



ISO 27001/27002 Die 10 Schritte zur erfolgreichen Umsetzung

Swiss Infosec AG
Centralstrasse 8A
CH-6210 Sursee

Maulbeerstrasse 10
CH-3001 Bern

Steinstrasse 21
CH-8036 Zürich

Fon +41 (0)41 984 12 12
Fax +41 (0)41 984 12 24
infosec@infosec.ch
www.infosec.ch

Meet Swiss Infosec!

Reto C. Zbinden, CEO, Swiss Infosec AG



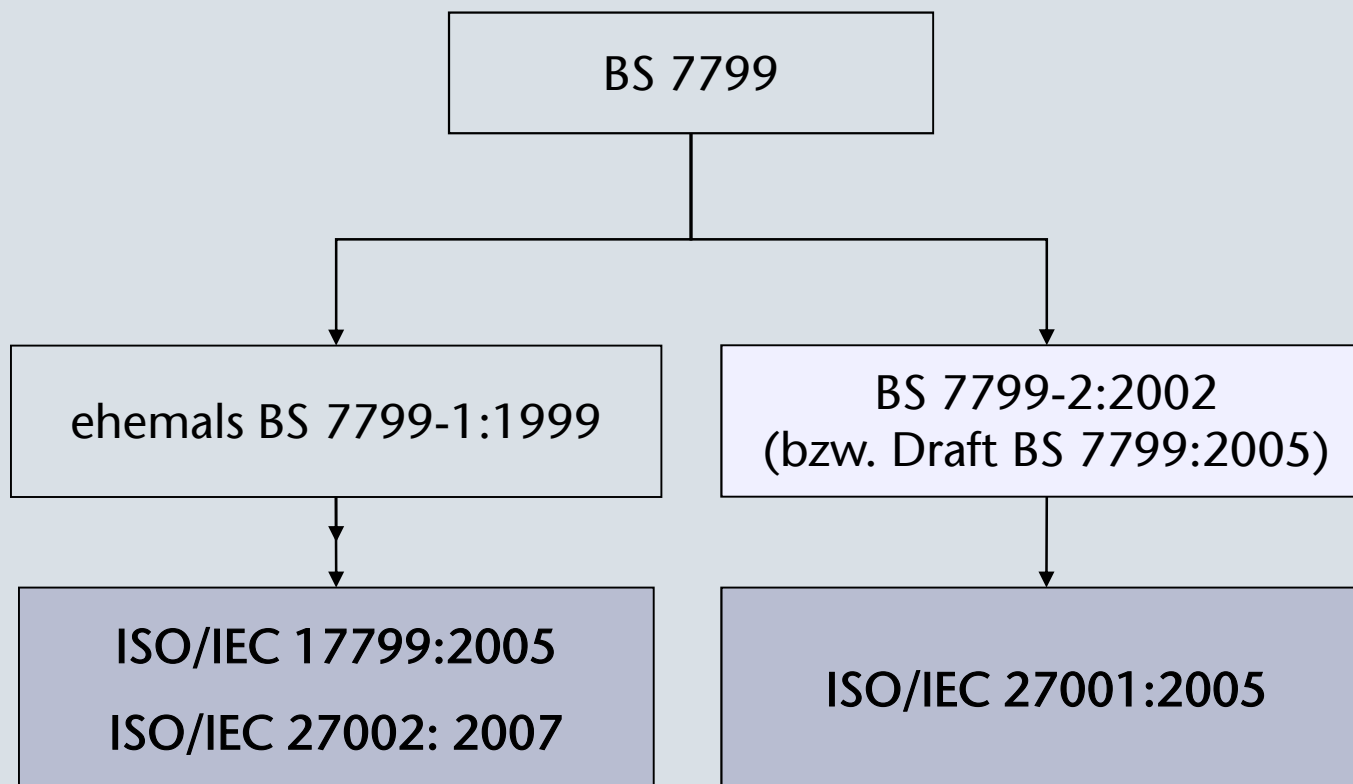


Was ist ein Informationssicherheits- Managementsystem

- Abkürzung: ISMS
- Gesamtheit der organisatorischen und konzeptionellen Massnahmen zur Steuerung und Optimierung der Informationssicherheit eines Unternehmens...
- **ISO 27001, DIE Norm bezüglich Informationssicherheit fordert den Aufbau und die laufende Verbesserung des ISMS einer Organisation.**

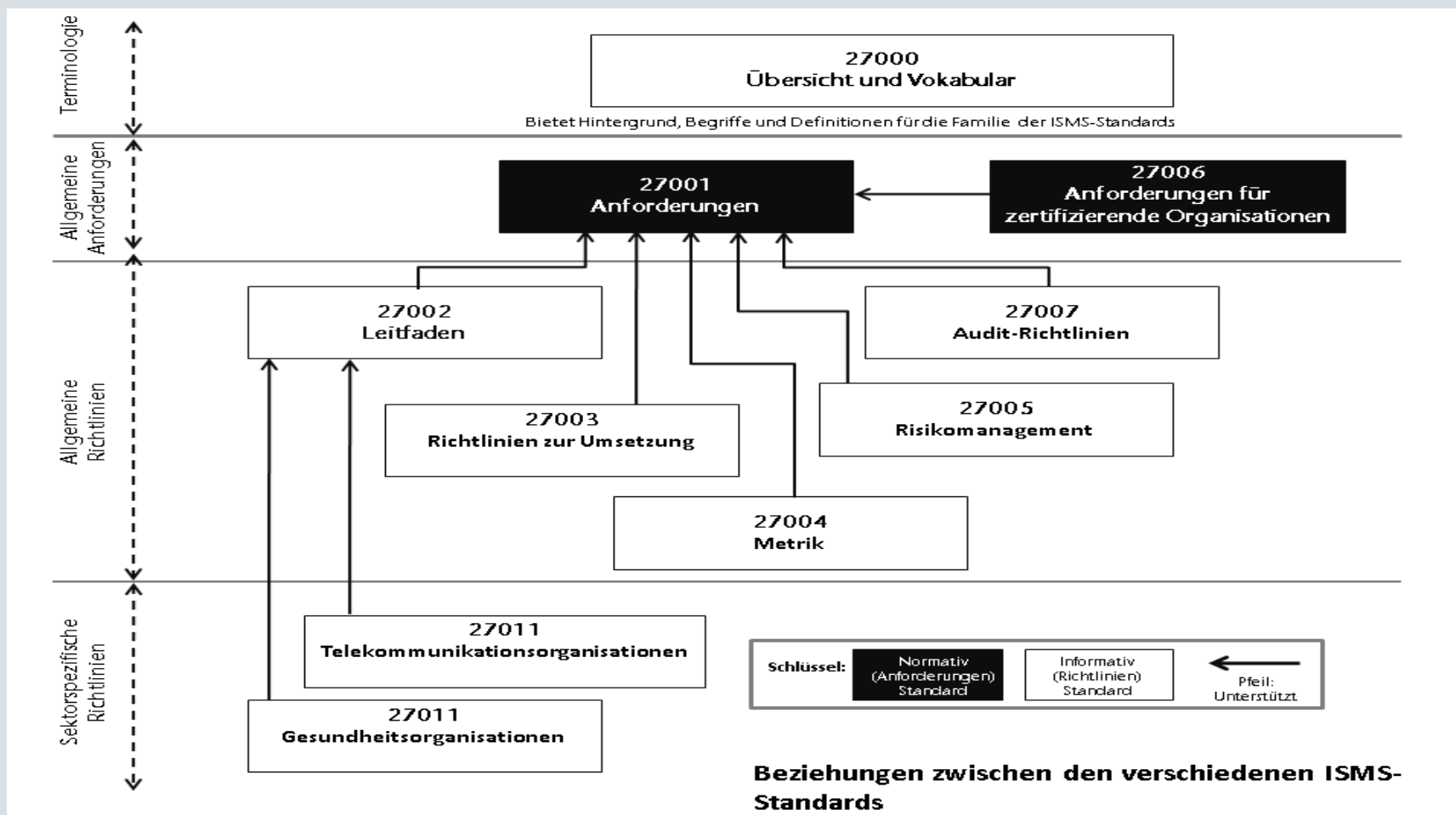


Geschichte BS 7799 / ISO 27001





Die 27000er Familie wie sie sich heute präsentiert





ISO 27001

- ISO 27001 ist die eigentliche Norm
 - Zertifizierungsgrundlage
- ISO 27001 behandelt das ISMS
- Unterstützt die Verwendung eines prozessorientierten Ansatzes für
 - Einführung, Implementierung
 - Betrieb, Überwachung
 - Wartung und
 - Verbesserung der Effektivität des ISMS einer Organisation.

**ISO 27002: 133 Controls, nur «Specifications»
Begründetes Abweichen jederzeit möglich!**





Anforderungen an das ISMS

- **Managementgremium**
 - Steuert, entscheidet, koordiniert
 - Übernahme Restrisiken
- **Regelmässige Überprüfung der Risikosituation**
 - Risiken identifizieren, bewerten
 - Massnahmen evaluieren
 - Nachvollziehbare Risikobehandlung bzw. Risikoumgang
- **Dokumentenlenkungssystem**
 - ISO 9000 (QS)/ISO 14000 (Umweltmanagement)
- **Lenkung der Nachweise**





ISMS: Zentrale Themen

Management Commitment

als zentrale Forderung:

Mitarbeiter können nur das leben, was vom Management vorgegeben wird

Das Inventar (Inventory of Assets):

Verzeichnis aller zu schützenden Objekte, die mit Informationen assoziiert sind und deren definierte Eigner

Schwachstellen-/Risikoanalyse:

Angewendet auf die zu schützenden Objekte, die einer Risikobehandlung unterzogen werden

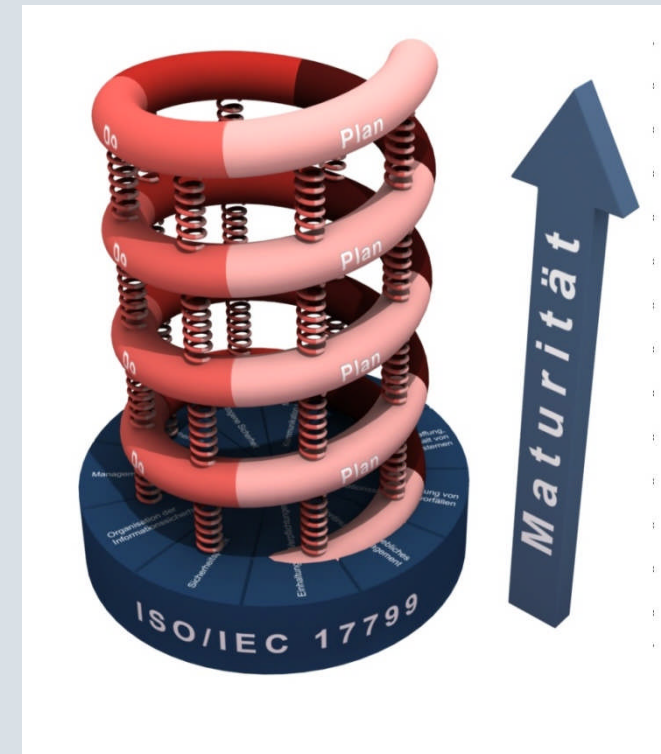
Auf Risikoanalyse-Basis werden Controls etabliert, um Risiken zu mindern.

Controls werden zum Statement of Applicability zusammengeführt.



Unternehmensspezifisches ISMS

- Jedes ISMS ist einem kontinuierlichen Verbesserungs- und Reviewprozess unterworfen (Plan-Do-Check-Act, PDCA). Es gewinnt dadurch ständig an **Maturität**.
- Das ISMS besteht aus diversen ‚kleinen‘ ISMS bzw. **Controls**. Mängel wichtiger Controls haben direkte Auswirkungen auf das gesamte ISMS.





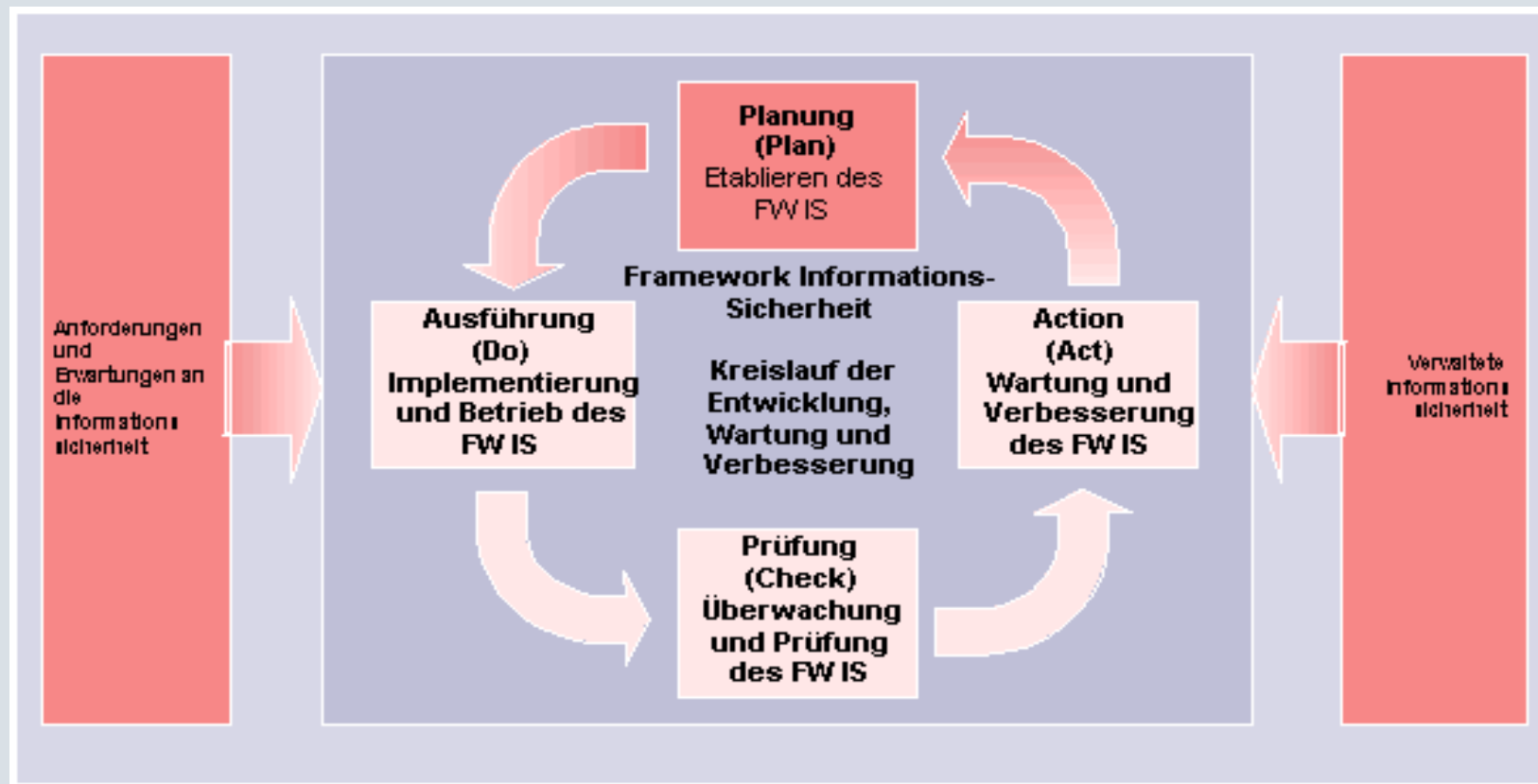
Vorteile der Einführung eines ISMS

- Einheitliches Framework unternehmensweit
- Fördert Konvergenz innerhalb des Unternehmens
(gleiche Verfahren, gleiche Standards, gleiche Sprache)
- Unternehmensweit, einheitliche Sichtweisen
- Abgrenzung, Klarstellung AKV im Bereich Sicherheit für
Verantwortungsträger und Units
- Ganzheitlicher Ansatz
- International, standardisierter Ansatz
- Transparenz bezüglich Sicherheitsprozesse und AKV



PDCA Prinzip

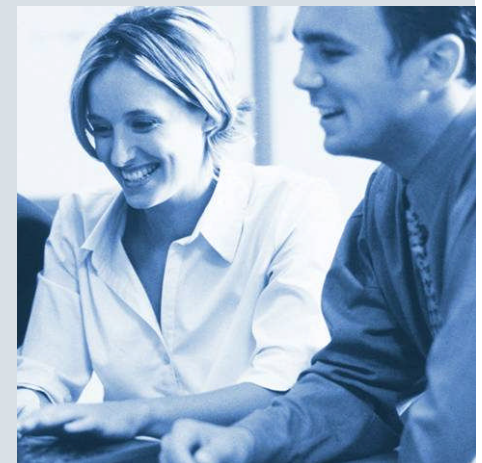
- **Plan:** Planung / Grundlagen / Bedürfnis
- **Do:** Umsetzungsmassnahmen / Betrieb
- **Check:** Überwachung / Prüfung
- **Act:** Fortlaufende Verbesserung





Schritt 1: Informationssicherheitspolitik

- Zeigt Ziele der Informationssicherheit auf
- Definiert den Stellenwert der IS innerhalb des Unternehmens
- Definiert auch den Scope
- Regelt Verantwortung für IS
- Legt Grundsätze für Massnahmen fest
- Schutzgrad definieren
- Risiken aktiv übernehmen
- Restrisiken erkennen
- Rahmen für Informationssicherheit





Schritt 1: Informationssicherheitspolitik

Ziel

- Sicherheit elektronischer **Informationen** bei
 - Speicherung
 - Übertragung und
 - Verarbeitung
- Sicherheit der **Informatikmittel**
- Sicherheit der **Informationsträger**
 - herstellen
 - wahren und
 - aktiv fördern



Schritt 1: Informationssicherheitspolitik

Verantwortungen

- **Unternehmensleitung**
 - zeichnet Sicherheitskultur vor
 - genehmigt Risikobewertung
 - delegiert Umsetzung und Pflege

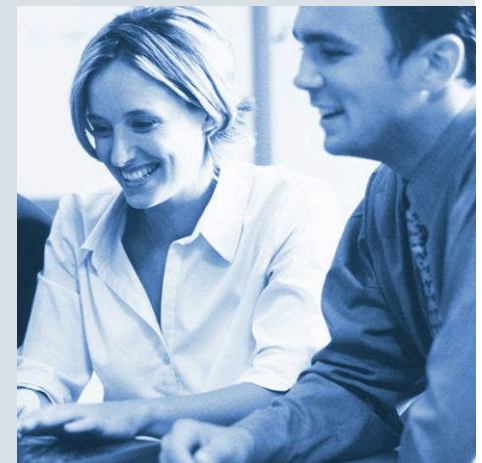
- **Funktionsträger/Vorgesetzter**
 - führt Risikobewertung durch
 - formuliert Massnahmen
 - setzt Massnahmen um
 - Kontrolliert

- **Mitarbeiter/Benutzer**
 - wendet Massnahmen an
 - meldet Sicherheitslücken



Schritt 2: Inventarisierung der zu schützenden Objekte

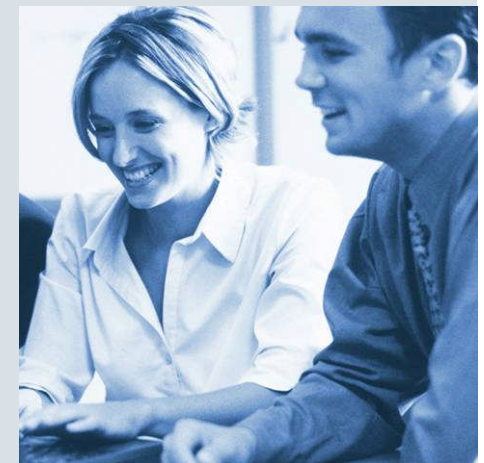
- Identifikation der Informationsbestände , Applikationen, Systeme, Netze
- Definition und Bildung von Gruppen innerhalb der oben erwähnten Objektarten (bspw. Clients, Workstations, NT-Server)





Schritt 3: Klassifizierung

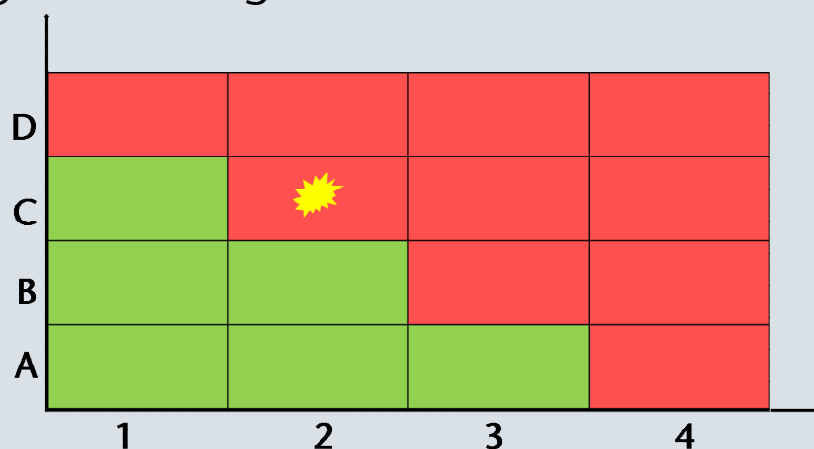
- Festlegung der standardisierten Schutzanforderungen bpsw. in den Bereichen Vertraulichkeit, Verfügbarkeit, Vertrauenswürdigkeit, Datenschutzrelevanz, usw.
- Klassifizierung erfolgt durch den Eigner
- Dokumentation der erfolgten Klassifizierung bezüglich der inventarisierten Schutzobjekte im Inventar





Schritt 4: Durchführung Risikoanalyse

- $RISIKO = \text{Schadensausmass} \times \text{Eintretenswahrscheinlichkeit}$
- Eine **Gefährdung** tritt mit einer gewissen Wahrscheinlichkeit und einem möglichen Schaden bezüglich eines **Objektes** ein
 - „**Ausfall** (Risiko) des **Netzwerkes** (Objekt) wegen **Stromausfall** (Gefährdung)“
Schadensausmass „hoch“ (C) x Eintretenswahrscheinlichkeit „mittel“ (2)
 - Festlegung der Kategorisierung
 - Festlegung der zulässigen Risiken





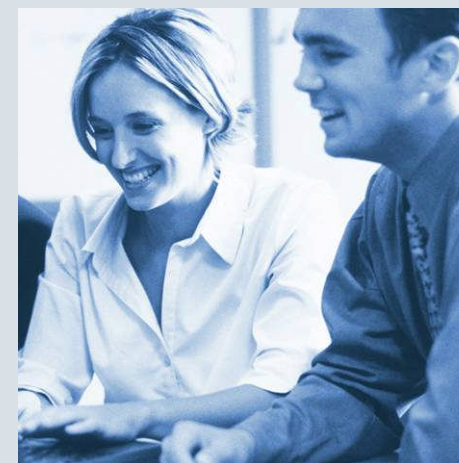
Schritt 5: Erarbeitung und Nachführung Risktreatment Plan

- Es werden teilweise unter Bezugnahme auf die Controls 27002 Massnahmen definiert zur Reduktion der nicht akzeptablen Risiken.
- Der Stand der Massnahmen wird im Risktreatment Plan laufend dokumentiert.



Schritt 6: Prozeduren

- Die durch 27001/27002 geforderten Prozeduren sind festzulegen
 - Beispiele:
 - Dokumentenlenkung
 - Verbesserungsprozess
 - Audit Vorgehen und Planung
 - Security Incident Management
 - Business Continuity Management





Schritt 7: Gap Analyse 27002

- Die Controls 27002 werden auf Einhaltung überprüft.
- Nicht relevante Controls werden identifiziert und begründet ausgeschlossen
- Die Dokumentation der Gap Analyse erfolgt im Statement of Applicability





Domains/ Kapitel des ISO 27002

- Sicherheitspolitik
- Sicherheitsorganisation
- Asset Management
- Personelle Sicherheit
- Physische und umgebungsbezogene Sicherheit
- Management von Kommunikation und Betrieb
- Zugriffs-Management
- System-Beschaffung, Entwicklung, Unterhalt
- Security Incident Management
- Kontinuitätsmanagement
- Einhaltung von Verpflichtungen / Compliance



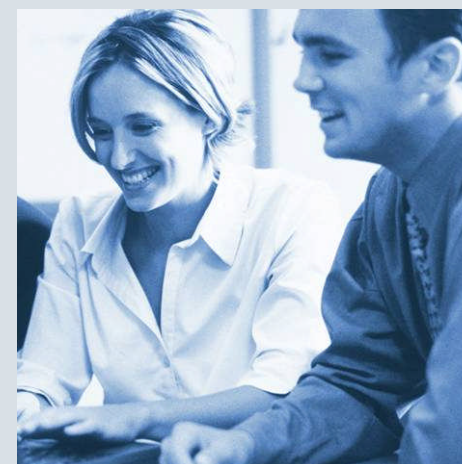
Schritt 8: Umsetzung der identifizierten Gaps

- Die identifizierten und relevanten Gaps bezüglich Controls 27002 sind umzusetzen.



Schritt 9: Statement of Applicability / Nachweise

- Im Statement of Applicability ist die Umsetzung der relevanten Controls umfassend zu dokumentieren.
- Die entsprechenden Vorgabe- und Nachweisdokumente sind zu referenzieren.





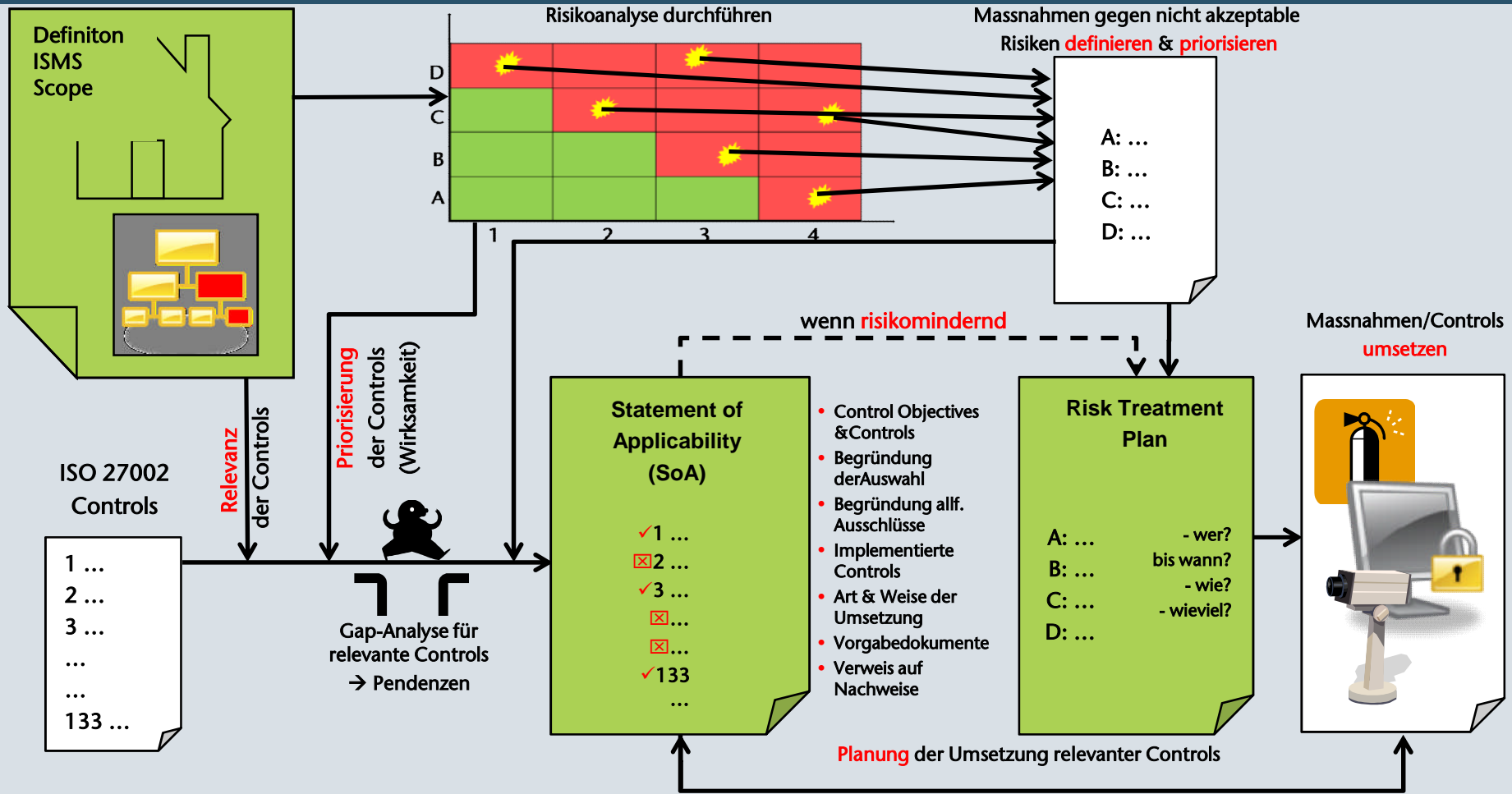
Schritt 10: Ausbildung und Vorbereitung der Zertifizierung

- Gremien, Funktionen, Vorgaben, Prozesse sind “zu leben”
- Die Mitarbeiter sind stufen- und funktionsgerecht auszubilden
- Die Zertifizierung kann geplant und durchgeführt werden.





Zusammenfassung





Wir danken Ihnen
für Ihre Aufmerksamkeit

Diskussionsrunde
Fragen

