secuvera:
Cybersicherheit. Nachhaltig.

ISO 27032
Noch ein Managementsystem?
Einordnung & Relevanz

verinice.XP 2025, Berlin

Ann-Kathrin Udvary
Viktor Rechel

verinice.XP

Viktor Rechel

secuvera:
Cybersicherheit. Nachhaltig.

- seit 2019 bei der secuvera
- Stellv. Technischer Leiter (ISO 27001)
  - Sicherheitsberatung (u.a. ISMS nach ISO 27001, Cyber-Sicherheits-Checks, Interne Audits, Ext. ISB)
- Leitender Cybersicherheitsberater
  - Pentest (u.a. System, Web / API, iOS-Apps, Cloud Security Assessments)
- Interner Umwelt- & Informationssicherheitsbeauftragter
- Autor & Referent
  - Informatik aktuell, secIT, secIT specials, verinice.XP, heise Academy, Internet Security Days
- Zertifizierungen
  - BSI-zertifizierter Penetrationstester, TR-Prüfer (DiGAs), CISSP, ISO 27001 Lead Auditor, Cyber Security Practitioner

Ann-Kathrin Udvary

secuvera:
Cybersicherheit. Nachhaltig.

- seit 2019 bei der secuvera
- Leitende Cybersicherheitsberaterin
  - Sicherheitsberatung
  - ISMS nach ISO 27001 (u.a. Beratung Aufbau & Aufrechterhaltung, Audits)
  - BCM nach ISO 22301 und BSI-Standard 200-4 (u.a. Beratung Aufbau, BIA)
  - Externe ISB
- Autorin & Referentin
  - iX, verinice.XP, CYBERWOMEN, heise Academy
- Zertifizierungen
  - ISO 27001 Lead Auditorin, BCM-Praktikerin

Geschäftsbereiche

secuvera:
Cybersicherheit. Nachhaltig.

BSI-Prüfstelle

Common Criteria, BSZ
TR-Prüfungen

Industrial Security (IEC 62443)

Penetrationstests

u. a. Webanwendungen, Ransomware-Simulation, Red-Teaming, AD-Analysen

Sicherheitsberatung

BSI-Grundschutz /
ISO 27001 / TISAX®

CISO as a Service (CaaS)

Schulung und Herstellerberatung

OWASP® Top 10, SSDL, ISO 27001, Cyber für KMU

Zertifizierungen und CRA

secuvera:
Cybersicherheit. Nachhaltig.

- >40 Mitarbeitende
- IT-Sicherheit seit 1988

- BSI-Grundschutz Auditoren,
  -Berater & -Praktiker
- ISO 27001 Lead Auditoren
- BCM Praktiker
- BSI-zertifizierte Pentester
- Common Criteria Evaluatoren
- Cyber Security Practitioner
- KRITIS-Prüfer
- TR-Prüfer
- ..

Abgrenzung der ISO 27032

ISO / IEC 27032

secuvera:
Cybersicherheit. Nachhaltig.

- **Titel: „Cybersecurity – Guidelines for Internet Security“**
- Neufassung 2023-06
- Englische Fassung
- Ergänzungsmöglichkeit zur ISO 27001
- Schnittstellen zu ISO 27001 / ISO 27002:2022
- „Guidelines“, explizit für den Bereich Cybersicherheit / Internetsicherheit
- Zusammenhang zwischen „Internetsicherheit, Websicherheit, Netzwerksicherheit und Cybersicherheit“

Managementsystem vs. Best Practice

secuvera:
Cybersicherheit. Nachhaltig.

Managementsystem

- Koordinierter Prozess zur Steuerung von Zielen (z. B. Informationssicherheit bei ISMS)
- Meist allgemeinere Anforderungen, da Anpassbarkeit auf das entsprechende Unternehmen gewünscht ist
- Meist Zertifizierungsfähigkeit, ergo Unternehmen können sich nach der Norm zertifizieren lassen
- Beispiele: ISO/IEC 27001, ISO 9001, BSI-Standard 200-1

Best Practice

- Vorgehensweisen, die sich in der Praxis bewährt haben
- Meist spezifischere Aspekte, die direkter angewendet werden können
- Keine verbindliche Umsetzung
- Keine Zertifizierungsfähigkeit
- Beispiele: Technische Richtlinien des BSI

ISO / IEC 27032 als Best Practice

secuvera:
Cybersicherheit. Nachhaltig.

- ISO / IEC 27032 ist als Best Practice anzusehen
  - Soll Hilfestellungen zu spezifischen Anwendungsfällen / Maßnahmen geben
  - Kein eigenständiges Managementsystem, sondern Erweiterung des ISMS auf „Cybersicherheit“
- Entweder eigenständige Betrachtung als „Best of“-Maßnahmen oder Einbindung in ein bestehendes ISMS

Inhalte der ISO 27032

Struktur der ISO 27032

secuvera:
Cybersicherheit. Nachhaltig.

Kapitel 1-4

- Anwendungsbereich
- Referenzen
- Definitionen
- Abkürzungen

Kapitel 5

- Zusammenhang
- Internetsicherheit
- Web- sicherheit
- Netzwerksicherheit
- Cybersicherheit

Kapitel 6

- Übersicht Internetsicherheit

Kapitel 7

- Interessierte Parteien

Kapitel 8

- Risikomanagement für Internetsicherheit

Kapitel 9

- Sicherheitsmaßnahmen fürs Internet

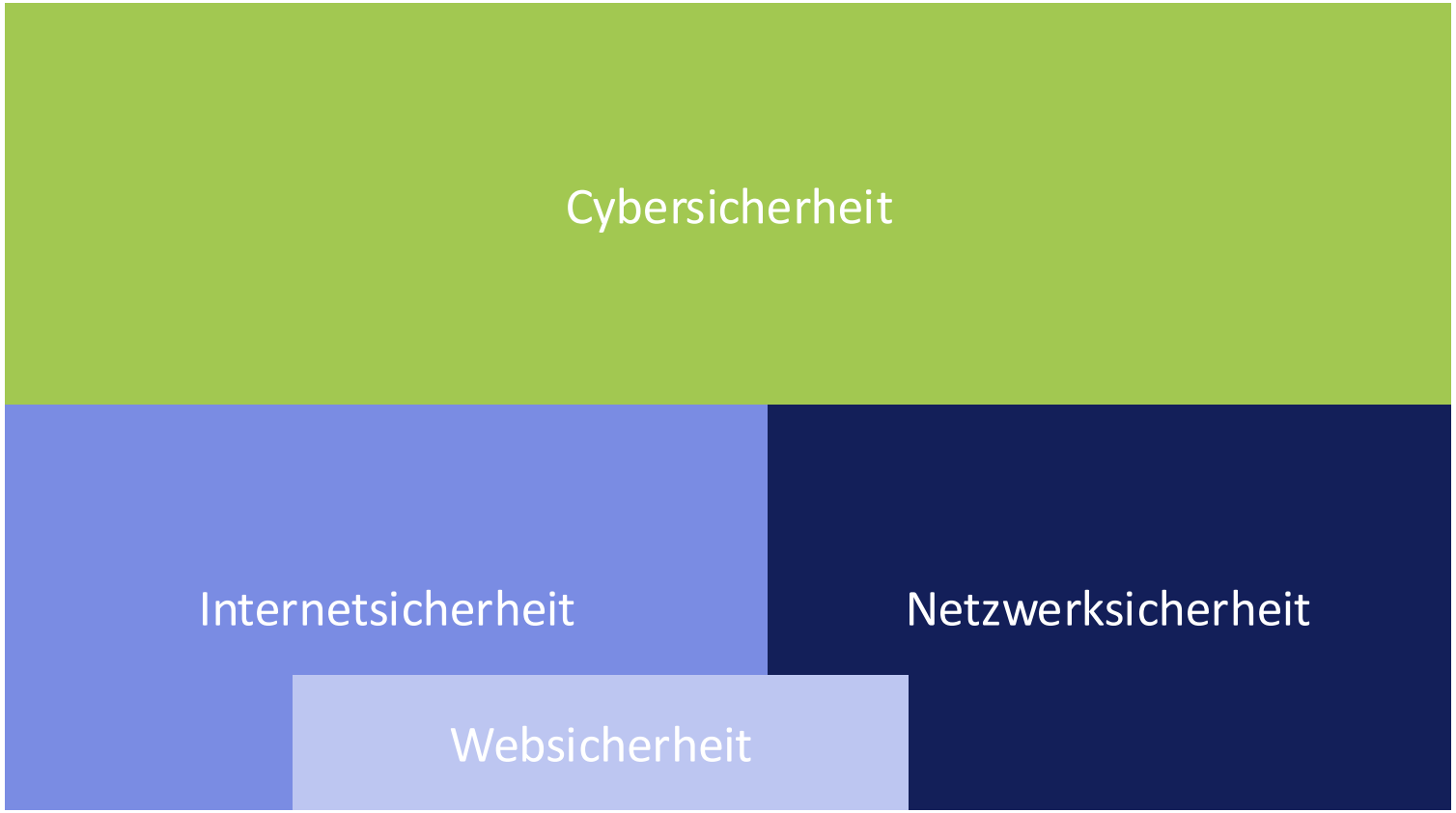
Anhang A

- Referenztabelle
- Kap. 9 <-> ISO 27002

„Das Internet ist für uns alle Neuland“

Angela Merkel, 2013

Kap. 5 – Zusammenhang Sicherheitsthemen

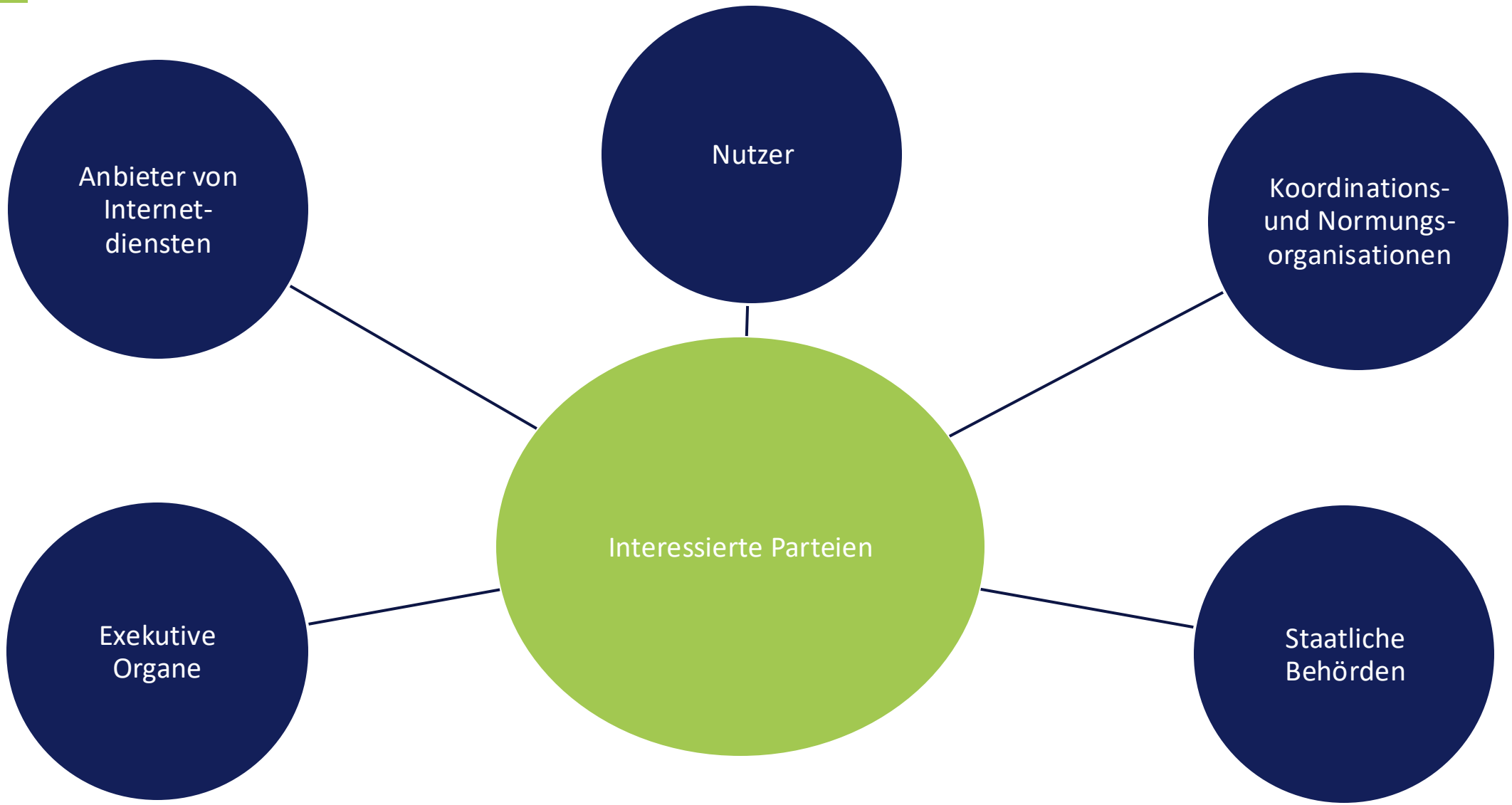


Kap. 6 – Übersicht Internet Sicherheit

secuvera:
Cybersicherheit. Nachhaltig.

- Auszug erwähnter Themen beim Thema Internetsicherheit:
  - Datenschutz
  - Künstliche Intelligenz
  - Internet of things
  - Verfügbarkeit & Verlust von personenbezogenen Daten
  - Angriffstechniken (bspw. Phishing, Schadhafte Webseiten) & -ziele (bspw. Finanzbetrug)
  - Weiterentwicklung von „Hacking personenbezogener Daten“ hin zu organisierter Cyberkriminalität

Kap. 7 – Interessierte Parteien



Kap. 8 – Risikomanagement für Internet Sicherheit

secuvera:
Cybersicherheit. Nachhaltig.

- Orientiert an ISO 31000 & ISO/IEC 27005
- Bedrohungen
  - Bspw. Malware, Offenlegung von personenbezogenen Daten, BYOD, Verfügbarkeit Infrastruktur, Malware as a Service
- Schwachstellen
  - Bspw. Schwachstellen in Anwendungen, insbesondere Webanwendungen
- Angriffsvektoren
  - Bspw. Port-Scanner, Mitlesen von Kommunikation, Malware, Manipulierte Webseiten, APT, Brute Force

Kap. 9 – Sicherheitsmaßnahmen fürs Internet

secuvera:
Cybersicherheit. Nachhaltig.

Regelungen / Richtlinien	Zugangs-verwaltung	Sensibilisierungen und Schulungen	Umgang mit Vorfällen	Inventarisierung / Asset Management
Dienstleister-management	BCM	Datenschutz	Schwachstellen-management	Netzwerk-management
Schutz vor Schadsoftware	Änderungs-management	Gesetzliche und regulatorische Anforderungen	Kryptographie	Anwendungs-sicherheit
Endgeräte-management	Überwachung / Monitoring			

Mapping Kap. 9 ISO 27032 <-> ISO 27001 / 27002

secuvera:
Cybersicherheit. Nachhaltig.

Regelungen / Richtlinien	Zugangs-verwaltung	Sensibilisierungen und Schulungen	Umgang mit Vorfällen	Inventarisierung / Asset Management
Dienstleister-management	BCM	Datenschutz	Schwachstellen-management	Netzwerk-management
Schutz vor Schadsoftware	Änderungs-management	Gesetzliche und regulatorische Anforderungen	Kryptographie	Anwendungs-sicherheit
Endgeräte-management	Überwachung / Monitoring			

Beispiele einer möglichen Anwendung

Beispiel – Asset Management

secuvera:
Cybersicherheit. Nachhaltig.

- IKT-Komponenten sollen inventarisiert werden
- Informationen sollen inventarisiert werden (bzgl. Speicherung, Verarbeitung, Übertragung)
- Regelungen zur zulässigen Handhabung von Werten sollen aufgestellt werden
- Kritikalität von Assets soll bewertet und erfasst werden
- Referenz auf ISO 27002

→ *Nichts wirkliches Neues…*
Anwendung unterscheidet sich nicht von 27001 oder IT-Grundschutz

Beispiel – Netzwerkmanagement

secuvera:
Cybersicherheit. Nachhaltig.

- Reduzierung (und restriktive Handhabung) der exponierten Systeme
- Sicherheitsmaßnahmen gegen Manipulation, unberechtigtem Zugriff, etc.
- Protokollierung & Überwachung sollte eingesetzt werden
- Anregung zur Einführung von DMZs (bzw. allgemein Netzwerktrennung)
- Richtlinie zum Umgang mit dem Internet (Internetdiensten, technische Maßnahmen im Kontext Netzwerksicherheit, Verschlüsselung)
- Firewall dringend empfohlen

→ *An manchen Stellen spezifischer als z. B. ISO 27002, aber auch nicht direkt anwendbar*

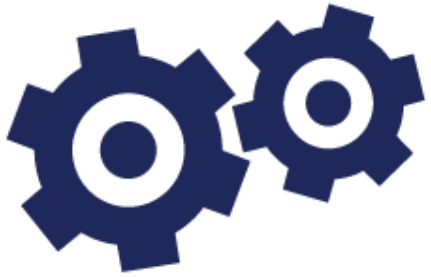
Beispiel – Anwendungssicherheit

secuvera:
Cybersicherheit. Nachhaltig.

- Zu beachtende Themen
  - Risikomanagement
  - Sichere Entwicklung (inkl. Threat Modelling, sichere Authentifizierung, Supply Chain, Session-Verwaltung, Datenvalidierung, sicheres Design, Security by Design, Secure Coding, Code Signing, statische Codeanalysen, Schwachstellenscans)
  - Zulässige Nutzung von Internetdiensten (inkl. Webfilterung)
  - Härtung von Webservern & Verwendung von Kryptographie
  - (Einforderung von) Sicherheitsprüfungen (z. B. nach Common Criteria)

→ *An manchen Stellen spezifischer als z. B. ISO 27002, manchmal aber zu hohe Anforderungen und nicht direkt anwendbar*

Vergleich mit anderen Standards / Best Practices



ISO 27000er-Reihe

secuvera:
Cybersicherheit. Nachhaltig.

- ISO 27001 als international führender Standard für ISMS
  - Behandelt ganzheitliche Informationssicherheit
- ISO 27002 als Umsetzungsempfehlungen für Informationssicherheitsmaßnahmen aus Anhang A der ISO 27001
  - Sammlung von Best-Practice zur Umsetzung der 93 Informationssicherheitsmaßnahmen
- Vielzahl branchen- und themenspezifische Erweiterungen, u.a.
  - ISO 27017 Cloud-Dienste
  - ISO 27019 Energieversorgung

Vergleich mit BSI

secuvera:
Cybersicherheit. Nachhaltig.

- Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt und pflegt unterschiedlichste Dokumente
  - BSI IT-Grundschutz (IT-Grundschutz-Kompendium mit Bausteinen)
  - BSI-Standards zur Internet-Sicherheit (ISi-Reihe)
  - Technische Richtlinien, z. B. 02102 zu kryptographischen Verfahren oder 03185 Sicherer Software-Lebenszyklus
  - Maßnahmenkatalog Ransomware
  - Basismaßnahmen der Cyber-Sicherheit
  - Sichere Konfiguration von […] (z. B. Microsoft Office, Libre Office, etc.)

Vergleich mit NIST

secuvera:
Cybersicherheit. Nachhaltig.

- National Institute of Standards and Technology (NIST) definiert verschiedenste Best Practices (in der Regel als Special Publications (SP))
  - Reihe SP 800: Computersicherheit
  - Reihe SP 1800: Cybersicherheit
  - SP 800-207 Zero Trust
  - SP 800-209 Security Guidelines for Storage Infrastructure
  - NIST SP 800-147 BIOS Protection Guidelines
  - SP 1800-16B: Securing Web Transactions:

Praxisrelevanz?

Anwendbarkeit der Hinweise

secuvera:
Cybersicherheit. Nachhaltig.

- Für den Einstieg wichtige und richtige Themenbereiche
- Einzelne Empfehlungen gehen oft zu tief (z. B. Common Criteria bei Anwendungen) und sind immer noch nicht direkt anwendbar
- Zielgruppe der Empfehlungen unklar
  - Definition des Internets vs. tiefgehende Empfehlungen
  - Jemand der bereits ein ISMS hat, kennt die Empfehlungen meist schon
  - Jemand der kein ISMS betreibt, wird die ISO 27032 nicht kennenlernen

„Hierarchie der Standards“

secuvera:
Cybersicherheit. Nachhaltig.

ISO 27032

- Best Practices für Internetsicherheit
- Zusammenfassung relevanter Themen
- Einstiegsdokumentation
- Umfang: 36 Seiten

ISO 27002

- Umfassendere Umsetzungsempfehlungen zu allgemeinen Informationssicherheitsmaßnahmen
- Umfang: 209 Seiten

ISO 27001

- Managementsystem, um Anforderungen in der Praxis umsetzen zu können
- Bei eigenen Controls nur rudimentäre Beschreibungen
- Umfang: 31 Seiten

Relevanz in Verbindung mit einem ISMS

secuvera:
Cybersicherheit. Nachhaltig.

- Einbindung in ein bestehendes ISMS per se gut machbar
  - Ergänzung relevanter Maßnahmen für das Risikomanagement
  - Abgleich mit der eigenen Umgebung
- Gerade wenn bei den betroffenen Themen Unklarheit herrscht, könnten Denkanstöße dabei sein

Kann man machen, muss man aber nicht ☺

secuvera:
Cybersicherheit. Nachhaltig.

Fragen?

audvary@secuvera.de
vrechel@secuvera.de

www.secuvera.de

secuvera:
Cybersicherheit. Nachhaltig.

Danke sehr!

audvary@secuvera.de
vrechel@secuvera.de

www.secuvera.de