ISO 27001:2022 – Neue Themen, neuer Aufbau

Know-how to go – ISO 27001 Novellierung

HiSolutions AG

Julia Vahldieck

Julia Vahldieck

Managing Consultant

Fachliche Schwerpunkte

- Umsetzung von Anforderungen aus ISO 27001, IT-Grundschutz, BSI-Standard 200-4 und ISO 22301
- Definition, Implementierung und Weiterentwicklung von vollumfänglichen Information Security, Business Continuity & Krisenmanagementsystemen
- Beratung zu den Themen Notfall- und Krisenmanagement (Prävention, Reaktion, Kommunikation, Übungen)

Qualifikationen

- Zertifizierter Lead Auditor ISO 27001
- Zertifizierter Lead Auditor ISO 22301
- Zertifizierte Datenschutzbeauftragte (TÜV SÜD)
- Prüfverfahrens-Kompetenz für § 8a BSIG
- BSI IT-Grundschutz-Praktiker

Agenda

1. Relevante Key Facts
2. Vorstellung der neuen Controls
3. Fazit für bestehende Managementsysteme nach ISO 27001

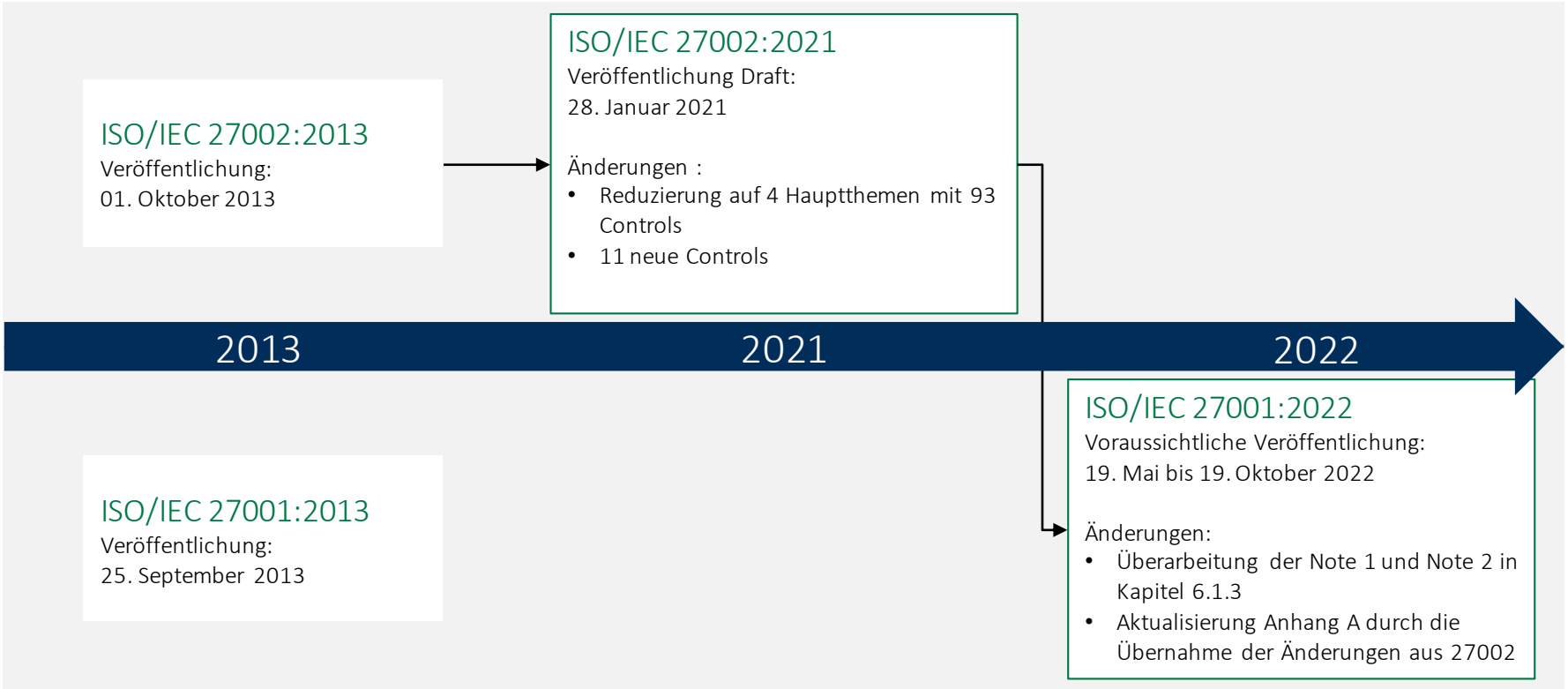
1. Relevante Key Facts

Aufgepasst!

In der ISO-Welt gibt es Neuigkeiten:

Neben der Neufassung der ISO/IEC 27002:2021 gibt es ab 2022 eine Änderung der ISO/IEC 27001!

Die neue ISO/IEC 27002:2021 erfordert die Anpassung der ISO/IEC 27001



Zusammenspiel der ISO 27001 und der ISO 27002:2021

ISO 27001 Kap. 4 bis 10: *Anforderungen an das ISMS*

Annex A: A.5 bis A.8: 93 Normative Controls

ISO 27002 Kap. 5 bis 8: *Leitfäden für die Umsetzung der Controls*

Annex A: Übersicht der Attribute aller Maßnahmen

Annex B: Mapping der bestehenden und neuen Controls

ISO 27001 ist zeritifizierungsfähig (*shall*), ISO 27002 ist es nicht (*should*)

Neue und überarbeitete Controls, um die Themenvielfalt zu erhalten und den Schutzbereich zu erweitern

Keine einzige Maßnahme wurde unverändert aus der bisherigen Norm übernommen:

Ein Control entfällt

Der FDIS listet 11 „neue“ Controls

Die anderen Controls wurden neu formuliert

56 Controls wurden auf 24 komprimiert

Die Controls werden nun in 4 (ehemals 14) Themen kategorisiert:

Organizational Controls

Physical Controls

People Controls

Technological Controls

Organizational Controls

Controls, die keine individuellen Personen, physischen Objekte oder Technologie betreffen

37 Maßnahmen zu Themengebieten, wie beispielsweise:

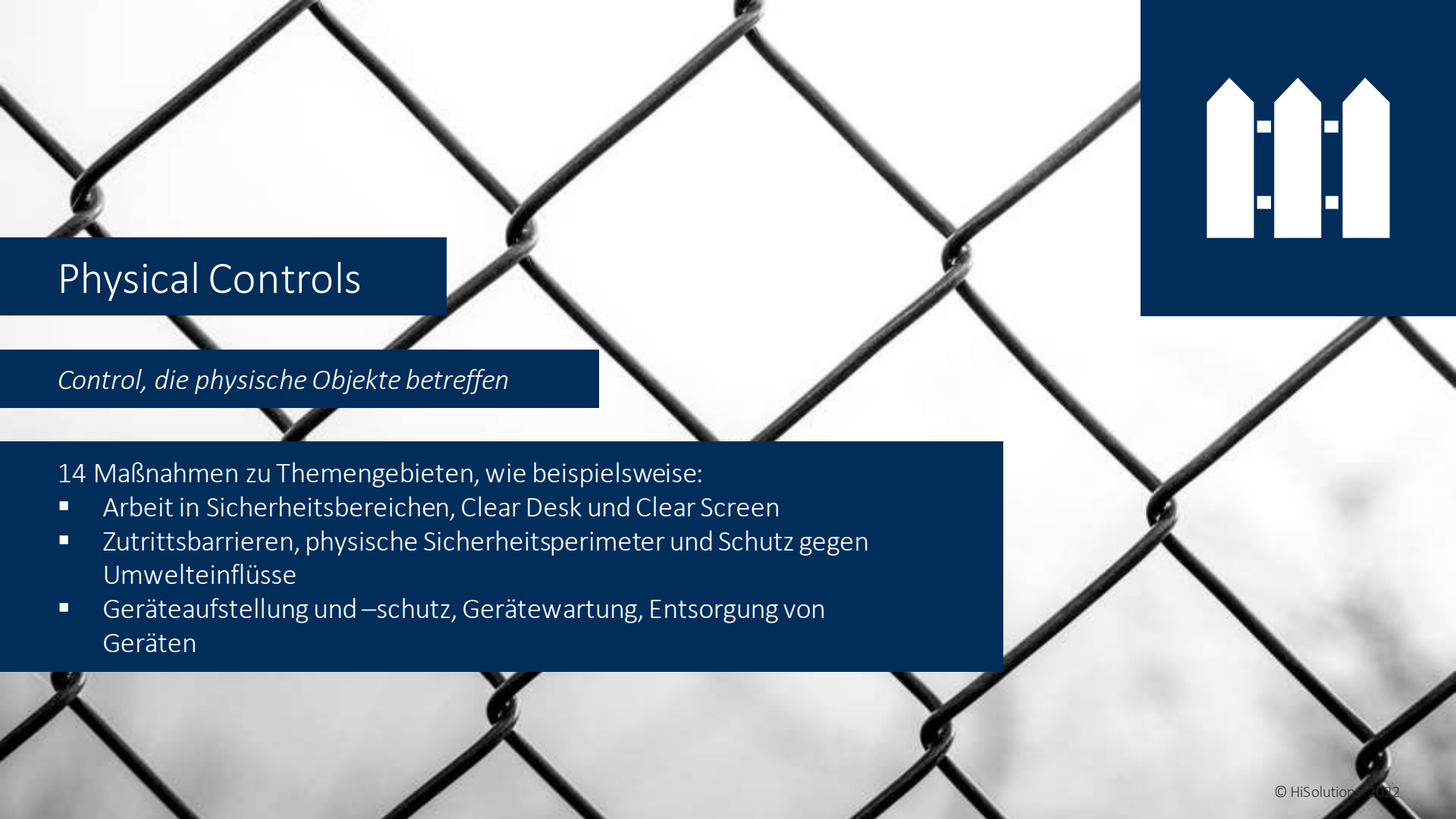
- Rollen, Sicherheitsvorgaben und Verantwortlichkeiten in der Informationssicherheit
- Dokumentation von Betriebsabläufen
- Reaktion auf Sicherheitsvorfälle, Beweissammlung sowie anschließendes Review und Learning
- Informationssicherheit in der Supply Chain und im Projektmanagement
- Identitätsmanagement und Zugriffskontrolle

People Controls

Controls, die individuelle Personen betreffen

8 Maßnahmen zu Themengebieten, wie beispielsweise:

- Einstellung und Überprüfung von Mitarbeitenden sowie Verhalten bei Positions- oder Arbeitgeberwechseln
- Informationssicherheits-Awareness, -bildung, -training und Event Reporting
- Remote-Arbeit



Physical Controls

Control, die physische Objekte betreffen

14 Maßnahmen zu Themengebieten, wie beispielsweise:

- Arbeit in Sicherheitsbereichen, Clear Desk und Clear Screen
- Zutrittsbarrieren, physische Sicherheitsperimeter und Schutz gegen Umwelteinflüsse
- Geräteaufstellung und –schutz, Gerätewartung, Entsorgung von Geräten

Technological Controls

Controls, die Technologie betreffen

34 Maßnahmen zu Themengebieten, wie beispielsweise:

- Kapazitätsmanagement
- Schutz gegen Schadsoftware
- Logging und Monitoring
- Netzwerksicherheit
- Sichere Entwicklung

Alle Controls der ISO 27002:2021 werden jetzt mit Attributen verknüpft

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
#Preventive, #Detective, #Corrective	#Confidentiality, #Integrity, #Availability	#Identify, #Protect, #Detect, #Respond, #Recover	z. B. #Governance, #Asset_management, #Information_ protection, #Human_resource_ security	#Governance_and_ Ecosystem, #Protection, #Defence, #Resilience

Mittels des Hashtags lassen sich Maßnahmen mit diesen Attributen in der Norm suchen

Attribute erhöhen die Transparenz und reduzieren Fehlinterpretationen bei der Anwendung

2. Vorstellung der neuen Controls

5.7 Threat intelligence

Systematische Datensammlung und kontinuierliches Monitoring der Bedrohungslage

5.23 Information security for use of cloud services

IS-Anforderungsbasierte Nutzung und Verwaltung von Cloud-Diensten

5.30 ICT readiness for business continuity

Implementierung der IKT-Bereitschaft auf Basis von BC-Zielen und IKT-Kontinuitätsanforderungen

7.4 Physical security monitoring

Permanente Perimeterüberwachung des Betriebsgeländes und von Räumlichkeiten, in denen sich kritische Systeme befinden

8.9 Configuration management

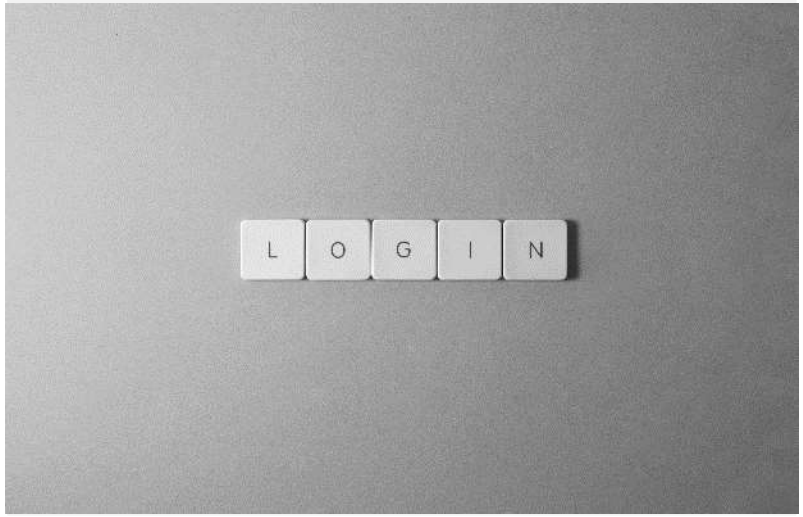
Kontrollierte Einführung, Dokumentation und Überwachung von Konfigurationen

8.10 Information deletion

Vernichtung nicht benötigter gespeicherter Informationen in Informationssystemen und -geräten

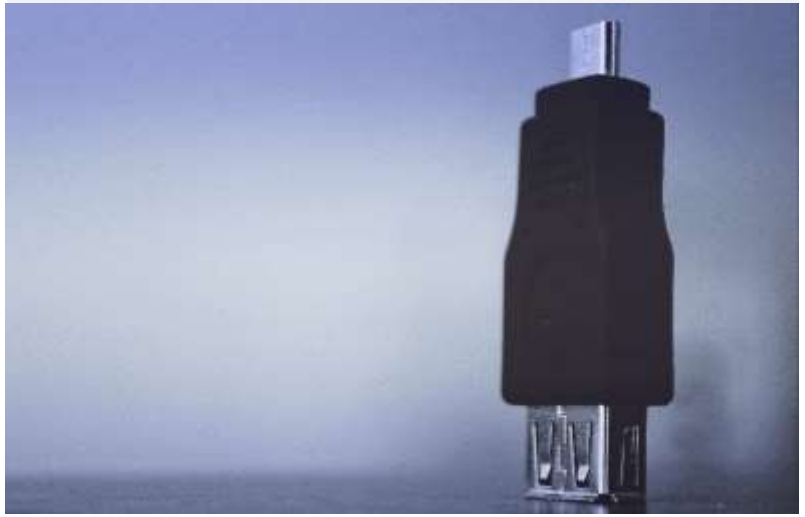
8.11 Data masking

Einsatz von Datenmaskierung in Übereinstimmung mit internen Richtlinien zur Zugriffskontrolle



8.12 Data leakage prevention

Maßnahmen zur Verhinderung von Datenlecks auf Systemen, Netzwerken und Endgeräten



8.16 Monitoring activities

Überwachung der Netze, Systeme und Anwendungen auf anomales Verhalten

8.23 Web filtering

Verwaltung des Zugangs zu externen Webseiten

8.28 Secure coding

Anwendung von sicheren Entwicklungsprinzipien in der Softwareentwicklung

3. Fazit für bestehende Managementsysteme nach ISO 27001

Fazit für bestehende Managementsysteme nach ISO 27001

Abgleich bestehender Sicherheitsvorgaben mit den neuen Controls der Norm

- 5.7 Threat intelligence
- 5.23 Information security for use of cloud services
- 5.30 ICT readiness for business continuity
- 7.4 Physical security monitoring
- 8.9 Configuration management
- 8.10 Information deletion
- 8.11 Data masking
- 8.12 Data leakage prevention
- 8.16 Monitoring activities
- 8.23 Web filtering
- 8.28 Secure coding

Überführung in das Informationssicherheits-risikomanagement

- Neue Controls fordern neue Risikobehandlungsmaßnahmen
- Bereits bestehende Controls sollten auf die neue Struktur des Annex A der Norm angeglichen werden

Statement of Applicability (Anwendbarkeitserklärung)

- Neue Controls müssen auf Anwendbarkeit geprüft werden
- Neue Struktur des Annex A fordert eine Neufassung des Statement of Applicability

Haben Sie Fragen?

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com