TeleTrusT - interner Workshop

27.06.2022, Berlin

ISMS 3.0: Was bringt die neue ISO/IEC 27001?

Axel von der Ohe, AURISCON GmbH, Berlin

Unternehmen und Referent

- Axel von der Ohe
- tätig als Berater im Bereich Informationssicherheitsmanagement für AURISCON GmbH, Berlin
- davor Geschäftsführer eines IT-Dienstleisters
- Die AURISCON GmbH
  - bietet Beratungs- und Prüfungsdienstleistungen für Betreiber von Informations- und Managementsystemen
  - unterstützt beim Informationssicherheitsmanagement und Notfallmanagement
  - bereitet auf Zertifizierungen gemäß ISO/IEC 27001 vor.

www.auriscon.info / Geschäftsführer: Dr. Rainer Rumpel

Mitglied bei

STANDARDS

POPULAR STANDARDS

Our greatest hits: the most popular ISO Standards, including our management system standards.

Here you can discover some of the best-known and most widely-used standards, as well as those that address recently emerged challenges affecting us all.

MANAGEMENT SYSTEM STANDARDS

Providing a model to follow when setting up and operating a management system, find out more about how MSS work and where they can be applied.

ISO 9000 FAMILY — QUALITY MANAGEMENT

The ISO 9000 family is the world's best-known quality management standard for companies and organizations of any size.

ISO/IEC 27001 — INFORMATION SECURITY MANAGEMENT

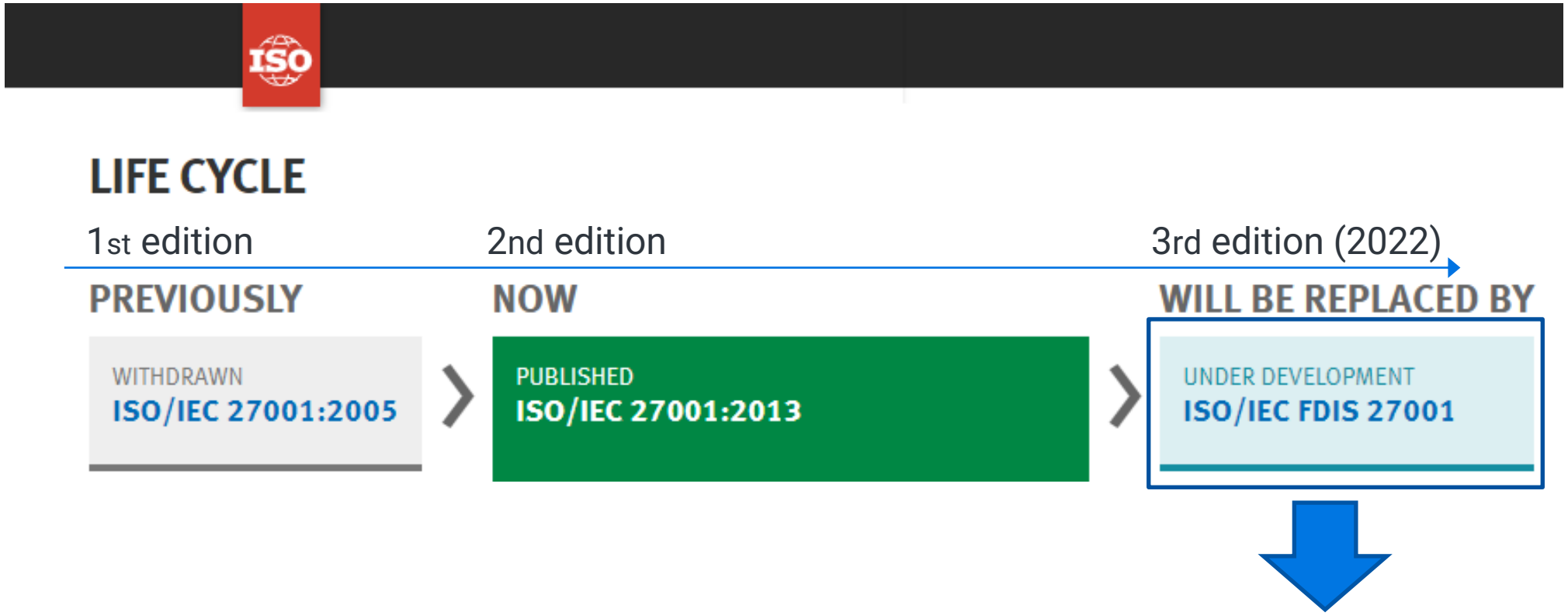
Providing security for any kind of digital information, the ISO/IEC 27000 family of standards is designed for any size of organization.

ISO 45000 FAMILY — OCCUPATIONAL HEALTH AND SAFETY

Reduce workplace risks and make sure that everyone gets home safely with ISO 45001.

Entwicklungsgeschichte

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Stage	Version	Description	Started	Status
50.00	1	Final text received or FDIS registered for formal approval	2022-06-09	Current

FDIS: Final Draft International Standard

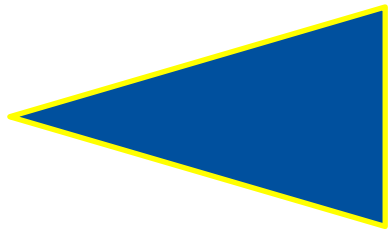
ISO/IEC 27001 - die wichtigste Änderung

Anpassung von Anhang A an die in der **dritten Ausgabe von ISO/IEC 27002 (2022)** definierten Steuerungsmaßnahmen

ISO/IEC 27001

Hauptteil

Anhang A



ISO/IEC 27002:2022 — Information security controls

- Foreword
- Introduction
- 1 Scope
- 2 Normative references
- ▸ 3 Terms, definitions and abbreviated terms
- ▸ 4 Structure of this document
- ▾ 5 Organizational controls
  - 5.1 Policies for information security
  - 5.2 Information security roles and responsibilities
  - 5.3 Segregation of duties
  - . . .
- ▾ 6 People controls
  - 6.1 Screening
  - 6.2 Terms and conditions of employment
  - 6.3 Information security awareness, education and training
  - . . .
- ▸ 7 Physical controls
- ▸ 8 Technological controls

93 controls

Die neue ISO/IEC 27001 (3rd ed.) - Auswirkungen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Neues Set an Security Controls
  - zwar inhaltlich ähnlich zu 2nd ed., aber
  - neu organisiert und
  - aktualisiert (auch neue Maßnahmen/Themen), z.B.

Configuration management (8.9)	
Stellt sicher, dass die Dienste korrekt mit den erforderlichen Sicherheitseinstellungen betrieben werden und die Konfiguration nicht durch unautorisierte oder fehlerhafte Änderungen kompromittiert wird.	

- **Die Anwendbarkeitserklärung (SoA) muss entsprechend der neuen Struktur von Anhang A (komplett) überarbeitet werden.**
- **Viele Maßnahmen müssen überarbeitet bzw. neu angewendet werden.**

Empfehlungen

- Regelmäßig bei iso.org prüfen, ob 3rd ed. publiziert ist
- ISO/IEC 27002:2022 kaufen
- In Kontakt bleiben mit der zuständigen Zertifizierungsstelle (falls zertifiziert)

- Auf Publikationen der DAkkS* achten (in der Regel gibt es mindestens 2 Jahre Übergangszeit in solchen Fällen)
- Gap-Analyse für die eigene Organisation durchführen

*https://www.dakks.de/de/akkreditierte-stellen-suche.html

Vielen Dank für Ihre Aufmerksamkeit!

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Axel von der Ohe

AURISCON GmbH
Kiplingweg 20, 14055 Berlin
Reg. Nr. im Handelsregister: HRB 132545 B (Berlin-Charlottenburg)
Tel.: +49 (0)30 25560986
E-Mail: kontakt@auriscon.de
Web: www.auriscon.de