Technische Realisierung von Datenschutz in Unternehmen

Prof. Dr. Hannes Federrath
Universität Regensburg

Begriffe

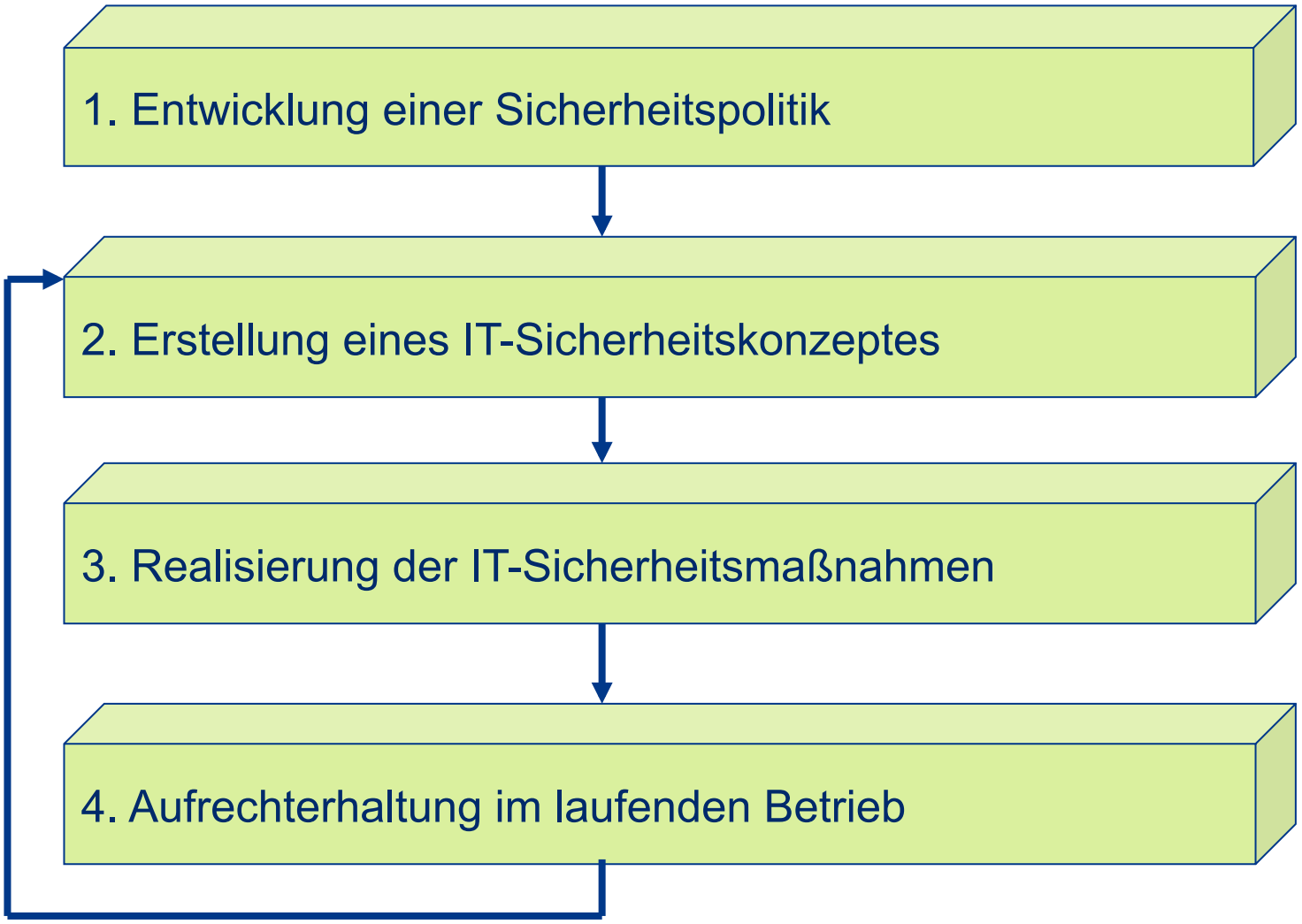
IT-Sicherheitsmanagement

- IT-Sicherheitsmanagement versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe (Security) und unbeabsichtigte Ereignisse (Safety) zu schützen.

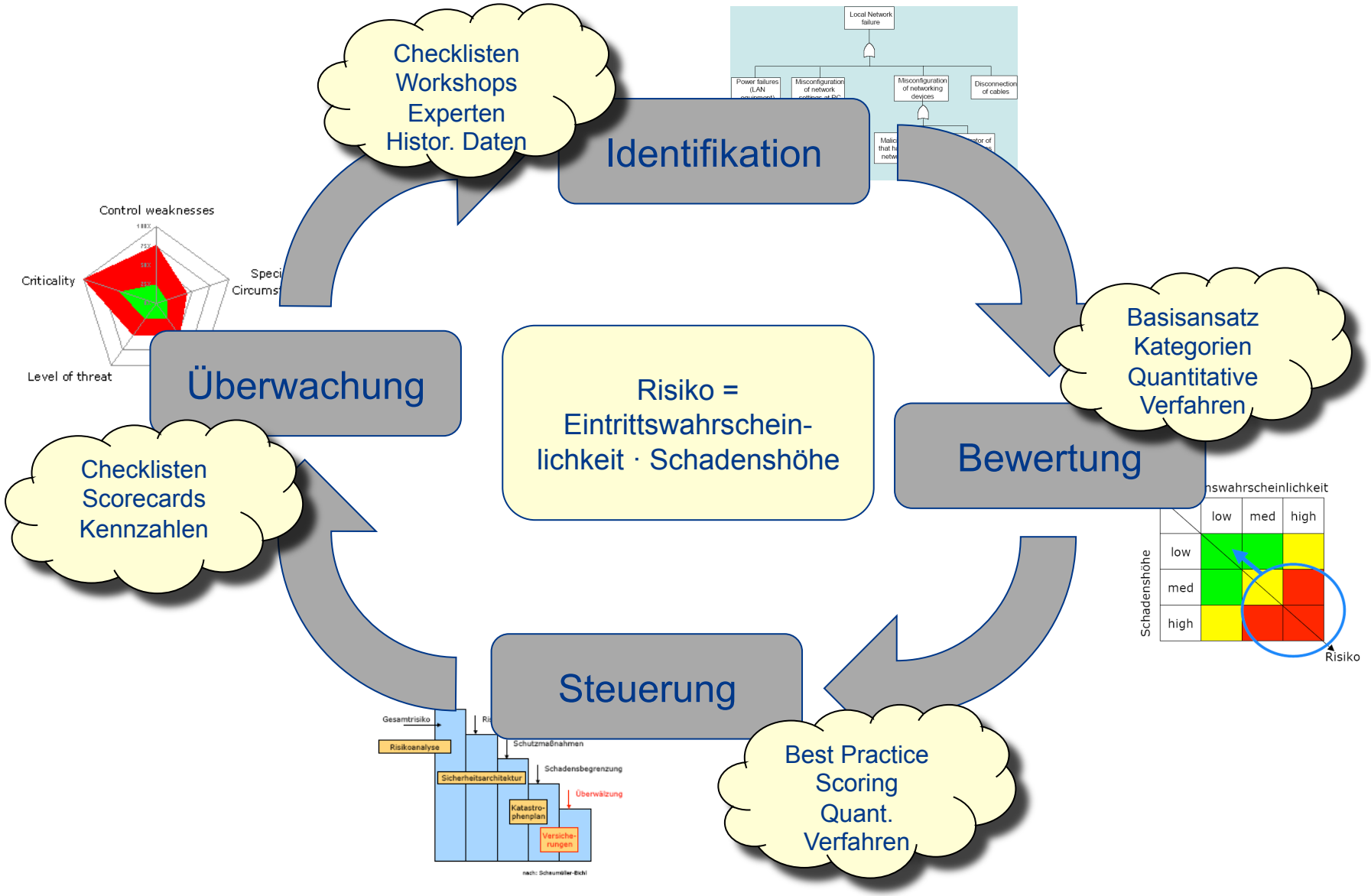
Datenschutz

- Mit dem Begriff Datenschutz wird das Recht des Einzelnen auf informationelle Selbstbestimmung umschrieben. «Das Grundrecht gewährleistet [...] die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.» (BVerfG) Eine Organisation hat technisch-organisatorische Maßnahmen zu treffen, um dieses Recht zu gewährleisten.

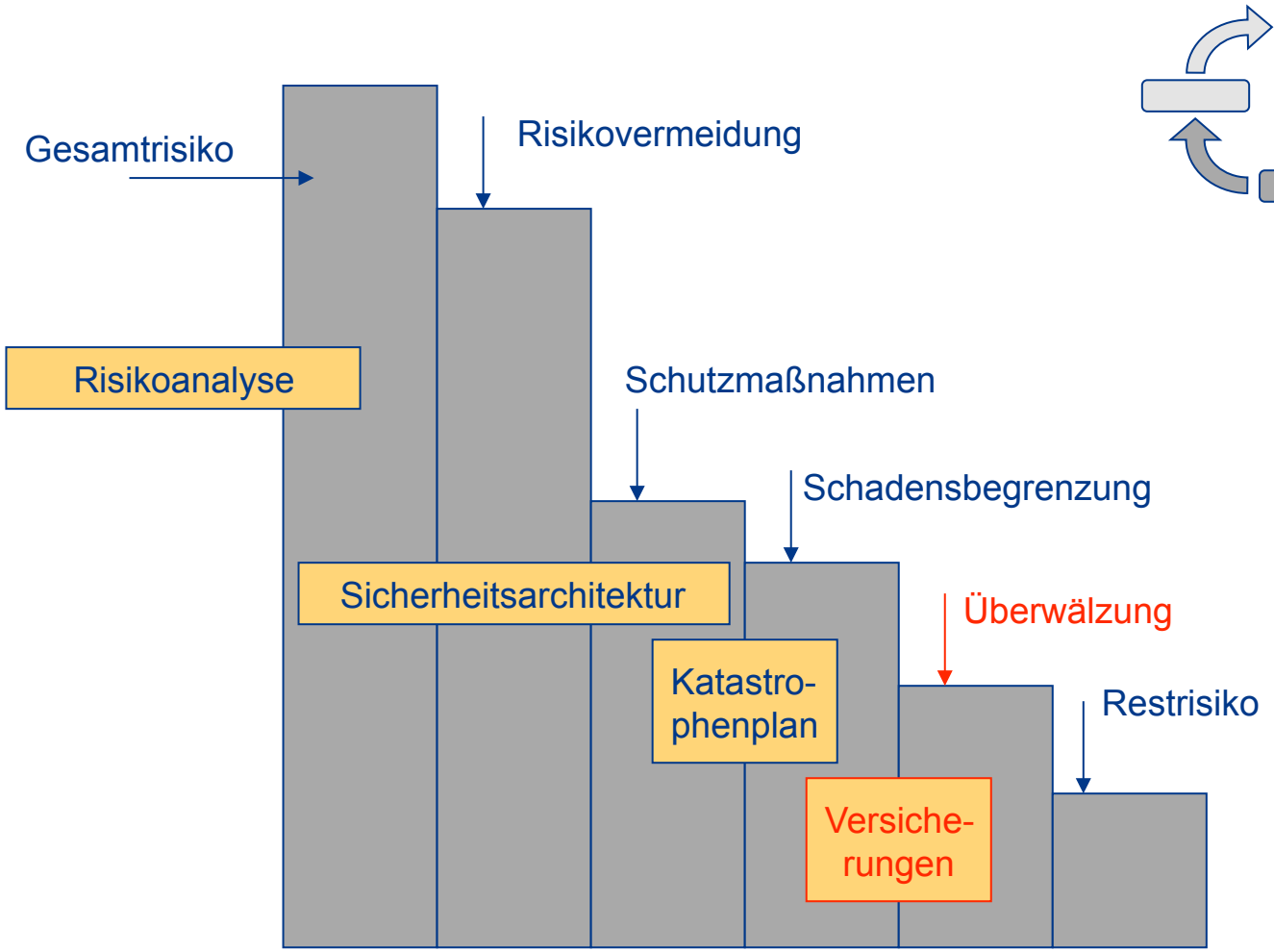
Sicherheitsmanagement-Vorgehensmodell



Risikomanagement Kreislauf

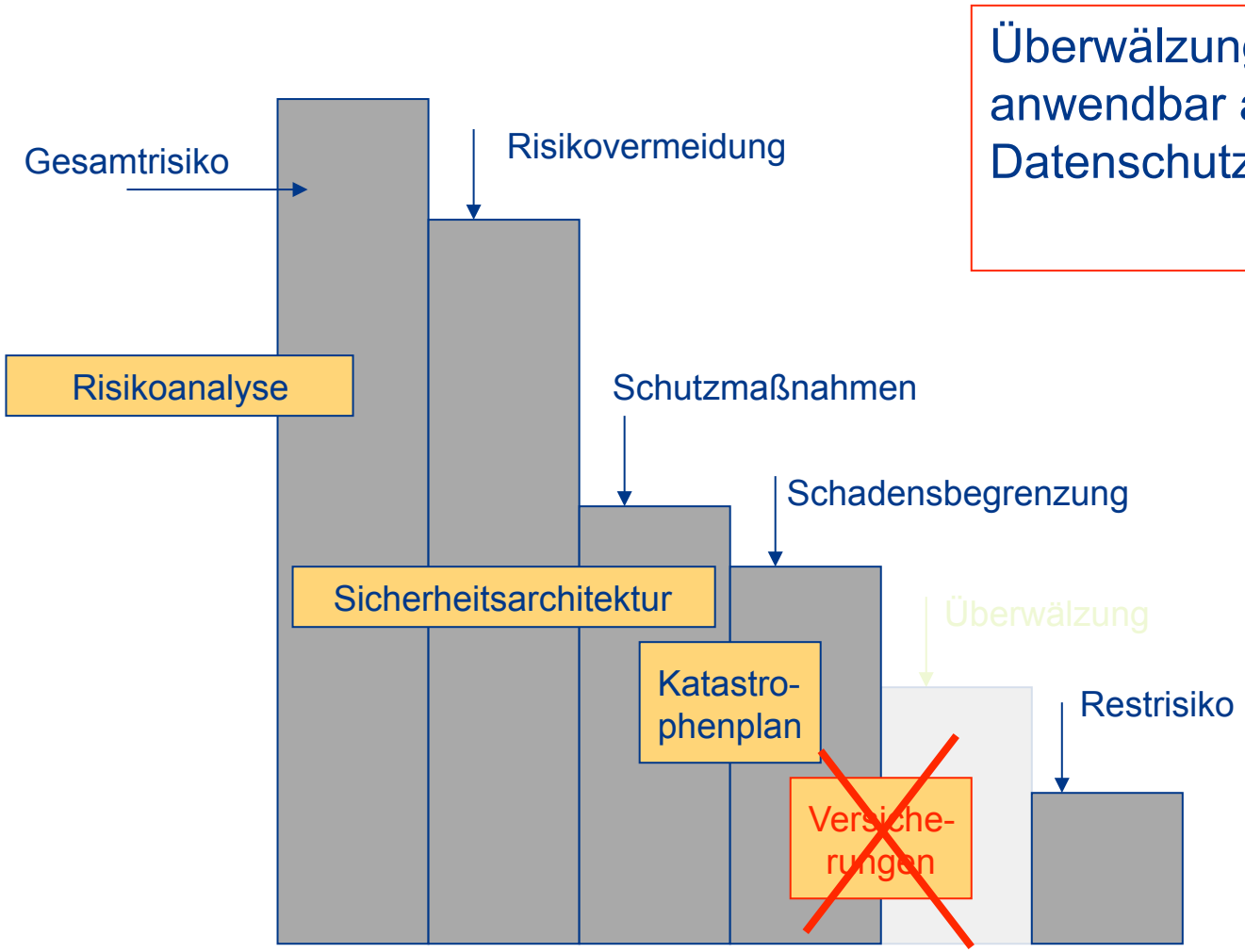


Risiko-Management für IT-Systeme



nach: Schaumüller-Bichl

Risiko-Management für IT-Systeme



Überwälzung nicht anwendbar auf Datenschutz

nach: Schaumüller-Bichl

Risiko-Management im Datenschutz

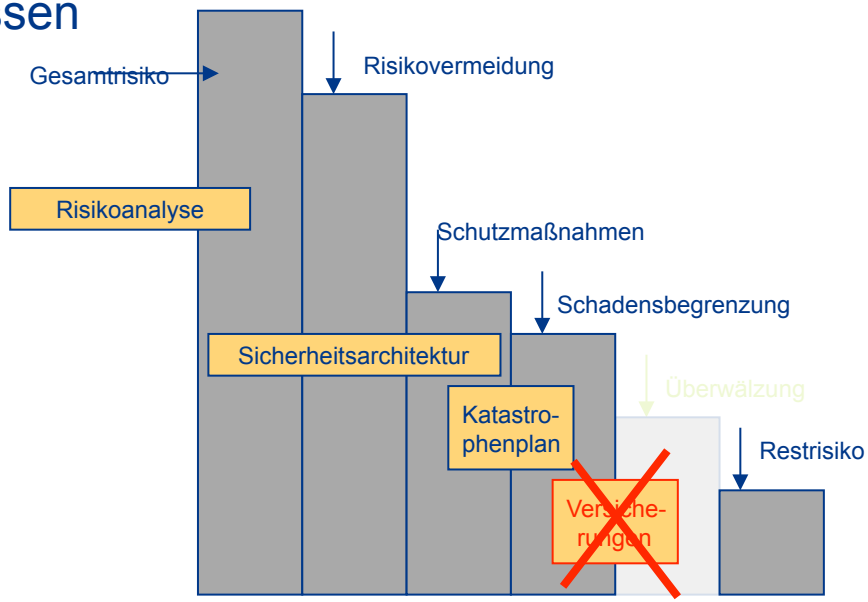
IT-Sicherheit:

- Risiko = Wahrscheinlichkeit · Schadenshöhe
- Schäden sind systematisch tolerierbar

Überwälzung nicht anwendbar auf Datenschutz

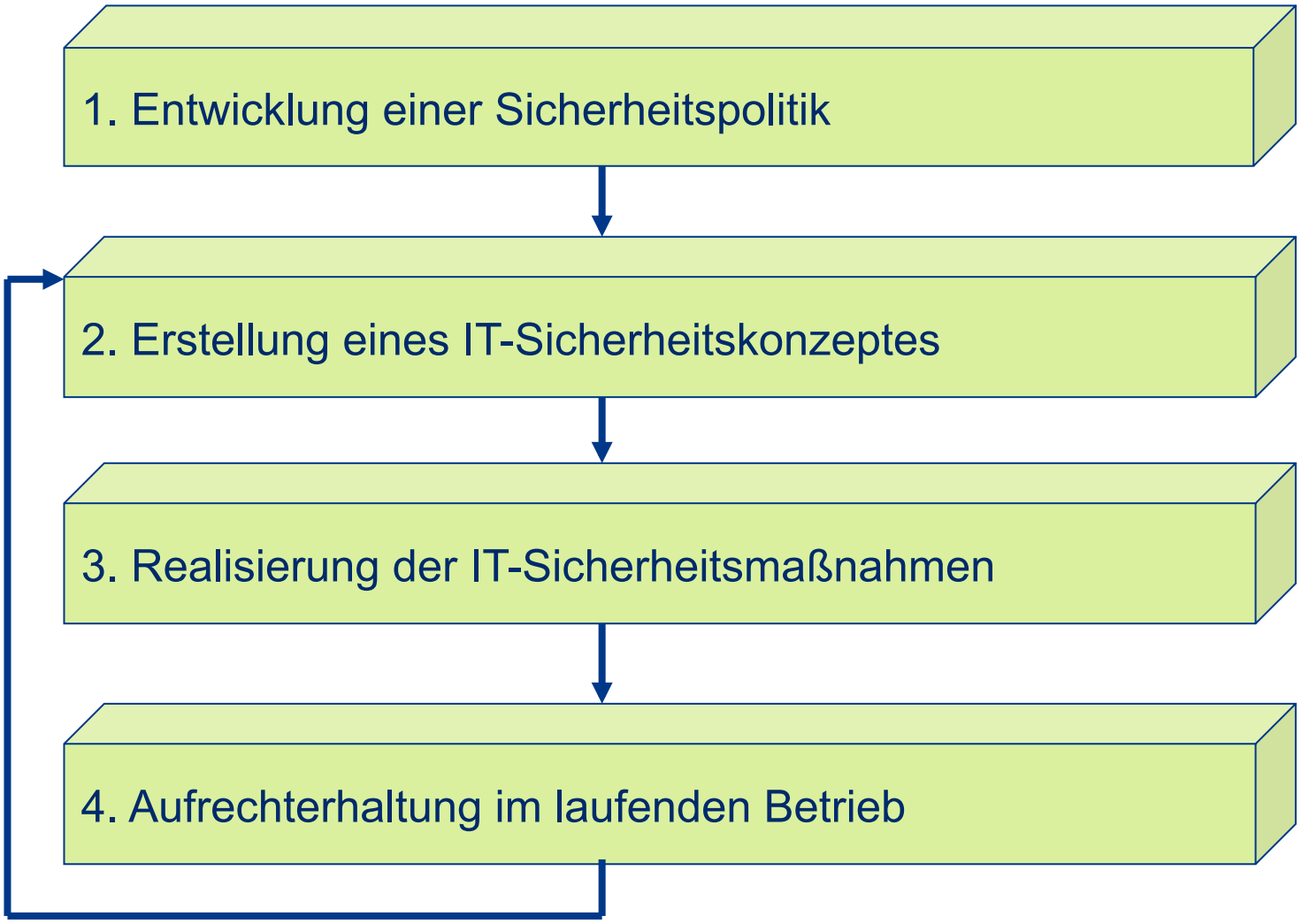
Datenschutz:

- Alles-Oder-Nichts-Ansatz
- Rechtliche Vorgaben müssen umgesetzt werden



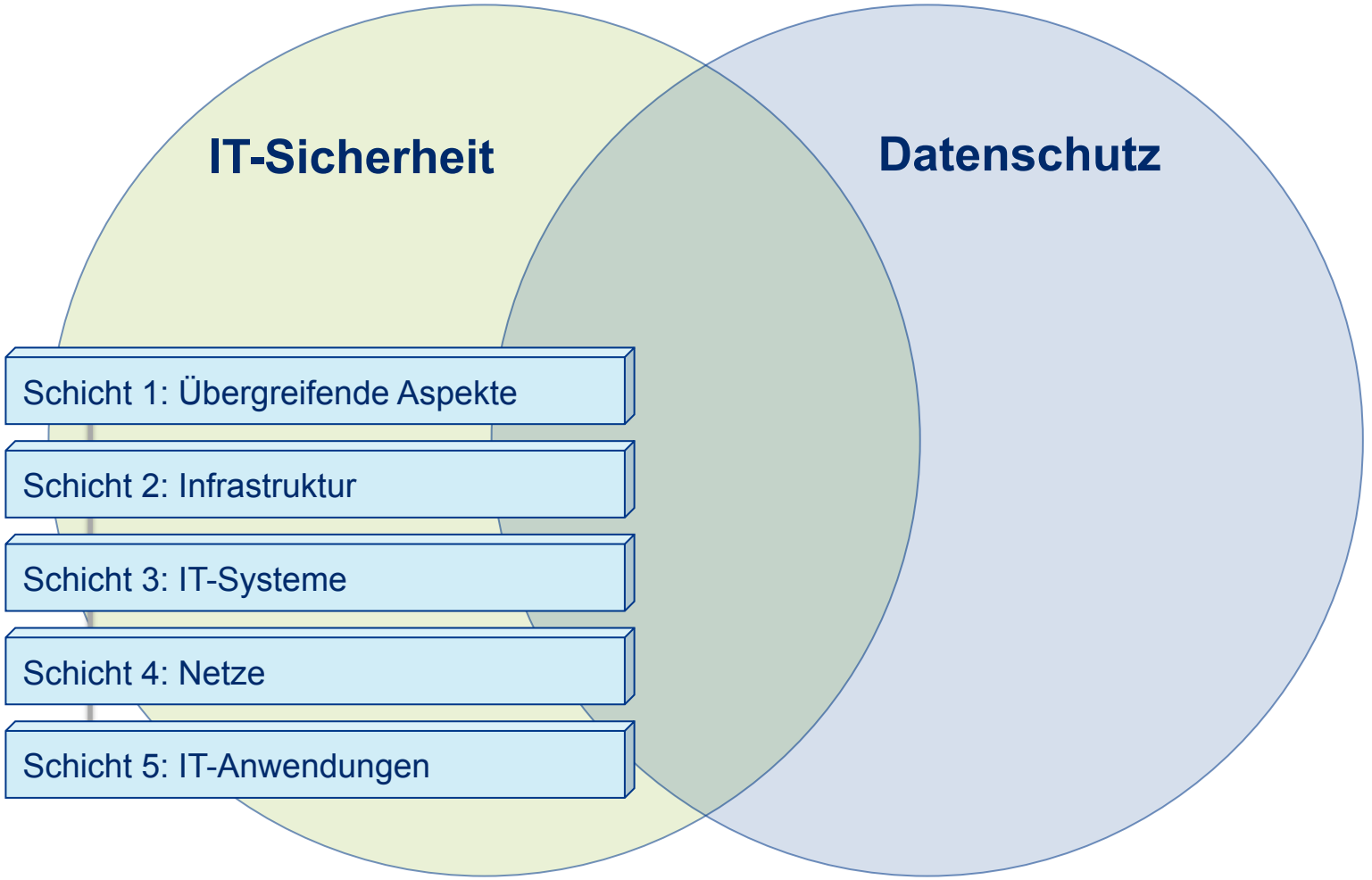
nach: Schaumüller-Bichl

Sicherheitsmanagement-Vorgehensmodell



Schichtenmodell nach IT-Grundschutz

Verknüpfung von Sicherheit und Datenschutz

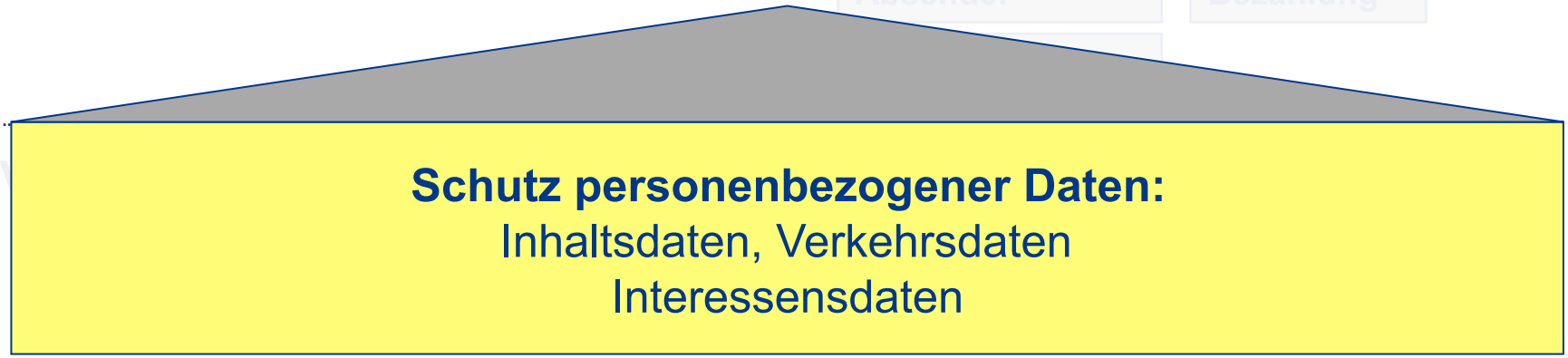


Was ist zu schützen?

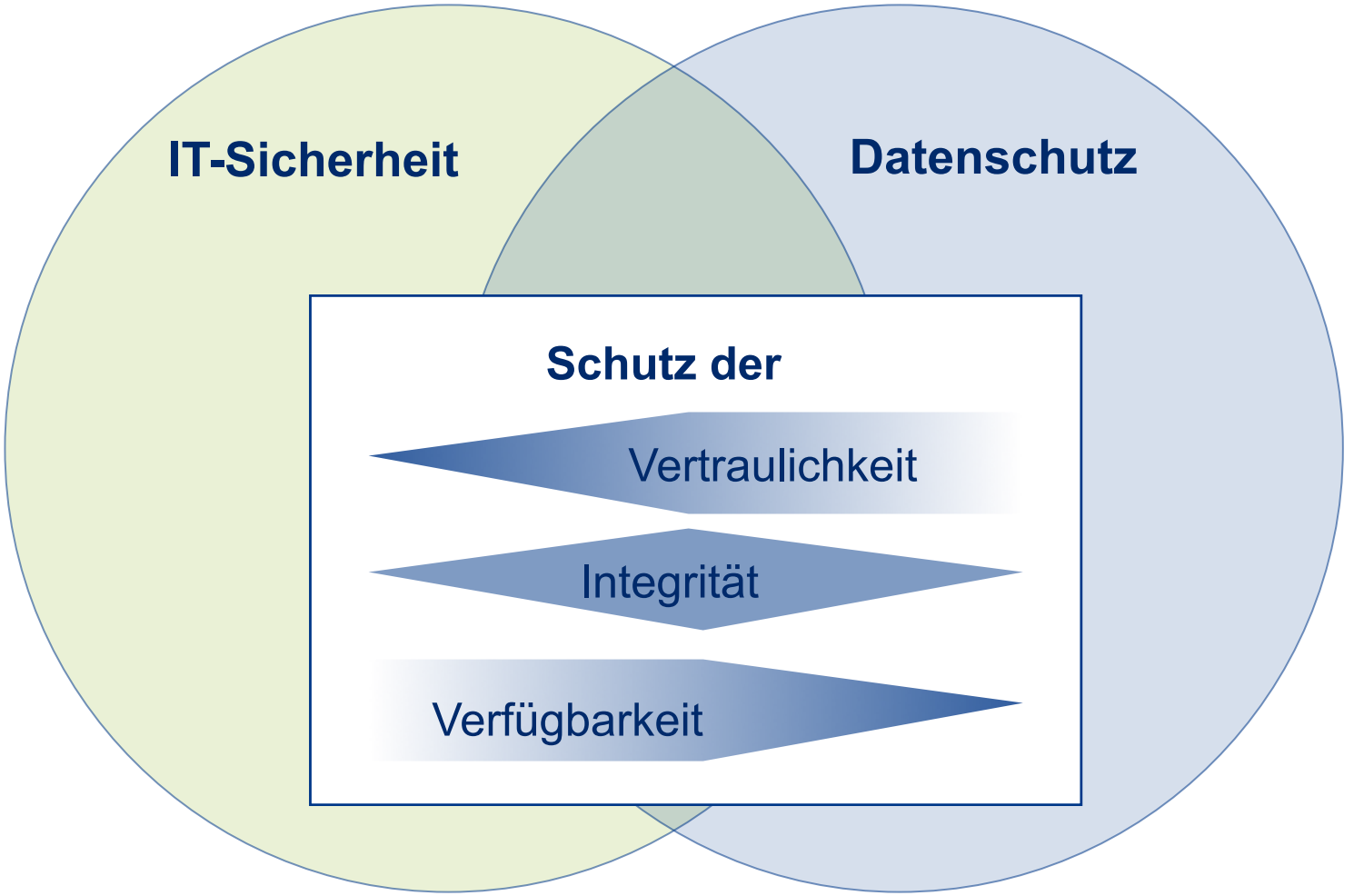
Kommunikationsgegenstand WAS?		Kommunikationsumstände WANN?, WO?, WER?
Vertraulichkeit Verdecktheit	Inhalte	Anonymität Unbeobachtbarkeit Sender, Ort, Empfänger
Integrität	Inhalte	Zurechenbarkeit Rechtsverbindlichkeit Absender, Bezahlung, Empfänger
Verfügbarkeit	Inhalte	Erreichbarkeit Nutzer, Rechner

Datenschutz

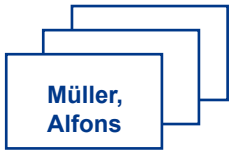
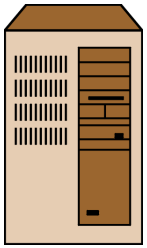
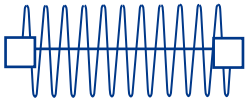
Kommunikationsgegenstand WAS?	Kommunikationsumstände WANN?, WO?, WER?
Vertraulichkeit **Verdecktheit**	**Anonymität** **Unbeobachtbarkeit**
Integrität	**Zurechenbarkeit** **Rechtsverbindlichkeit**



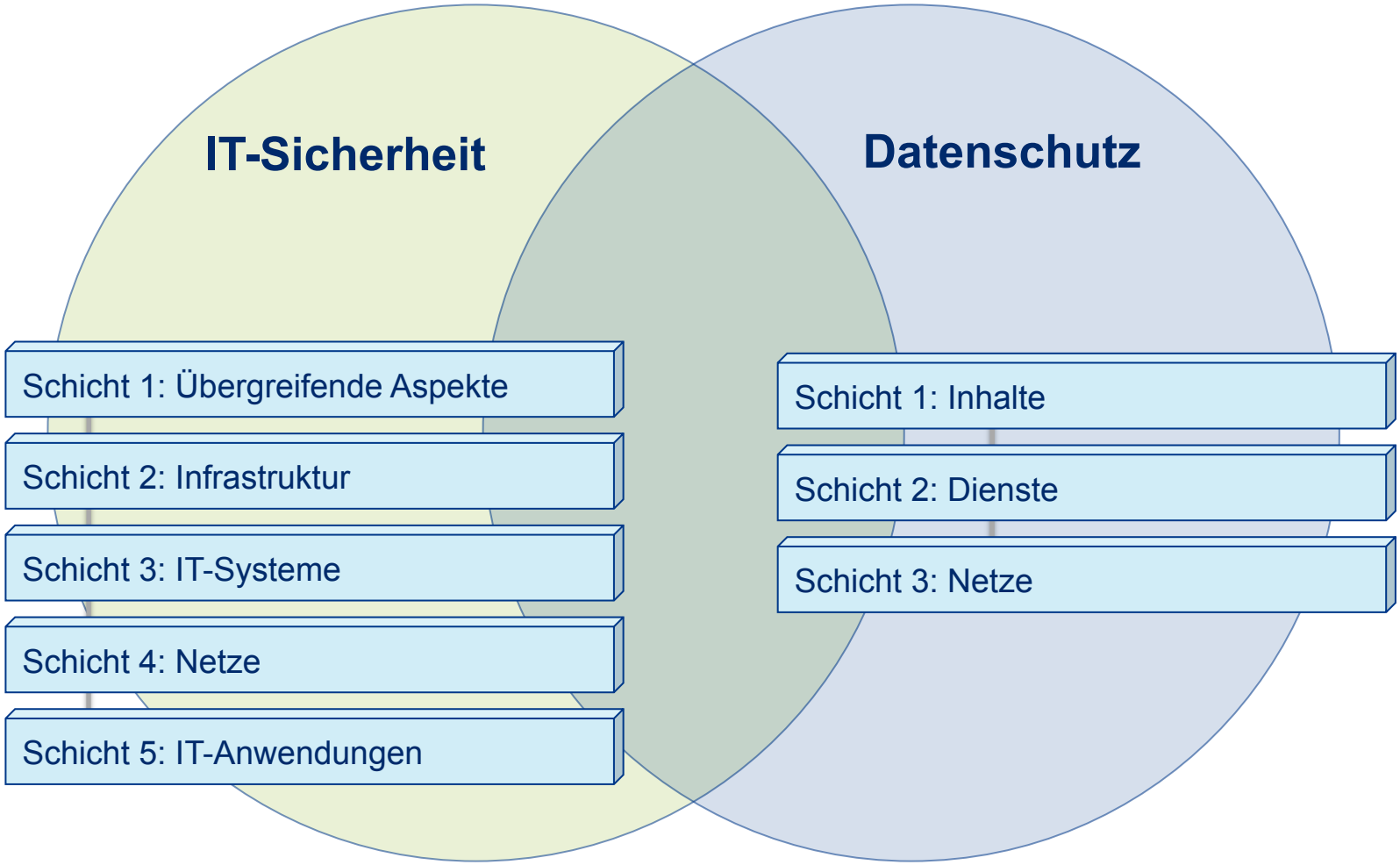
Verknüpfung von Sicherheit und Datenschutz



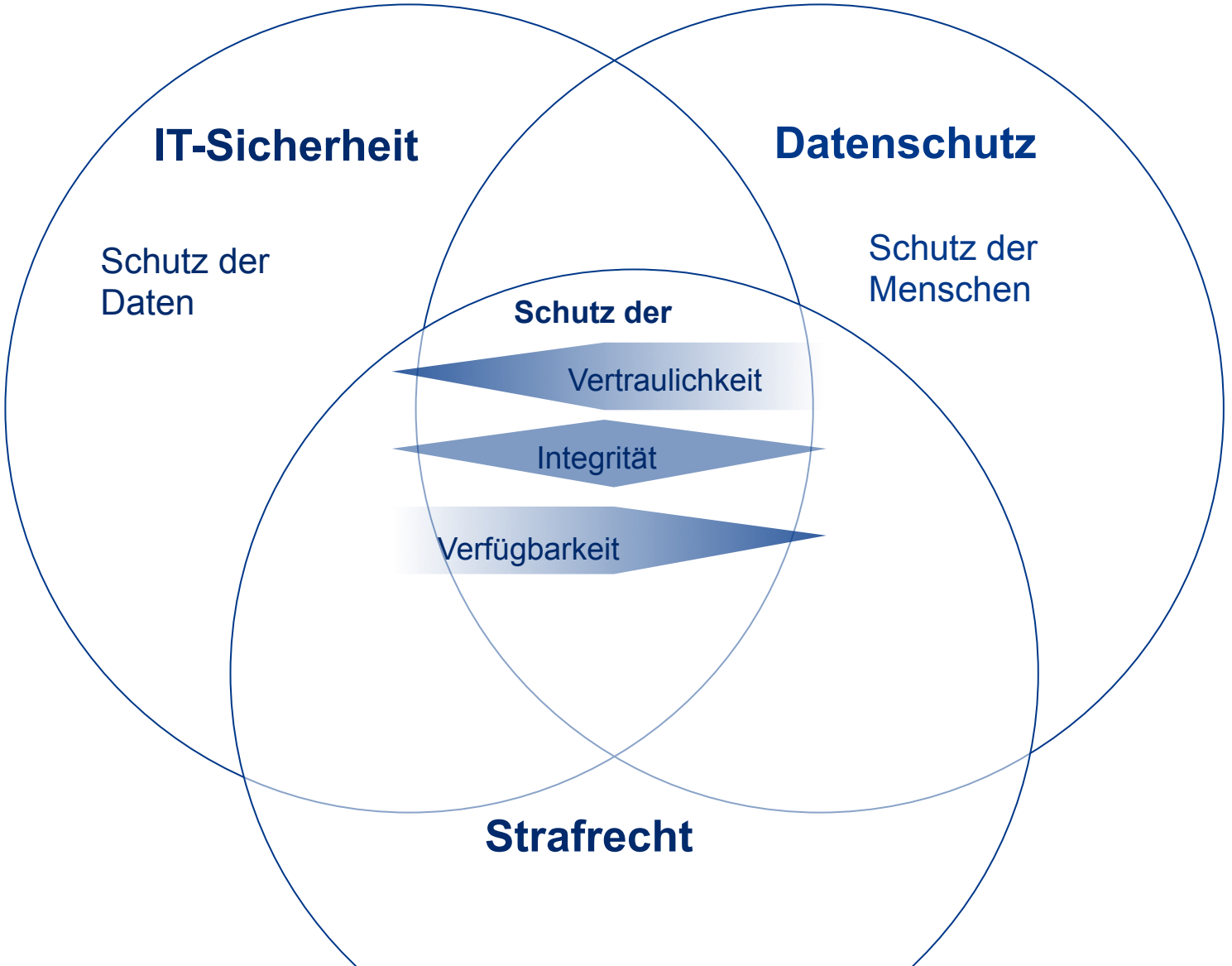
«Drei Schichten» des Datenschutzrechts in Netzen

Ebene der Anwendung/Inhalte		z.B. Kundendaten nach Warenbestellung im virtuellen Kaufhaus	**BDSG, LDSG**
Ebene der Dienste «Internet»		z.B. **Clickstream** nach Zugriff auf den Web-Server	**TMG**
Ebene der Netze «Telekommunikation»		z.B. **ISDN-Verkehr** über die Leitungen der Telekom zwischen dem Nutzer und dem Access-Provider	**TKG**

Verknüpfung von Sicherheit und Datenschutz



Verknüpfung von Sicherheit, Datenschutz und Strafrecht



IT-Sicherheit aus strafrechtlicher Sicht

Vertraulichkeit

- § 202a StGB Ausspähen von Daten
- § 203 StGB Verletzung von Privatgeheimnissen

Integrität

- § 263a StGB Computerbetrug
- § 265a StGB Erschleichen von Leistungen
- § 268 StGB Fälschung technischer Aufzeichnungen
- § 269 StGB Fälschung beweiserheblicher Daten
- § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung
- § 303a StGB Datenveränderung

Verfügbarkeit

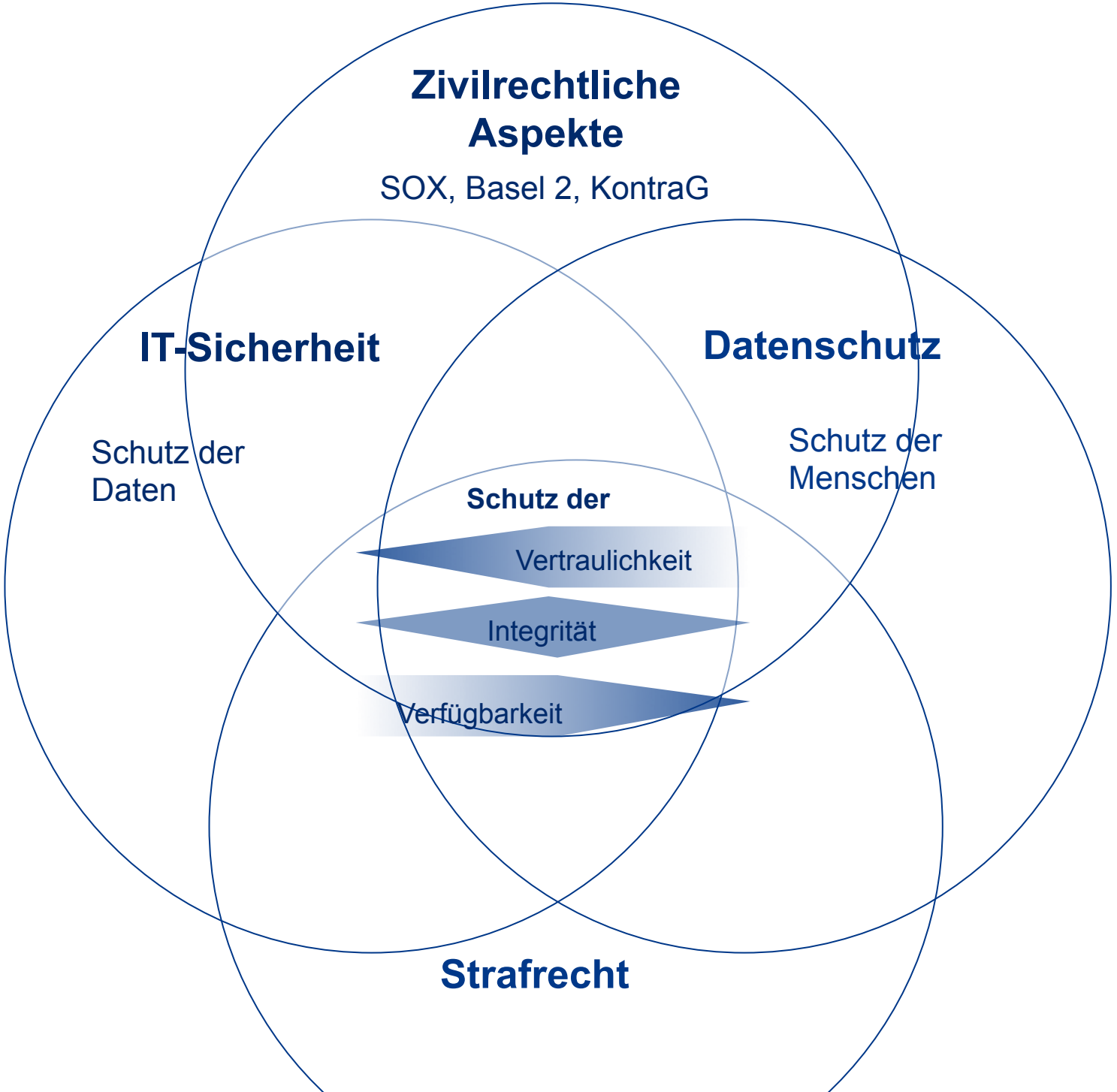
- § 303b StGB Computersabotage

Strafandrohung

- zwischen 2 und 5 Jahren Freiheitsstrafe oder Geldstrafe

Beschlagnahme von Beweismitteln

- § 94 Strafprozessordnung StPO
- Datenträger oder ganze Computersysteme


Zivilrechtliche Aspekte
SOX, Basel 2, KontraG
IT-Sicherheit
Schutz der Daten
Datenschutz
Schutz der Menschen
Schutz der
Vertraulichkeit
Integrität
Verfügbarkeit
Strafrecht

Goldene Regeln zur Umsetzung von Datenschutz

Aus Sicht der IT-Sicherheit:

- Informieren (Transparenz)
- Auskunftsverfahren etablieren
- Einwilligung, wo nötig
- Weniger (speichern) ist mehr (Datenschutz)
- Regelmäßige Sensibilisierung (wie Umwelt- und Arbeitsschutz)
- Sanktionen bei Verstößen klarmachen
- Aber: Kontrollieren und beraten, nicht gleich bestrafen!

Immer fragen: Was ist die Grundlage der Erhebung/Verarbeitung/Speicherung?

- Einwilligung?
- Gesetzliche Vorgabe?
- Aufrechterhaltung des laufenden Betriebs? (IT-Sicherheit)

Zusammenfassung

IT-Sicherheit

kaum gesetzliche Vorgaben

etablierte Standards (best practices), konkrete Vorgehensmodelle enthalten auch Datenschutz

meist freiwillig umgesetzt

Im Mittelpunkt stehen die Interessen des Betreibers und deren Nutzer.

Datenschutz

höhere Regelungsdichte

wenig konkrete Vorgaben (technisch organisatorische Maßnahmen nach BDSG § 9)

gesetzlicher »Zwang«

Im Mittelpunkt stehen die Interessen des Betroffenen.

IT-Sicherheit und Datenschutz

- Beides ist notwendig
- Ähnliche Mechanismen und Vorgehensweise
- Prävention ist besser als Reaktion
- IT-Sicherheit ohne Datenschutz geht nicht

Zusammenfassung

IT-Sicherheit

kaum gesetzliche Vorgaben

etab

Vorg

meis

Im M

Betr

Datenschutz

höhere Regelungsdichte

nig konkrete Vorgaben (technisch anisatorische Maßnahmen nach SG § 9)

setzlicher »Zwang«

Mittelpunkt stehen die Interessen des Betroffenen.

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg
D-93040 Regensburg

E-Mail: hannes.federrath@wiwi.uni-regensburg.de
WWW: http://www-sec.uni-regensburg.de

Phone +49-941-943-2870
Telefax +49-941-943-2888

IT-Sicherheit und Datenschutz

- Beides ist notwendig
- Ähnliche Mechanismen und Vorgehensweise
- Prävention ist besser als Reaktion
- IT-Sicherheit ohne Datenschutz geht nicht