Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

SECURITY
Standards und ISMS

April 27, 2023

Marc Stöttinger

> Security is a process not a product.
>
> Bruce Schneier

MOTIVATION SICHERHEITSSTANDARDS

- → **Bisher:** Identifikation von Bedrohungen und Vorgehen von Angreifern
- → **Aber:**
  - → Wo fangen wir an, IT-Sicherheit umzusetzen?
  - → Wo hören wir auf, IT-Sicherheit umzusetzen?
  - → Wie stellen wir eine sinnvolle Umsetzung sicher?
  - → Wie kommunizieren wir IT-Sicherheit intern/extern?
- → **Beispiel:**
  - → Entwicklung der IT-Sicherheit für Fahrzeuge im Fall von [FCA] Jeep Cherokee-Hack in 2015

BEISPIEL IM FALL JEEP CHEROKEE-HACK

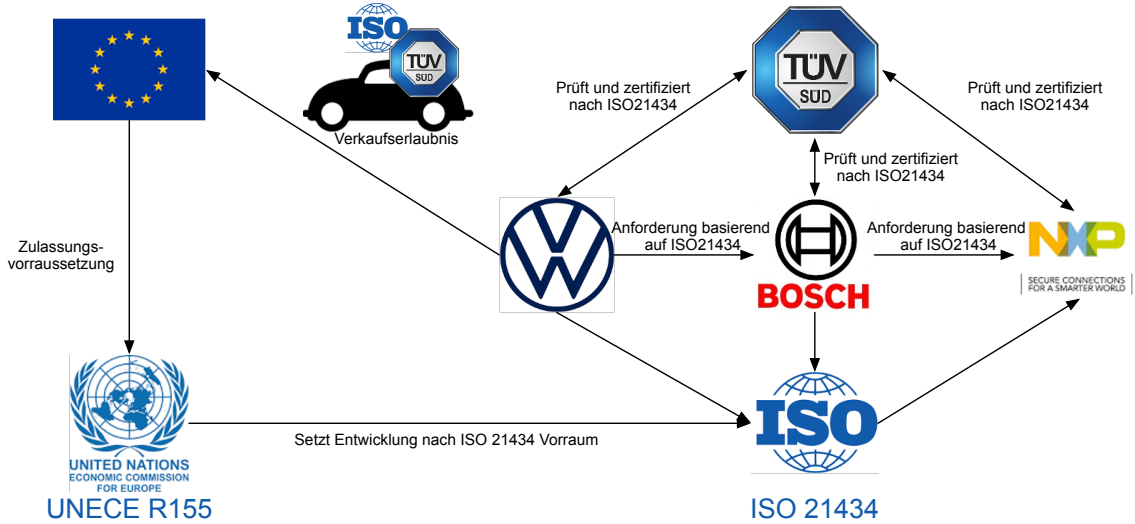
1. Sicherheitsforscher analysieren Multimedia System und WLAN Interface
   - → Schwachstellen existieren, um wahlfreie Befehle auf dem Multimedia System auszuführen
   - → Schwachstellen können via GSM ausgenutzt werden
   - → Ca. 300.000 anfällige Jeeps werden via GSM identifiziert

2. Weitere Sicherheitslücken identifiziert, um wahlfreie Nachrichten im Fahrzeugnetzwerk zu senden
   - → Fahrzeugnetzwerk enthält: Bremsen, Lenkung, Türsteuerung, ...
   - → Senden von Nachrichten an Fahrzeugnetzwerk ist möglich via GSM

3. Sie demonstrieren den Angriff via Remote Hack mit Reportern am Steuer

4. Rückrufaktion zum Patchen der Fahrzeugsoftware kostet FCA 1.4 Millionen Dollar

VERANTWORTUNGSKETTE IT-SICHERHEIT IM BEREICH AUTOMOTIVE



RECHTSFORMEN ZUR IT-SICHERHEIT

- Rechtsnormen mit Fokus auf IT-Sicherheit sind u.a.:
  - IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)
  - EU-Datenschutzgrundverordnung (DSGVO/GDPR)

- Viele weitere Rechtsnormen enthalten Vorgaben zum Thema IT-Sicherheit
  - Telekommunikationsgesetz (TKG): Verbot des Abhörens oder Veränderns von Kommunikation durch TK-Diensteanbieter
  - E-Health-Gesetz: Absicherung des Netzwerkes für medizinische Datenkommunikation
  - ...

- Anforderungen zur Erfüllung von Rechtsnormen können sowohl direkt vom Gesetzgeber als auch transitiv vom Kunden erhalten werden

IT-SICHERHEITSGESETZ 2.0

- Das **IT-Sicherheitsgesetz 2.0** (IT-SiG 2.0) von 2021
  - Umfasst Kritische Infrastrukturen (Energie, Gesundheit, Ernährung, ...)
  - Das BSI fungiert als zentrale Prüf- und Kontrollbehörde
  - Bis zu 2 Mio. Euro Bußgeld bei vorsätzlich fahrlässiger Handlung

- Das IT-SiG definiert verschiedene Anforderungen an Organisationen
  - Verfahren zur Angriffserkennung müssen umgesetzt werden
  - IT-Sicherheitsvorfälle müssen dem BSI gemeldet werden
  - Eingekaufte kritische Komponenten müssen vom Innenministerium genehmigt werden
  - Technische Maßnahmen nach branchenspezifischen Sicherheitsstandards (B3S) werden empfohlen

DATENSCHUTZGESETZE (DSGVO UND GDPR)

- Die Datenschutzgrundverordnung (DSVGO, Englisch GDPR) verlangt u.a:
  - **Zweckbindung:** Nur benötigte private Daten dürfen erhoben und verarbeitet werden
  - **Speicherbegrenzung:** Daten müssen gelöscht werden, wenn der Zweck verfällt

- Nutzer haben ein Rechte auf:
  1. **Information** zur Erhebung und Verarbeitung privater Daten
  2. **Zugriff, Änderung und Löschung** der gespeicherten privaten Daten
  3. **Einschränkung und Mitnahme** der gespeicherten privaten Daten
  4. **Widerspruch** gegen die Speicherung privater Daten
  5. **Vermeidung automatisierter Entscheidungsfindung** basierend auf privaten Daten

- Unternehmen müssen gespeicherte private Daten gegen Angriffe schützen und sind für Schäden haftbar

FOLGEN EINER DSGVO VERLETZUNG

→ Verletzungen des DSGVO werden mit **bis zu 4%** des jährlichen Einkommens geahndet [Fine, ENF]:

Höhe [Euro]	Angeklagter	Grund
405.000.000	Meta	Instagram Daten von Kindern nachlässig behandelt (z.B. Profil standardmäßig öffentlich)
35.258.708	H&M	Erfassung privater Urlaubs- und Gesundheitsdaten von Mitarbeitenden
50	Privatperson	Unerlaubter Einsatz einer Dashcam

→ Verarbeitung privater Daten im Unternehmen muss kontrolliert werden:
- → Bewusstsein der Mitarbeitenden für Umgang mit privaten Daten
- → Zentrales und sicheres Speichern privater Daten
- → Kontrolle und Protokollierung des Zugriffs auf private Daten
- → Review der erhobenen Daten sowie der Konzepte zur Sicherung mit Juristen

RECHTSNORMEN UND STANDARDS

- → Rechtsnormen (z.B. UNECE R155) sind verpflichtende Richtlinien
  - → Gesetzgebung ist ein langwieriger Prozess
  - → Rechtsnormen können den “Stand der Technik” nicht zeitnah abbilden
- → Standards (z.B. ISO21434) sind empfehlende Richtlinien
  - → Bilden den “Stand der Technik” einer Branche ab
  - → Erlaubt Unternehmen einer Branche eine effiziente Prüfung auf Einhaltung von Anforderungen
  - → Standardisierung kann “relativ” flexibel durch Unternehmen einer Branche angepasst werden
- → Rechtsnormen verweisen häufig auf umzusetzende Standards

STANDARDS IM BEREICH IT-SICHERHEIT

- Es existieren verschiedene Standards in der IT-Sicherheit

- IT-Sicherheit im Unternehmen:
  - **ISO/IEC27000 Familie:** Anforderung und Implementierung eines ISMS
  - **BSI Grundschutz (BSI 200-x):** Empfehlungen zu Methoden, Prozessen und Prozeduren
  - **B3S:** Branchenspezifische Sicherheitsstandards im Rahmen des IT-SiG 2.0

- IT-Sicherheit für Produkte:
  - **Common Criteria:** Sichere Produktentwicklung und Anforderungen an Zertifizierung
  - **ETSI EN 303 645:** Sichere Entwicklung von IoT Geräten
  - **ISO21434:** Sichere Entwicklung von Fahrzeugen

EINSCHUB: INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEM (ISMS)

- Grundphilosophien der IT-Sicherheit
  - IT-Sicherheit muss an Unternehmen angepasst und regelmäßig überprüft werden
  - IT-Sicherheit muss sowohl auf technischer- als auch auf Prozessebene implementiert werden

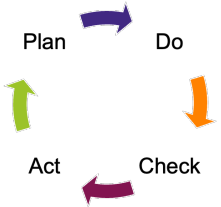
- Ein **ISMS** ist ein System zur Definition, Überprüfung, Erhalt und Verbesserung der IT-Sicherheit
  - Betrachtet sowohl technische Maßnahmen als auch Prozesse
  - Wird von der Unternehmensleitung vorgegeben
  - Wird auf das gesamte Unternehmen angewendet

- Ein ISMS nutzt den **Plan-Do-Check-Act (PDCA)** Zyklus zur ständigen Verbesserung

WARUM EIN ISMS?

- Sicherheit ist kein Zustand sondern ein Prozess
  - Sicherheit unterliegt einer kontinuierlichen Dynamik (Änderung von Gesetzen, neue Angriffe oder technischer Fortschritt)

- Sicherheit muss aktiv gewartet, aufrecht erhalten und verbessert werden
  - Systemeinführung planen
  - Sicherheitsmaßnahmen definieren und umsetzen
  - Erfolgskontrollen durchführen
  - Schwachstellen und Verbesserungsmöglichkeiten finden
  - Maßnahmen verbessern
  - Sicherheitsaspekte bei Außerbetriebnahme berücksichtigen



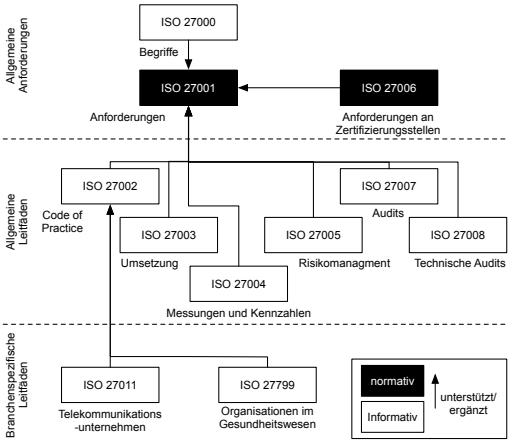
ISMS RELEVANTE KOMPONENTEN UND STANDARDS

- **Komponenten**
  - Management-Prinzipien
  - Ressourcen
  - Mitarbeiter
  - Sicherheitsprozess
    - Sicherheitsrichtlinen
    - Sicherheitskonzept

- **Standards**
  - ISO 27000
    - Zertifizierung nach ISO/IEC 27001
    - Organisationen
    - Personen
  - BSI-Standard 200 (kompatibel ISO/IEC 27001)

ISO/IEC 27000 FAMILIENÜBERSICHT

- → Informationen zum ISMS sind in der ISO 27000 Familie spezifiziert
- → Die ISO 27000 Familie umfasst mehrere, sich gegenseitig unterstützende, Standards
- → Ein ISMS kann mittels der ISO 27000 Familie von externen Gutachtern zertifiziert werden



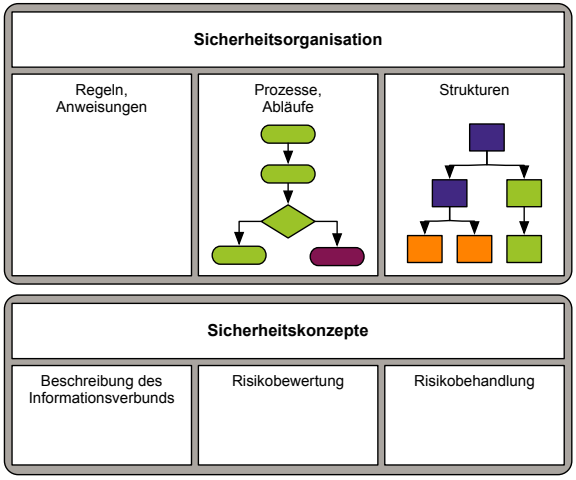
ISO/IEC 27002

Best Practice Sammlung zur Umsetzung eines ISMS

- Enthält Abschnitte zu:
  - Weisungen und Richtlinien zur Informationssicherheit
  - Organisatorische Sicherheitsmaßnahmen und Managementprozesse
  - Verwaltung und Klassifizierung von Assets
  - Personelle Sicherheit
  - Physikalische Sicherheit und öffentliche Versorgungsdienste
  - Netzwerk- und Betriebssicherheit (Daten und Telefonie)
  - Zugriffskontrolle
  - Systementwicklung und Wartung
  - Umgang mit Sicherheitsvorfällen
  - Notfallversorgung
  - Einhaltung rechtlicher Vorgaben, der Sicherheitsrichtlinien und Audits

BSI STANDARD 200-X ÜBERSICHT

- → **200-1:** Managementsystem für Informationssicherheit
- → **200-2:** IT-Grundschutz-Methodik
- → **200-3:** Risikomanagement
- → **100-4:** Notfallmanagement
- → **200-4:** Business Continuity Management (Community Draft)



COMMON CRITERIA

- Standard zur Bewertung der Sicherheit von IT-Produkten
  - Zertifizierung aus Eigeninitiative (z.B: Alleinstellungmerkmal)
  - Zertifizierung nötig für den Einsatz in manchen Branchen

- CC Zertifizierungen sind zweigeteilt in:
  - **Protection Profile (PP):** Beschreibung der Sicherheitsfunktionalität
  - **Evaluation Assurance Level (EAL):** Vertrauenswürdigkeit in die Umsetzung der Sicherheitsfunktionalität (EAL1 bis EAL7)

- Beispiele für EAL Stufen
  - **EAL1:** Produkt wurde gegen die Spezifikation getestet und eine Dokumentation existiert
  - **EAL3:** Es werden zusätzlich methodische Security-Tests durchgeführt
  - **EAL7:** Produkt wurde formal designed, verifiziert und getestet. Beispiel: [Diod]

COMMON CRITERIA - BEISPIEL

- Gesundheitsanwendungen in Deutschland werden mittels „sicherer Router“ an die Telematikinfrastruktur (TI) angebunden [KoCoBox]

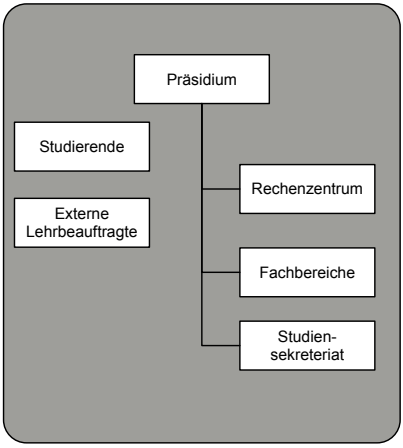
- Für diese Router existiert das CC Profil [PP0098]
  - Umfasst u.a. die Funktion “Sichere Verbindung”
  - Router müssen nach EAL3 zertifiziert sein

Wert	zu schützende Eigenschaften des Wertes	Erläuterung, ⇒ davon abgeleitete Bedrohungen und Annahmen
Authentisierungs-geheimnisse bei der Speicherung und Bearbeitung im EVG	Integrität, Vertraulichkeit	Die Vertraulichkeit und Integrität von Authenti-sierungsgeheimnissen (z. B. Passwort für Administratorauthentisierung, evtl. PIN für die gSMC-K) ist zu schützen. ⇒ A.AK.Konnektor, A.AK.Admin_EVG, A.AK.phys_Schutz

IMPLEMENTIERUNG EINES ISMS FÜR COMPASS

→ Zertifizierung der IT-Sicherheit wird in Zukunft größere Rolle spielen [KoalVertrag]:
"Wir verpflichten alle staatlichen Stellen ... sich regelmäßig einer externen Überprüfung ihrer IT-Systeme zu unterziehen."

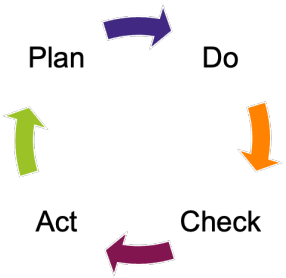
→ Wir wollen ein ISMS implementieren, um für zukünftige Rechtsnormen gewappnet zu sein



UMSETZEN EINES ISMS

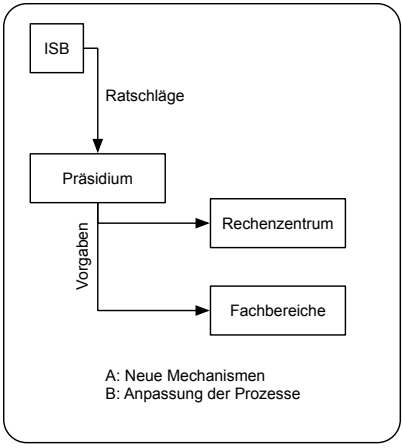
1. **Initial: ISMS** Definieren
   - 1.1 Management Support einholen und Rollen besetzen
   - 1.2 Relevante Gesetze identifizieren
   - 1.3 Umfang des ISMS definieren

2. **Wiederkehrend:** ISMS Durchlaufen
   - 2.1 **Plan:** Risikomanagement durchführen
   - 2.2 **Do:** Maßnahmen implementieren, Ressourcen allozieren und Mitarbeitende schulen
   - 2.3 **Check:** ISMS überwachen und Maßnahmen gegen definierte Kennzahlen prüfen
   - 2.4 **Act:** Verbesserungen am ISMS identifizieren



INITIAL: MANAGEMENT SUPPORT EINHOLEN UND ROLLEN BESETZEN

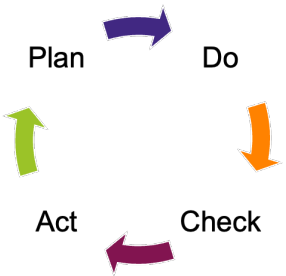
- → Ein ISMS wird Top-Down implementiert
  - → Unternehmensleitung spezifiziert grobe **Richtlinien**, um Bedrohungen zu adressieren
  - → Betroffene Bereiche müssen **Prozesse** und **technische Maßnahmen** implementieren, um Konformität mit Richtlinie zu erreichen
- → Relevante Rollen vergeben
  - → Informationssicherheitsbeauftragter (ISB)
  - → Ansprechpartner für Organisationseinheiten



INITIAL: UMFANG DES ISMS DEFINIEREN

→ Der ISMS Umfang definiert **schützenswerte Kernprozesse** und **organisatorische Einheiten**, die Maßnahmen umsetzen müssen

→ Umfang des ISMS sollte von der Organisationsleitung abgenommen werden



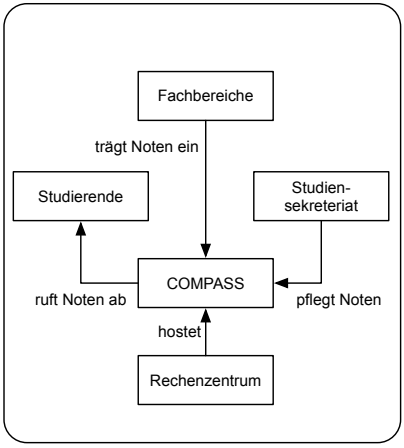
KERNPROZESSE UND UMFÄNGE FÜR COMPASS

Tauschen Sie sich mit Ihrem Sitznachbar 3 Minuten aus:

→ Überlegen Sie, was die Kernprozesse von COMPASS sind und welche Schutzziele für die Kernprozesse benötigt werden.

INITIAL: UMFANG DES ISMS FÜR COMPASS DEFINIEREN

- → Kernprozesse einer Hochschule:
  - → Bewerbung und Zulassung
  - → Studierendenmanagement
  - → Lehre, Prüfungen (und Forschung)
- → Beispielprozess:
  - → Notenmanagement
- → Bestätigung des Umfangs:
  - → "Ein Ziel des ISMS der HSRM ist der Schutz der **Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität** des Kernprozesses **Lehre und Prüfungen** und umfasst das Studienbüro, das Rechenzentrum und die Fachbereiche."

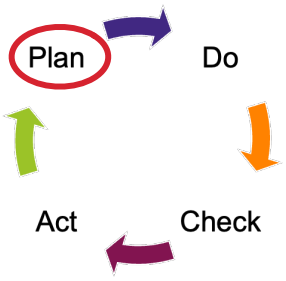


PLAN: RISIKOMANAGEMENT DURCHFÜHREN

- → **Zentrale Aufgabe:**
  - → Identifikation der konkreten Angriffe und Bedrohungen für den ISMS
  - → Umfang und Aufstellen einer Maßnahmenplanung

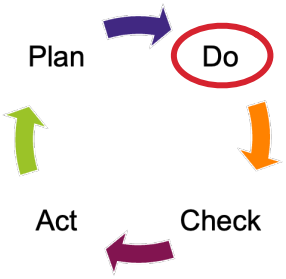
- → **Ergebnis:**
  - → Priorisierte Liste an technischen- und Prozessmaßnahmen zum Schutz vor Bedrohungen
  - → Verifikationskriterien für die Maßnahmen

- → **Beispiel:**
  - → Maßnahme: Sicheres Backup zum Wiederherstellen des COMPASS Notensystems
  - → Verifikation: Probedurchlauf Wiederherstellung von COMPASS in <= 1 Tag



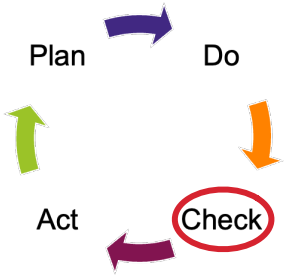
DO: MASSNAHMEN IMPLEMENTIEREN

- → **Zentrale Aufgabe:**
  - → Identifizierte Maßnahmen implementieren und Erkenntnisse zur Umsetzung gewinnen
- → **Ergebnis:**
  - → Technische- und Prozessmaßnahmen sind auf Basis der Vorgaben umgesetzt
- → **Beispiel:**
  - → Backuplösung wurde angeschafft, in Infrastruktur integriert und läuft täglich
  - → Prozesse zum Wiedereinspielen wurden definiert



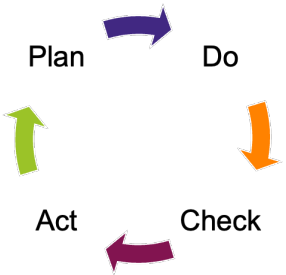
CHECK: MASSNAHMEN ÜBERPRÜFEN

- → **Zentrale Aufgabe:**
  - → Effektivität und Einhaltung der Maßnahmen überprüfen
  - → Verbesserungspotential identifizieren
- → **Ergebnis:**
  - → Feedback über Effektivität und Verbesserungspotential
- → **Beispiel:**
  - → Backup benötigt 2 Tage statt, wie geplant maximal 1 Tag
  - → Fehlende Einträge in COMPASS Notendatenbank beim Re-import
  - → Noch nicht bewertete Klausuren werden vom Backupsystem nicht gespeichert



ACT: VERBESSERUNGEN UMSETZEN

- **Zentrale Aufgabe:**
  - Identifizierte Verbesserungen am ISMS Prozess umsetzen
  - Änderungen kommunizieren und prüfen
- **Ergebnis:**
  - Änderungen am ISMS Umfang und Vorgehen
- **Beispiel:**
  - Es wird mehr Bandbreite zu den **Backupsystemen** benötigt
  - Digitales Prüfungssystem, betrieben von Dienstleistung Lehre & Studium, muss auch vom ISMS Umfang abgedeckt werden



LANGFRISTIGES ZIEL DES ISMS

→ Ziel des ISMS ist eine langfristige Absicherung durch inkrementelle Verbesserungen
   1. Passt sich mit der Zeit an die individuellen Bedürfnisse der Organisation an
   2. PDCA Zyklus sollte z.B. alle 1-2 Jahre durchgeführt werden
   3. Bestehende Maßnahmen sollten regelmäßig überprüft werden

→ Alle Schritte des ISMS sollten ausreichend dokumentiert werden

→ Die Qualität eines ISMS kann mittels Reifegradmodellen gemessen werden

Quelle: RGM- letzter Besuch 26.03.2023

ZUSAMMENFASSUNG

- → Gesetze und Standards im Bereich der IT-Sicherheit
- → Zusammenspiel zwischen Gesetzen und Standards
- → Relevante Rollen sowie den Inhalt des Umfangs im ISMS
- → Hintergrund des PDCA Zyklus im ISMS