Informationsblatt zur Umstellung auf die ISO/IEC 27001:2022 für die Kunden der ÖHMI EuroCert GmbH

Cybersecurity, Cloud-Sicherheit und mehr Datenschutz: seit Oktober 2022 präsentiert sich die ISO-Familie mit der jüngsten Version der internationalen Norm ISO/IEC 27001 „Information security, cybersecurity and privacy protection - Information security management systems - Requirements“

Harmonized Structure (HS) vs. High Level Structure (HLS) und die ISO/IEC 27001:2022:

Die bisherige High Level Structure (HLS) wird durch die sogenannte Harmonized Structure (HS) ersetzt und die ISO/IEC 27001 gehörten zu den ersten ISO-Normen, die bereits an die HS angepasst wurden. Als würdiger Nachfolger der HLS bildet die HS einen einheitlichen Grundgerüst für alle ISO-Normen. Somit bietet sie zugleich eine entsprechende Vorlage nicht nur für die Ausarbeitung von neuen, sondern auch für zukünftige Überarbeitung von bereits bestehenden ISO-Normen.

Das ISO-Tandem 27001-27002:

Die Auflistung mit den möglichen Security Controls bzw. Sicherheitsmaßnahmen im normativen Anhang A der neuen ISO/IEC 27001:2022 wurde aus dem bereits im Februar 2022 veröffentlichten und rundum aktualisierten Leitfaden ISO/IEC 27002:2022 übernommen. Die überarbeitete ISO/IEC 27002 enthält eine vereinfachte Taxonomie und up-to-date Sicherheitsmaßnahmen und dient nach wie vor als Umsetzungsanleitung für die ISO/IEC 27001. Somit erhalten die beiden ISO-Normen ihr Image als erfolgreiches Norm-Tandem aufrecht und halten zugleich Schritt mit dem aktuellen Stand der Technik.

Die NEUE ISO 27001: Prozessbezug/ Prozessorientierung als Schwerpunkt

Die Anpassung an die HS rückt die Anforderung an den Prozessbezug entsprechend sehr stark in den Fokus eines wirksamen Informationssicherheitsmanagementsystem. Klar definierte Prozesse, deren Wechselwirkung sowie die Erarbeitung zielführender Kriterien für die Steuerung der Prozesse bilden die Grundlagen für ein wirksames Managementsystem.

Eine weitere wesentliche Ableitung aus der HS präsentiert sich mit dem neuen **Abschnitt 6.3**. Dieser bringt mit sich die Anforderung, eine geplante Umsetzung bei ISMS-Änderungen durchzuführen.

ÖHMI

EuroCert®

Ein Unternehmen der ÖHMI Holding

Zertifizierungen nach
- **ISO 9001**
- **ISO 14001**
- **ISO 45001**
- **ISO 27001**
- **ISO 50001**
- **IT-Sicherheitskatalog**
- **EfbV**
- **GMP+ / REDcert**
- **AZAV**

Akkreditierte Zertifizierungsstelle gemäß Urkunden-Nr.:
D-ZM-16015-01-00
D-ZE -16015-01-00

ÖHMI EuroCert® GmbH

Tel. +49 391 8189-141
Fax +49 391 8189-140

E-mail:
oehmi@oehmi-cert.de
www.oehmi-cert.de

Hausanschrift:
Berliner Chaussee 66
D-39114 Magdeburg

Büro Berlin:
Kurfürstendamm 21
D-10719 Berlin

Geschäftsführer:
Dipl.-Ing. Olaf Unger

Registergericht
Amtsgericht Stendal
HRB 108352

Deutsche Bank
BLZ 810 700 00
Konto 14 24 837
IBAN:
DE86810700000142483700
BIC: DEUTDE8MXXX

Stadtsparkasse Magdeburg
BLZ 810 532 72
Konto 302 105 39
IBAN:
DE24810532720030210539
BIC: NOLADE21MDG

Ust.-Id Nr.: DE 351990608
St.-Nr.: 102/108/01370

Inhaltliche Änderungen in den einzelnen Abschnitten der ISO 27001:2022

Die Abschnitte 4, 6 und 8 der ISO 27001 enthalten die wesentlichen inhaltlichen Änderungen. Darüber hinaus gibt es in den Abschnitten 5.3, 6.1.3, 7.4, 9.2, 10.1 einige etwas geringfügigeren Präzisierungen, Anpassungen sowie Klarstellungen.

Die NEUE ISO 27001: Wesentliche inhaltlichen Änderungen

1. **Abschnitt 4.4: Information security management system / Informationssicherheitsmanagementsystem**

Das Schwerpunktthema **Kontext der Organisation** wird um die Anforderung, erforderliche und nachvollziehbare **Prozesse sowie deren Wechselwirkungen** im Rahmen des ISMS zu bestimmen, ergänzt. Mit der dieser ausdrücklichen Anforderung an die Prozessorientierung wird die ISO 27001 in Einklang mit dem sogenannten Best - Practice -Ansatz anderer bestehenden Managementsysteme gemäß HS gebracht. Um diese Prozesse werden dann Die Maßnahmen/ Controls zur Informationssicherheit aus Anhang A werden dann um diese Prozesse entsprechend angepasst und ausgestaltet.

2. **Abschnitt 6.3: Planning of changes/ Planung von Änderungen**

Hierzu besteht die Anforderung, dass eine geplante Umsetzung aller ISMS relevanten Änderungen zu erfolgen hat. Somit sind die ISMS-Verantwortlichen in der Pflicht den ISMS-bezogene Veränderungsprozess auch entsprechend zu beherrschen.

3. **Abschnitt 8.1: Operational planning and control/ Betriebliche Planung und Steuerung**

Der Abschnitt zur **betrieblichen Planung und Steuerung** untermauert den der Prozessorientierung beigemessenen hohen Stellenwert. Alle ISMS affinen Unternehmen haben geeignete Prozesse zu realisieren, so dass Maßnahmen zur Bewältigung der Informationssicherheitsrisiken umgesetzt werden können. **NEU** dabei ist Anforderung zur Festlegung von **Prozesskriterien** für die Prozesssteuerung.

Die NEUE ISO 27001: Abschnitte mit geringfügigen Änderungen

1. **Abschnitt 5.3: Organisation Organizational roles, responsibilities and authorities / Rollen, Verantwortlichkeiten und Befugnisse**

Die Verantwortlichkeiten und Befugnisse für Rollen mit Bezug zur Informationssicherheit sind demnach **innerhalb der Organisation** bekannt zu machen.

2. **Abschnitt 6.1.3: Information security risk treatment / Informationssicherheitsrisikobehandlung**

Hiermit wird eine größere Flexibilität bei der Auswahl, Gestaltung und Erweiterung der Referenzmaßnahmen aus Anhang A (Liste **möglicher /possible** Informationssicherheitsmaßnahmen/ **controls**) durch Norm eingeräumt. Dadurch zeigt die neue ISO 27001 - Version zudem auf, dass der Managementsystemrahmen für organisationsspezifische Maßnahmensätze geöffnet ist.

3. **Abschnitt 7.4: Communication/ Kommunikation**

Die neue ISO 27001 regelt in diesem Abschnitt weiterhin die Notwendigkeit für interne und externe Kommunikation im Rahmen des ISMS mit entsprechenden Festlegungen zum Worüber, Wann mit Wem und Wer. Ergänzend dazu kommt noch das **WIE** (im Sinne von **wie** erfolgt die der Kommunikation) als willkommene und praktikable Vereinfachung im Vergleich zu früheren Anforderungen.

4. **Abschnitt 9.2: Internal Audit/ Internes Audit und Abschnitt 9.3 Management review/ Managementbewertung**

Die zwei Abschnitte wurden an die Harmonized Structure der ISO 27001:2022 angepasst und entsprechende neu untergliedert.

5. **Abschnitt 10.1: Continual improvement/ Fortlaufende Verbesserung**

Die **prospektive** fortlaufende Verbesserung in diesem Abschnitt wird jetzt dem **retrospektiven** Umgang mit Nichtkonformitäten und Korrekturmaßnahmen im **Abschnitt 10.2 (Nichtkonformität und Korrekturmaßnahmen (Nonconformity and corrective action))**, vorangestellt. Keine weiteren inhaltliche Änderungen wurden dabei durchgeführt. Durch diese Reihenfolge-Änderung wird die Bedeutung des Prozesses zur fortlaufenden Verbesserung nochmals hervorgehoben und eindeutig unterstreicht.

Die NEUE ISO 27001: Wesentliche Änderungen im Anhang A der ISO 27001:2022

Im Gegensatz zu ihren Vorgängerinnen umfasst die neue ISO 27001 statt 114 nur noch 93 Sicherheitsmaßnahmen/ controls. Diese sind zudem in 4 Hauptkategorien untergliedert. Diese vier Abschnitte enthalten die Themenbereiche **Organisatorische Maßnahmen** mit 37 zugeteilten Sicherheitsmaßnahmen, **Personenbezogene Maßnahmen** mit 8 zugeteilten Sicherheitsmaßnahmen, **Physische Maßnahmen** mit 14 zugeteilten Sicherheitsmaßnahmen sowie den Themenbereich **Technische Maßnahmen** mit 34 zugeteilten Sicherheitsmaßnahmen

Die neuen Sicherheitsmaßnahmen im Anhang A der ISO 27001:2022

Neben einiger Streichungen und Zusammenfassungen von Sicherheitsmaßnahmen im Anhang A der neuen ISO 27001, werden durch die Norm auch **elf neue Sicherheitsmaßnahmen** vorgegeben. Diese umfassen:

A.5.7: Threat Intelligence / Bedrohungsintelligenz (NEUE Organisatorische Maßnahme)
- Bestimmung von Schutzmaßnahmen aufgrund von gesammelten und entsprechend analysierten Bedrohungsinformationen

A.5.23: Information Security for use of Cloud Services / Nutzung von Cloud-Diensten (NEUE Organisatorische Maßnahme)
Diese Maßnahme zielt auf die Sicherstellung von einem sicheren Prozess für Onboarding, Nutzung, Verwaltung sowie Ausstieg bei Cloud Anbietern ab.

A.5.30: ICT readiness für Business Continuity / IKT-Bereitschaft für Business Continuity (NEUE Organisatorische Maßnahme)
Diese Maßnahme umfasst Anforderungen an Wiederherstellungsmaßnahmen und setzt die technischen Maßnahmen als neuen Schwerpunkt.

A.7.4: Physical Security Monitoring / Physische Sicherheitsüberwachung (NEUE Physische Maßnahme)
- Abschreckung und Schutz vor unbefugtem Zugriff
- Einrichtung von Überwachungsmaßnahmen, Einbruchsalarme etc.

A.8.9: Configuration Management / Konfigurationsmanagement (NEUE Technologische Maßnahme)
- korrekte Einstellung von Sicherheitsmaßnahmen sowie Sicherung der Konfiguration

A.8.12: Data Leakage Prevention / Verhinderung von Datenlecks (NEUE Technologische Maßnahme)
- Überwachung und Erkennung von Datenverlust, Offenlegung, Datenleck

A.8.10: Information Deletion / Löschung von Informationen (NEUE Technologische Maßnahme)
- Anforderungen zur Datenspeicherung in Verbindung mit DSGVO sowie GDPR.

A.8.11: Data Masking / Datenmaskierung (NEUE Technologische Maßnahme)
- Beschränkung, Anonymisierung und Pseudonymisierung von Daten

A.8.12: Monitoring activities / Überwachung von Aktivitäten (NEUE Technologische Maßnahme)
- proaktive Überwachung von abweichenden Aktivitäten

A.8.23: Web Filtering / Webfilterung (NEUE Technologische Maßnahme)
- Ausfilterung von gefährlichen Webseiten

A.8.28: Secure Coding / Sicheres Coding (NEUE Technologische Maßnahme)
- Sichere Kodierung ohne Schwachstellen oder Anfälligkeiten für Angriffe

WICHTIGE Informationen zur Umstellung auf die neue Revision der ISO 27001:

Hiermit möchten wir Ihnen einigen wichtigen Informationen in Zusammenhang mit der Umstellung auf die neue ISO/IEC 27001:2022 anbieten:

In einem ersten Schritt werden (voraussichtlich ab dem 01.05.2023) durch die DAkkS Umstellungsbegutachtungen für den Geltungsbereich ISO/IEC 27001:2022 für alle akkreditierten Zertifizierungsstellen durchgeführt. Die Umstellung der Akkreditierungen sollte laut dem Umstellungsplan von DAkkS bis zum 31.10.2023 abgeschlossen werden. So dass es voraussichtlich ab dem 01.11.2023 mit der Auditierung der Zertifikatsinhaber zur Umstellung auf die ISO/IEC 27001:2022 durch die Zertifizierungsstelle begonnen werden kann.

Übergangsfrist
Die Übergangsfrist für die neue ISO/IEC 27001:2022 beträgt 3 Jahre und endet somit am 31.10.2025. Somit müssen alle bestehenden Zertifikate nach DIN EN ISO/ IEC 27001:2017 bis zum 31. Oktober 2025 umgestellt worden sein, da sie ansonsten ihre Gültigkeit nach diesem Datum verlieren.

Zertifikate, die im Rahmen einer Erst- oder Re-Zertifizierung nach DIN EN ISO/ IEC 27001:2017 nach Veröffentlichung der neuen Revision ausgestellt werden, erhalten entsprechend eine verkürzte Gültigkeit bis zum 31.10.2025.

Vorgehensweise zur Umstellung:

- die Umstellung auf die ISO/IEC 27001:2022 kann in Verbindung mit einem Überwachungsaudit, Re-Zertifizierungsaudit oder durch ein separates Sonderaudit durchgeführt werden.

- die Umstellung auf die neue Revision der ISO 27001 umfasst nicht nur eine Dokumentensichtung. Es sollen insbesondere die technologischen Sicherheitsmaßnahmen/ Controls auditiert werden

- die Umstellung muss mindestens Folgendes umfassen, ist aber nicht darauf beschränkt (bzw. Sie müssten im Vorfeld des Umstellungs-/Übergangsaudits mindestens Folgendes vorbereitet/erarbeitet haben):
    - eine GAP-Analyse von ISO/IEC 27001:2022 sowie die Notwendigkeit von Änderungen an Ihrem ISMS
    - die Aktualisierung der Erklärung zur Anwendbarkeit/ Statement of Applicability (SoA)
    - die Aktualisierung des Risikobehandlungsplans

- die Implementierung und Wirksamkeit der neuen oder geänderten Sicherheitsmaßnahmen/ Controls, die von Ihnen gewählt wurden.

Zusätzlicher Aufwand für die Umstellung auf die ISO/IEC 27001:2022

Die Umstellungsregeln sehen bei der Umstellung auf die neue Revision im Rahmen einer Re-Zertifizierung vor, eine Vor-Ort-Aufwanderhöhung um 10%, jedoch mindestens 0,5 PT (=Personentage) vor Ort. Wenn die Umstellung im Rahmen einer Überwachung stattfindet, dann beträgt die Vor-Ort-Aufwanderhöhung 20%, jedoch mindestens 0,5 PT (=Personentage) vor Ort.

Vor diesem Hintergrund und unter Berücksichtigung Ihren Fortschritt bei der Umsetzung der Umstellungsmaßnahmen, wäre es wichtig, dass wir gemeinsam einen geeigneten Umstellungszeitpunkt suchen und finden. Setzen Sie sich zeitnah mit uns in Verbindung. Wir stehen Ihnen unterstützend zur Seite.

Ihr ÖHMI EuroCert – Team