Erfahrungen bei der Erstellung und Umsetzung von Sicherheitskonzepten im IT-Verbund IMISE/KKSL

Ronald Speer[1,2]

[1]Koordinierungszentrum für Klinische Studien, Universität Leipzig
[2]Institut für Medizinische Informatik, Statistik und Epidemiologie, Universität Leipzig

imise.

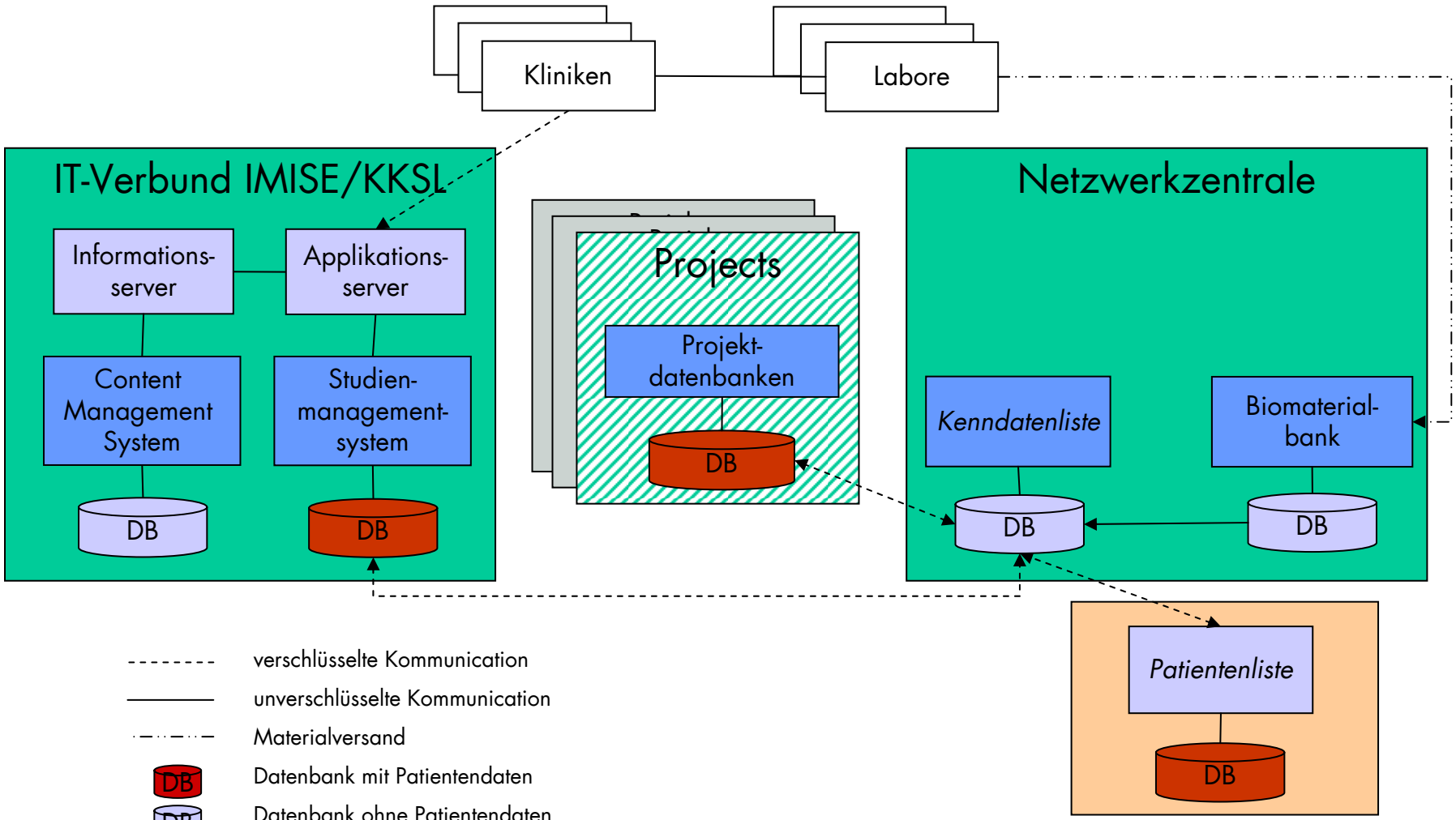
KKSL
KOORDINIERUNGSZENTRUM FÜR KLINISCHE STUDIEN LEIPZIG

UNIVERSITÄT LEIPZIG

IT-Verbund IMISE/KKSL

- verschiedene Forschungsverbünde
  - KN Lymphome,
  - KN Herzinsuffizienz,
  - KN Sepsis
  - Krebshilfe (MMML, HNPCC, BRCA, GLIOM)
  - Studiengruppen (GSHNHL, KHD)
- Application Service Providing
  - KKS Halle
- Bereitstellung von Diensten
  - Patientenliste, Kenndatenliste,
  - Studiendatenbanken, Safetymanagement,
  - Materialdatenbanken, etc.

IT-Struktur eines FV
(Beispiel KN Herzinsuffizienz)



imise.

KKSL KOORDINIERUNGSZENTRUM FÜR KLINISCHE STUDIEN LEIPZIG

UNIVERSITÄT LEIPZIG

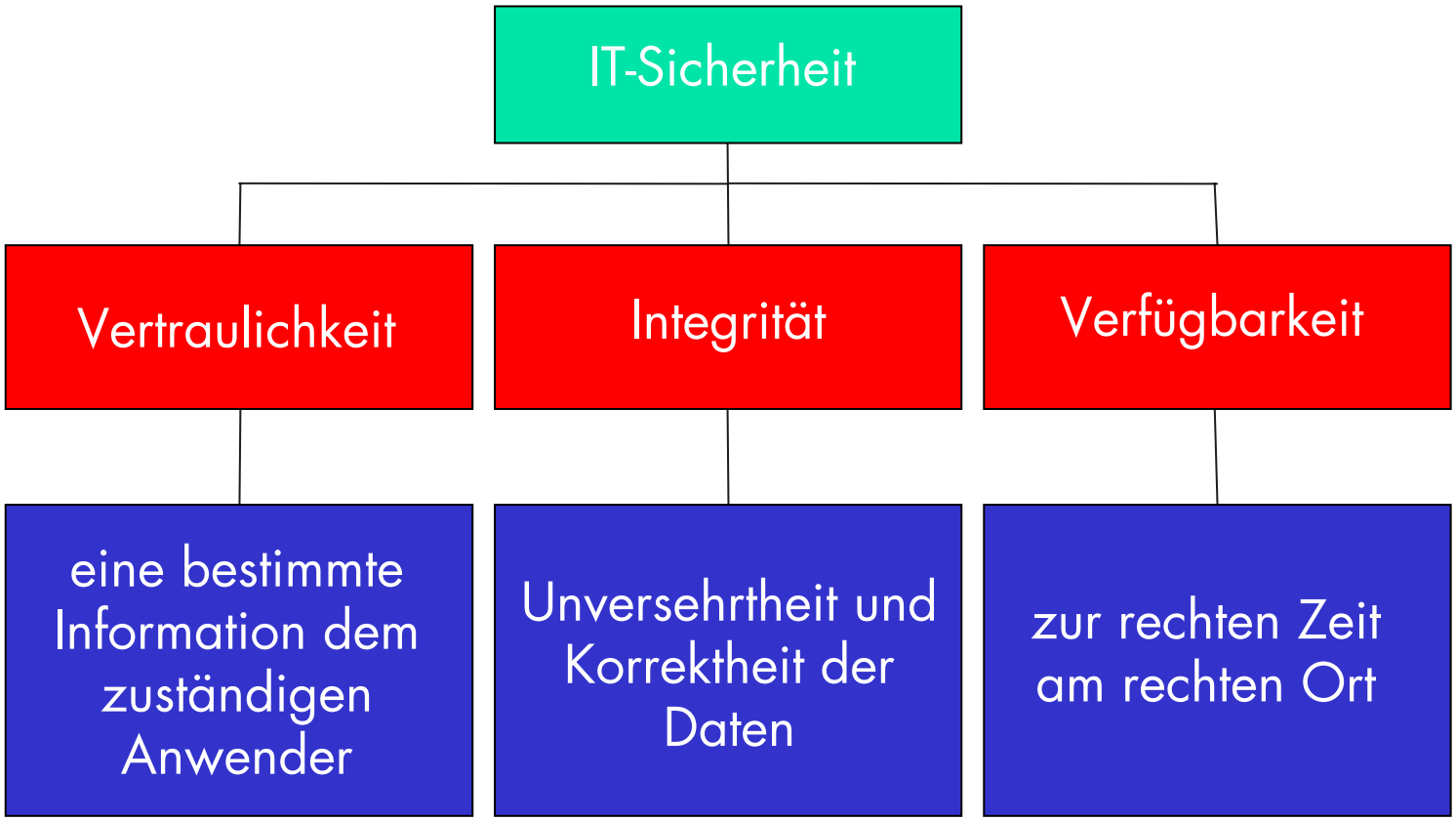
Motivation

- Erstellung Sicherheitskonzept notwendig:
  - Akzeptanz bei externen Partnern
  - Arbeitsgrundlage für eigene Aufgaben
  - IT-Qualitätssicherung
  - Sponsor-Audits
  - Begutachtung und Reviews
  - Validierung der Systeme und Verfahren
  - …

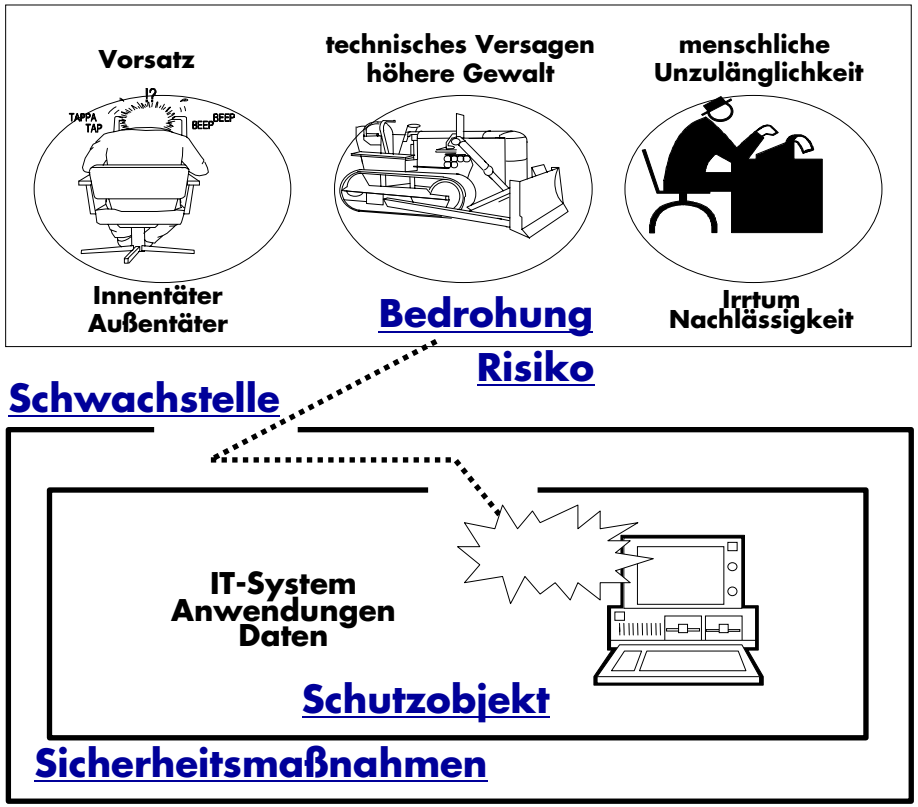
Fragen

- Wie sind die gesetzlichen Anforderungen ?
- Wie ist das Vorgehen bei der Erstellung ?
- Wer sind die Ansprechpartner ?
- Wer prüft/zertifiziert das Sicherheitskonzept ?
- Gibt es Vorarbeiten oder Muster für ein derartiges Sicherheitskonzept ?
- Was bedeutet IT-Sicherheit ?

Grundwerte der IT-Sicherheit



Bedrohungen für die IT-Sicherheit



aus „Folien zum IT-Grundschutz “, Bundesamt für Sicherheit in der Informationstechnik, Bonn

IT-Sicherheitsprozess

Methoden für Sicherheitskonzepte

- CobiT
  - Control Objectives for Information and Related Technology
  - ISACA (Information Systems Audit and Control Association)
- ISO/IEC 17799 und BS 7799
  - ISO/IEC 17799:2005 (Information technology – Code of practice for information security management)
- ITSEC / Common Criteria
  - Common Criteria for Information Technology Security Evaluation
- IT-Grundschutzhandbuch
  - Bundesamt für Sicherheit in der Informationstechnologie

Vergleich der Methoden

System-bezogen		IT-GSHB	ISO 9000 ISO 13335 ISO 17799 CobiT
	Task Force Sicheres Internet	DS-Produktaudit	
Produkt-bezogen	FIPS 140 ITSEC/CC		
	Technisch		Nicht technisch

aus „IT-Sicherheitskriterien im Vergleich“, INITI@TIVE D21, Berlin 2001

IT-Grundschutzhandbuch

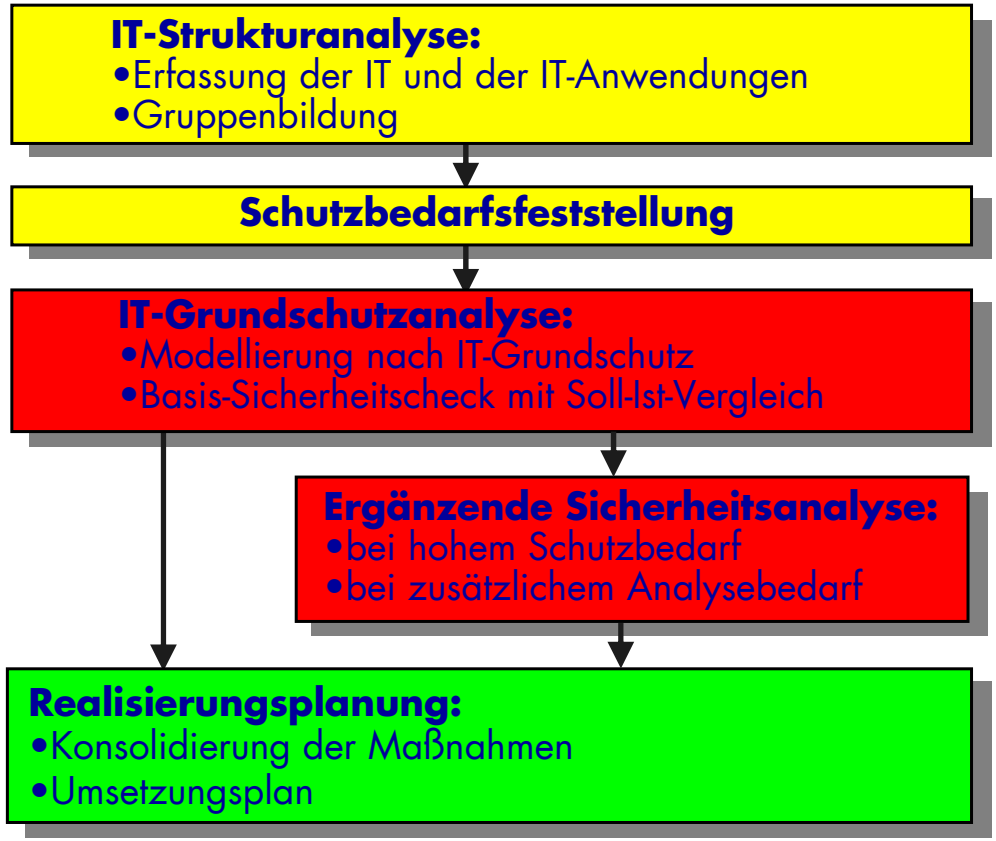
Vorgehen

- Basis eines IT-Grundschutzkonzepts ist der initiale Verzicht auf eine detaillierte Risikoanalyse
- Annahme von pauschalen Gefährdungen
- umfangreiche Maßnahmenkataloge
- Unterstützung durch GSTOOL

Idee

- Gesamtsystem enthält typische Komponenten (z.B. Server und Clients, Betriebssysteme)
- Pauschalisierte Gefährdungen und Eintrittswahrscheinlichkeiten
- Empfehlung geeigneter Bündel von Standard-Sicherheitsmaßnahmen
- konkrete Umsetzungshinweise für Maßnahmen

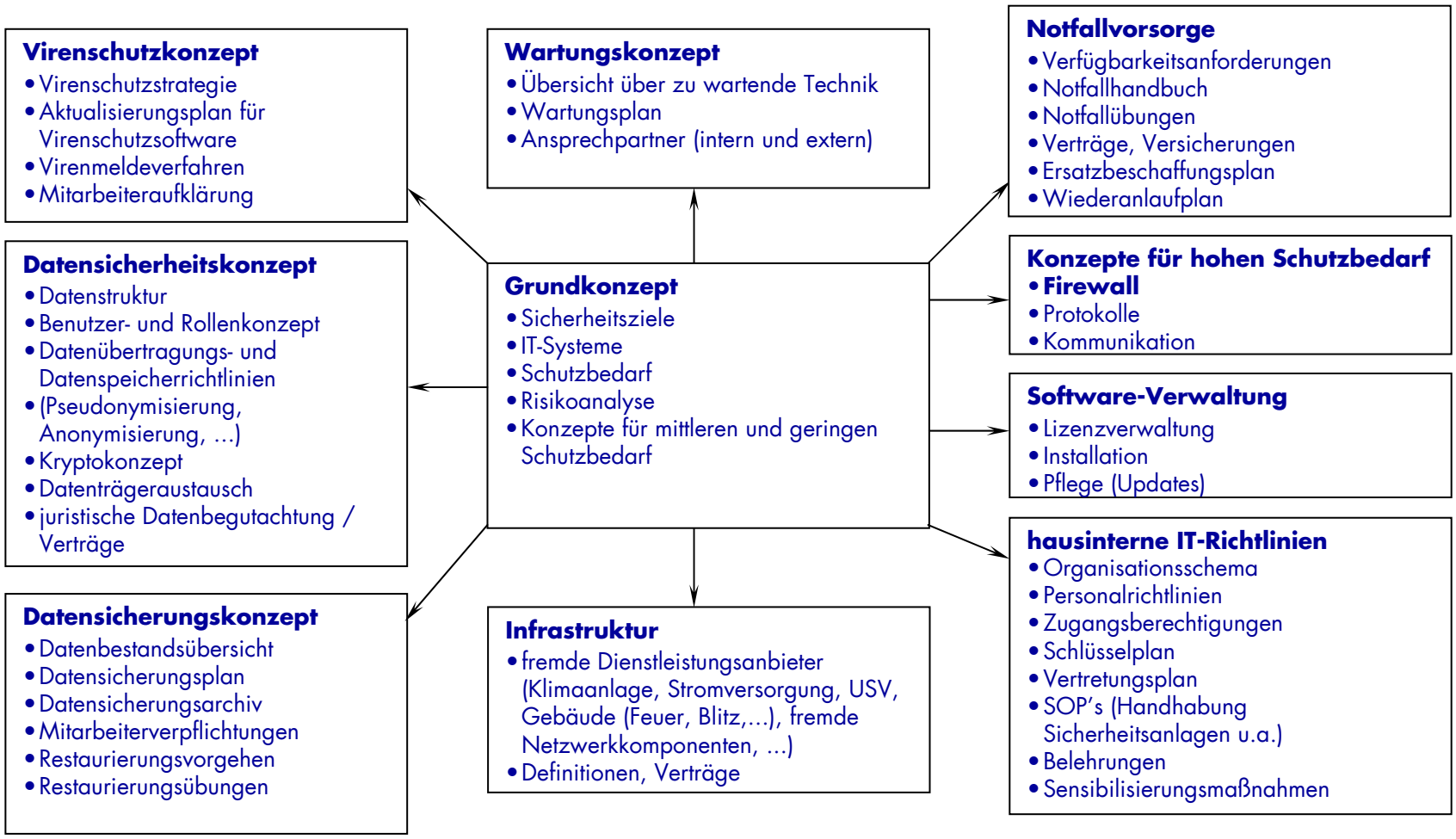
Vorgehen IT-Grundschutz



Realisierung im IT-Verbund

- Etablierung eines IT-Sicherheitsmanagements
- Erstellung eines Grundkonzeptes auf Basis des IT-Grundschutzhandbuches
- Erarbeitung weiterer Module
- Umsetzung der Maßnahmen
- Überprüfung der Umsetzung durch Audits und Tests (Extern, Intern)
- Zertifizierung des Sicherheitskonzeptes (BSI)

Module des Sicherheitskonzeptes



Fazit IT-Grundschutz

Vorteile

- arbeitsökonomische Anwendungsweise durch Soll-Ist-Vergleich
- kompakte IT-Sicherheitskonzepte durch Verweis auf Referenzquelle
- praxiserprobte Maßnahmen mit hoher Wirksamkeit
- Systemunabhängigkeit, Erweiterbarkeit und Aktualisierbarkeit
- Überprüfung und Nachweis des Umsetzungsgrades der Maßnahmen

Nachteile

- fehlende Risikoanalyse
- zu hoher Detaillierungsgrad
- fehlende Maßnahmen für hohen und sehr hohen Schutz bedarf
- hohe Anforderungen an Ressourcen

Kombination von Methoden

- ISO 17799 + IT-Grundschutzhandbuch

→ ISO 17799 beschreibt Management von Informationssicherheit
→ prozess-orientierter Ansatz
→ generische Maßnahmen im Sinne von „Best Practise“
→ Absicherung gegen relevante Bedrohungen durch konkrete Maßnahmen aus dem IT-Grundschutz

- strikte Trennung von Steuerung und Umsetzung

- ISO 27799: Security management ISO 27799: Security management in in health using ISO/IEC 17799

Fazit

- prinzipiell IT-Grundschutz gut geeignet
- Problem der zusätzlichen Maßnahmen bei hohem Schutzbedarf
- Risikoanalyse / Detaillierungsgrad

→ Kombination mit ISO 27799 ?

- Ressourcenanforderungen problematisch
- Aufwand für Pflege und Aktualisierung

➧ bei Planung berücksichtigen !

Vielen Dank für ihre Aufmerksamkeit !

Kontakt
Ronald Speer
ronald.speer@imise.uni-leipzig.de

Vielen Dank an
Barbara Heller, Wolfgang Dolak,
Frank Meineke, Jan Ramsch