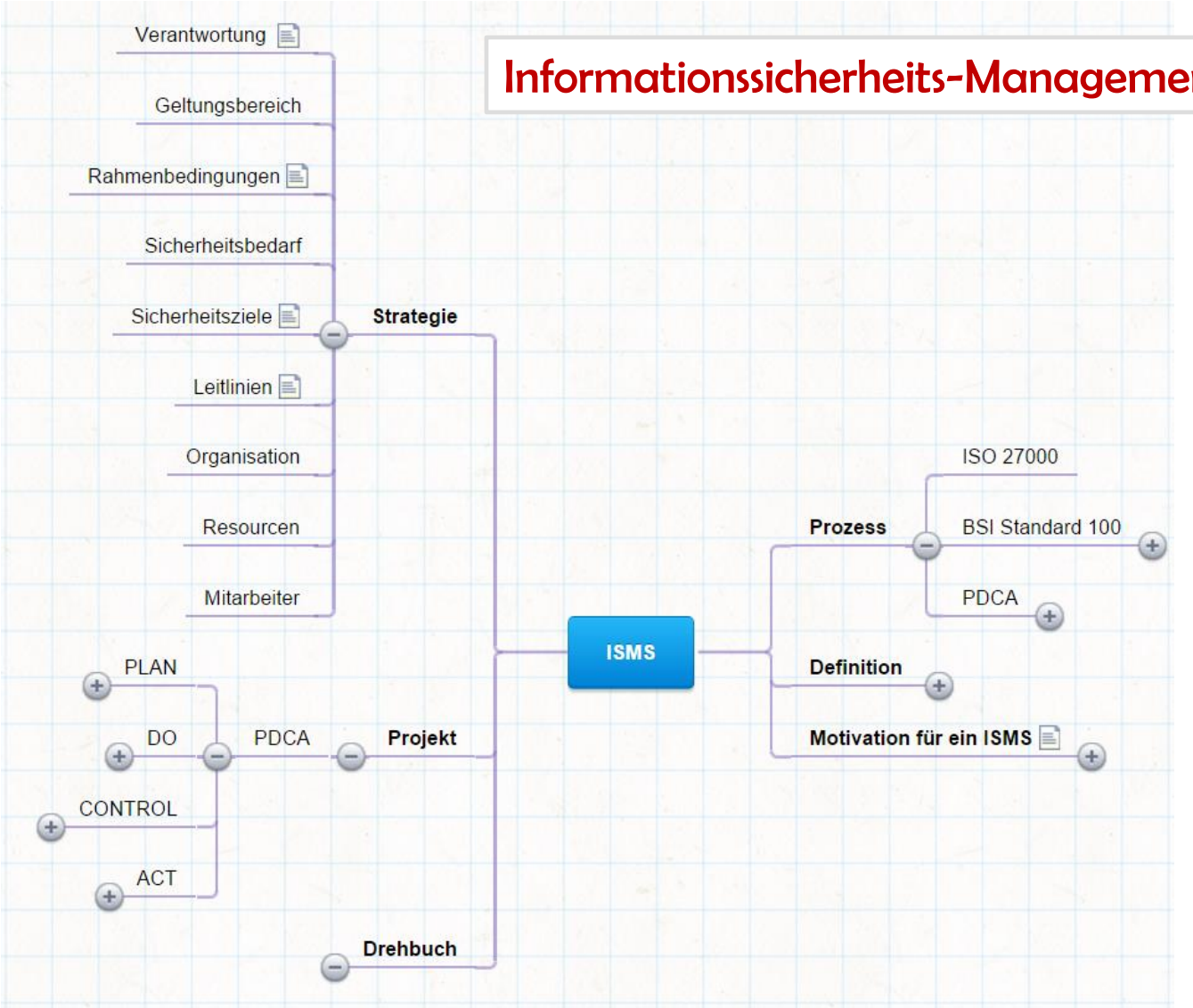
Informationssicherheit

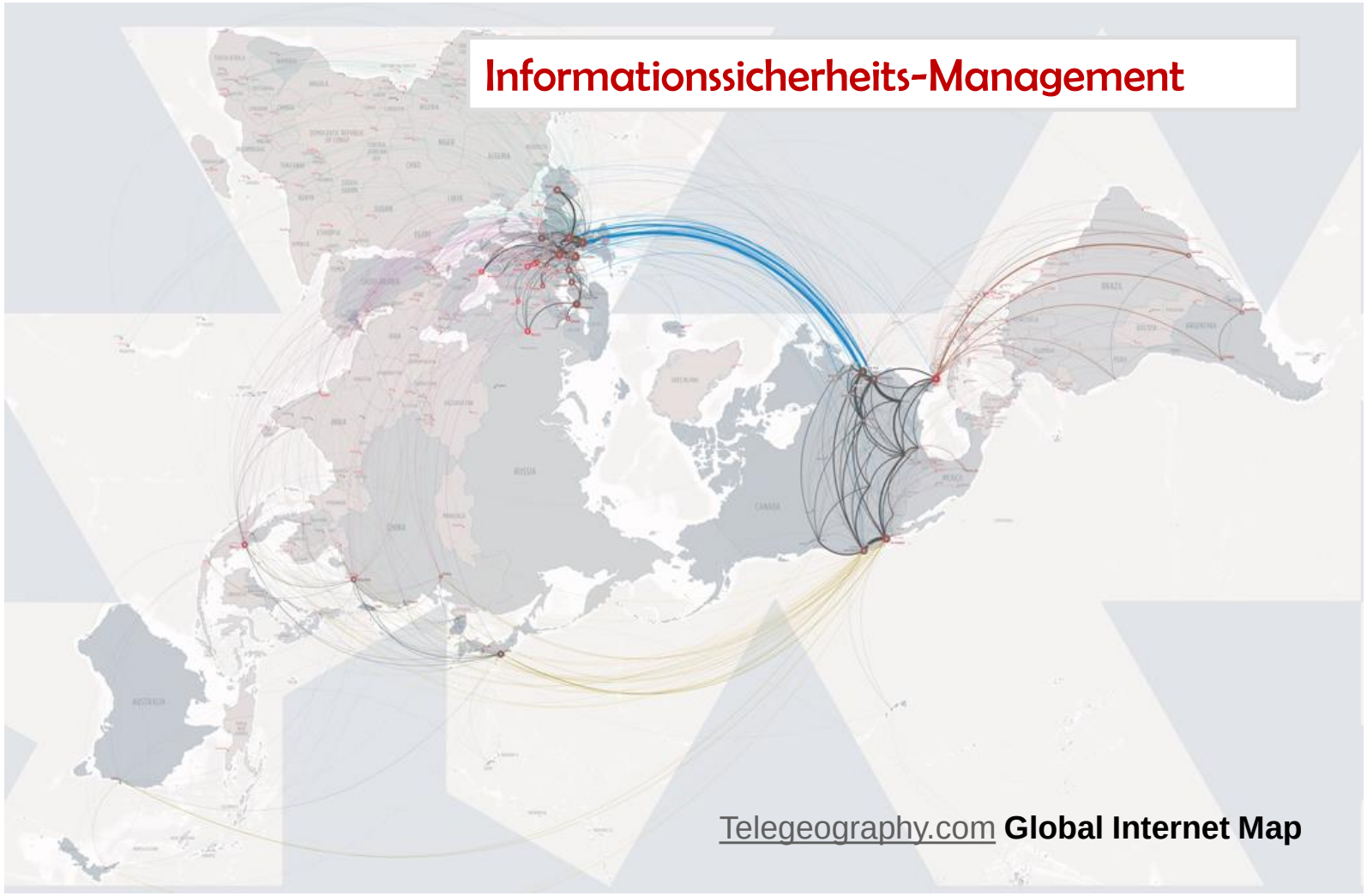
ISMS

Informationssicherheits-Managementsystem

https://wolf-it-architekt.de/

Informationssicherheits-Management




Informationssicherheits-Management
Telegeography.com Global Internet Map

Informationssicherheits-Management

- Informationen sind wichtige Werte für ein Unternehmen
  - strategisches und technisches Wissen
  - mit Hilfe von IT verwaltet (~ 80%)
  - auf Datenträgern und auf Papier
  - in den Köpfen der Mitarbeiter
- Informationen sind in der globalisierten Welt vielfältigen Gefährdungen ausgesetzt
- Informationen müssen hinreichend gut geschützt werden
- Durch Verlust, Offenlegung oder Manipulation entstehen hohe Schäden

Informationssicherheits-Management

- Anforderungen an die Informationenssicherheit
  - Vertraulichkeit, Verlässlichkeit, Verfügbarkeit der Information
  - Investitionswerte erhalten
  - Datenschutz gewährleisten
  - Kontinuität der Geschäftsprozesse sicherstellen
  - Vertrauen bei Kunden und Partnern bewahren

Informationssicherheits-Management

- Risiken für die Informationenssicherheit
  - Cyber-Kriminalität
  - Innentäter
  - Irrtümer und Notfälle

Informationssicherheits-Management

- Risiken für die Informationenssicherheit
  - Cyber-Kriminalität
    - Denial Of Service (DOS / DDOS)
    - Wirtschaftsspionage als bezahlte Dienstleistung
    - Identitätsdiebstahl
    - Missbrauch von IT-Systemen (Botnetze, Email-Spam, Propaganda)
    - Erpressungstrojaner (Entschlüsselung gegen Lösegeld)
  - Innentäter
  - Irrtümer und Notfälle

Informationssicherheits-Management

- Risiken für die Informationenssicherheit
  - Cyber-Kriminalität
  - Innentäter
    - Diebstahl von Hardware
    - Datendiebstahl
    - Wirtschaftsspionage
    - Sabotage
  - Irrtümer und Notfälle

Informationssicherheits-Management

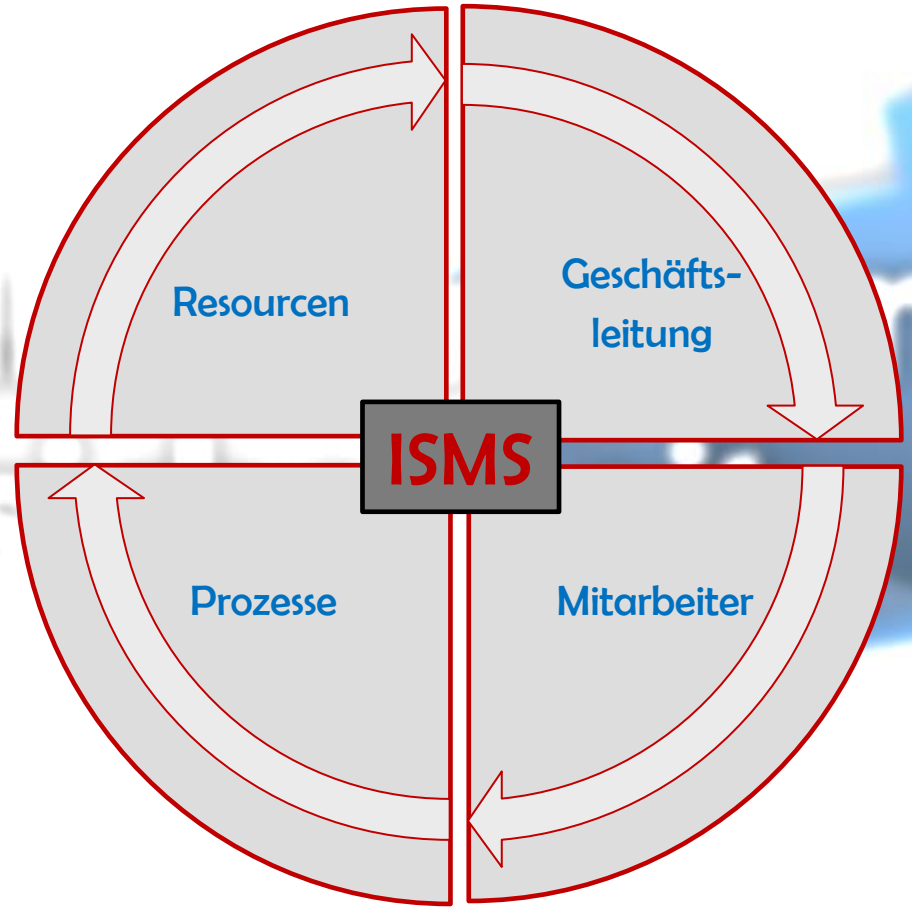
- Risiken für die Informationenssicherheit
  - Cyber-Kriminalität
  - Innentäter
  - Irrtümer und Notfälle
    - Plattencrash
    - Hardwareausfall
    - Softwarefehler
    - Höhere Gewalt
    - Krankheit
    - Menschliches Versagen

Informationssicherheits-Management

- Risiken für die Informationenssicherheit
  - müssen analysiert und bewertet werden
  - müssen mit geeigneten Massnahmen behandelt werden
- Informationenssicherheits-Management hat Fokus auf Effizienz und Wirtschaftlichkeit

Definition

Definition



Definition

- Information ist nicht nur IT
  - strategisches und technisches Wissen
  - mit Hilfe von IT verwaltet (~ 80%)
  - auf Datenträgern und auf Papier
  - in den Köpfen der Mitarbeiter
- Grundwerte der Informationssicherheit
  - Vertraulichkeit, Verlässlichkeit, Verfügbarkeit
  - Authentizität, Verbindlichkeit, Nichtabstreitbarkeit
- Informationssicherheit vs. IT-Sicherheit

Definition

- Verantwortung der Unternehmensleitung
- Mitarbeiter
- Sicherheitsprozess
- Resourcen

Definition

- Verantwortung der Unternehmensleitung
  - Organisationsstruktur
  - Planung, Lenkung, Koordination
  - Kommunikation
  - Allgemeine Sicherheitsziele
  - Kontrolle und kontinuierliche Verbesserung
- Mitarbeiter
- Sicherheitsprozess
- Resourcen

Definition

- Verantwortung der Unternehmensleitung
  - Organisationsstruktur
  - Planung, Lenkung, Koordination
  - Allgemeine Sicherheitsziele
  - Kontrolle und kontinuierliche Verbesserung

Sicherheitsmanagement

- Mitarbeiter
- Sicherheitsprozess
- Resourcen

Definition

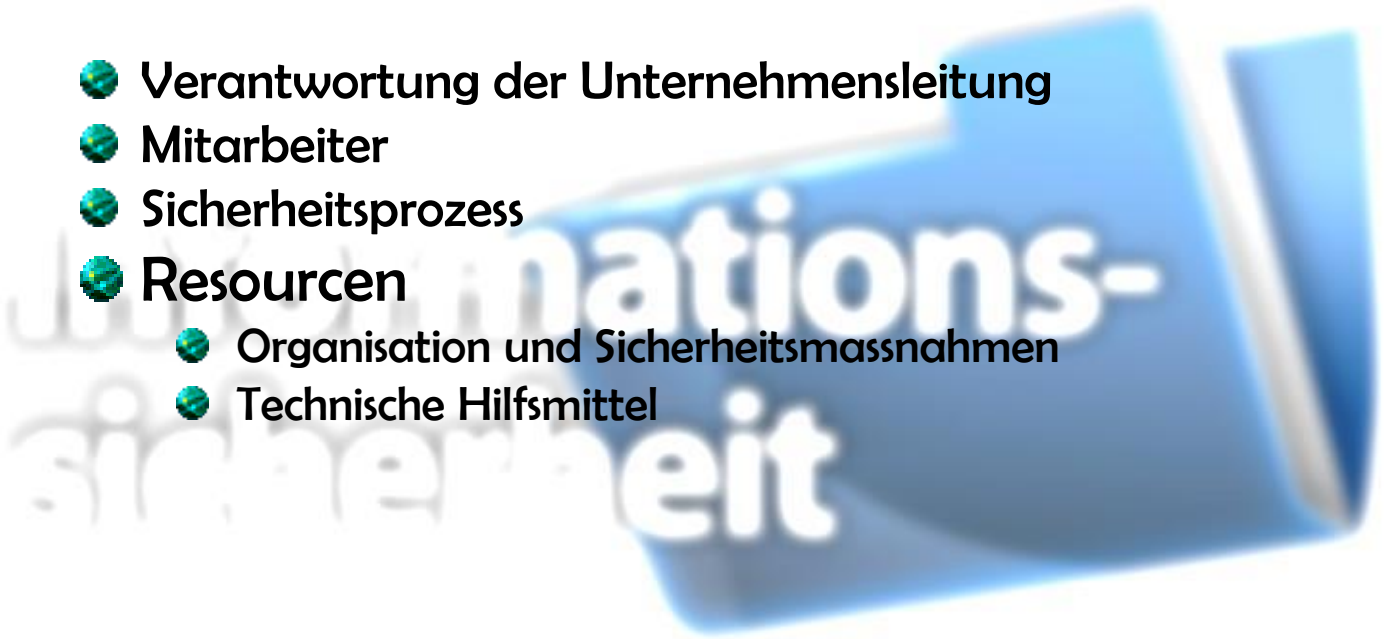
- Verantwortung der Unternehmensleitung
- Mitarbeiter
  - Informationssicherheits-Beauftragte
  - Datenschutzbeauftragte
  - Administratoren
  - Anwender
- Sicherheitsprozess
- Resourcen

Definition

- Verantwortung der Unternehmensleitung
- Mitarbeiter
- Sicherheitsprozess
  - Sicherheitsziele
  - Risikoanalyse und Risikobehandlung
  - Regeln, Anweisungen, Massnahmenkatalog
  - Umsetzung und Kontrolle
  - kontinuierliche Verbesserung
- Resourcen

Definition

- Verantwortung der Unternehmensleitung
- Mitarbeiter
- Sicherheitsprozess
- Resourcen
  - Organisation und Sicherheitsmassnahmen
  - Technische Hilfsmittel

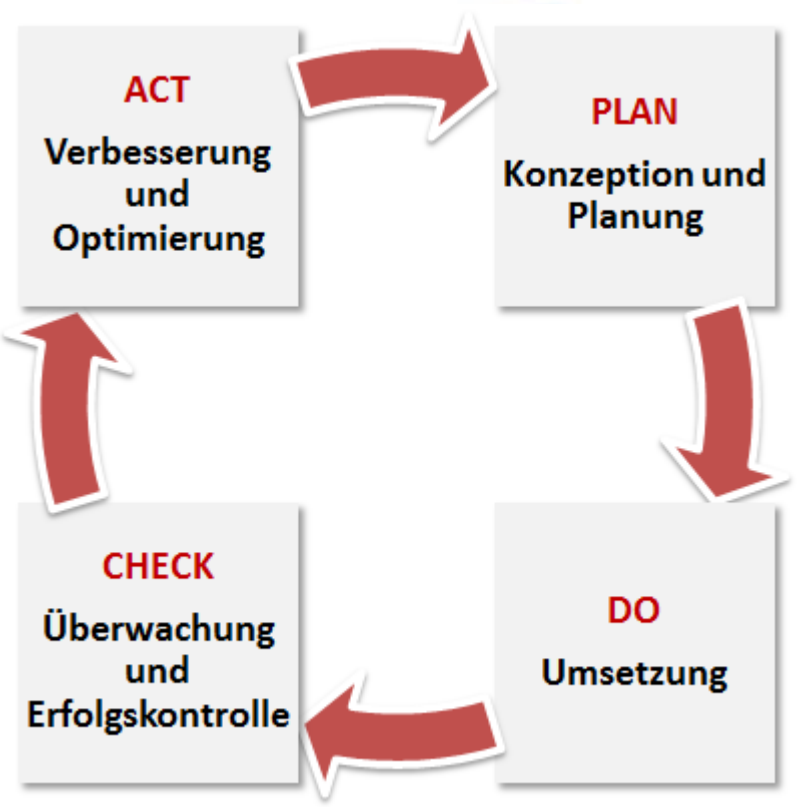


Sicherheitsprozess

Sicherheitsprozess

PDCA

- ✓ PLAN
- ✓ DO
- ✓ CHECK
- ✓ ACT



Sicherheitsprozess

ISO 27000

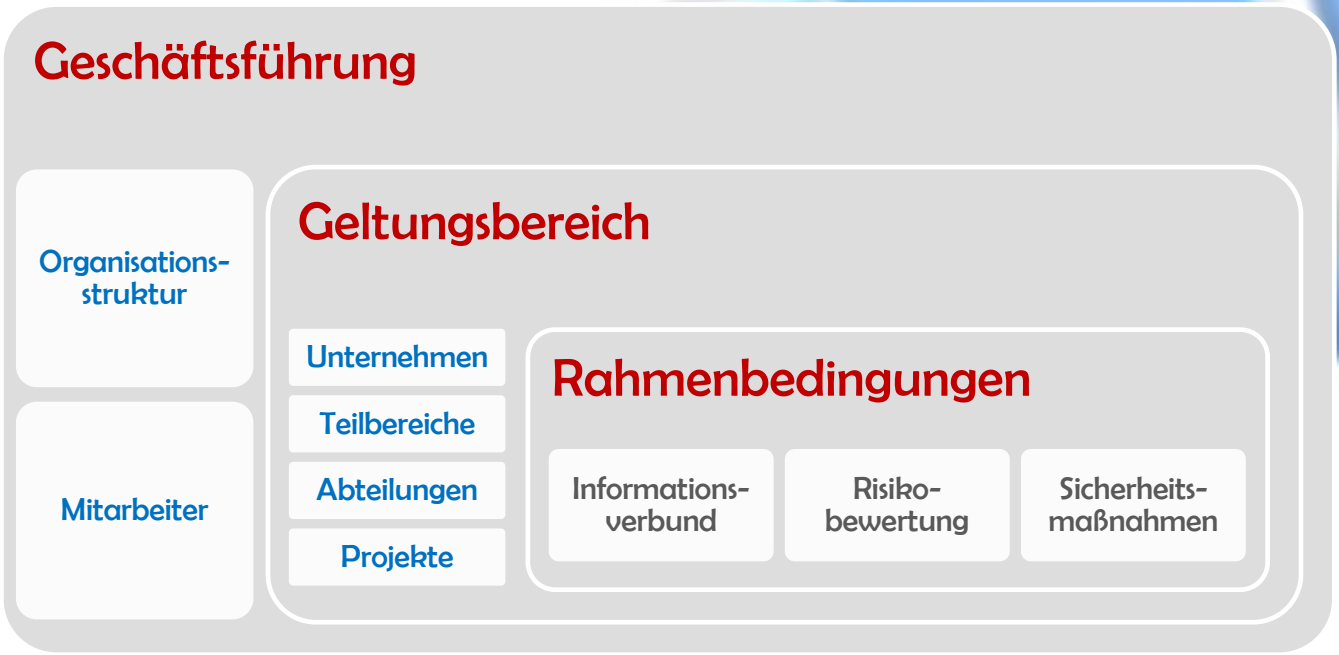
BSI-Standard 100

100-1 Überblick
100-2 Aufbau eines ISMS
100-3 Risikoanalyse
100-4 Notfallmanagement

IT-Grundschutz-Kataloge

Strategie

Strategie


Geschäftsführung
Organisations-struktur
Mitarbeiter
Geltungsbereich
Unternehmen
Teilbereiche
Abteilungen
Projekte
Rahmenbedingungen
Informations-verbund
Risiko-bewertung
Sicherheits-maßnahmen

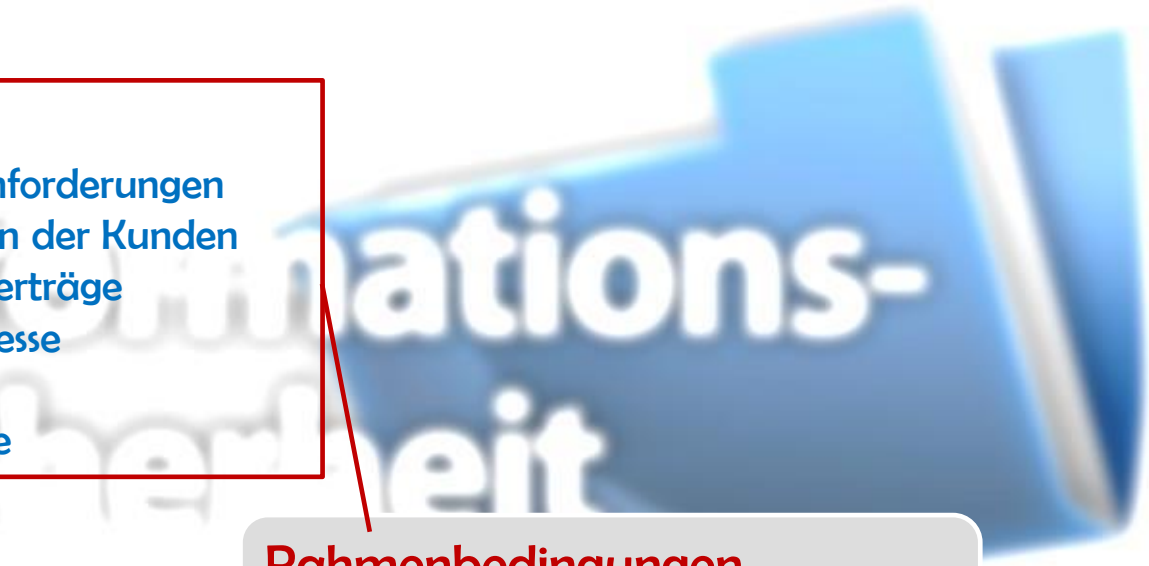
Strategie

Rahmenbedingungen

- Informations-verbund
- Risiko-bewertung
- Sicherheits-maßnahmen

Strategie

- Geschäftsziele
- Gesetzliche Anforderungen
- Anforderungen der Kunden
- Bestehende Verträge
- Geschäftsprozesse
- Bedrohungen
- Sicherheitsziele



Rahmenbedingungen

Informations-verbund	Risiko-bewertung	Sicherheits-maßnahmen

Strategie

Geschäftsziele
Gesetzliche Anforderungen
Anforderungen der Kunden
Bestehende Verträge
Geschäftsprozesse
Bedrohungen
Sicherheitsziele

Rahmenbedingungen

Informations-verbund

Risiko-bewertung

Sicherheits-maßnahmen

Gebäude
Raum
Mitarbeiter
Applikationen
IT-Systeme
Datenträger

Strategie

Geschäftsziele
Gesetzliche Anforderungen
Anforderungen der Kunden
Bestehende Verträge
Geschäftsprozesse
Bedrohungen
Sicherheitsziele

Rahmenbedingungen

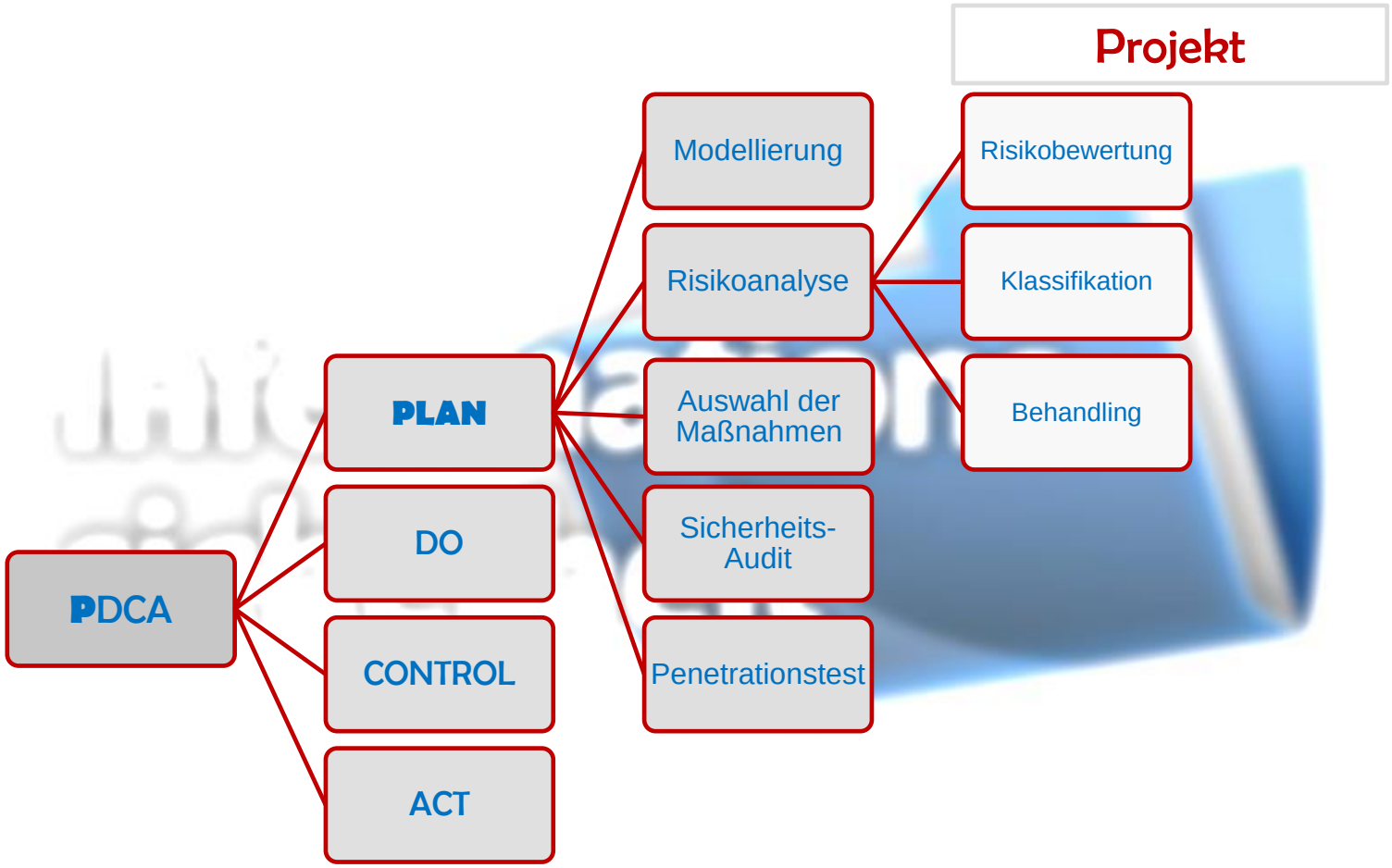
- Informations-verbund
- Risiko-bewertung
- Sicherheits-maßnahmen

Gebäude
Raum
Mitarbeiter
Applikationen
IT-Systeme
Datenträger

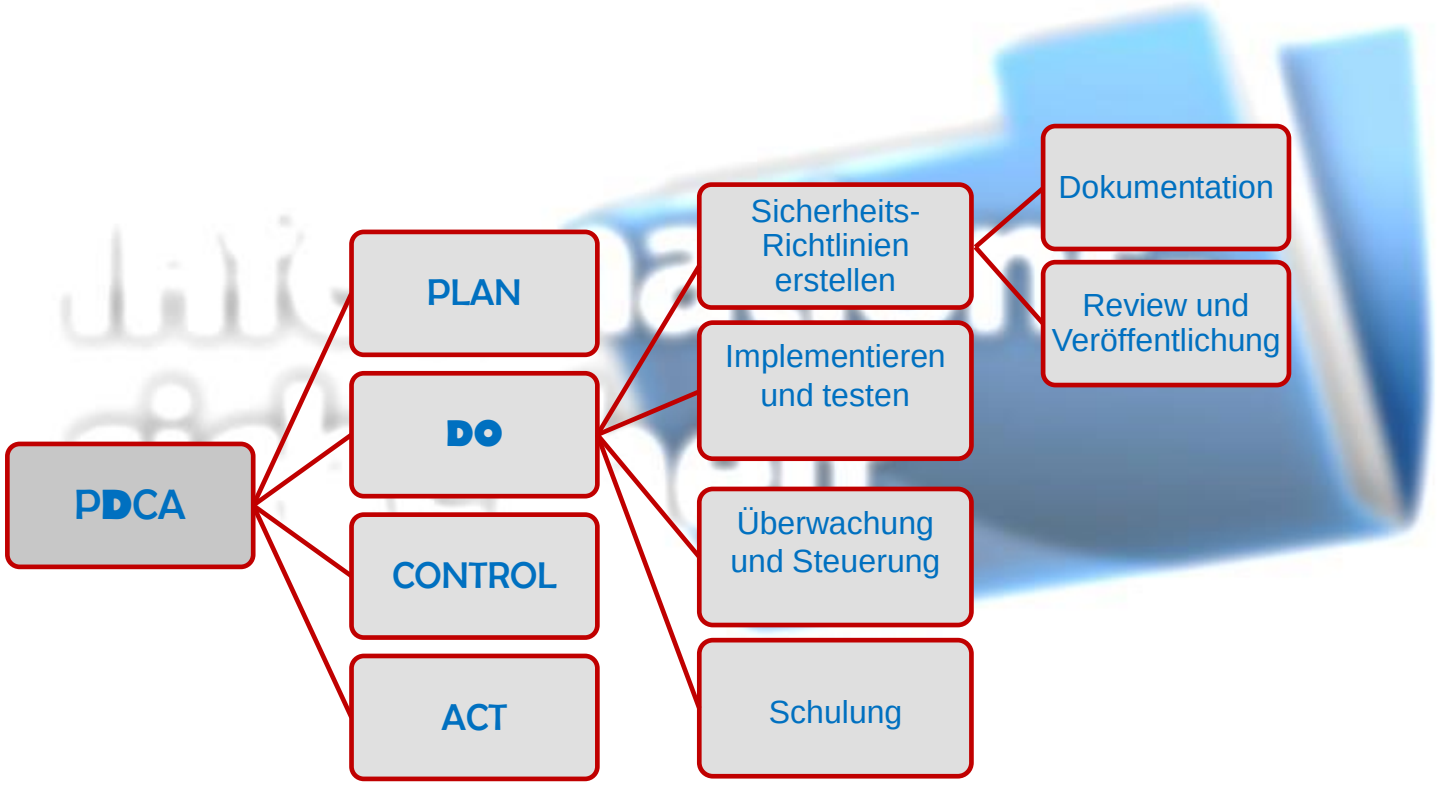
BSI
IT-Grundschutz
Maßnahmen-katalog


Projekt
Informations-
sicherheit

Projekt


Projekt
PDCA
PLAN
DO
CONTROL
ACT
Modellierung
Risikoanalyse
Auswahl der Maßnahmen
Sicherheits-Audit
Penetrationstest
Risikobewertung
Klassifikation
Behandling

Projekt


PDCA
PLAN
DO
CONTROL
ACT
Sicherheits-Richtlinien erstellen
Implementieren und testen
Überwachung und Steuerung
Schulung
Dokumentation
Review und Veröffentlichung

Projekt


PDCA
PLAN
DO
CONTROL
ACT
Erfolgskontrolle
Optimierung
Wirksamkeit
Interne Audits
Penetrations-Tests
Wirtschaftlichkeit
Anpassung an Rahmen-bedingungen

Projekt


PDCA
PLAN
DO
CONTROL
ACT
Kleine Maßnahmen sofort umsetzen
PDCA
PLAN
DO
CONTROL
ACT

Drehbuch

5 Schritte zu Informationssicherheit

- Geltungsbereich
- Rahmenbedingungen
- Sicherheitsziele und Prioritäten global definieren
- Leitlinien

- Informationsverbund
- Risikobewertung
- Maßnahmenkatalog

- Internes Audit in Kurzform
- Penetrationstest: manueller Test der IT-Komponenten im realen Umfeld
- Ziele: Bestandsaufnahme Informationssicherheit, Identifikation von Schwachstellen

- PDCA (PLAN, DO, CONTROL, ACT)
- Aufbau eines ISMS
- Ausbau, Erweiterung, Anpassung eines bestehenden ISMS
- Planung und Durchführung als Projekt

- Kontinuierliche Kontrolle und Verbesserung
- Regelmäßige Berichte
- Audits und PenTest
- Korrektive Maßnahmen

IT-Sicherheit als Dienstleistung

- **Beratung Informationssicherheits-Management (ISMS)**
- **Regelmäßige Sicherheits-Audits**
- **Regelmäßige Penetrationstests**
- **Appliance Security-Scout für bedienerlose Penetrationstests 24x7**
- **Schulungen, Mitarbeitersensibilisierung**

wolf@wolf-it-architekt.de