2026 CAMPUS TAGE

DSN Akademie

10 Jahre DSGVO

Und jetzt?
Gemeinsam weiterdenken!

DSN Akademie

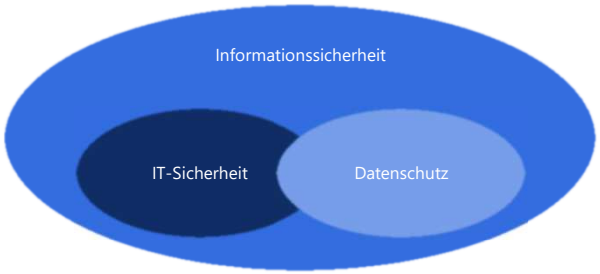
ISMS in der Theorie -
Ein normativer Blick in die Begrifflichkeit

Julius Seyer
Berater Informationssicherheit

datenschutz nord Gruppe
T +49 (0)40 59 36 160 417
E-Mail jseyer@datenschutz-nord.de

www.dsn-group.de

Was ist Informationssicherheit?



DSN Akademie

?

Themenbereiche und Schnittstellen

DSN Akademie

- Kapazitätssteuerung
- Netzwerksicherheit
- Räume- und Gebäudemanagement
- Notfall- und Krisenmanagement
- **Informationssicherheit**
- Anwendungsverwaltung
- Sensibilisierung
- Zugriff-, Zutritt- und Zugangskontrolle
- Personalsicherheit
- Operative Technik (OT)
- Compliance

ISMS
Grundidee

- „Managementsystem" umfasst **alle Regelungen**, die für die Zielerreichung der Organisation sorgt.
- Managementsystem für Informationssicherheit wird als **Informationssicherheits-Managementsystem (ISMS)** bezeichnet.
- „Information" als Wert umfasst **nicht nur IT**, sondern **alle Aspekte der Sicherung der Informationswerte** einer Organisation.
- Informationssicherheit basiert auf **dauerhafter Erfüllung** von **Anforderungen** und **nachhaltiger Begrenzung der Risiken**.
- Ein ISMS legt fest, mit welchen **Instrumenten und Methoden** das Management der Organisation die auf Informationssicherheit ausgerichteten Aktivitäten **nachvollziehbar lenkt** (plant, einsetzt, durchführt, überwacht und verbessert).

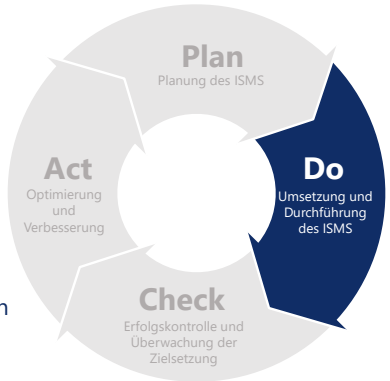
PDCA-Zyklus
(aka Deming Cycle)

PDCA
Plan

Planung:
- Sicherheitsleitlinie
- Organisation
- Ziele
- Geltungsbereich

PDCA
Do

Umsetzung der Planung, Durchführung:
- Sicherheitskonzept
- Werteinventar
- Schutzbedarfsanalyse
- Gesetze, Verträge, SLAs
- Risikoanalyse
- Risikobewertung
- Extrahieren/ Auswählen von Maßnahmen
- Realisierungsplanung und Umsetzung



PDCA
Check

Erfolgskontrolle Zielerreichung:

- Reaktion auf Änderungen
- Detektion von Vorfällen
- Überprüfung der Einhaltung
- Überprüfung der Eignung und Wirksamkeit der Sicherheitsmaßnahmen
- interne Audits
- Managementbewertung

PDCA
Act

Beseitigung von Mängeln und Schwächen, Optimierung und Verbesserung:

- Reaktion
- Reflexion
- Verbesserung

PDCA-Zyklus
(aka Deming Cycle)

Struktur ISO/IEC 27001

Gemäß harmonized structure nach Annex SL:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

„Kapitel"

Annex A. Information security control reference

„Anhang/Annex"

Kapitel 4-10.2

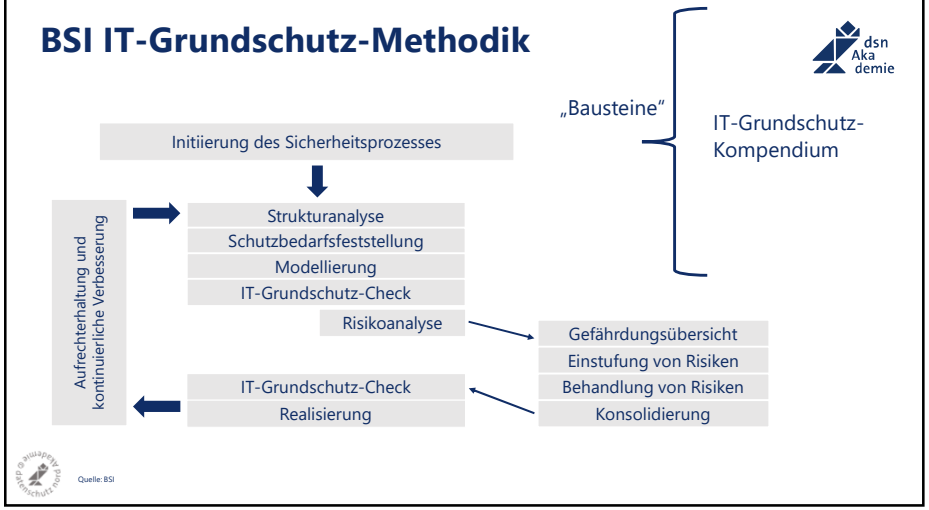
Anhang A ISO/IEC 27001

93 “Informationssicherheitsmaßnahmen”

Aufgeteilt in 4 Themenbereiche:

- Organisatorisch
- Personell
- Physisch
- Technisch

BSI IT-Grundschutz-Methodik



Quelle: BSI

IT-Grundschutz-Kompendium

47 “Elementare Gefährdungen”

~110 “Bausteine”

Aufgeteilt in:

- 2 “Ober”-Kategorien
- 10 “Unter”-Kategorien

Quelle: BSI

Informationssicherheits-Managementsystem

Nutzen ISMS

Etabliertes ISMS:

- Interne Prozesse und Verfahren sind stabiler und effizienter.
- Der Mehraufwand ist geringer als der Effizienzgewinn.
- Steigerung der Qualität und Effizienz durch unabhängige Prüfungen.

Ganzheitlicher Ansatz:

- Überblick über Status der Informationssicherheit.
- Messbarkeit der Informationssicherheit.
- Haftungs- und sonstige Risiken werden minimiert.

Zusammenfassende Standardsicht

Informationssicherheits-Managementsystem

Informationssicherheit	Managementsystem
Organisatorische Themen	PDCA-Zyklus
Personelle Themen	Prozessorientiert
Physische Themen	Rahmenbedingungen
Technische Themen	Risikomanagement

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!

Konsul-Smidt-Straße 88 • 28217 Bremen
T +49 (0) 421 69 66 32-298
Mail: akademie@dsn-group.de

www.dsn-group.de/dsn-akademie