelten die in diesem Schreiben für die ISO/IEC 27001 getroffenen Aussagen analog auch für die deutsche Übersetzung der ISO/IEC 27001, den Standard DIN EN ISO/IEC 27001.

TÜV NORD CERT wird bei der DAkkS einen Antrag auf Erweiterung und Umstellung der Akkreditierung auf die neue Ausgabe ISO/IEC 27006-1:2024 der Norm stellen.

Fortsetzung der ISO 27001 Zertifizierung mit der neuen Ausgabe der ISO 27006

Die neue Normversion ISO/IEC 27006-1:2024 erfordert keine Anpassung Ihres Informationssicherheitsmanagementsystems (ISMS), weil die ISO 27001 selbst von den Überarbeitungen in der ISO/IEC 27006-1:2024 nicht betroffen ist.

Weder die Gültigkeit noch das Ablaufdatum von bestehenden Zertifikaten sind durch die Überarbeitungen in der ISO/IEC 27006-1:2024 berührt.

Im Folgenden noch einige von IAF und DAkkS getroffene Festlegungen für Sie zur Info:

- Audits nach Anforderungen der ISO/IEC 27006-1:2024 dürfen erst dann durchgeführt werden, wenn die Erweiterung und Umstellung der Akkreditierung abgeschlossen ist.
- Sobald die Erweiterung und Umstellung der Akkreditierung auf die ISO/IEC 27006-1:2024 durch die DAkkS vorliegt (Akkreditierungsübergang), muss TÜV NORD CERT jedes Audit zur Erstzertifizierung und Rezertifizierung nach der neuen Version ISO/IEC 27006-1:2024 durchführen.
- Jedes Audit, das nach dem 31.03.2026 beginnt, muss grundsätzlich nach der neuen Version ISO/IEC 27006-1:2024 durchgeführt werden.
- Für die Kunden, die vor dem Datum des Akkreditierungsübergangs zertifiziert wurden, kann TÜV NORD CERT für Überwachungsaudits nach der Akkreditierung für ISO/IEC 27006-1:2024 entweder ISO/IEC 27006:2015 oder ISO/IEC 27006-1:2024 verwenden.
- Da es keine zusätzlichen oder geänderten Anforderungen an Ihr ISMS gibt, wird keine zusätzliche Auditzeit in den Umstellungsaudits erforderlich.

Zertifikate, die nach der Umstellung auf die neue Normversion ISO/IEC 27006-1:2024 erstellt werden, enthalten zur eindeutigen Identifikation einen Verweis auf die dann angewendeten Zertifizierungsregeln aus der ISO/IEC 27006-1:2024.

Wichtigste Änderungen in der neuen Ausgabe der ISO 27006

Überarbeitung der Anforderungen zur Auditzeitberechnung

Neue Konzepte wirken sich auf die Berechnung der Auditzeit aus, insbesondere hinsichtlich der Bestimmung der initialen Anzahl von Personen (vgl. C.2.1 und C.3.4 der ISO/IEC 27006-1:2024) und der Klärung der Berechnung der Auditzeit für Organisationen mit mehreren Standorten (vgl. C.6 der ISO/IEC 27006-1:2024).

Verfeinerung der Anforderungen für Fernaudits („Remote Audits“)

Ein Remote-Audit ist dadurch definiert, dass der Auditor das Audit nicht vor Ort durchführt, sondern digital zugeschaltet ist. Bisher war der Remote-Anteil bei ISMS-Audits auf 30 Prozent der gesamten Vor-Ort-Auditzeit begrenzt. Diese Begrenzung wurde mit der neuen Normversion aufgehoben, und es sind jetzt sogar bis zu 100 Prozent Remote-Anteil möglich.

Die Ermittlung des exakten Anteils erfolgt dabei im Rahmen einer „Risikoanalyse bezüglich des Einsatzes eines Remote Audits für den Kunden“, wobei unterschiedliche Faktoren (verfügbare Infrastruktur, Branche, Auditart, Geltungsbereich, Art des Unternehmens, usw.) in diese Risikoanalyse einfließen (vgl. 9.1.3.3 der ISO/IEC 27006-1:2024).

Die hier genannten Änderungen haben zur Folge, dass sich die im Rahmen der Angebotsphase vom Kunden einzuholenden Informationen etwas umfangreicher gestalten als zuvor.

Zusammenfassung

Um eine erfolgreiche Zertifizierung eines ISMS nach ISO 27001 fortsetzen zu können, ist es nicht notwendig, das System entsprechend dem aktualisierten Standard ISO/IEC 27006-1:2024 anzupassen, auch wenn sich einige Aspekte in den Zertifizierungsprozessen ändern. Es ist außerdem auch keine zusätzliche Auditzeit in den Umstellungsaudits erforderlich.

Wir freuen uns auf die Fortsetzung der Zusammenarbeit mit Ihnen.

Kontakt

Dr. Karsten Grans
TIC Manager ISO 27001

TÜV NORD CERT
Am TÜV 1
45307 Essen

servicecenter-isms@tuev-nord.de
tuev-nord-cert.de

Link zur Website

24-0586-05/25