qSk!lls
innovation through education

Informationssicherheit im Mittelstand pragmatisch steuern

Die neue ISO/IEC 27001:2022

#SURVIVEANDPROSPER

RESILIENCE OPERATIONS

C E N T E R

Ihre Lage im Griff!

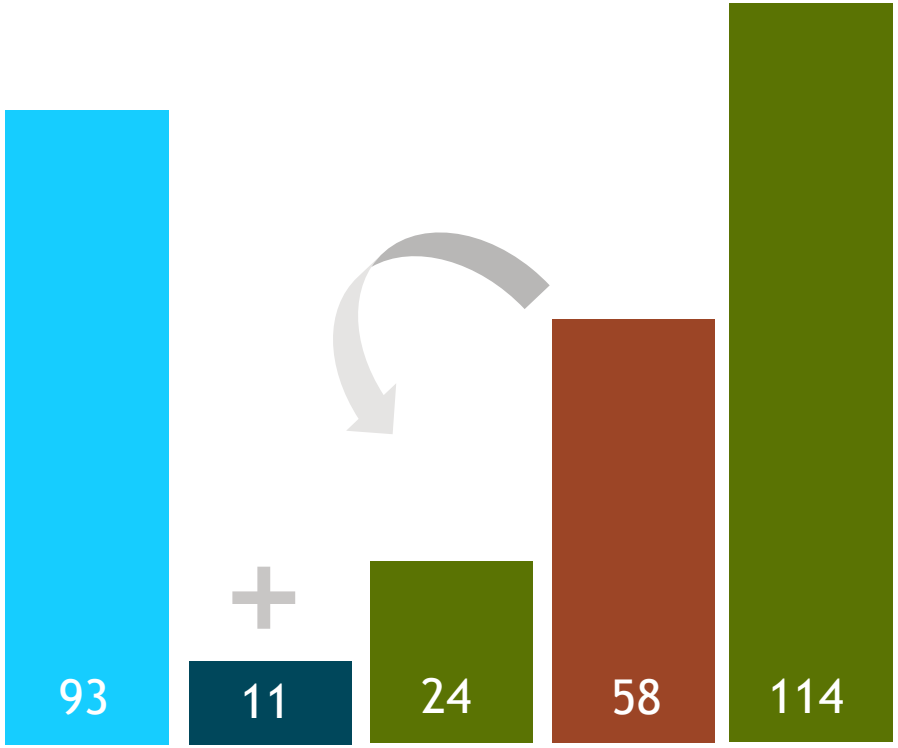
ISO/IEC 27002:2022 – neue Struktur

Veröffentlicht 15.02.2022 **ISO/IEC27002:2022**

→ **KORREKTUR** im März (kostenfrei)

- **58 Controls** aus der ISO 27002:2013 wurden **überprüft und überarbeitet** → Anpassung aktuelle Cybersicherheits- und Informationssicherheitslage
- **24 Controls aus** Version 2013 **zusammengeführt**
- **11 Controls Neu**

Gesamtzahl der **Controls sank** von 114 **auf 93**



Stand zur ISO/IEC 27001:2022

qSk!lls
innovation through education

Life cycle

Previously

Published
ISO/IEC 27001:2013

Published
ISO/IEC 27001:2013/Cor 1:2014

Published
ISO/IEC 27001:2013/Cor 2:2015

Now

Under development
ISO/IEC 27001

Stage: **60.00** (Under publication)

00	10	20	30	40	50	**60** Publication	90	95

60.00 2022-09-23
International Standard under publication

60.60
International Standard published

Und was passiert mit ISO/IEC 27001:2022?

24. Oktober 2022 **3rd Edition** der ISO/IEC 27001:2022

- Anhang A wird ersetzt durch Controls aus der **ISO/IEC 27002:2022**
- **ISO/IEC 27000:2018** Definitionen stellen Anforderungen dar
- Neues Kapitel 6.3 – Managing Changes
- Mehr Fokus auf **Prozesse und Prozess-Steuerung** des ISMS
- Steuerung ausgelagerter Prozesse umfasst nun auch **Produkte und Dienstleistungen** die genutzt werden

Neue Struktur Anhang A

Die Kontrollsätze sind nun in vier (4) Kategorien statt in vierzehn (14) Kontrolldomänen unterteilt. (früher A.5 bis A.18)

Es gibt nun 4 Themenfelder, die keiner Reihenfolge oder Priorisierung unterliegen:

- **Physical Controls** → betrifft physische Objekte
- **People Controls** → betrifft alles rund um (individuelle) Personen
- **Technological Controls** → betrifft alles rund um Technologie
- **Organizational Controls** → „Der Rest“

#Hashtag – wir bauen unsere eigene Stuktur

qSk!lls
innovation through education

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
8.27	Secure system architecture and engineering principles	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.28	Secure coding	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.29	Security testing in development and acceptance	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #Information_security_assurance #System_and_network_security	#Protection
					#System_and_	

Quelle: ISO/IEC 27002:2022, Table A.1

#Hashtag – wir bauen unsere eigene Stuktur

- Alle Controls mit Attributen verknüpft – diese können semantisch zusammengefasst werden
- Dienen der Bildung von Sichten (Views) auf das gesamte Controlset

Vorteile:

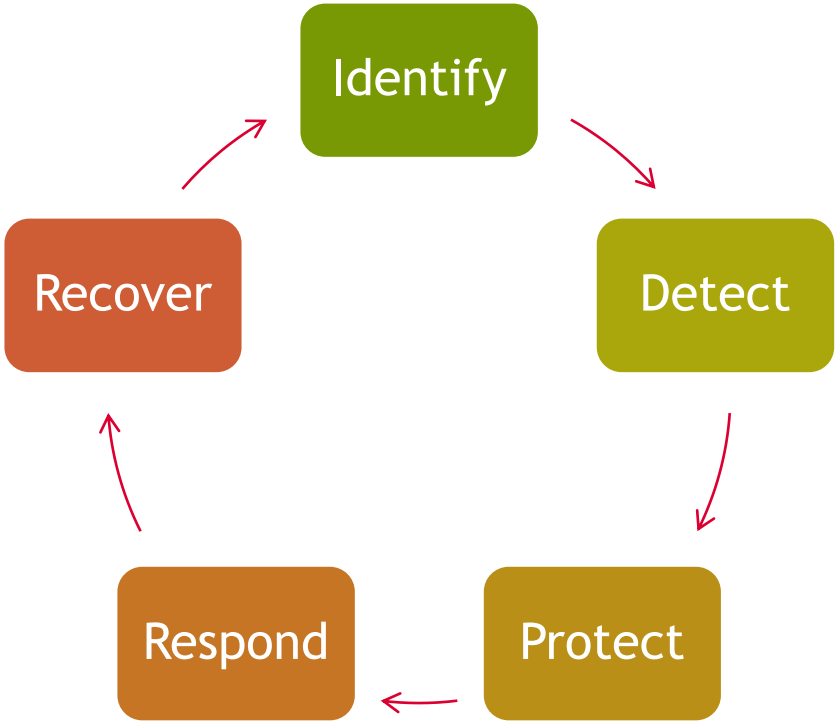
- Durch die Verwendung der Attribute lassen sich die Maßnahmen suchen und gruppieren
- Erhöhung der Flexibilität
- Verringerung der Fehlinterpretation in der Anwendung

Control Type

- Preventive
- Detective
- Corrective

immer bezogen auf einen potenziellen Security Incident

Cybersecurity Concepts



aus Cybersecurity Framework ISO/IEC TS 27110

Organizational Capabilities

Adressat Management	Adressat Fachabteilung	Adressat IT
Governance	Asset_management	System_and_network_security
Information_security_event_management	Human_resource_security	Application_security
Information_protection	Supplier_relationships_security	Secure_configuration
Legal_and_compliance	Physical_security	Identity_and_access_management
Information_security_assurance	Continuity	Threat_and_vulnerability_management

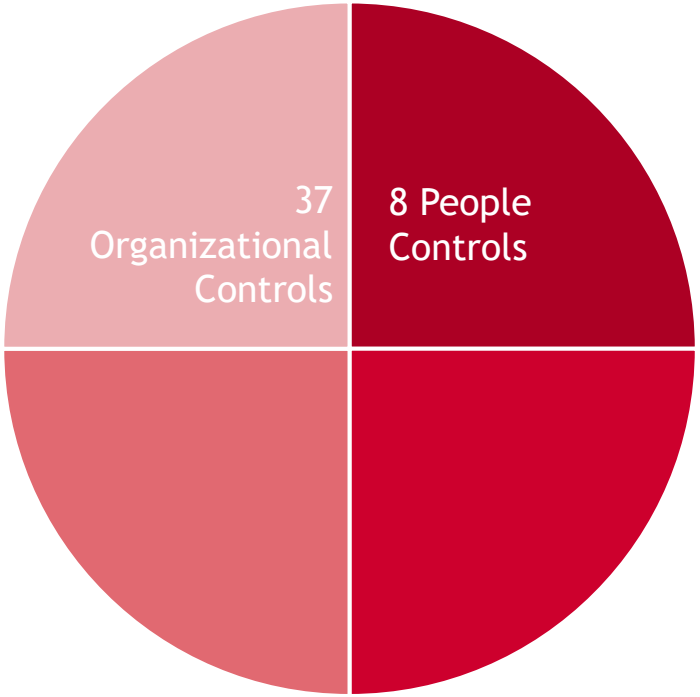
Security Domains

- Governance_and_Ecosystem
- Protection
- Defence
- Resilience

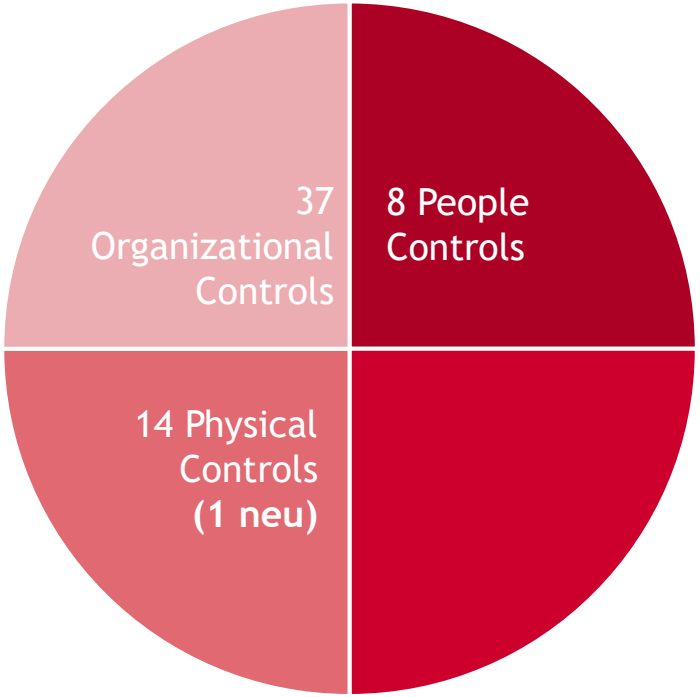
→ Soll Blick auf Dienstleistungen und Produkte abbilden

Organisational Controls

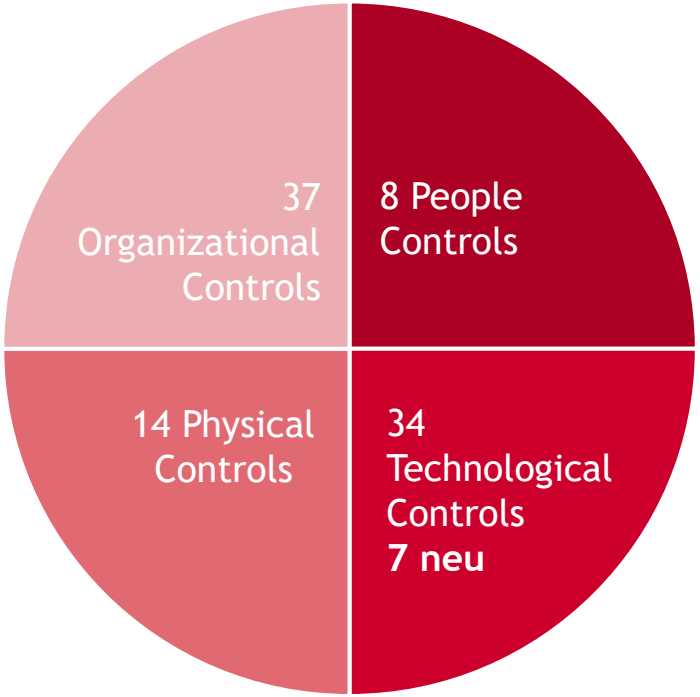
People Controls



Physical Controls



Technological Controls



Controls Eleven ;-)

- **5.7 Threat intelligence** – systematische Datensammlung und kontinuierliches Beobachten der Bedrohungslage
- **5.23 Information security for use of cloud services** – Informationssicherheit über Lebenszyklus der Nutzung von Cloud-Diensten berücksichtigen
- **5.3 ICT readines for business continuity** – Implementieren der IKT-Bereitschaft auf der Basis von BC-Zielen und IKT-Kontinuitätsanforderungen
- **7.4. Physical security monitoring** –Perimeterüberwachung des Betriebsgeländes und von Räumlichkeiten, in denen sich kritische Systeme befinden
- **8.9 Configuration management** – kontrollierte Einführung und Überwachung von Konfigurationen
- **8.10 Information deletion** – Vernichtung nicht benötigter Informationen in Informationssystemen und -geräten

Controls Eleven ;-)

- **8.11 Data masking** – Einsatz von Datenmaskierungen in Übereinstimmung mit internen Richtlinien zur Zugriffskontrolle
- **8.12 Data leakage prevention** – Maßnahmen zur Verhinderung von Datenlecks in Systemen, Netzwerken und Endgeräten
- **8.16 Monitoring activities** – Überwachung der Netze, Systeme und Anwendungen auf anormales Verhalten
- **8.23 Web filtering** – Verwaltung des Zugriffs auf externen Webseiten
- **8.28 Secure coding** – Anwendung von sicheren Entwicklungsprinzipien in der Softwareentwicklung

Was passiert mit existierenden Zertifizierungen?

Übergangsfrist – ISO/IEC 27001:2022

- Bereits zertifizierte Unternehmen → Übergangsfrist zwei/drei Jahre (?) – Entscheidung steht noch aus!
- Zeitraum beginnt vermutlich 24. Oktober 2022
- Anwendung der Normen ab Veröffentlichung möglich
- Umstellung im Rahmen der regulären Audits möglich (Überwachung und Re-Zertifizierung)

Was ist nun zu tun?

- Gap-Analyse auf neue Controls UND neue Guidance zur Umsetzung – was ist relevant für Sie?
- Überprüfen Ihrer Richtlinien und Prozesse zur Erfüllung der neuen Controls.
- Überprüfen Sie das Risikoregister → welche neuen Controls sind relevant?
- Aktualisierung der Statement of Applicability (SoA), um sie an den aktualisierten Anhang A anzupassen
  - Wenn möglich Control-Owner definieren
  - Nutzen Sie die „#Hashtags“ um für Sie passende Gruppierungen festzulegen
- Achten Sie auf den höheren Prozessfokus in der ISO/IEC 27001
- Beachten Sie Definitionen aus ISO/IEC 27000:2018

Herausforderungen

- Threat Intelligence → wie aktuell an Informationen kommen?
- Monitoring Activities → Anomalie-Erkennung
- Data Leakage Prevention → braucht gute Erkennungsmechanismen und selbstlernende Unterstützung
- Data Masking → Was, wann und wie? Pseudonymisierung, Anonymisierung
- Configuration Management → Achtung: Kleinteiligkeit!
- Cloud-Lebenszyklus – wie im Detail steuern?

Wird es einfacher oder schwerer, Controls zu implementieren

Auch wenn die **Anzahl der Controls** sich **reduziert** hat, ist das kein Hinweis darauf, dass die Themenvielfalt abgenommen hat. Es wurden Controls zusammengefasst, z.B. im Zugriffsrechte-Management. Auf der anderen Seite wurden viele neue Controls ergänzt und neue Schwerpunkte gelegt, welche v.a. die die Vermeidung, Entdeckung und Reaktion bezüglich Cyberangriffen sowie den Schutz von Daten stärker in den Fokus rücken.

Die Änderungen wissen durchaus zu gefallen, zumindest auf den ersten Blick, weil es in der alten Fassung Überschneidungen von Controls oder kleinteilige Aufsplittungen gab, über deren Zweck sich trefflich „frotzeln“ ließ. Einige davon wurden aufgelöst.

Auch die Stärkung des Monitorings der IT-Landschaft ist direkt anschlussfähig an die geplanten Anforderungen des IT-Sicherheitsgesetzes 2.0 das „Systeme zur Angriffserkennung“ fordert im Sinne von Intrusion, Detection und Prevention Systemen.

Jetzt den qSkills-Kurs zur neuen ISO/IEC 27001:2022 buchen

https://www.qskills.de/qs/workshops/security/sc121update2022fuerisoiec2700127002/

24. Oktober 2022

qSkills Security Summit

Cybersecurity in Krisenzeiten -
Maßstäbe für die Zukunft setzen

https://www.qskills-security-summit.de/

Jetzt das Whitepaper für die neue ISO/IEC 27001:2022 herunterladen!

https://resilienceoperations.center/informationssicherheitsmanagementsystem/

RESILIENCE OPERATIONS

CENTER

Vielen Dank für Interesse.

Was fehlt Ihnen noch, um Ihre Lage im Griff zu haben?

Resilience Operations Center GmbH
Neumeyerstr. 48
90411 Nürnberg - Deutschland
+49 911 477 528-0
hello@ResilienceOperations.Center
ResilienceOperations.Center