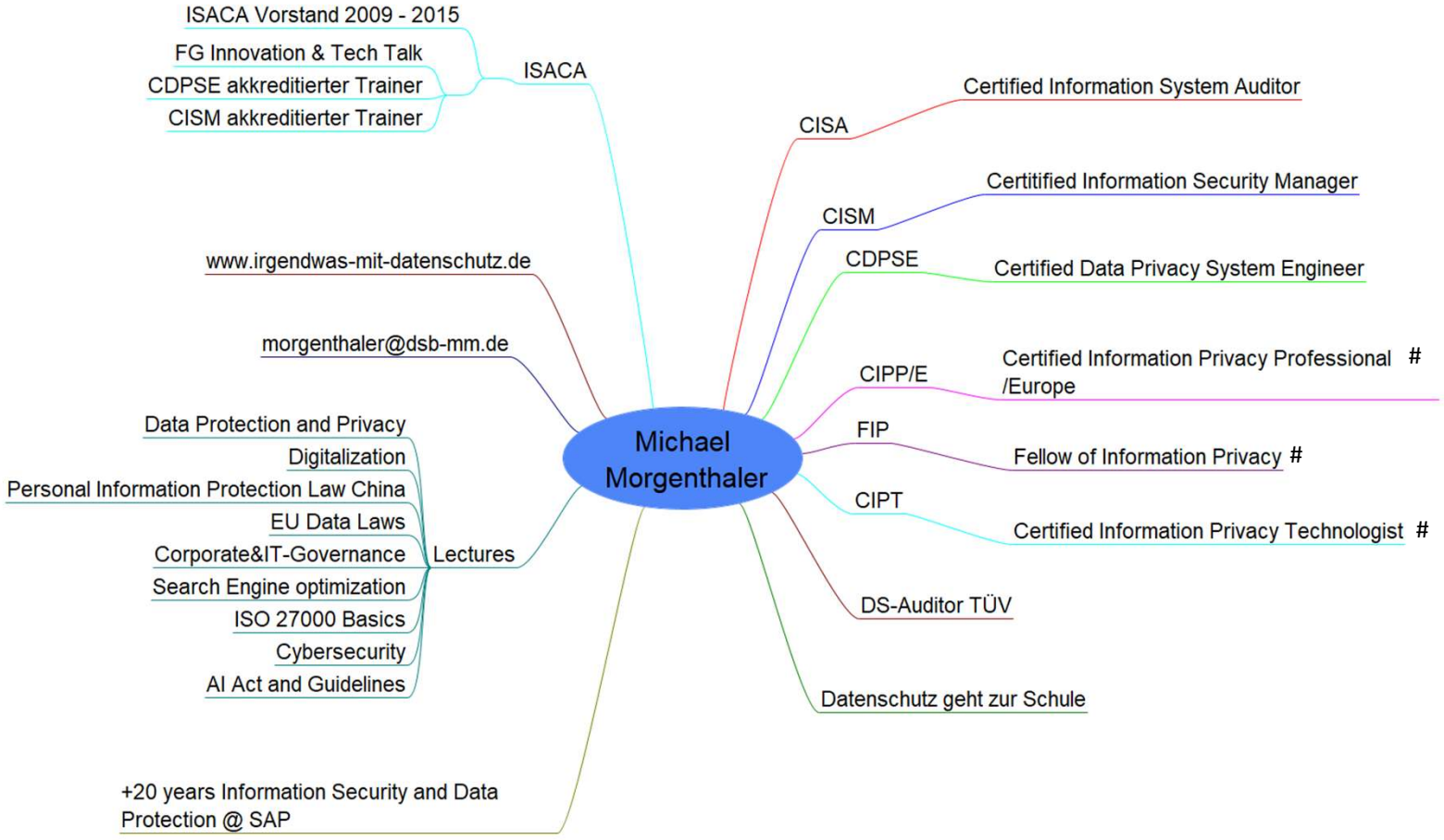
ISO/IEC 27701 - Grundlagen des Datenschutz-Managements

MICHAEL MORGENTHALER
CISA, CISM, CDPSE, DS-AUDITOR (TÜV)

Danke, das ich hier sein darf..



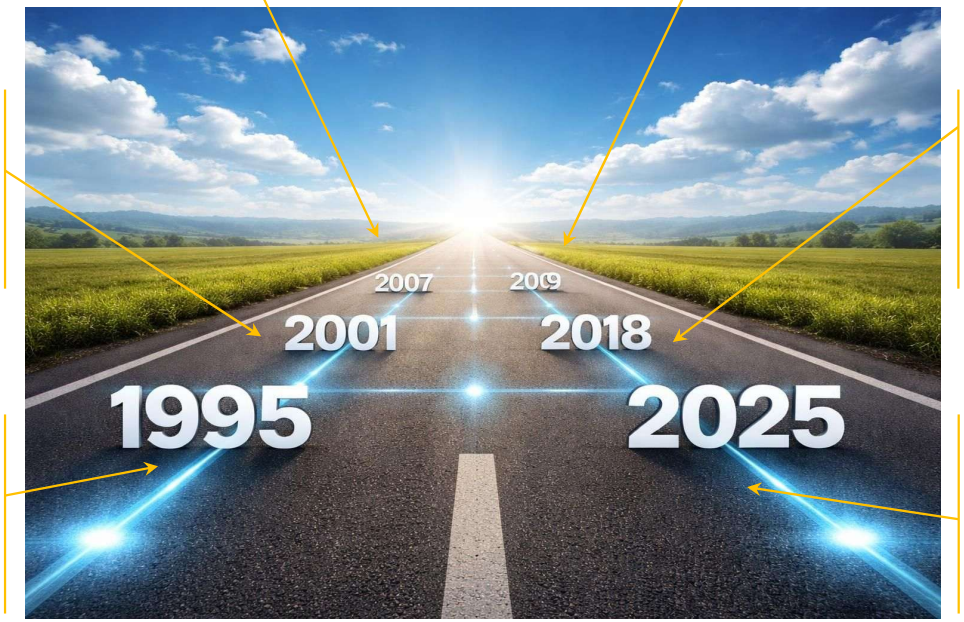
certified till 12/2025 only

Ein langer Weg…

Referentenentwurf für ein „Bundesdatenschutzauditgesetz“

Juli 2009: Auditgesetz im Bundesrat gescheitert
August 2009 BDSG Novelle insb. §11 zur Auftragsverarbeitung

Novelle des BDSG
§ 9a Datenschutzaudit
…werden durch besonderes Gesetz geregelt



DSGVO
Verordnung (EU) 2016/679
BDSG n.F. §9a gestrichen

Richtlinie 95/46/EG

ISO 27701

Bild mit DUCK.AI generiert; Prompt: eine Strasse mit einem Zeitstrahl, die Werte für 1995, 2001, 2007, 2009, 2018 und 2025 werden aufsteigend von links nach rechts angezeigt

Zertifizierungen

Artikel 42 DSGVO Zertifizierung

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

Bildquelle Pixabay – Gerd Altmann

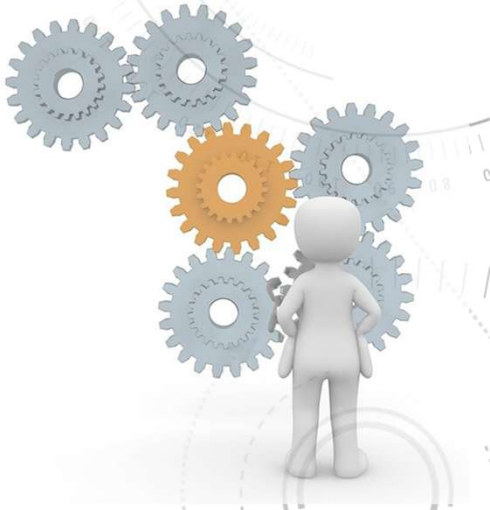
z.B. AUDITOR gemäß Art 28 DSGVO für Cloudanbieter
European Privacy Seal (EuroPriSe) für Unternehmen

Managementsysteme

- Qualitätsmanagement, ISO 9001, Umweltmanagement, ISO 14000, Sicherheitsmanagement, Gesundheitsmanagement,
- Arbeitsschutzmanagement, Performance Management, Performance Measurement, Risikomanagement, Sicherheitsmanagement, Finanzmanagement, Nachhaltigkeitsmanagement,
- Energiemanagement, Kundenmanagement, Personalmanagement, Lieferantenmanagement, Informationsmanagement, Wissensmanagement, Innovationsmanagement,
- Baumanagement, Mess-Management, Datenschutz-Management, Informationssicherheits-Management

Managementsysteme

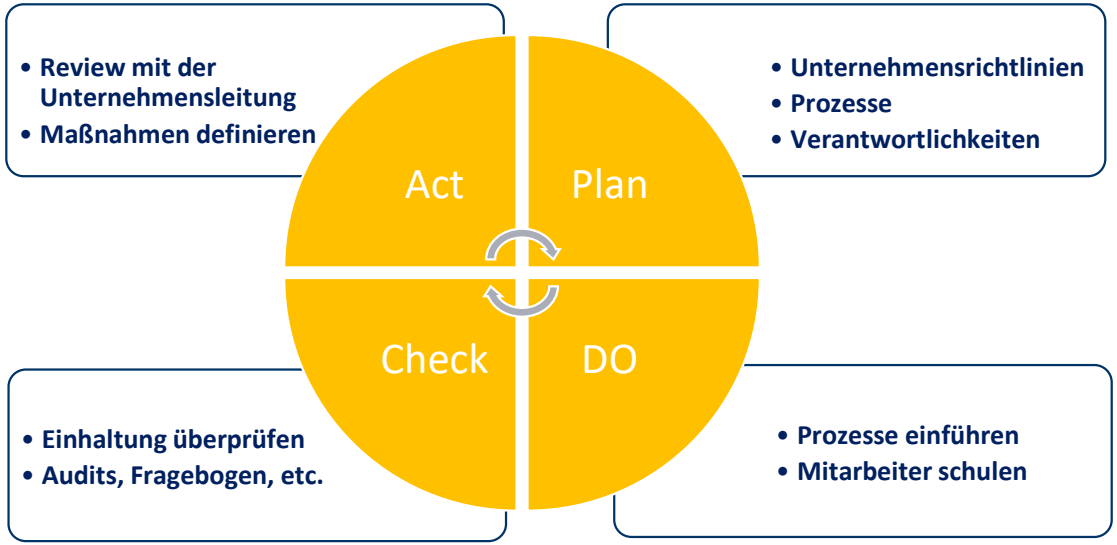
- Standardisierte Vorgaben zur Organisation, Dokumentation, zu Prozessen und Verfahren im Unternehmen
- Eindeutig abgegrenzte Anwendungsbereiche
- Standards formulieren Anforderungen zur Überprüfung und Zertifizierung
- Häufig in Form einer Norm erstellt/veröffentlicht durch Standardisierungs-Organisationen (ISO, DIN,..)
- Angestrebtes Ziel: die Ziele des Unternehmens für den Anwendungsbereich sind definiert und werden mittels der Anwendung des Managementsystems dauerhaft erreicht
- Per se keine technischen Systeme, sondern ein System zusammenwirkender Maßnahmen



Bildquelle: Pixabay
Peggy + Marco Lachmann

Kontinuierlicher Verbesserungs-Prozess (PDCA)

- Iterativer Ansatz, der es ermöglicht das ein eingeführtes Management-System nicht statisch bleibt, sondern sich stets verbessert
- Damit lassen sich geänderte Gesetze, Unternehmensziele oder auch durch Audits oder Sicherheitsvorfälle festgestellte Missstände in die Prozesse integrieren und verbessern die Prozesse



Datenschutzmagementsystem (DSMS)

Ziel: Einhaltung der Datenschutzgesetze und der Nachweis nach Art 5 (2) DSGVO

Für das Unternehmen

- Rechtssicherheit und Nachweis
- Reduzierung der Vorfälle mit Personenbezogene Daten
- Prozesse nach anerkannten, überprüfbaren Standards (Effizienz)

Für Externe

- Nachweise des Ist-Zustandes als Auftragsverarbeiter
- Vertrauensbildung bei den Kunden

Bildquelle: Pixabay
Peggy + Marco Lachmann

Datenschutzmagementsystem (DSMS)

Ziel: Einhaltung der Datenschutzgesetze und der Nachweis nach Art 5 (2) DSGVO

Für einen strukturierten Ansatz zum wirksamen Management des Datenschutzes ist zu klären:

- Was soll das DSMS schützen?
- Welche Regelungen sind anzuwenden?
- Wie dokumentiert und überwacht man Regeln nachvollziehbar?
- Welche Zuständigkeiten gibt es im DSMS?
- Konkrete Maßnahmen, um das erforderliche Niveau zu erreichen

Bildquelle: Pixabay
Peggy + Marco Lachmann

Standard

- Einheitliche Art und Weise etwas zu beschreiben, herzustellen oder durchzuführen
- Kann sich auf Ziele oder Realisierungen beziehen
- Formal beschrieben in Form einer Norm (Normung oder Normierung)
  - Essentielle Merkmale werden durch offizielle Normengremien zusammengestellt und mittels Abstimmungsverfahren verabschiedet
  - Umgangssprachlich aber auch verwendet für faktische Festlegungen in der Praxis, z.B. durch Unternehmen gesetzte „Standards“, De-Facto-Standards
  - Anwendung kann zur Zielerreichung verpflichtend (normativ) oder informativ/optional sein

Bildquelle: Pixabay - Gerd Altmann

ISO 27000-Standardfamilie (Auswahl)

ISO/IEC 27000-Familie: eine Reihe von Standards, deren Fokus auf Best-Practice-Empfehlungen zur Organisation der Informationssicherheit im Kontext eines Information Security Management Systems (ISMS) liegt

Normative Standards

- ISO 27001
- ISO 27006
- ISO 27009
- ISO 27701:2025

Sektorspezifisch/Maßnahmenspezifisch

- ISO 27010
- ISO 27011
- ISO 27017
- ISO 27019
- ISO 27031
- ISO 27032
- ISO 27033

Nicht-Normative Standards

- ISO 27002
- ISO 27003
- ISO 27004
- ISO 27005
- ISO 27007
- ISO 27013
- ISO 27014
- ISO 27016
- ISO 27018

ISO 27701:2025

Oktober 2025

- Ursprünglich: ISO/IEC 27701:**2019** als Erweiterung/Ergänzung zu ISO 27001
- ISO/IEC 27701 ist nun eine **eigenständige Norm**
- bestehend aus Elementen der bisherigen Normen ISO/IEC 27701:2019, ISO/IEC 27001:2022 und ISO/IEC 27002:2022.
- lässt sie sich in andere bestehende Managementsysteme wie ISO 9001, ISO/IEC 27001 und ISO/IEC 42001 integrieren
- Umfassende **Datenschutzkontrollen** für Verantwortliche als auch für Auftragsverarbeiter und **Leitlinien zur Umsetzung** und Aufrechterhaltung eines PIMS
- Zu beachten: ISO/IEC 29100:2024-02 Privacy Framework
  DIN ISO 31000:2018-10 Risiko-Management - Leitlinien

Bildquelle: Pixabay
Peggy + Marco Lachmann

Quellen:
https://www.iso.org/standard/27701 ab 225,- CHF
www.dinmedia.de/de/norm/din-en-iso-iec-27701/ ab 204,- €

ISO 27701:2025 <=> DIN EN ISO/IEC 27701:2026-02

Februar 2026

- **ISO/IEC 27701:2025** englische Fassung der ISO

  Information security, cybersecurity and privacy protection - Privacy information management systems - Requirements and guidance (ISO/IEC 27701:2025)

- **EN ISO/IEC 27701:2025** identische englische Fassung als Europäische Norm

- **DIN EN ISO/IEC 27701:2026-02** deutsche Fassung

  Informationssicherheit, Cybersicherheit und Datenschutz - Datenschutz-Managementsysteme - Anforderungen und Hinweise (ISO/IEC 27701:2025); Deutsche Fassung der EN ISO/IEC 27701:2025

Bildquelle: Pixabay
Peggy + Marco Lachmann

Quellen:
https://www.iso.org/standard/27701 ab 225,- CHF
www.dinmedia.de/de/norm/din-en-iso-iec-27701/ ab 204,- €

ISO27701 Kapitelstruktur

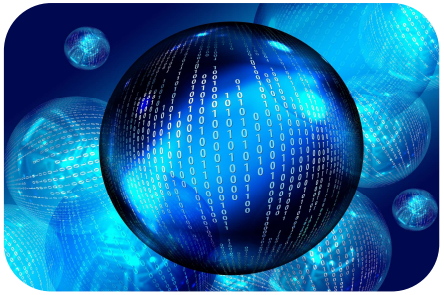
Organisation

Führung

Planung

Unterstützung

Betrieb



Bewertung

Verbesserung

Anhänge

ISO27701 Kap 4

Organisation

- Welche externen und internen Faktoren beeinflussen die Ausrichtung des Unternehmens?
- Wer nimmt intern oder extern Einfluss auf die Organisation?
- Welche Teile der Organisation sollen durch das DSMS verwaltet werden?
- Das DSMS muss alle Anforderungen der Norm erfüllen und gemäß dem PDCA-Zyklus aufrechterhalten werden.

ISO27701 Kap 4 und 5

Organisation

- Welche externen und internen Faktoren beeinflussen die Ausrichtung des Unternehmens?
- Wer nimmt intern oder extern Einfluss auf die Organisation?
- Welche Teile der Organisation sollen durch das DSMS verwaltet werden?
- Das DSMS muss alle Anforderungen der Norm erfüllen und gemäß dem PDCA-Zyklus aufrechterhalten werden.

Führung

Aufgaben, die durch die Leitung der Organisation durchzuführen sind, damit das DSMS dauerhaft, wirkungsvoll und erfolgreich umgesetzt werden kann.

- Unterstützung durch das Management
- Integration in die Organisationsprozesse
- Verabschiedung einer Unternehmensrichtlinie
- Festlegen von Verantwortlichkeiten

ISO27701 Kap 6

Planung

Definiert wie das Unternehmen Chancen und Risiken erfasst und bewertet. Das Risikomanagement bezogen auf Datenschutzrisiken ist der zentrale Ansatzpunkt.

- Bestimmen der Chancen und Risiken
- Maßnahmen die risikobasiert zu ergreifen sind
- Prozess des Risiko-Managements in Bezug auf personenbezogene Daten
  - Ermittlung der Risiken
  - Risikobeurteilung
  - Risikobehandlung

ISO27701 Kap 6

Planung

Definiert wie das Unternehmen Chancen und Risiken erfasst und bewertet. Das Risikomanagement bezogen auf Datenschutzrisiken ist der zentrale Ansatzpunkt.

- Bestimmen der Chancen und Risiken
- Maßnahmen die risikobasiert zu ergreifen sind
- Prozess des Risiko-Managements in Bezug auf personenbezogene Daten
  - Ermittlung der Risiken
  - Risikobeurteilung
  - Risikobehandlung

Risikobeurteilung

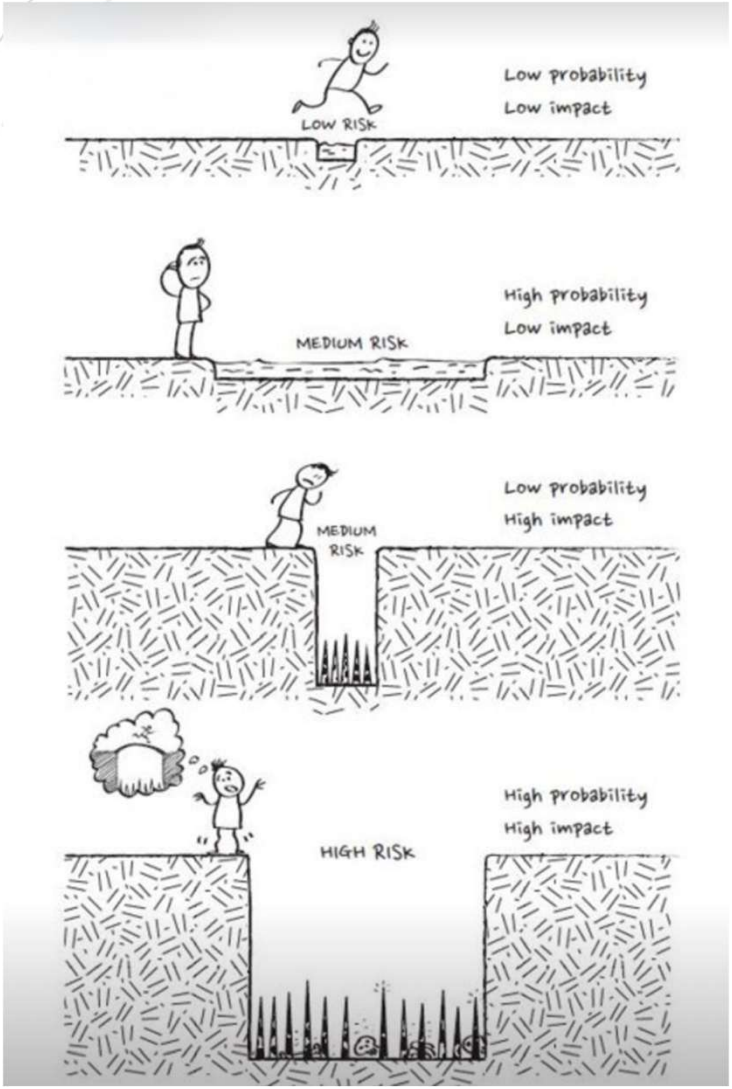
Das Unternehmen definiert seine individuelle Risikomatrix, die dazugehörigen Metriken und die Schwellwerte für die Einordung.

Risiko = Eintrittswahrscheinlichkeit * Auswirkung

Risikokategorie	Ereignis	Auswirkung	Wahrschein-lichkeit (1-5)	Schaden (1-4)	Risiko
Unbefugter Zugang zu pb Daten	Unbefugte beim DL erhalten Zugang	Imageschaden, Bußgeld, Wettbewerbs-nachteil	3	3	9

Eintrittswahrscheinlichkeit

Auswirkung	Selten	Niedrig	Mittel	Hoch	Sehr hoch
Katastrophal	Mittel	Mittel	Hoch	Sehr hoch	Sehr hoch
Schwerwiegend	Niedrig	Mittel	[illegible]	Hoch	Sehr Hoch
Tragbar	Niedrig	Niedrig	Mittel	Mittel	Hoch
Irrelevant	Minimal	Niedrig	Niedrig	Mittel	Mittel



Bildquelle: Marcel Hofmann

ISO27701 Kap 6

Planung

Im Rahmen der Risikobehandlung sind Maßnahmen zu ergreifen. Die Norm liefert in Anhang A einen Maßnahmenkatalog. Die Organisation muss erklären

- Welche Maßnahmen zur Informations-Sicherheit umgesetzt sind, welche zur Behandlung der Datenschutzrisiken erforderlich sind und dies begründen
- Wenn Maßnahmen nicht umgesetzt werden, ist dies zu begründen und zu dokumentieren.

Die Maßnahmen sind wesentliches Kriterium für eine Zertifizierung.

Risikobeurteilung

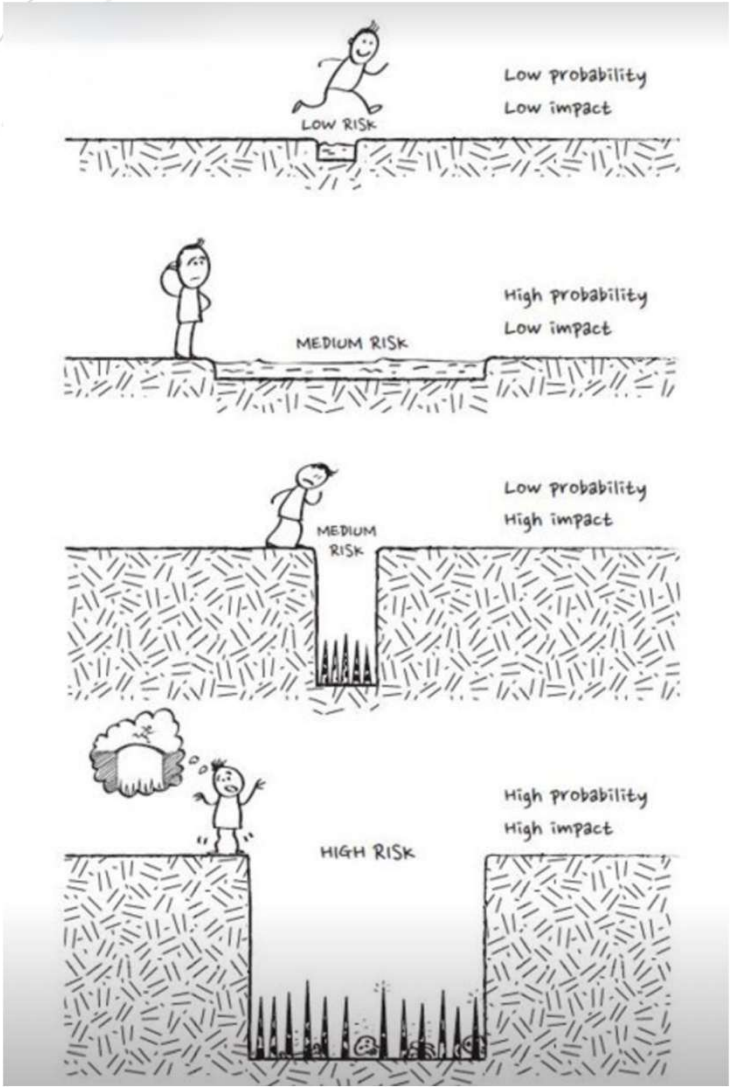
Das Unternehmen definiert seine Risikomatrix, die dazugehörigen Metriken und die Schwellwerte für die Einordung.

Risiko = Eintrittswahrscheinlichkeit * Auswirkung

Nach der Zuordnung der Maßnahmen wird das verbleibende Risiko bewertet und geprüft, ob es damit akzeptabel ist (gemäß festgelegten Kriterien)

Eintrittswahrscheinlichkeit

Auswirkung	Selten	Niedrig	Mittel	Hoch	Sehr hoch
Katastrophal	Mittel	Mittel	Hoch	Sehr hoch	Sehr hoch
Schwerwiegend	Niedrig	Mittel	Mittel	Hoch	Sehr Hoch
Tragbar	Niedrig	N[illegible]	Mittel	Mittel	Hoch
Irrelevant	Minimal	Niedrig	Niedrig	Mittel	Mittel



Bildquelle: Marcel Hofmann

ISO27701 Kap 6 und 7

Planung

Definiert wie das Unternehmen Chancen und Risiken erfasst und bewertet. Das Risikomanagement bezogen auf Datenschutzrisken ist der zentrale Ansatzpunkt.

- Bestimmen der Chancen und Risiken
- Maßnahmen die risikobasiert zu ergreifen sind
- Prozess des Risiko-Managements in Bezug auf personenbezogene Daten
  - Ermittlung der Risiken
  - Risikobeurteilung
  - Risikobehandlung

Unterstützung

Vorgaben zur Unterstützung finden sich ähnlich in anderen Managementsystemen. Sie beziehen sich auf allgemeine Anforderungen, die nicht DS spezifisch sind

- Ressourcen
- Wissen/Knowhow
- Kommunikation
- Dokumentation

ISO27701 Kap 8

Betrieb

Nicht Betrieb eines IT Systems, sondern Betreiben der Prozesse des DSMS.

- Prozesse
- Geplante Änderungen steuern und Folgen ungeplanter Änderungen beurteilen
- Umsetzungspläne mit timelines
- Dokumentation

ISO27701 Kap 8 und 9

Betrieb

Nicht Betrieb eines IT Systems, sondern um die Prozesse des DSMS.

- Prozesse
- Geplante Änderungen steuern und Folgen ungeplanter Änderungen beurteilen
- Umsetzungspläne mit timelines
- Dokumentation

Bewertung

Der erreichte Stand und die Wirksamkeit des DSMS muss überprüft und die Ergebnisse adressiert werden (Check“ des PDCA).

- Bewertung des DSMS und seiner Prozesse
- Wirksamkeit
- Ziele der Überwachung
- Kennzahlen
- Auditprogramm
- Managementbewertung

ISO27701 Kap 10

Verbesserung

die Prozesse, die zur kontinuierlichen Verbesserung („Act“) führen

- Konformität/Nicht-Konformität
- Korrekturen
- Maßnahmenbewertung
- Eignung und Wirksamkeit fortlaufend verbessern

ISO27701 Kap 10 und Anhänge

Verbesserung

die Prozesse, die zur kontinuierlichen Verbesserung („Act“) führen

- Konformität/Nicht-Konformität
- Korrekturen
- Maßnahmenbewertung
- Eignung und Wirksamkeit fortlaufend verbessern

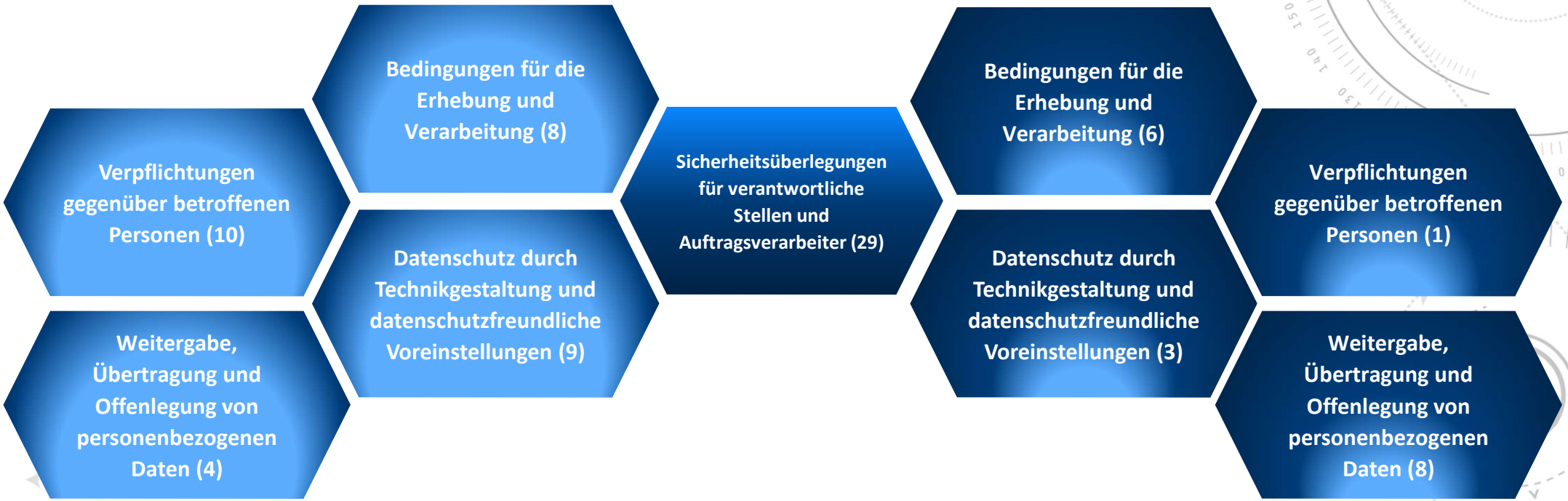
Anhänge

Anhang A (normativ) DSMS-Referenzmaßnahmenziele und -Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter
Anhang B (normativ) Hinweis zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter
Anhang C (informativ) Zuordnung zu ISO/IEC 29100
Anhang D (informativ) Zuordnung zur Datenschutz-Grundverordnung
Anhang E (informativ) Zuordnung zu ISO/IEC 27018 und ISO/IEC 29151
Anhang F (informativ) Übereinstimmung mit ISO/IEC 27701:2019

Maßnahmenziele und Maßnahmen

….für verantwortliche Stellen

…. für Auftragsverarbeiter



Die Organisation kann weitere Maßnahmen definieren und ins DSMS aufnehmen.

Maßnahmenziele und Maßnahmen

….für verantwortliche Stellen

Maßnahmenziele und Maßnahmen

….für verantwortliche Stellen

Laut Kap. 6.1.3 Risikobehandlung ist jede Maßnahme zu bewerten, ob sie angewendet wird oder nicht und dies ist jeweils zu begründen und zu dokumentieren.

Maßnahmenziele und Maßnahmen

….für verantwortliche Stellen

Die Organisation muss immer dann, <…>, die Notwendigkeit einer Datenschutz-Folgenabschätzung bewerten <…>.

Maßnahmenziele und Maßnahmen

Anhang B (normativ): Hinweis zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter

Die Verarbeitung von personenbezogenen Daten erzeugt Risiken für betroffene Personen. Diese Risiken sollten durch eine Datenschutz-Folgenabschätzung beurteilt werden. <…>.

Die Organisation sollte die Elemente bestimmen, die für den Abschluss einer Datenschutz-Folgenabschätzung notwendig sind. <…>

Weitere Anhänge

Anhang C

- Aufgeteilt in 2 Unterkapitel werden die Zuordnung der Maßnahmen aus Anhang A zu den Datenschutzprinzipien der ISO/IEC 29100 gemapped

Anhang D

- Tabellarische Aufstellung der Kapitel und Anhänge der Norm im Vergleich zur DSGVO

Anhang E

- Zuordnung der Kapitel und Anhänge der Norm zu ISO/IEC 27018 (zum Schutz personen-bezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung) und ISO/IEC 29151 (Leitfaden für den Schutz personenbezogener Daten)

Anhang F

- Beidseitiges tabellarisches Mapping ISO27701:2019 zu ISO 27701:2025 und umgekehrt, für bereits eingeführte DSMS basierend auf ISO 27701:2019)

Zertifizierung
=
Konformitätsbewertungsprogramm

Zertifizierung vs Akkreditierung

Zertifizierung

- Audit eines Unternehmens(-teils) durch einen Zertifizierer und Bestätigung der Einhaltung der Norm

Akkreditierung

- „Zertifizierer der Zertifizierer“ gewährt Unternehmen das Recht, Zertifizierungen durchzuführen und Zertifikate zu erstellen
- Unternehmen wird so zum **Zertifizierer**
- Zertifikate sind gegenseitig anerkannt
- In Deutschland ist die **Deutsche Akkreditierungsstelle GmbH** als nationale Akkreditierungsstelle hierzu berechtigt (=> https://www.dakks.de/)

Bildquelle: Pixabay sclker-free-vector-images

Zertifizierung vs Akkreditierung

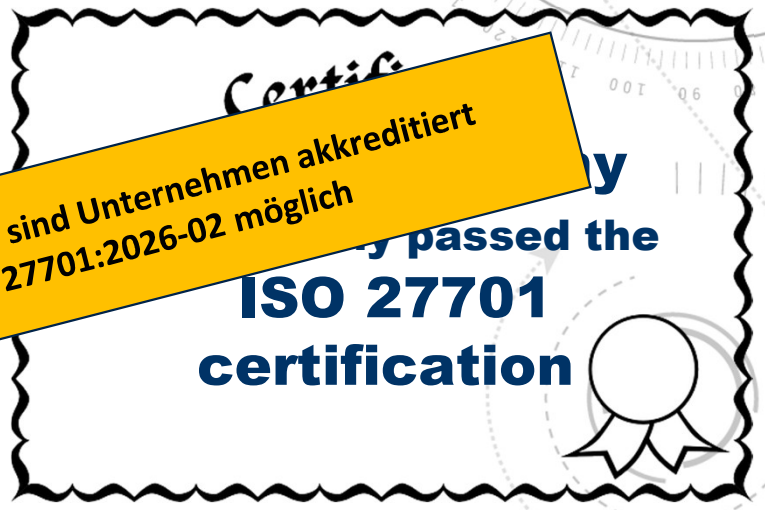
Zertifizierung

- Audit eines Unternehmens(-teils) durch einen Zertifizierer und Bestätigung der Einhaltung der Norm

Akkreditierung

- „Zertifizierer der Zertifizierer“ gewährt Unternehmen das Recht, Zertifizierungen durchzuführen und Zertifikate zu erstellen
- Unternehmen wird so zum **Zertifizierer**
- Zertifikate sind gegenseitig
- In Deutschl… …sstelle GmbH als … …erzu berechtigt
  …ks.de/)

März 2026: Derzeit weder die Grundlagen der Akkreditierung definiert noch sind Unternehmen akkreditiert
=> keine Zertifizierung gegen ISO/IEC 27701:2025 oder DIN EN ISO 27701:2026-02 möglich



Bildquelle: Pixabay sclker-free-vector-images

Übersicht: https://www.dakks.de/de/akkreditierte-stellen-suche.html

Zertifizierung

- Zur Zertifizierung/Zertifikatserteilung ist ein externes, von akkreditierten Zertifizierern durchgeführtes Audit zwingend notwendig
- Geprüft wird die Einhaltung des Standards ISO 27701 auf Basis des definierten Anwendungsbereiches
- Werden keine Defizite festgestellt, wird das Zertifikat erteilt
- Bei Defiziten werden diese im Auditbericht erfasst inkl. Vorschlägen zur Verbesserung

Bildquelle: Pixabay sclker-free-vector-images

Auditscope

- Bezogen auf definierten Anwendungsbereich des DSMS
- Abgeleitet aus der Erklärung zur Anwendbarkeit des Standards (Statement of Applicability) => Kap 4
- Beinhaltet auch die Prüfung, ob Erklärung angemessen
- Das Audit beinhaltet immer alle Inhalte der Kap 4-10 und der Maßnahmen aus den Anhängen
- Der Auditscope wird mit dem Zertifikat dokumentiert

Bildquelle: Pixabay sclker-free-vector-images

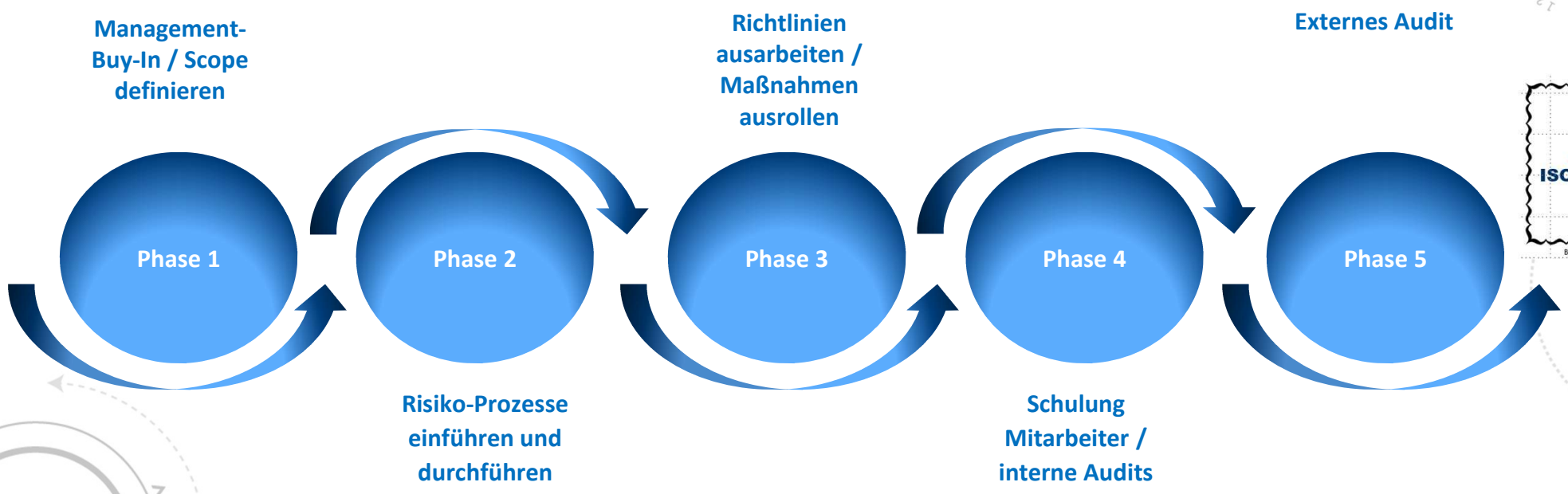
Auditbericht

- Beinhaltet alle im Audit getroffenen Beobachtungen
- Feststellung von
  - Verbesserungen zum vorherigen Audit
  - Sehr wichtigen Abweichungen (major non conformity)
  - Wichtigen Abweichungen ((minor) non conformity)
  - etc.

Bildquelle: Pixabay sclker-free-vector-images

Next Steps

- Weitere Entwicklung zur Zertifizierung beachten
- Stellungnahmen der Aufsichtsbehörden beachten
- Prozesse starten (Phasen exemplarisch) – andere MS im Unternehmen beachten



Vielen Dank für Ihre Aufmerksamkeit!

Kontakt: morgenthaler@dsb-mm.de oder via LinkedIn