sec4you
Advanced IT-Audit Services Ges.m.b.H.

Internationale IT-Sicherheitsstandards und deren Weiterentwicklung

Manfred Scholz CISA CISM / V1.0

Nutzen von Normen und Standards

Gemeinsame Regeln führen zu vergleichbaren Ergebnissen

Nutzen von Normen und Standards

Stand der Technik!

Herausforderung bei der Auswahl

Grundschutzhandbuch (BSI)

ISO/IEC 20000

ISAE 3402

IT-SEC

ITIL

COBIT

Six Sigma

Österreichische Sicherheitshandbuch

ISO TR 13335

Allianz für Cybersicherheit

ISO/IEC 27001

ISO 27033

NIST

ÖNORM S2109

OWASP

Eurocloud Star Audit

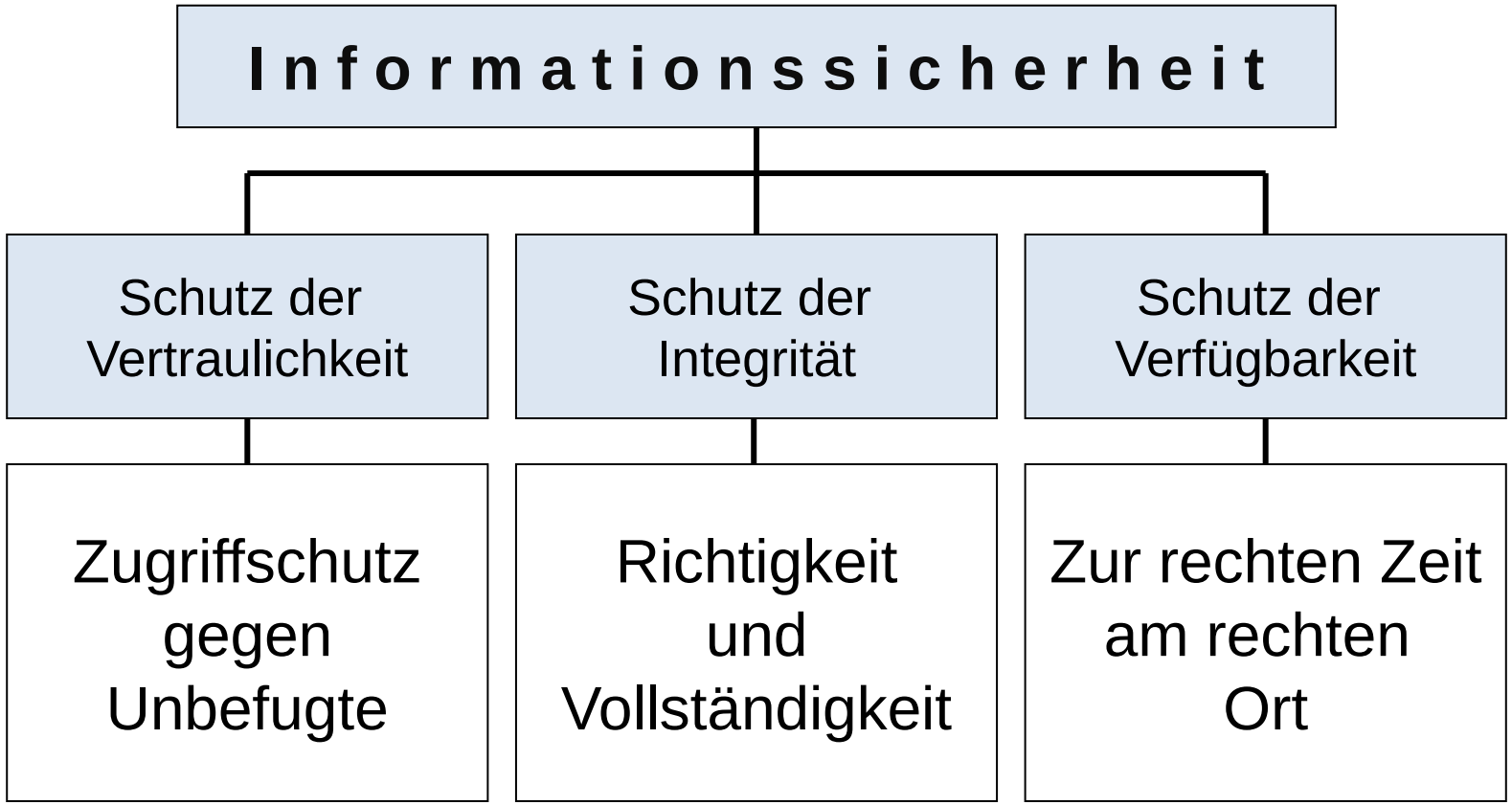
ÖNORM A7700

ISO/IEC 27001 Information Security Management System

ISO/IEC 27000

- 27000 (Begriffe und Definitionen)
- **27001 (Anforderungen der Zertifizierung)**
- **27002 (Code of Practice) → Empfehlungen!**
- 27003 (Leitfaden zur Implementierung)
- 27004 (Messung)
- 27005 (Risikomanagement BS7799 Teil 3)
- 27006 (Anforderungen an Zertifizierer)
- 27007 (Richtlinien für Auditoren)
- u.v.a. spezifische Themen (z.B. Cloud, Energie)

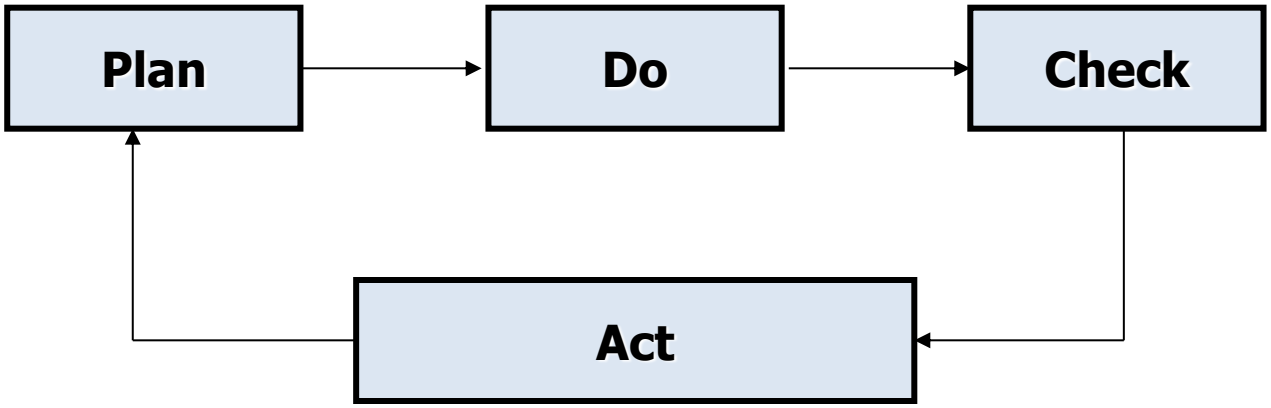
ISO/IEC 27001



ISO 27001 (Kapitel 4 - 10)

4. Kontext der Organisation
5. Führung
6. Planung
7. Unterstützung
8. Einsatz
9. Leistungsauswertung
10. Verbesserung

PDCA-Prozess / KVP



Sicherheit ist ein Prozess

ISO 27001 (Anhang A)

A.5 Sicherheitsleitlinien
A.6 Organisation der Informationssicherheit
A.7 Sicherheit des Personals
A.8 Wertemanagement
A.9 Zugriffskontrolle
A.10 Kryptographie
A.11 Schutz vor physischen Zugang und Umwelteinflüssen
A.12 Betriebssicherheit
A.13 Sicherheit der Kommunikation
A.14 Anschaffung, Entwicklung und Instandhaltung von Systemen
A.15 Lieferantenbeziehungen
A.16 Management von Informationssicherheitsvorfällen
A.17 Informationssicherheitsaspekte des Business Continuity Management
A.18 Richtlinienkonformität

IT-Grundschutzkataloge (BSI)

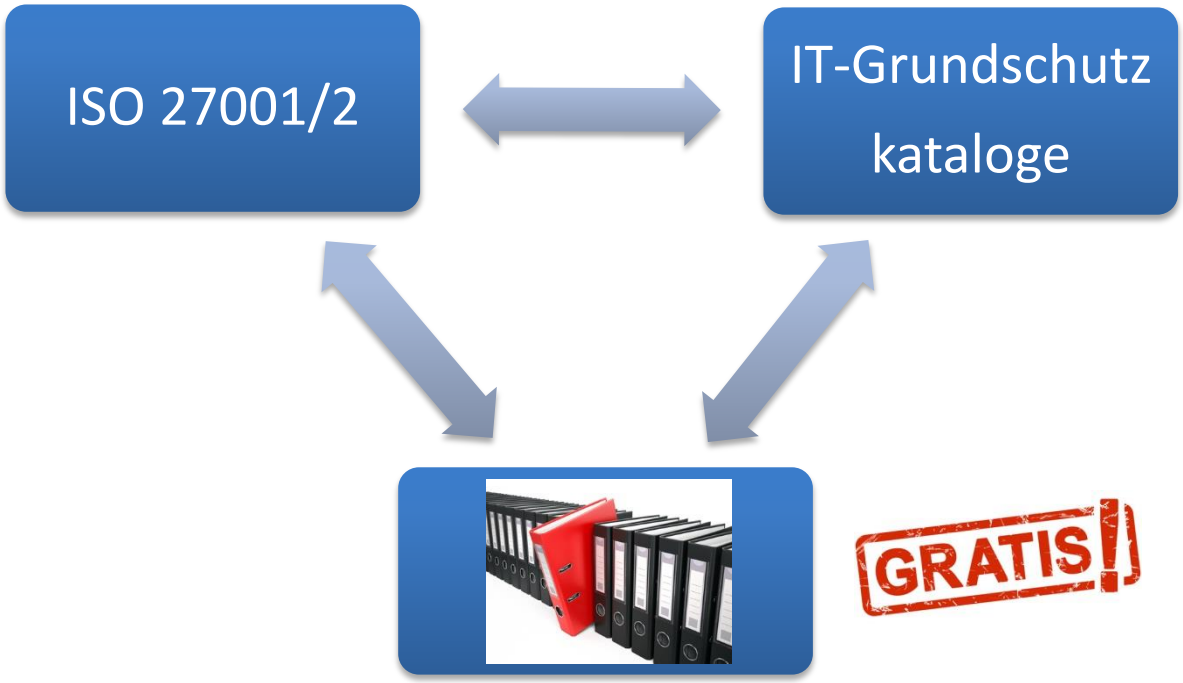
Gefährdungen
G0 Elementare Gefährdungen
G1 Höhere Gewalt
G2 Organisatorische Mängel
G3 Menschliche Fehlhandlungen
G4 Technisches Versagen
G5 Vorsätzliche Handlungen

Maßnahmen
M1 Infrastruktur
M2 Organisation
M3 Personal
M4 Hardware und Software
M5 Kommunikation
M6 Notfallvorsorge

Österreichische Sicherheitshandbuch

https://www.sicherheitshandbuch.gv.at

Österreichische Sicherheitshandbuch



https://www.sicherheitshandbuch.gv.at

Spezialthema: Web-Anwendungen

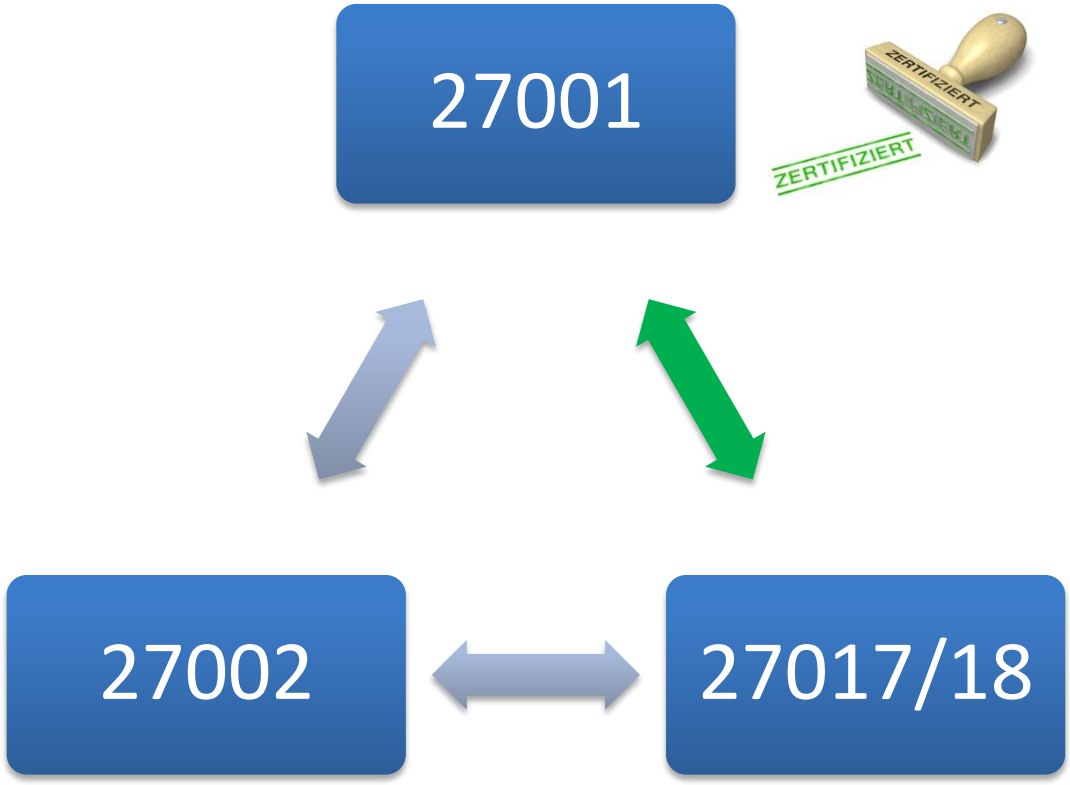
Spezialthema: Web-Anwendungen

- ÖNORM A7700
- OWASP Open Web Application Security Projekt (www.owasp.org)
- BSI Leitfaden zur Entwicklung sicherer Webanwendungen. Empfehlungen und Anforderungen (Auftragnehmer / Auftraggeber)

Spezialthema: Cloud Services

- **ISO 27017** Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- **ISO 27018** Code of practice for protection of **personally identifiable information** (PII) in public clouds acting as PII processors
- Eurocloud Star Audit (https://eurolcloud-staraudit.eu)

ISO/IEC 27017/18



Leitfäden der Eurocloud

www.eurocloud.at/projekte/publikationen/leitfaeden.html

Zukünftige Entwicklungen

Zertifizierungen als Lösungsansatz?

Finale

Das schwächste Glied bestimmt den Erfolg!

Finale

Danke für die Aufmerksamkeit

Manfred.Scholz@sec4you.com
http://www.sec4you.com
XING, LinkedIn
Tel.: +43 2262 72857