secuvera

Cybersicherheit. Nachhaltig.

Die neue ISO 27001: Was kommt auf uns zu?

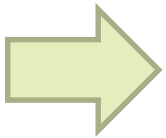
Björn Lemberg
Ann-Kathrin Udvary

verinice.XP

Göttingen, 22.02.2023

Motivation

- Überblick zur Neufassung der ISO 27001
  - Hintergrund
  - Aufgaben
  - Rahmenbedingungen



Morgen mehr im Vortrag: „ISO27001:2022 ISO27005:2022: The next Generation of ISMS“

Agenda

- **Über uns**
- Entwicklung der 27001
- Neues in der ISO 27001:2022
- Zeitlicher Ablauf
- Zusammenfassung & Fazit

Über uns

- Gegründet 1. Juli 1982
- Gäufelden bei Stuttgart
- IT-Sicherheit seit 1988
- Heute reiner IT-Sicherheitsdienstleister
- Aktuell ca. 30 Mitarbeitende
- Inhabergeführt
- Herstellerunabhängig

- BSI-zert. IT-Sicherheitsdienstleister
- Geschäftsbereiche
  - Sicherheitsberatung (BSI IT-Grundschutz / ISO 27001)
  - Penetrationstests / Webanwendungsprüfungen
  - BSI-Prüfstelle für Common Criteria

Ann-Kathrin Udvary

- Seit 2019 bei secuvera
- Leitende Cybersicherheitsberaterin
- Schwerpunkte:
  - ISMS nach ISO 27001 & IT-Grundschutz
  - Datenschutz nach EU DS-GVO und ISO 27701
  - BCM nach BSI-Standard 200-4 und ISO 22301
- Zertifizierungen
  - ISO 27001 Auditorin

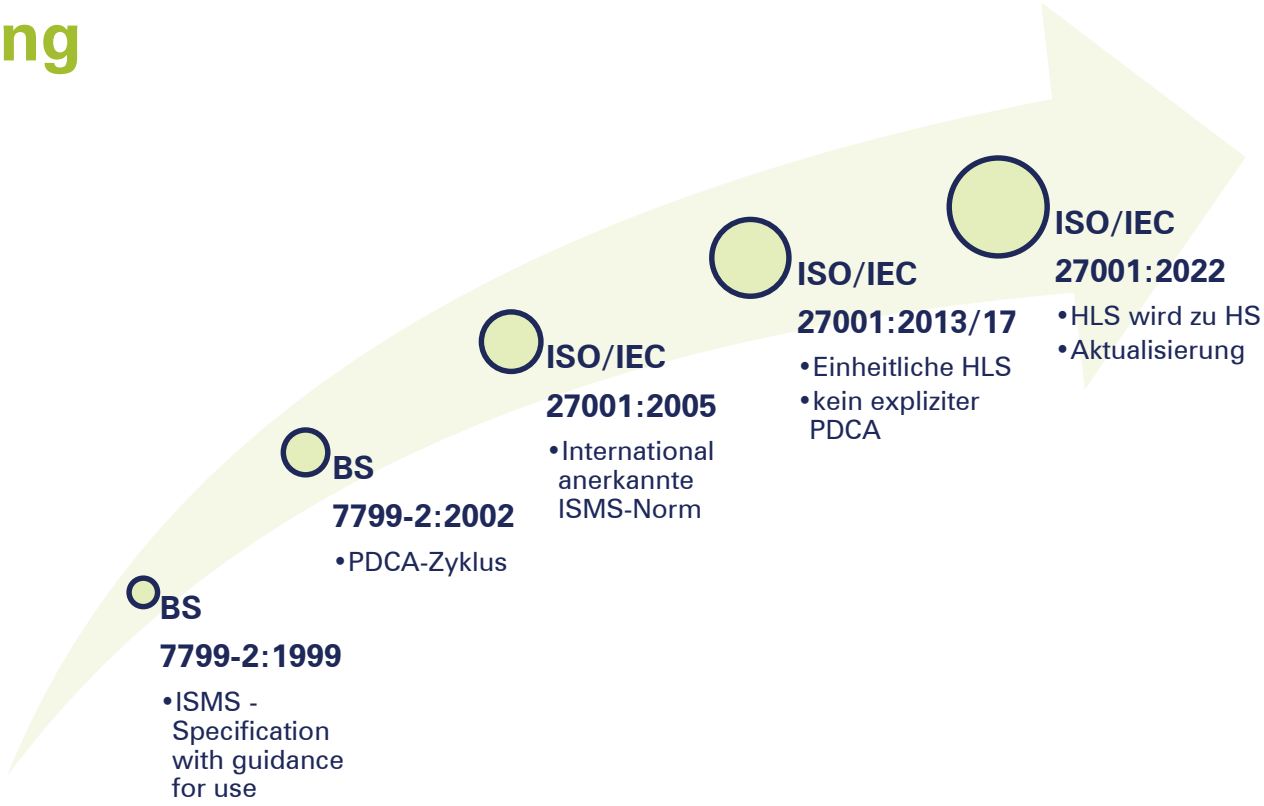
Björn Lemberg

- Seit 2012 bei secuvera
- Leitender Cybersicherheitsberater
- Verantwortungsbereiche
  - ISO 2700x
  - VDA-ISA
  - Datenschutz
- CISSP, 27001 Auditor, DSB

Agenda

- ✓ Über uns
- **Entwicklung der 27001**
- Neues in der ISO 27001:2022
- Zeitlicher Ablauf
- Zusammenfassung & Fazit

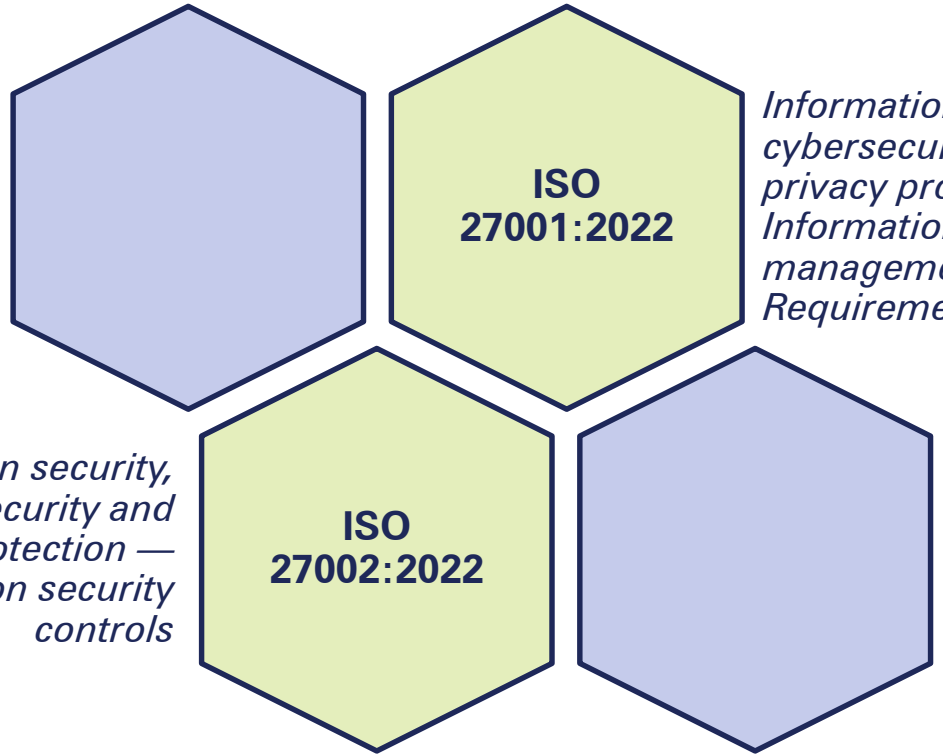
Entwicklung



Agenda

- ✓ Über uns
- ✓ Entwicklung der 27001
- **Neues in der ISO 27001:2022**
- Zeitlicher Ablauf
- Zusammenfassung & Fazit

Überblick


ISO
27001:2022
Information security, cybersecurity and privacy protection – Information security management systems - Requirements
Information security, cybersecurity and privacy protection — Information security controls
ISO
27002:2022

Veränderungen im Management

- Kleine Anpassungen
  - Neue Unterkapitel
  - Angepasste Unterkapitel
  - Anpassungen in der Beschreibung
  - Erklärung zur Anwendbarkeit (SoA)

➢ Kaum wesentliche Änderungen im Managementsystem

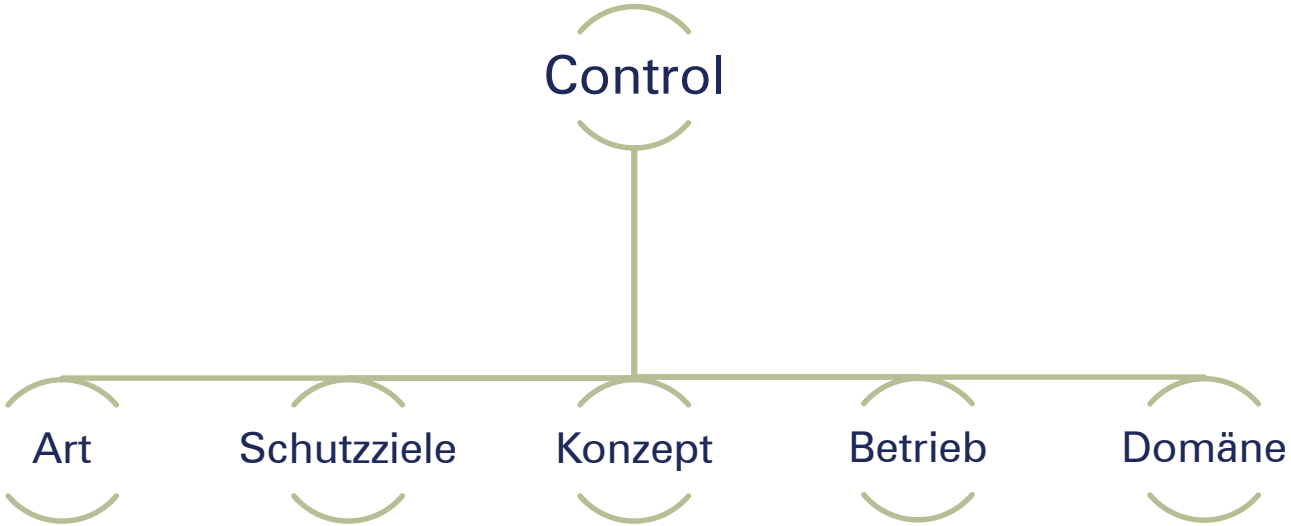
Harmonized Structure

Veränderungen im Anhang A & ISO 27002

- Neue Struktur inkl. Themenbereichen
  - Vollständig neue Controls
  - Alte Controls neuen Themenbereiche zugeordnet
  - Keine Controls inhaltlich entfallen
  - Neue Ebenen
- Neue Attribute
  - Werden den jeweiligen Controls zugeordnet

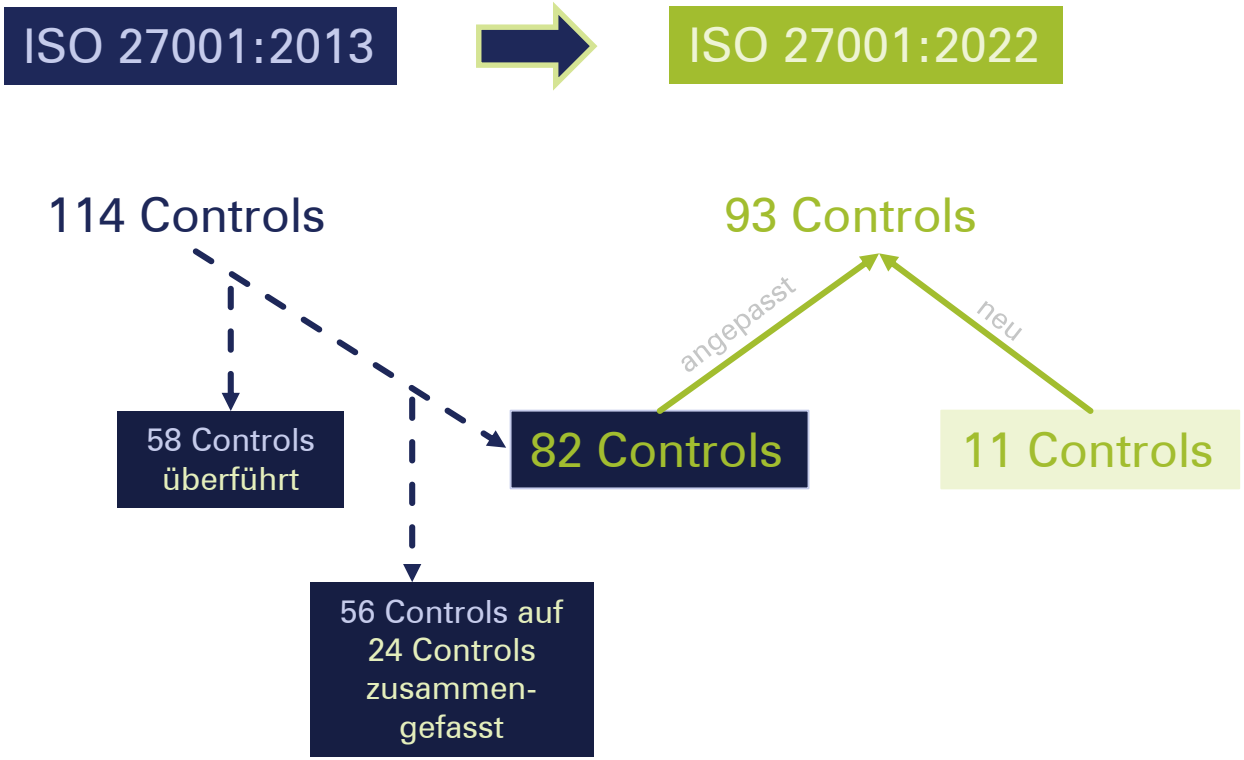
Neue Struktur

Neue Attribute 27002



Intention verdeutlichen

Übersicht Controls



Mapping

- Anhang der ISO 27002
  - Zuordnung der Attribute zu den Controls
  - Zuordnung der Controls
    - Neu (2022) ⇨ Alt (2013)
    - Alt (2013) ⇨ Neu (2022)

Bedrohungsanalyse

- Informationen zu Bedrohungen
  - Bekanntes & Potentielles
  - Sammeln, Analysieren & Reagieren
- Angemessene Maßnahmen zur Abhilfe ergreifen
  - Auswirkungen verringern

Informationssicherheit bei der Nutzung von Cloud-Diensten

- Steuerung der Beziehung entlang Lebenszyklus
  - Anforderungen & Auswahl
  - Verträge
  - Überwachung
  - Exit-Strategie
- Sonderfall der Lieferantenbeziehung
- Cloud-Strategie festlegen

IKT-Bereitschaft für Notfallmanagement

- Basierend auf den Zielen zum Notfallmanagement & IKT Anforderungen
  - Planen
  - Umsetzen
  - Überprüfen
  - Testen
- Sicherstellen der Verfügbarkeit von Informationen und Werten
- Notfallpläne & Szenarien

Überwachung der physischen Sicherheit

- Gefahrenmeldeanlage
- Videoüberwachung
- Wach- und Schließdienste
- Melde- / Alarmierungsketten beachten

Konfigurationssteuerung

- Sicherheitskonfiguration in Bezug auf
  - Hardware, Software
  - Dienstleistungen
  - Netzwerke
- Entlang des Lebenszyklus
- Dokumentation
- Bezug zum Änderungsmanagement

Löschung von Informationen

- „logische“ Ergänzung zur Vernichtung
- Löschung wenn Speicherung nicht mehr notwendig
- wichtig im Datenschutz
- Aufbewahrungsfristen identifizieren
- DIN 66398 stellt Löschkonzept vor

Datenmaskierung

- Übereinstimmung mit übergreifenden Regelungen
  - Schnittstellen beachten
- Beachtung geltender Gesetzgebung
- Minimierung sensibler Daten
- Anonymisierung & Pseudonymisierung
- DSB einbeziehen

Verhinderung von Datendiebstahl

- Schutz für sensitive Daten
- Bedarf auch in Klassifizierung berücksichtigen
- Angemessenheit auch hinsichtlich Datenschutz

Überwachung von Aktivitäten

- Überwachung von Auffälligkeiten
  - Netzwerke
  - Systeme
  - Anwendungen
- Erkennung & Bewertung potentieller Vorfälle
- Ergreifen von Maßnahmen
- Tool-Unterstützung

Filtern von Netzdiensten

- Kontrolle des Zugangs zu externen Inhalten
- Black-/White-Listing
  - verdächtige Server
  - illegale Inhalte
- Sperren unerwünschter Funktionen
  - Upload-/Download-Funktionen
  - Aktive Inhalte
- Anforderungen & Fähigkeiten berücksichtigen

Sichere Programmierung

- Grundsätze anwenden
- Senkung von potentiellen Sicherheitsrisiken in der Software
- Entwickler:innen einbeziehen
  - Erweiterte Schulungen
- Entlang des Lebenszyklus (Vor, Während und Nach der Programmierung)

Agenda

- ✓ Über uns
- ✓ Entwicklung der 27001
- ✓ Neues in der ISO 27001:2022
- **Zeitlicher Ablauf**
- Zusammenfassung & Fazit

Zeitlicher Ablauf

- Neu-Zertifizierungen ab 10.2023
- Umstellungen bis 10.2025
- DAkkS-Akkreditierungen
- Umstellung mit Auditierenden planen!

Agenda

- ✓ Über uns
- ✓ Entwicklung der 27001
- ✓ Neues in der ISO 27001:2022
- ✓ Zeitlicher Ablauf
- ▪ **Zusammenfassung & Fazit**

Zusammen-fassung

- Umstellung
  - Managementsystem
    - Vorgaben ergänzen
  - Risikobehandlung & Controls
    - Neue Controls im Fokus
    - Entlang SoA / Mapping-Tabellen
    - Im Rahmen von Reviews
      Wirksamkeitsprüfungen
      Verbesserungen

Fazit

- Änderungen überschaubar
  - Feinschliff im MS
  - Controls ergänzt
  - Datenschutz-Sicht erweitert
- Umstellung frühzeitig planen und in Zyklus einbeziehen

Richtiges bleibt richtig,
möchte aber erweitert werden

secuvera

Cybersicherheit. Nachhaltig.

Vielen Dank für Ihre Aufmerksamkeit!

Bei Fragen und Anregungen sprechen Sie uns gerne an

Ihre Ansprechpartner:innen:

Björn Lemberg
blemberg@secuvera.de
+49 7032 9758 19

Ann-Kathrin Udvary
audvary@secuvera.de
+49 7032 9758 48