Informationen zur Umstellung auf ISO/IEC 27001:2022-10

Stand: 18.11.2022

1. Hintergrund

Im Februar 2022 wurde die neue **ISO/IEC 27002:2022-02** (auf Englisch) veröffentlicht.

Am 25. Oktober 2022 wurde die neue **ISO/IEC 27001:2022-10** (auf Englisch) veröffentlicht. Für die Durchführung der Umstellung auf die neue Norm hat das International Accreditation Forum (IAF) die damit verbundenen Anforderungen für Akkreditierungsstellen, Zertifizierungsstellen und die zu prüfenden Organisationen veröffentlicht (IAF MD 26:2022).

Stand heute hat die Deutsche Akkreditierungsstelle GmbH (DAkkS) noch keine Umstellungsanleitung veröffentlicht. Zukünftige Änderungen der unten aufgeführten Angaben können daher nicht ausgeschlossen werden.

2. Änderungen an ISO/IEC 27001:2022-10

Folgende Änderungen wurden an der ISO/IEC 27001:2022-10 im Vergleich zur Vorgängerversion durchgeführt.

- Jedes Kapitel der Norm wurde redaktionell überarbeitet und die Anforderungen teilweise konkretisiert.
- Anhang A verweist auf die Maßnahmen in ISO/IEC 27002:2022-02

Alle Kapitel der ISO 27001 wurden überarbeitet. Die Änderungen sind überwiegend redaktioneller Art. U. a. wurden die Anforderungen an die Erklärung zur Anwendbarkeit konkretisiert und insbesondere Kapitel 9 „Bewertung der Leistung“ neu strukturiert.

Die wesentlichen inhaltlichen Änderungen betreffen jedoch den normativen Anhang A.

Bisher enthielt die ISO/IEC 27001:2013* 114 Maßnahmen in 14 Abschnitten. Die neue ISO/IEC 27001:2022-10 wird entsprechend der ISO/IEC 27002:2022-02 93 Maßnahmen in 4 Abschnitten enthalten. Davon sind 11 neu, 24 wurden aus bestehenden Maßnahmen zusammengeführt und 58 Maßnahmen wurden aktualisiert.

Insbesondere wurde die Maßnahmenstruktur überarbeitet. Die bestehende Themenstruktur wurde aufgelöst.

Die Maßnahmen werden zukünftig den vier Abschnitten „Organisatorische Maßnahmen“, „Personenbezogene Maßnahmen“, „Physische Maßnahmen“ und Technologische Maßnahmen zugeordnet.

Zusätzlich werden alle Maßnahmen mit Attributen versehen (und können frei um Attribute ergänzt werden), um eigene Sichten/Sortierungen zu ermöglichen.

3. Notwendige Tätigkeiten des Kunden zur Umstellung auf ISO/IEC 27001:2022-10

Der Kunde hat **dafür Sorge zu tragen**, dass die **Anforderungen** der ISO/IEC 27001:2022-10 **erfüllt** werden. Das ISMS und die umgesetzten Maßnahmen sind entsprechend zu prüfen. Hierzu sind **mindestens folgende Tätigkeiten** notwendig:

1) Durchführung einer GAP-Analyse
2) Ermittlung der Änderungsnotwendigkeiten am ISMS
3) Aktualisierung der Erklärung zur Anwendbarkeit
4) Aktualisierung des Risikobehandlungsplans (sofern notwendig)
5) Durchführung aller notwendigen Änderungen
6) Zur Verfügungstellung der obigen Informationen an die Zertifizierungsstelle zur Ermittlung des Auditaufwands

4. Umstellungsaudit

4.1. Anforderungen an das Umstellungsaudit

Die Umstellung auf die ISO/IEC 27001:2022-10 ist mithilfe eines Umstellungsaudits durch die UIMCert GmbH zu prüfen.

Das Umstellungsaudit kann erfolgen als:

1) Separates Audit oder
2) In Verbindung mit einer Überwachung oder Rezertifizierung.

Das Umstellungsaudit darf nicht nur aus einer Dokumentationsprüfung bestehen, sondern muss als reguläres Vor-Ort-Audit erfolgen. Die Durchführung als Remote-Audit ist zulässig, sofern die Auditziele auf diese Weise erreicht werden können. Dies ist im Einzelfall zu prüfen.

Das Umstellungsaudit muss mindestens folgende Inhalte umfassen:

1) Prüfung der GAP-Analyse
2) Prüfung der ermittelten Änderungsnotwendigkeiten am ISMS
3) Prüfung der durchgeführten ISMS-Änderungen
4) Prüfung der Erklärung zur Anwendbarkeit
5) Prüfung des Risikobehandlungsplans
6) Überprüfung der neuen oder geänderten Maßnahmen

Auf Basis der Ergebnisse des Umstellungsaudit erfolgt durch die Zertifizierungsstelle die Entscheidung über die Umstellung.

Bei erfolgreicher Umstellung wird ein neues Zertifikat ausgestellt. Die Umstellung hat keine Auswirkung auf die Zertifikatslaufzeit.

4.2. Aufwand

Der Mindestaufwand für die Prüfung der Umstellung wird im IAF-Dokument festgelegt und beträgt 0,5 Audittage.

Der tatsächliche Aufwand hängt jedoch von der Komplexität des ISMS und den tatsächlichen Änderungen ab.

Der tatsächlich notwendige Aufwand wird von der UIMCert auf Basis der eingereichten Unterlagen aus 4.1 ermittelt. Je ausführlicher und genauer die Unterlagen sind, desto genauer kann die notwendige Auditzeit ermittelt werden.

Hinweis: Für Dritte unzureichend nachvollziehbare Dokumente führen zu einem planmäßig erhöhten Auditaufwand.

5. Fristen

Die Umstellung der Zertifizierung auf die ISO/IEC 27001:2022-10 muss innerhalb eines vorgegeben Zeitrahmens erfolgen.

5.1. Erstzertifizierung

Erstzertifizierungen sind nach 12 Monaten nach Erscheinen der Norm (also ab 25. Oktober 2023) ausschließlich nach ISO/IEC 27001:2022-10 möglich.

5.2. Bestehende Zertifizierung

Die Umstellung der Zertifizierung auf ISO/IEC 27001:2022-10 muss spätestens 36 Monate nach Erscheinen der Norm (also bis 24. Oktober 2025) abgeschlossen sein. Der individuelle Umstellungszeitpunkt wird als Bestandteil eines Umstellungsauditprogramm für jeden Kunden separat festgelegt.

6. Konsequenzen

Mit Ablauf der Übergangsfrist laufen alle Zertifizierungen nach ISO/IEC 27001:2013* aus oder sind zu entziehen.

Erfolgt eine Umstellung (abgeschlossene Umstellung) nicht spätestens bis zum 24. Oktober 2025 erlischt die Zertifizierung.

7. Sonstiges

Das Dokument IAF MD 26:2022 ist hier verfügbar:

https://iaf.nu/iaf_system/uploads/documents/IAF_MD_26_Transition_requirements_for_ISOIEC_27001-2022_09082022.pdf

*Die ISO/IEC 27001:2013 einschließlich der beiden Korrekturen Cor 1:2014 und Cor 2:2015 entspricht der deutschen **DIN EN ISO/IEC 27001:2017**.