

Security

Felix Widmer
TCG Tan Consulting Group GmbH
Hanflaenderstrasse 3
CH-8640 Rapperswil SG

Voice +41 (0)55 214 41 56
Fax +41 (0)55 214 41 57
Mobile +41 (0)79 336 56 76
E-Mail felix.widmer@tan-group.ch
Web www.tan-group.ch



Security

- Überblick
- Ziele und Rahmenbedingungen
- Methode / Modell
- IT-Grundschutz vs. Risikoanalyse



IT-Security ist ein Prozess...

IT-Security Analysen

- Ist-Aufnahme/Machbarkeitsstudie
- Schutzbedarf
- Bedrohungen & Schwachstellen
- Risiko.

IT-Security Betrieb

- Administration
- Monitoring
- Auditing/Revision
- Reporting.

IT-Security Policy

- Grundsätze
- Richtlinien & Standards
- Produktbezogene Richtlinien
- Hilfsmittel.

IT-Security Umsetzung

- IT-Grundschutz
- Erweiterter IT-Schutz
- Ziel- & Erfolgskontrolle.

IT-Security Planung

- IT-Sicherheitsmassnahmen
- Soll-/Ist-Vergleich.

Feedback

Sicherheitsziele

- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Verbindlichkeit

der Informationen, Prozesse und Systeme.

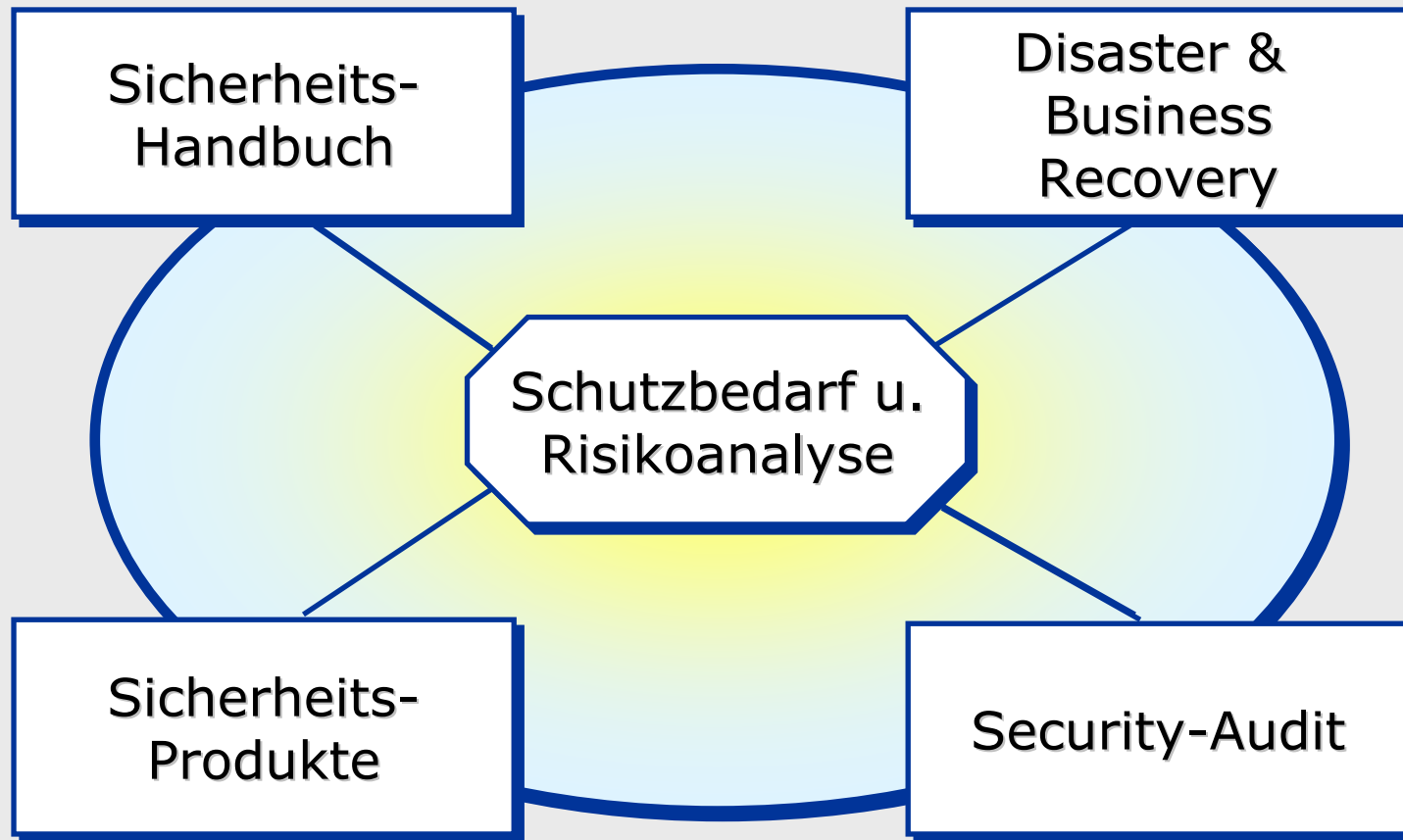


Rahmenbedingungen

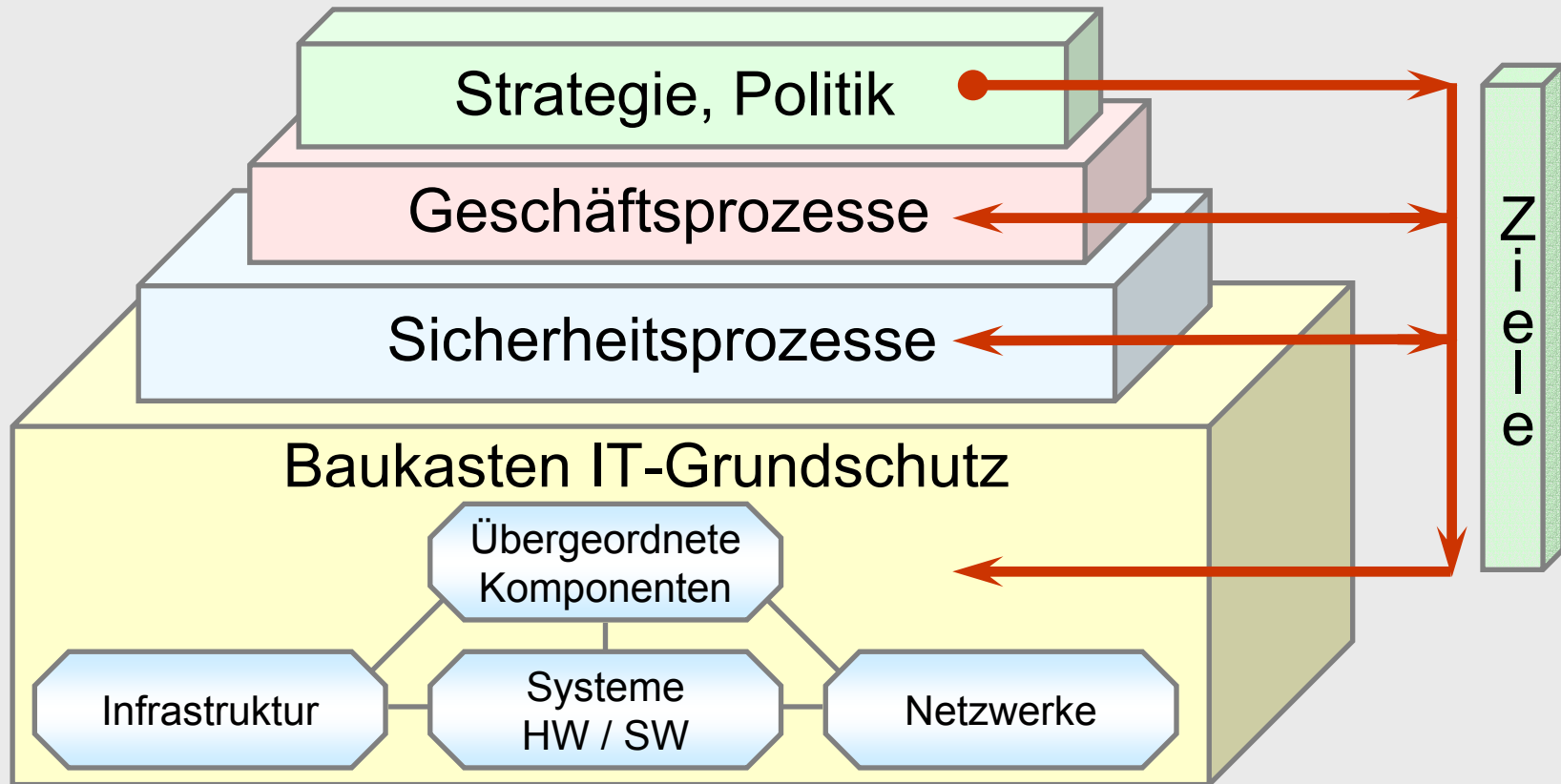
- Angemessenheit
- Wirtschaftlichkeit
- Technische Machbarkeit.



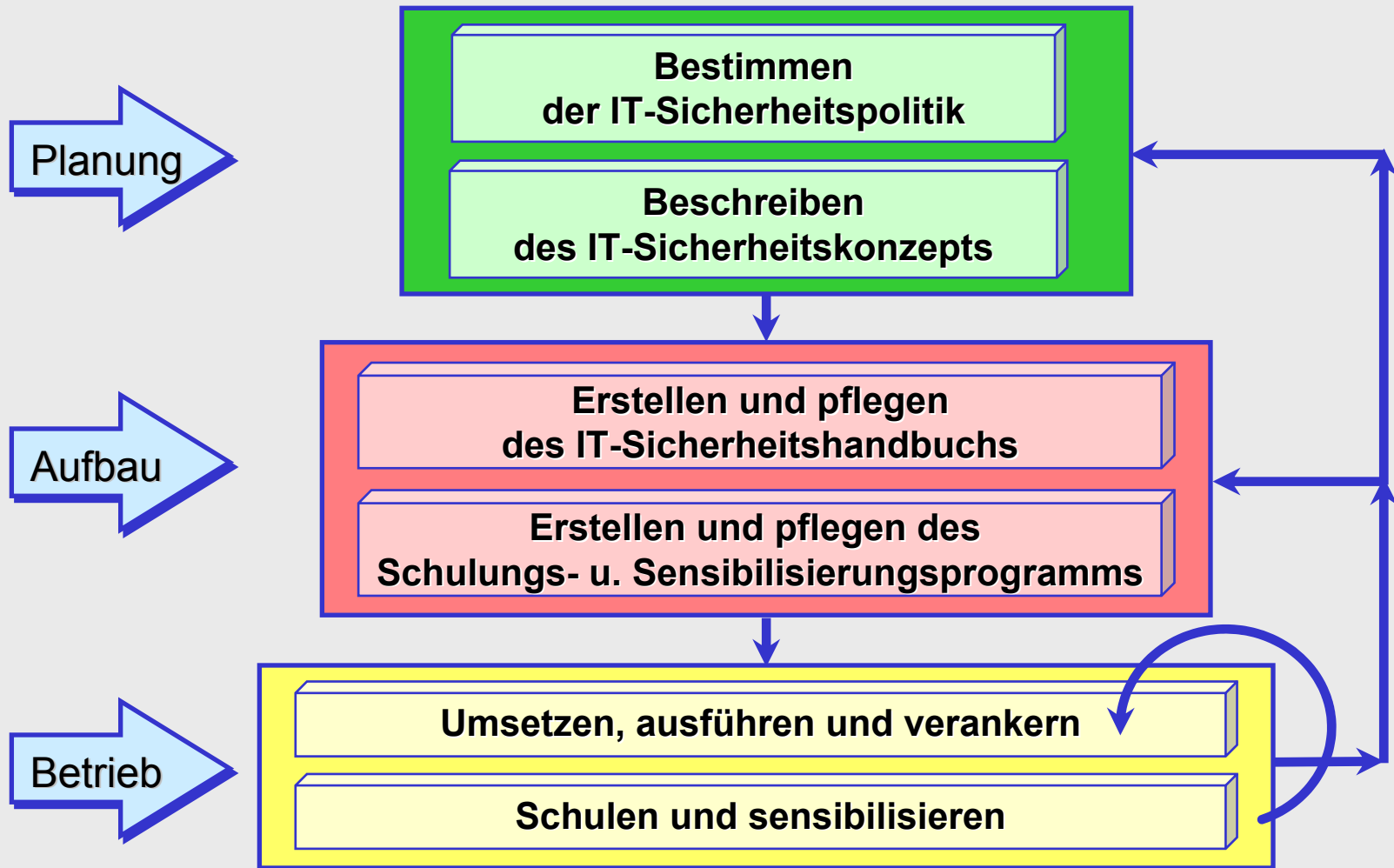
Security Portfolio



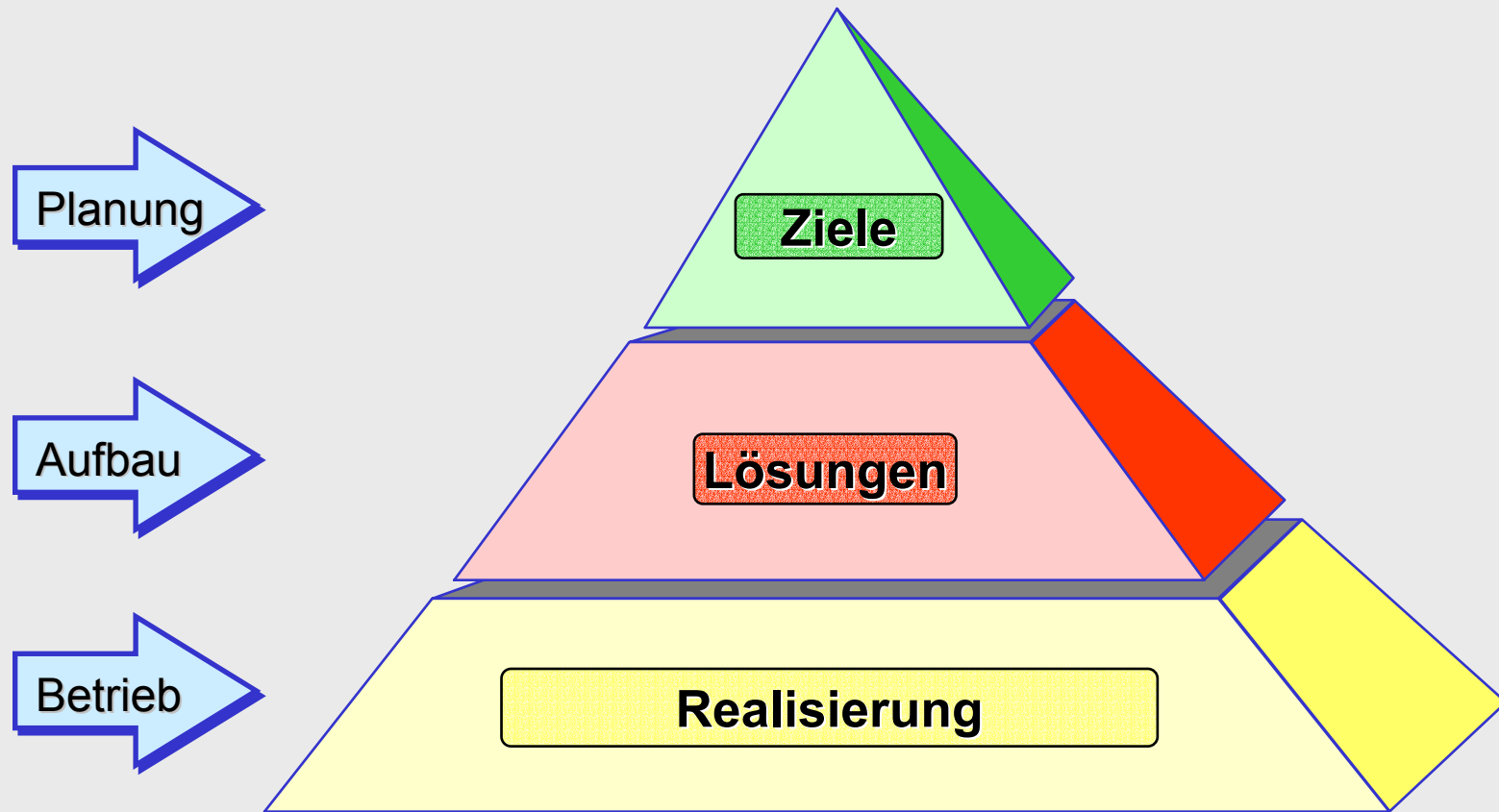
Methode: Security by Objectives



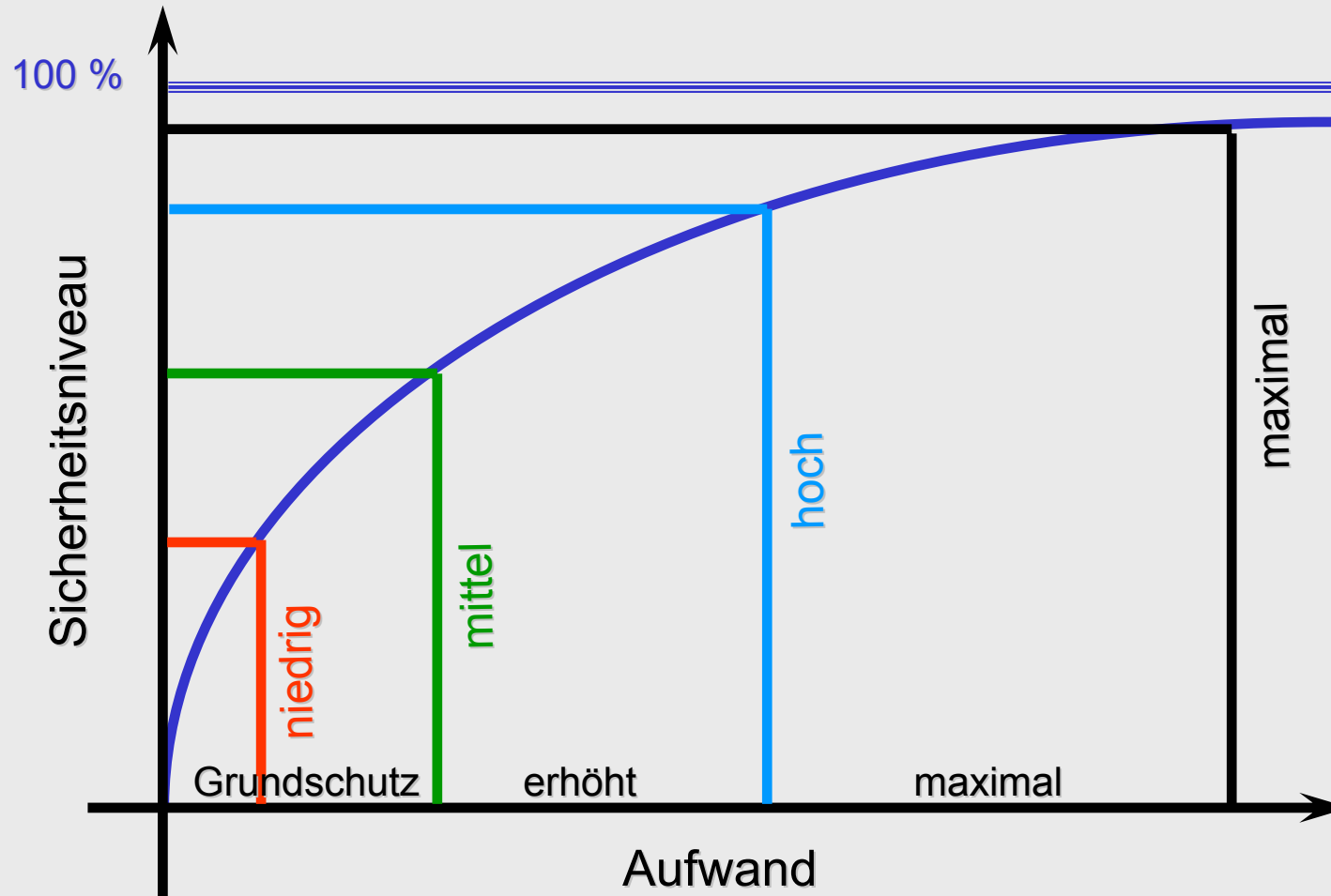
Prozess: IT-Sicherheitsmanagement



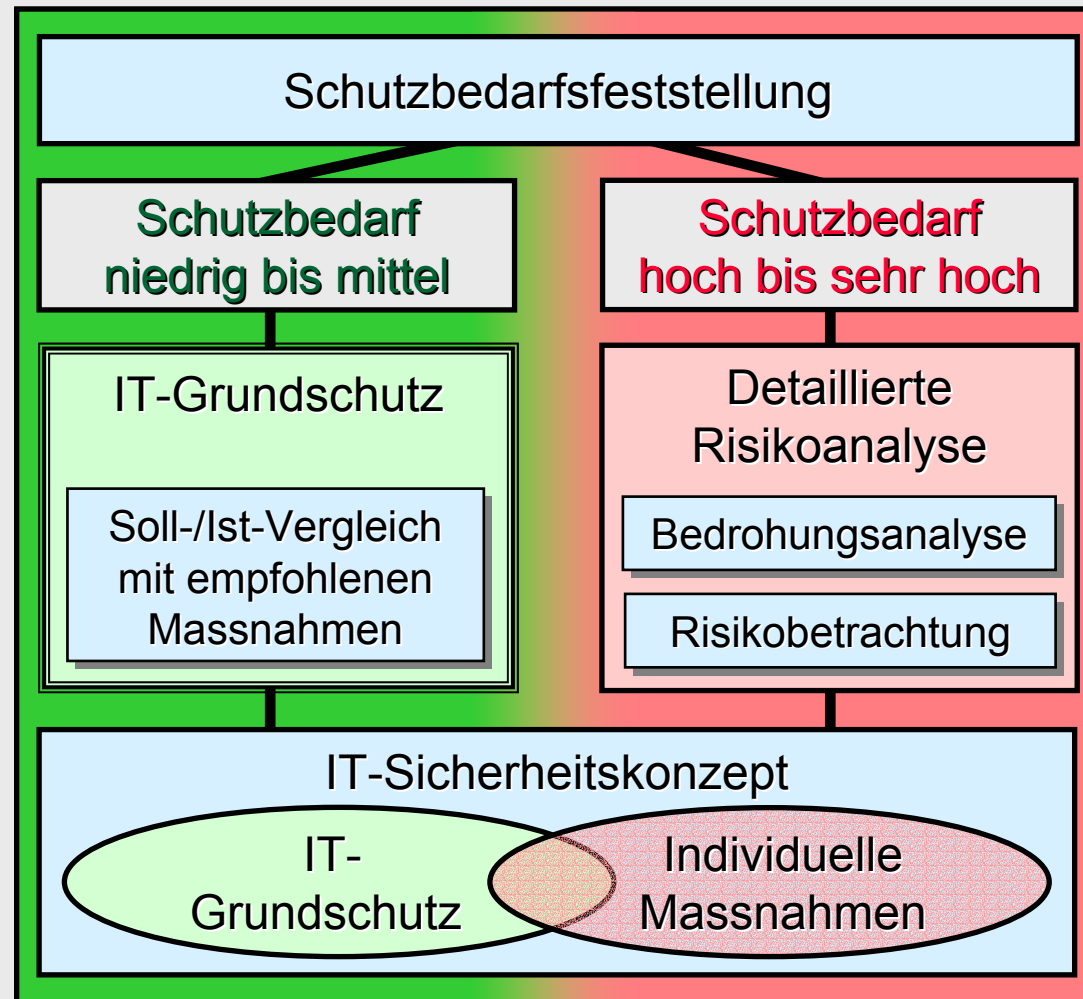
Vorgehensmodell



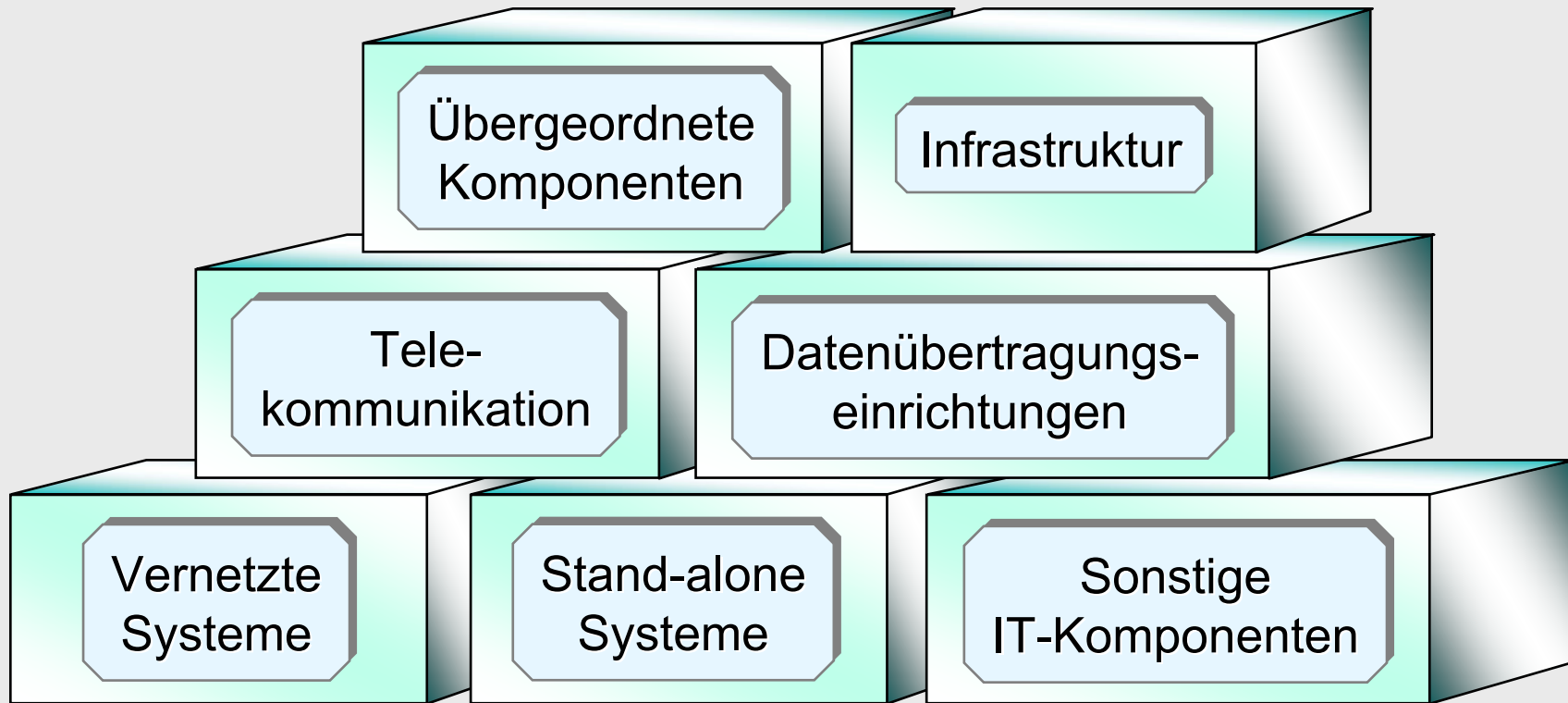
Ausgangspunkt: Schutzbedarf



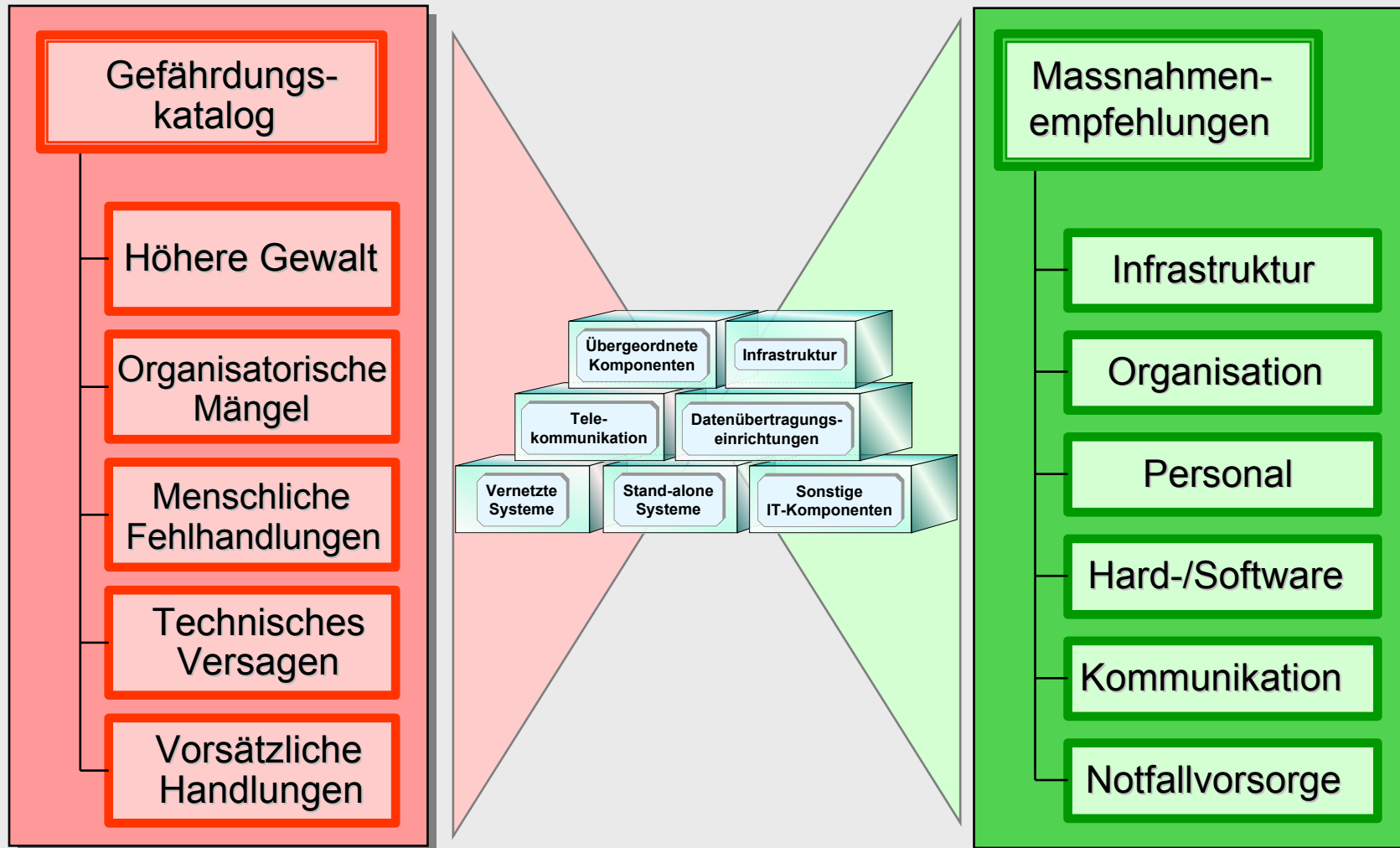
Schutzbedarfsfeststellung



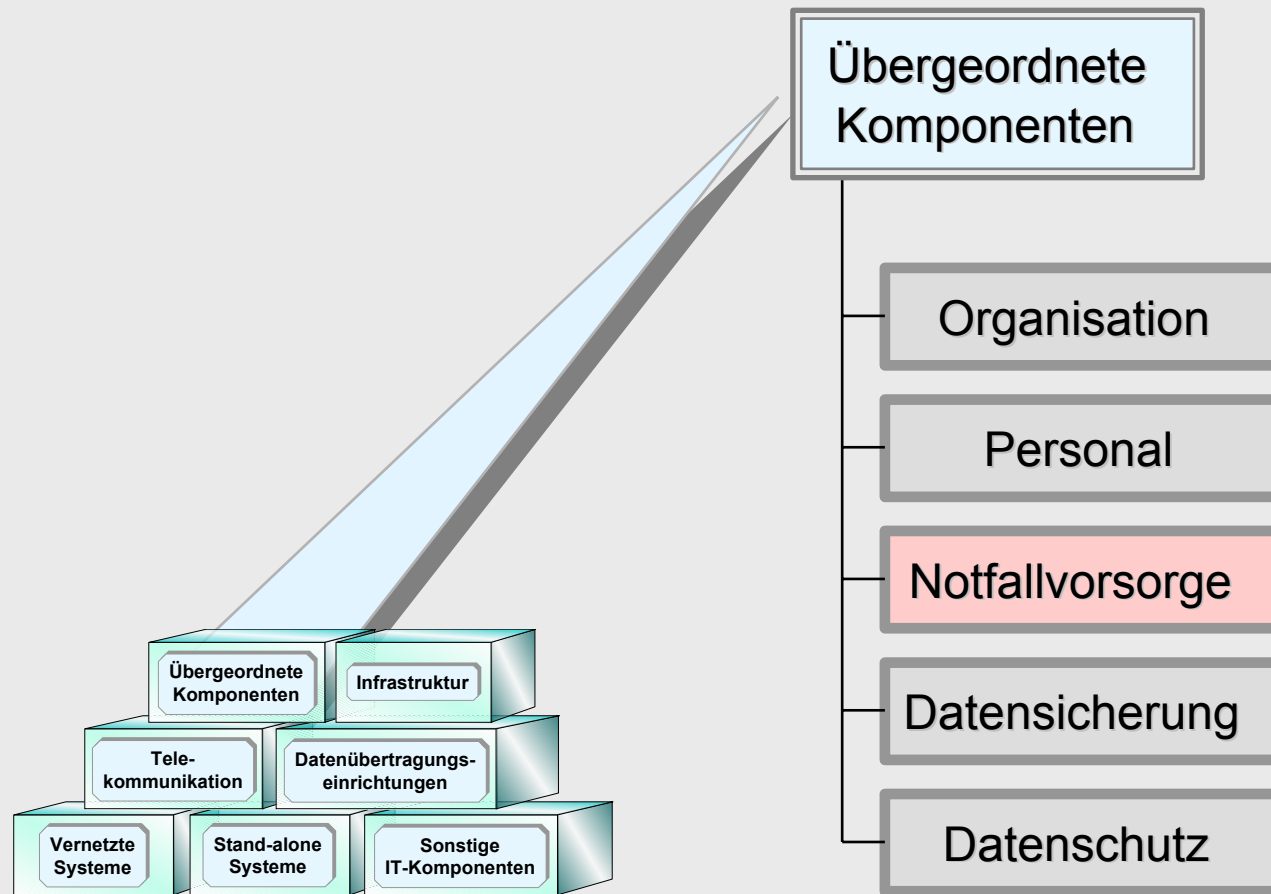
IT-Grundschutz: Baukasten....



....IT-Grundschutz: Baukasten....

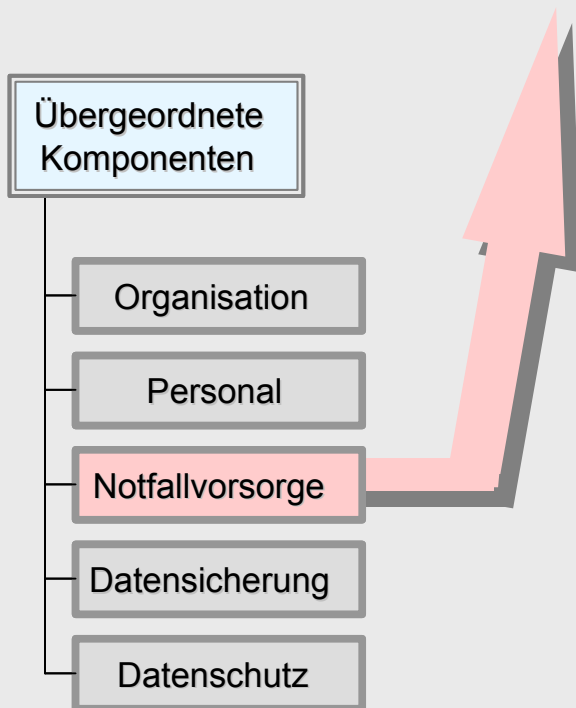


....IT-Grundschutz: Baukasten....



....IT-Grundschutz: Baukasten

- Gefährdungslage
 - G 1.2
 - Ausfall des IT-Systems



- Massnahmenempfehlungen
 - M 6.1
 - Erstellung einer Übersicht der Verfügbarkeitsanforderungen
 - M 6.2
 - Notfall-Definition, Notfall-Verantwortliche(r)
 -
 - M 6.8
 - Alarmierungsplan
 -
 - M 6.12
 - Durchführung von Notfall-übungen

IT-Grundschutz: Pro & Contra

o Schutzbedarfsfeststellung

- + Bedrohungs- & Risikoanalyse entfällt (80/20-Regel).
- + Wirtschaftliche Realisierung eines mittleren Schutzniveaus.
- Nicht geeignet für Risikoanalysen.

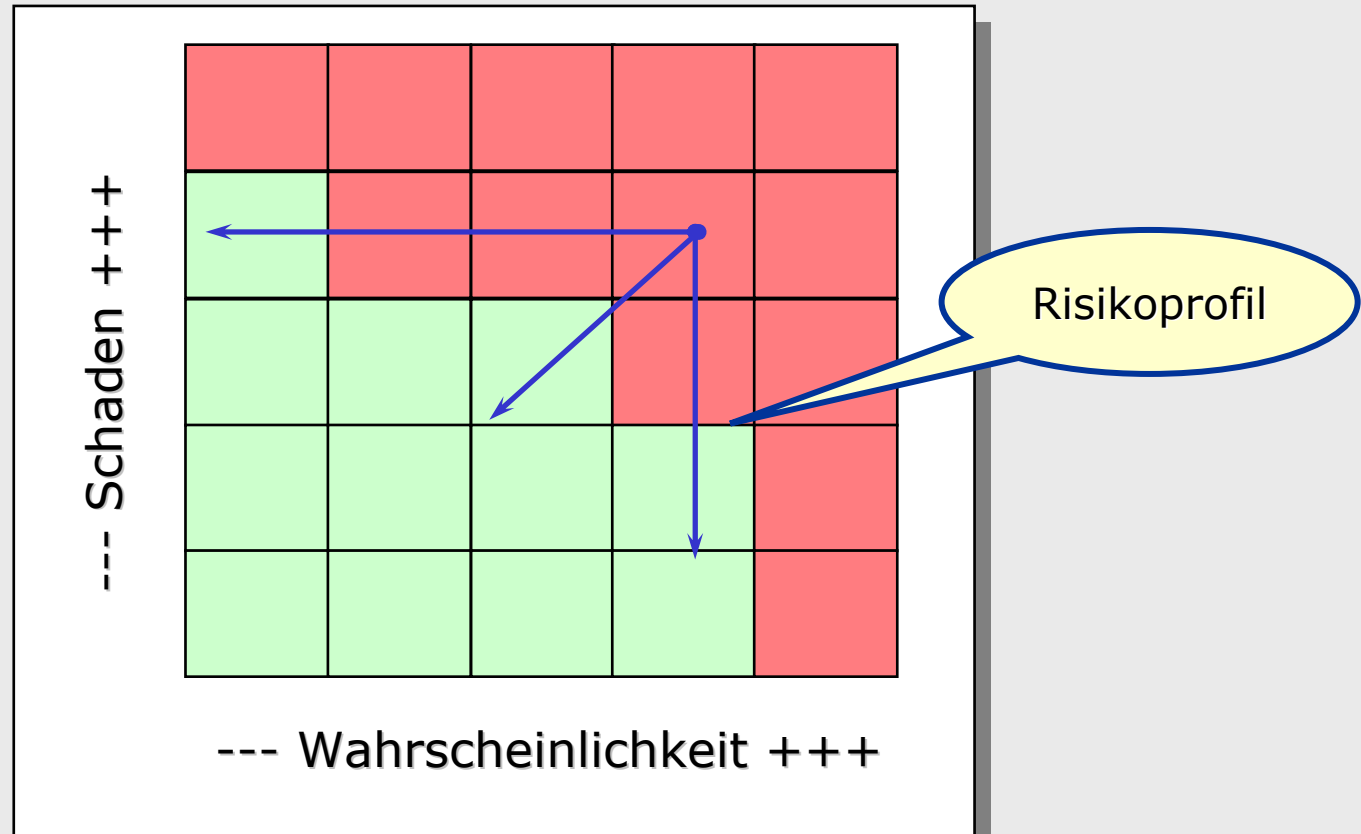


IT-Grundschutz: Pro & Contra

- Sicherheitskonzept/-handbuch
 - + Realisierung der Ausführungsebene (praxisbezogene, direkt umsetzbare Massnahmen).
 - + Erarbeitung von (Teil-)Konzepten wie
 - Firewall-Konzept
 - Notfallvorsorge-Konzept.
 - Nicht zielorientiert.
 - Kein konzeptioneller Überbau.



Risikoanalyse: Prinzip



Risikoanalyse: Begriffe

○ Bedrohung/Gefährdung

- Potenzielle Gefahr/Gefahrenquelle
- Potenzielle Leistungsstörung.

○ Schwachstelle

- Potenzielle Verwundbarkeit
- Potenzielle Schutzlosigkeit.

○ Schaden

- Einwirken von Gefährdungen auf Schwachstellen.



Risikoanalyse: Begriffe

o Risiko

- = potenzieller Schaden X Eintrittswahrscheinlichkeit.

o Problem

- Quantifizierung des Schadens
- Abschätzen der Eintrittswahrscheinlichkeit.



IT-Security: Quellen

○ IT-Grundschutzhandbuch

- Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn
<http://www.bsi.de>

○ Code of Practice for Information Security Management (CoP)

- BS 7799:1999
- British Standards Institution
<http://www.bsi-global.com>

