

# **IT-Risikomanagement**

**Auf die Schwachstellen kommt es an!**

**Michael Haack**  
**11. Februar 2008**

# IT-Risikomanagement

## Was ist Risikomanagement?

**Gefahr, dass Ziele nicht erreicht werden können**

Im Alltag

- Gesundheit
- Finanzielle Sicherheit
- Familie

Beispiele für Maßnahmen

- Winterreifen
- Fahrradhelm
- Grippeimpfung
- Geschwindigkeitsbegrenzer

**Maßnahmen** wirken

- vorbeugend (präventiv)
- wiederherstellend (rekonstruierend)
- erkennend (detektiv)



# IT-Risikomanagement

## Risikomanagement im Unternehmen

- Finanzrisiken (Währungen, Kredite)
- Produktionsmittel (Rohstoffe)
- Zulieferer (Insolvenzen)
- Markt und Absatz (Konjunkturschwankungen, politische Schwankungen)
- Rahmenbedingungen (Regelungen und Gesetze)
- Personal (Altersstruktur, Wissen)



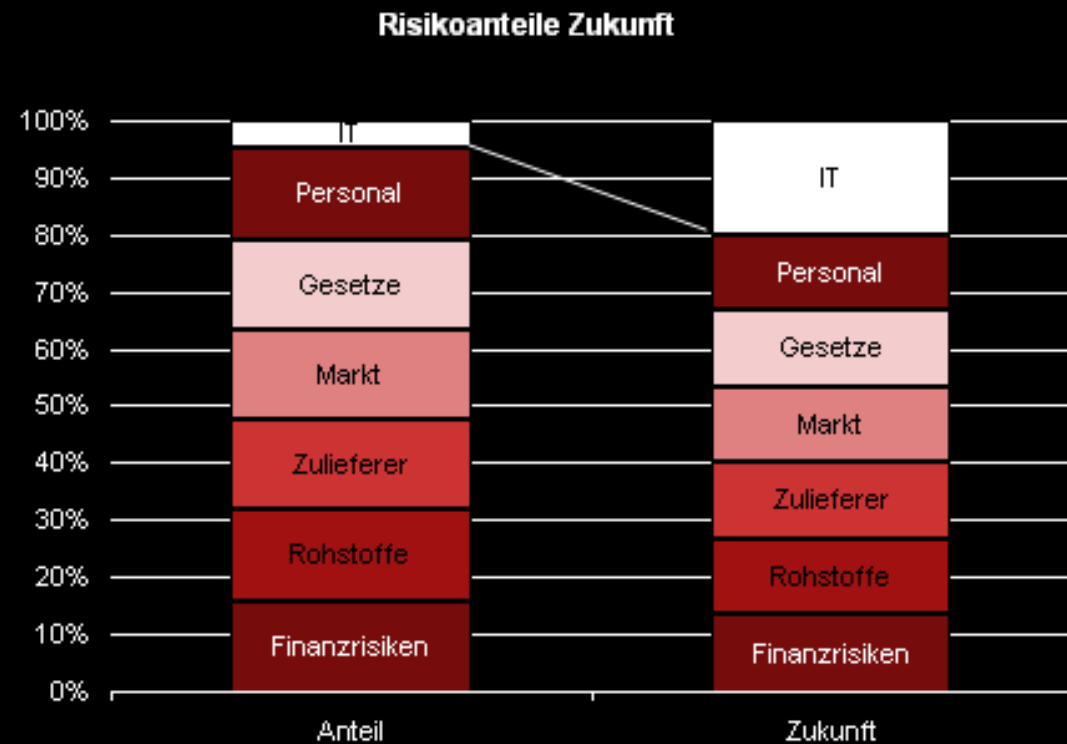
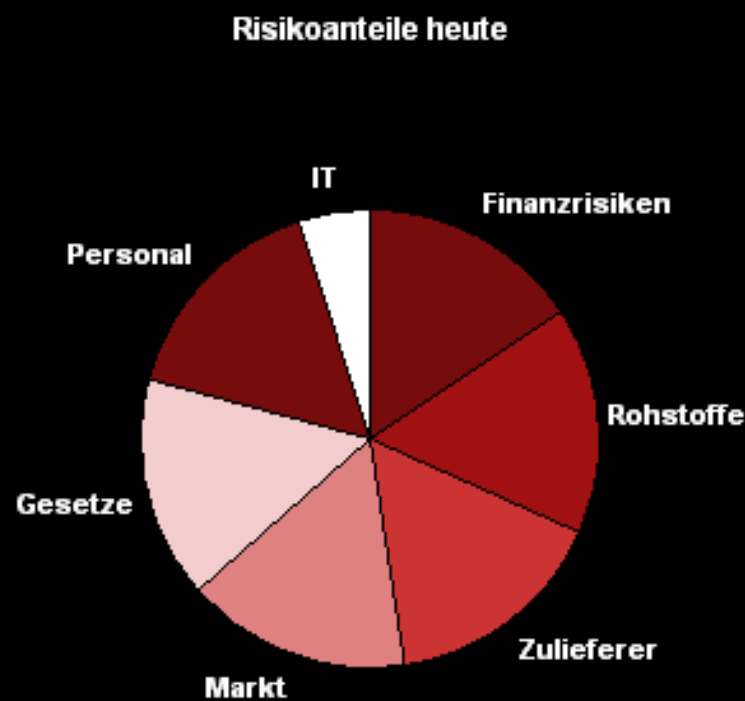
– ...

- **IT: Risiken, die sich durch die Nutzung der IT ergeben**

# IT-Risikomanagement

## Rolle der IT

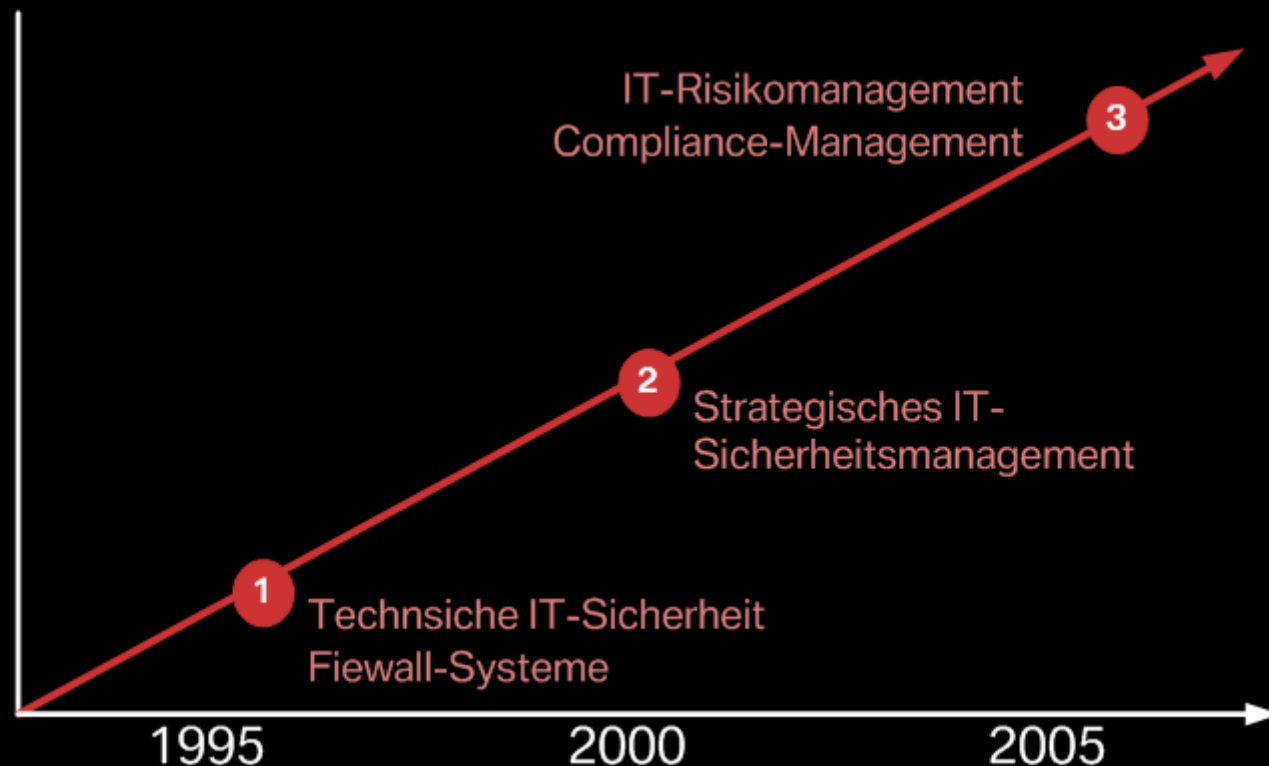
Die **Abhängigkeiten von der IT wachsen** stetig und damit auch der Anteil des IT-Risikos am Unternehmensrisiko.



# IT-Risikomanagement

## Entwicklung des IT-Risikomanagements

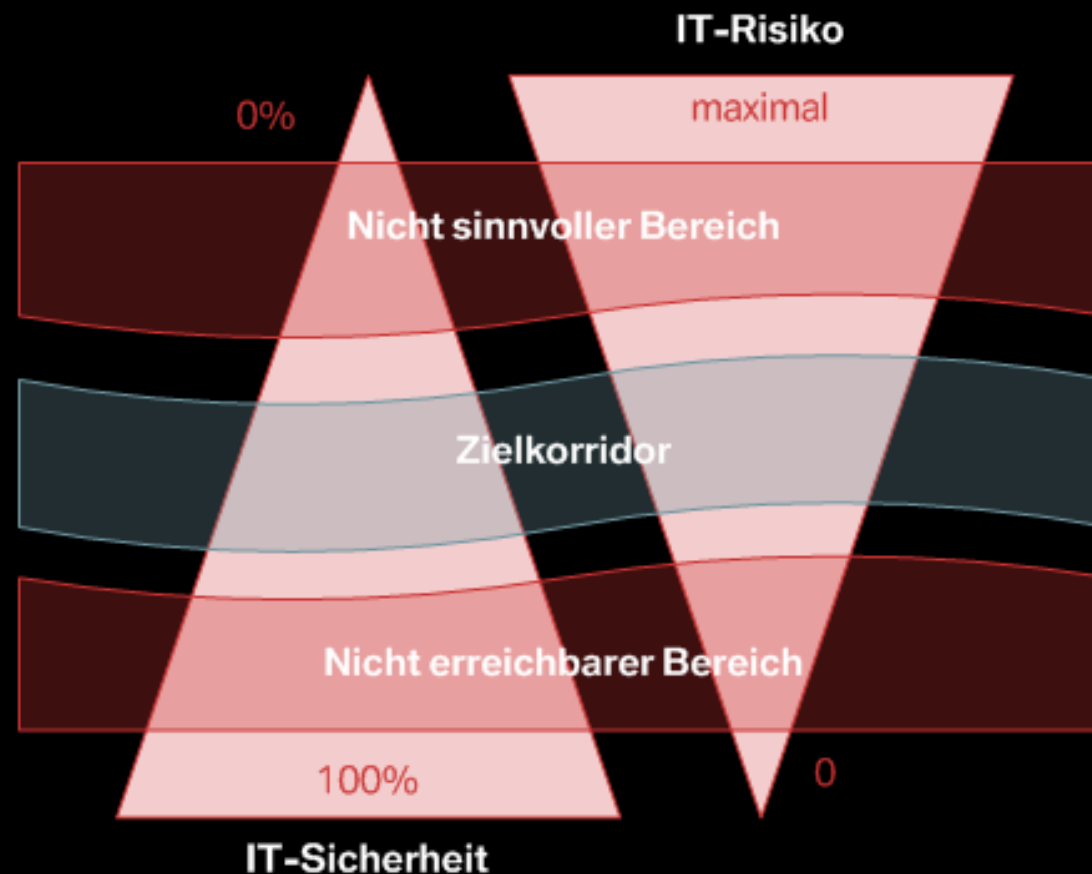
Lange Zeit fand das IT-Risikomanagement lediglich in Form einer unbewerteten **Steigerung der IT-Sicherheit** statt - vornehmlich technisch basiert vor dem Hintergrund der Verbreitung des Internets (Netzwerksicherheit, Firewallsysteme).



# IT-Risikomanagement

## Risiko- vs. Sicherheitsmanagement

**IT-Sicherheit** ist der Zustand eines IT-Systems, in dem die Risiken, die beim Einsatz des IT-Systems aufgrund von **Bedrohungen** vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind.



# IT-Risikomanagement

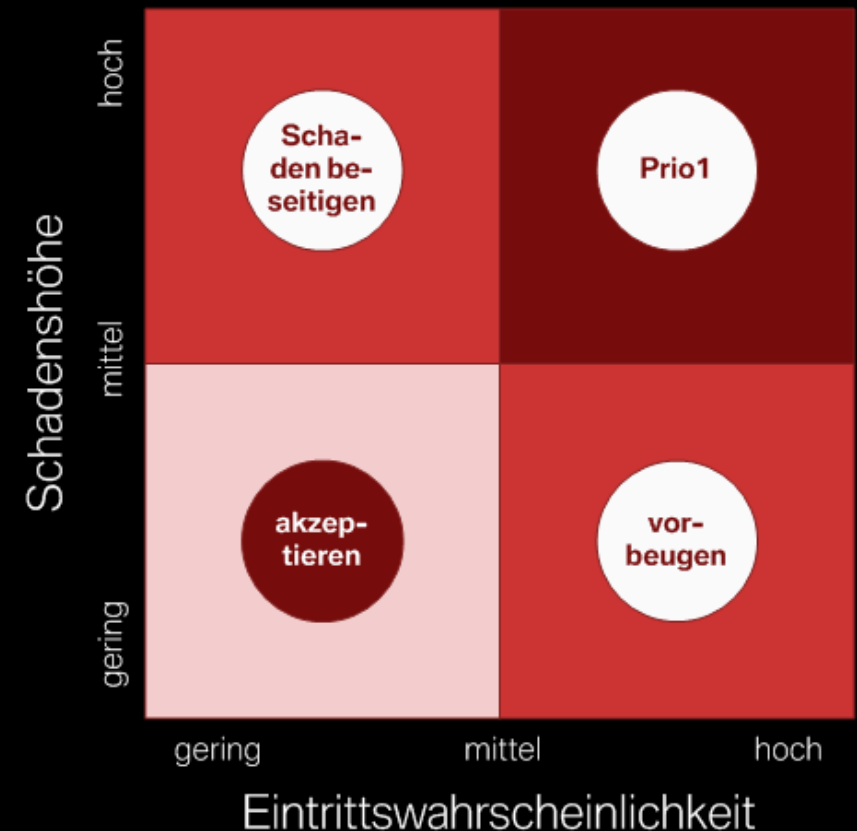
## Ermittlung von Risiken (allgemein)

Bewertung einzelner Risikoszenarien

- nach **potenzieller Schadenshöhe** sowie
- **Eintrittswahrscheinlichkeit**.

Beispiele für Szenarien

- Veröffentlichung von vertraulichen Informationen
- Ausfall von 1 Stunde
- Ausfall von 1/2 Tag
- Ausfall von 1 Tag
- Personalausfall
- Zulieferer-Insolvenz
- Virenvorfall
- Hackerangriff
- Datenfehler



# IT-Risikomanagement

## Nachteile des Vorgehens

- sehr **aufwändig**, weil ein ganzer Katalog von Risiko-Szenarien abgearbeitet werden muss - unabhängig von der Relevanz der einzelnen Risiken im Einzelfall (Meteoriteneinschlag)
- keine ausreichende Beschäftigung mit den **Ursachen** (z. B. bei Ausfallrisiken)
- **Schadenshöhen** können nur vermutet werden
- **Eintrittswahrscheinlichkeiten** sind nur schwer zu schätzen
- nicht vergleichbare Ergebnisse aufgrund der **Einzeleinschätzung** vieler Beteiligten (eine Checkliste ersetzt keine Erfahrung!)
- **Verflechtungen** und **Abhängigkeiten** in der IT-Infrastruktur werden nicht (ausreichend) berücksichtigt

⇒ Doppelnennungen, Ungenauigkeiten

⇒ Falsche Management-Entscheidungen



# IT-Risikomanagement

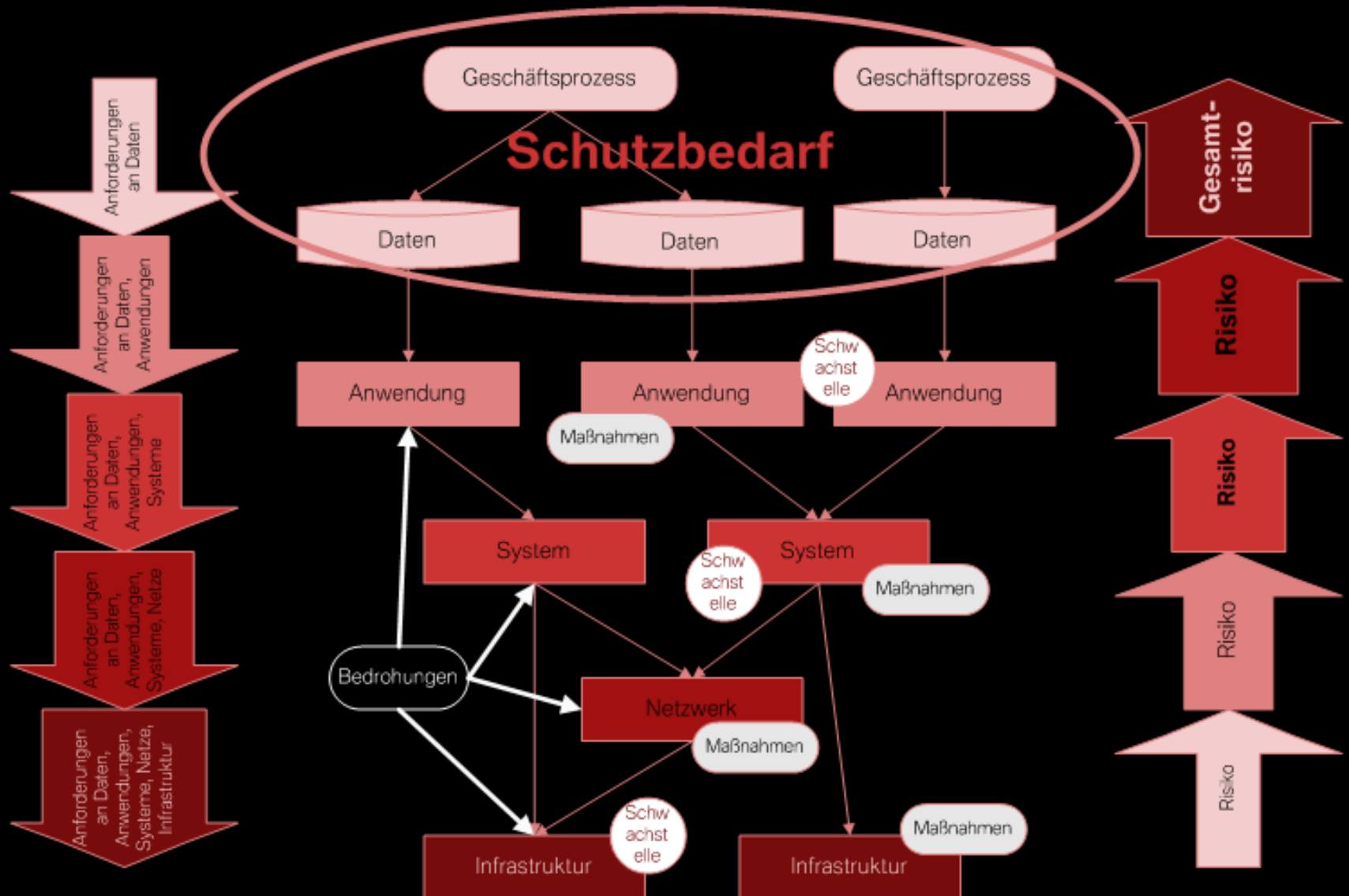
## Verbesserungsansätze

- **Aggregation** der Risiken in der gesamten IT-Infrastruktur
- **Beschränkung** auf die wesentlichen Risiken und deren Ursachen
- **Zentralisierung** der Bewertung auf wenige Spezialisten mit Erfahrungswissen, um genauere Werte für Eintrittswahrscheinlichkeiten und Schadenshöhen zu erhalten



# IT-Risikomanagement

## Gesamtheitlicher Ansatz



# IT-Risikomanagement

## Beschränkung auf die wesentlichen Risiken

Welches sind die wesentlichen Risiken?

Diejenigen, die sich aufgrund von **Schwachstellen** ergeben!

Beispiele für **Schwachstellen**

- fehlende Prozesse für Zugriffsrechtevergabe und -entzug
- fehlende Verschlüsselung von vertraulichen Daten
- fehlende Vertreterregelungen und Notfallplanungen
- fehlende Plausibilitäts- und Datenformatsprüfungen
- unzureichende Systemhärtung
- fehlender Schutz vor Viren, Würmern etc.
- fehlende Protokollierung
- fehlende Überwachungsmaßnahmen (Monitoring)
- nicht ausreichende Netzwerk-Absicherung
- nicht ausreichende Redundanz
- fehlende Datensicherung



# IT-Risikomanagement

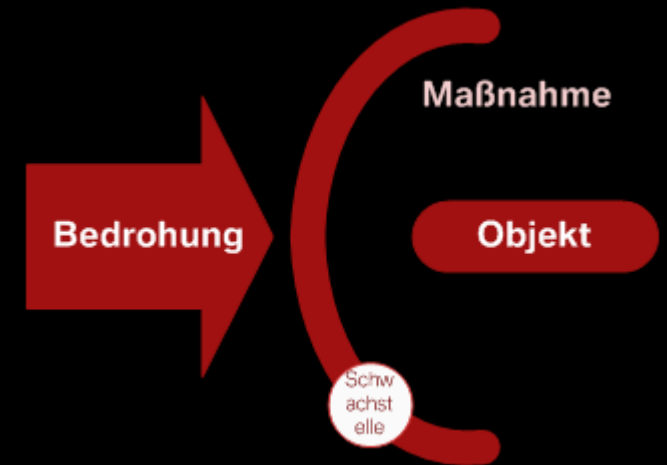
## Risiko-Ermittlung für einzelne Objekte



# IT-Risikomanagement

## Risiko-Ermittlung für einzelne Objekte

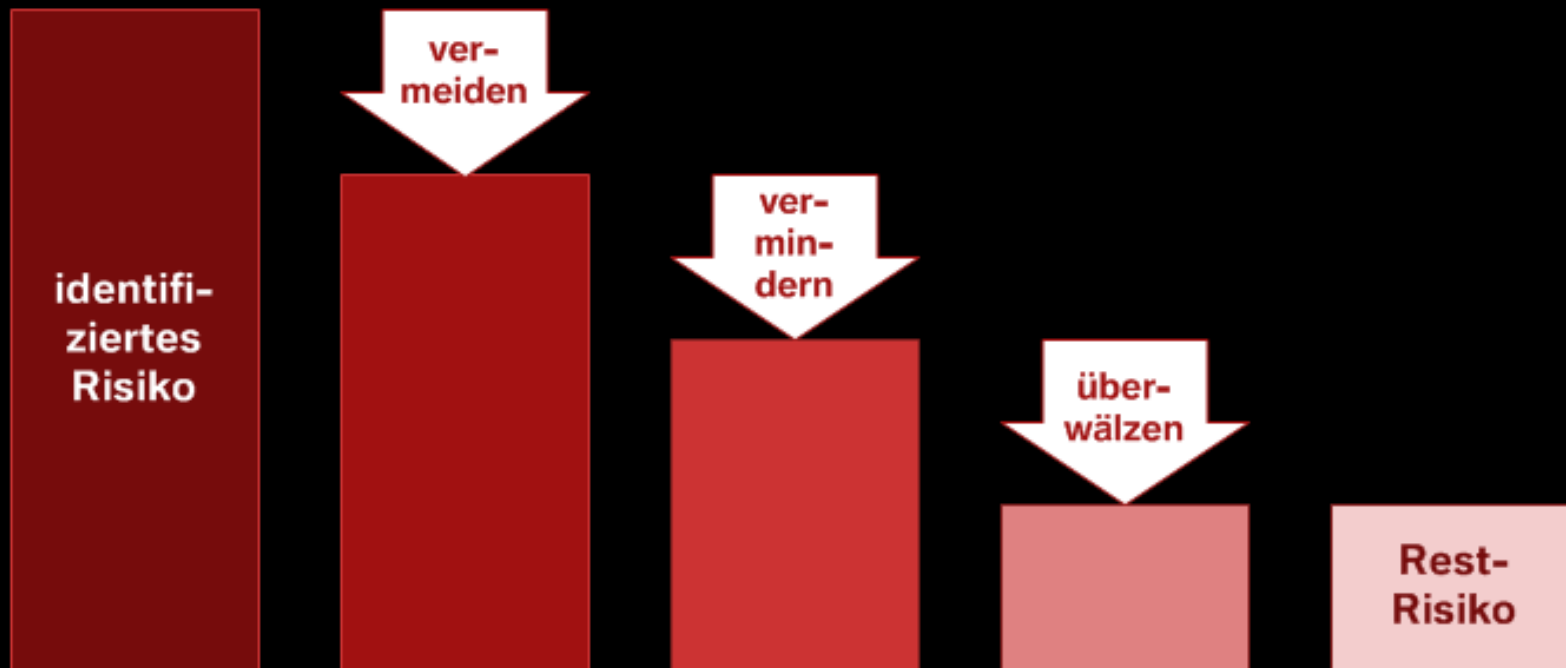
1. Ermittlung bzw. Abfrage des **Schutzbedarfs** aus dem Geschäftsprozess
2. Erfassen der **bestehenden Bedrohungen**
3. Untersuchung der **bestehenden Maßnahmen**
4. **Schwachstellenanalyse**: Sind bestehenden Bedrohungen in Anbetracht des Schutzbedarfs keine ausreichenden Maßnahmen entgegengestellt?
5. Risikoanalyse: Aggregation des Risikos an abhängige Objekte und Behandlung des **Risikos** mit Maßnahmen



# IT-Risikomanagement

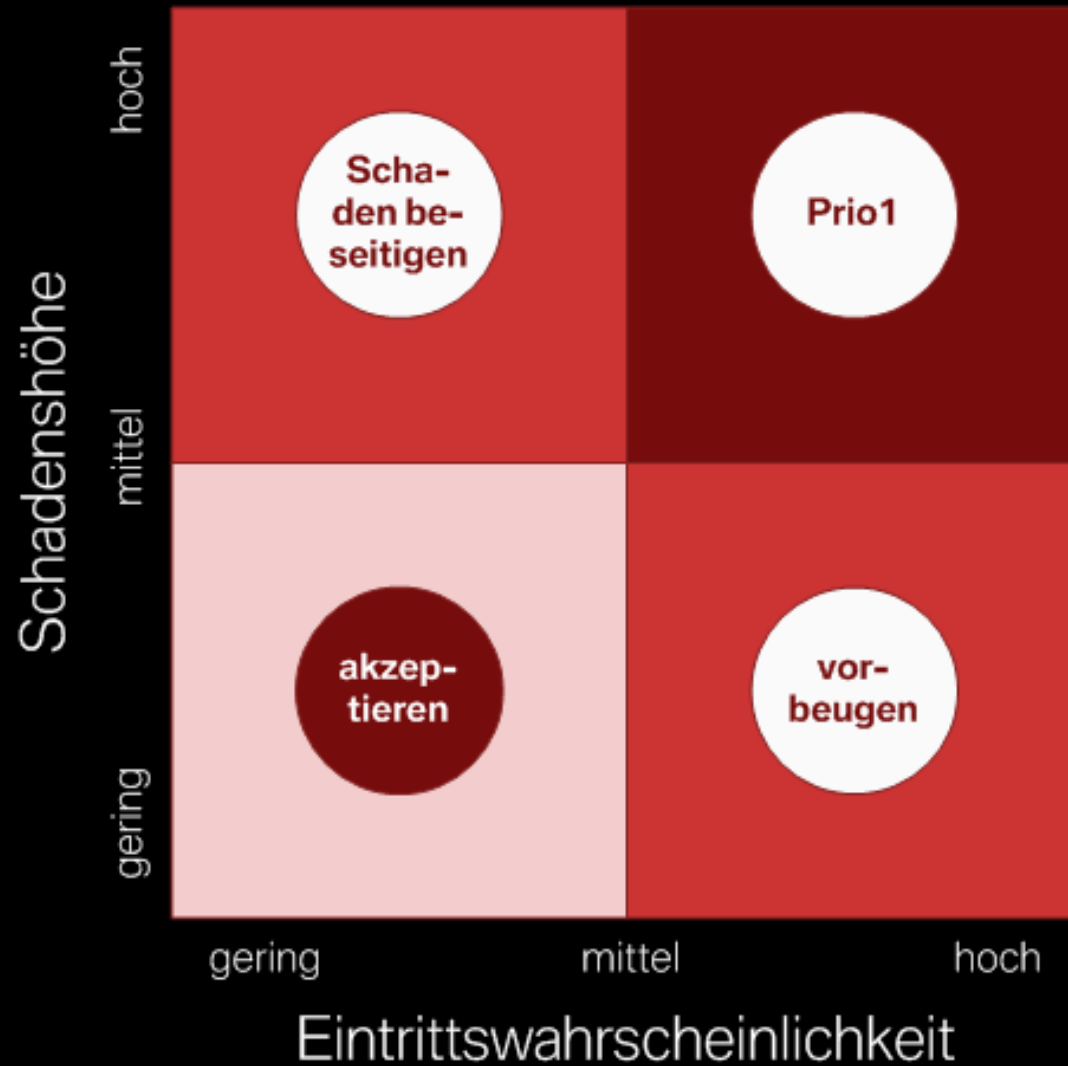
## Risiko-Behandlung

- **vermeiden** durch Alternativen
- **vermindern** durch Gegenmaßnahmen
- **überwälzen** durch Versicherung



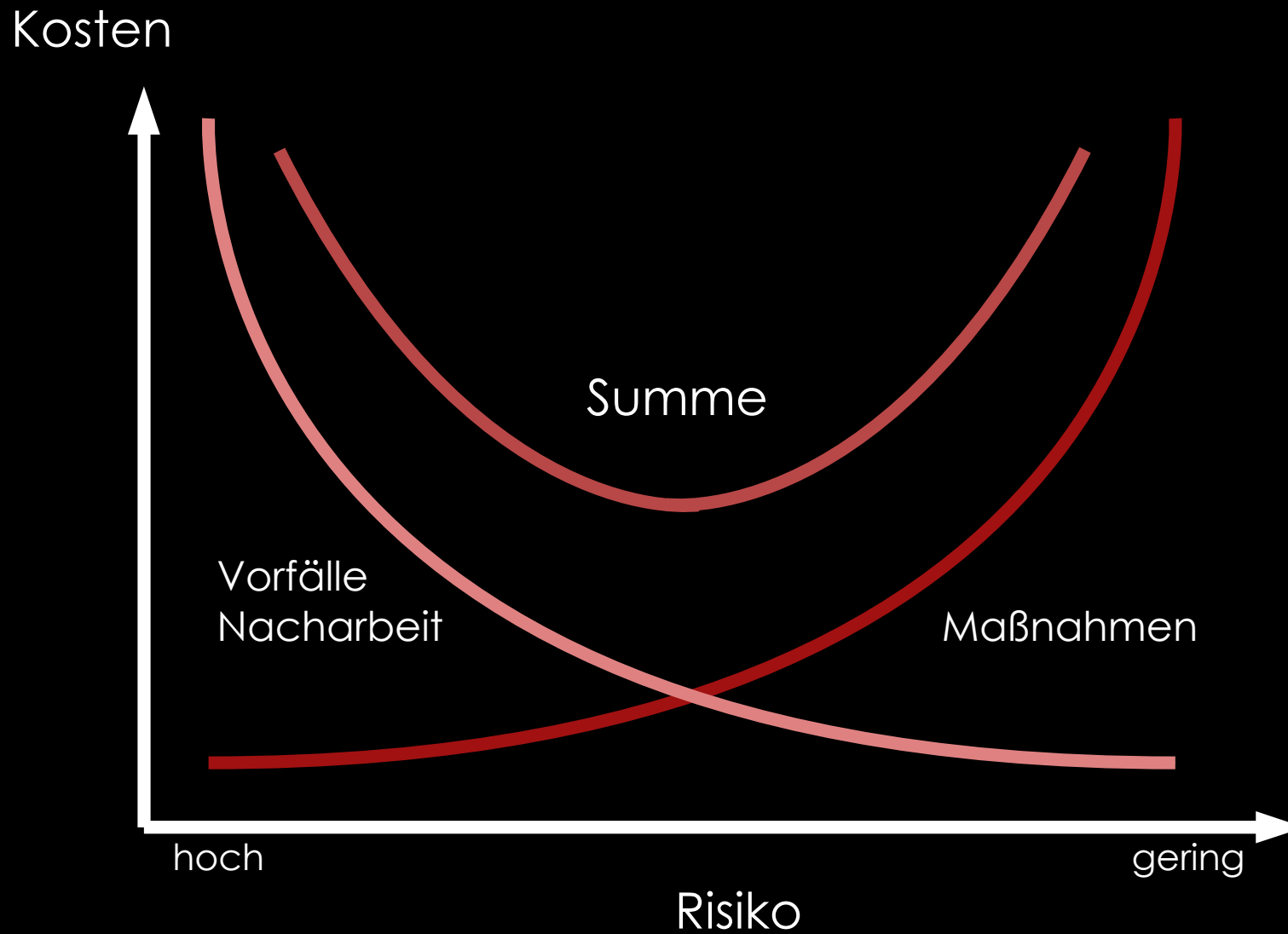
# IT-Risikomanagement

## Maßnahmen-Priorisierung

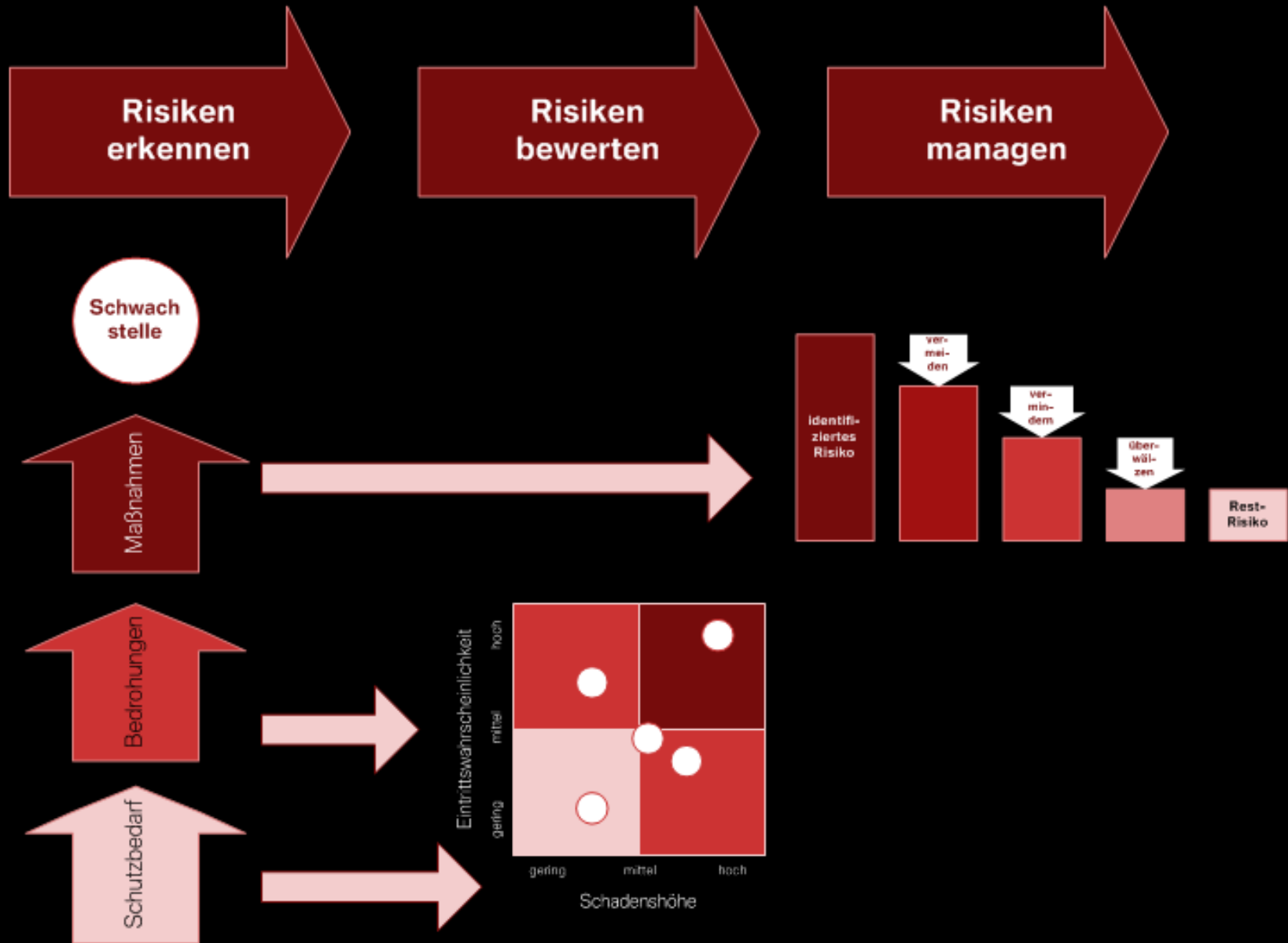


# IT-Risikomanagement

## Kostenbetrachtung



# IT-Risikomanagement Überblick



# IT-Risikomanagement

## Restrisiken

Neben den Risiken, die sich aus den Schwachstellen ergeben, gibt es diverse weitere Risiken - die **Restrisiken**

Merksatz

**Auch wenn es keine Schwachstellen mehr gibt, kann alles mögliche passieren, was Schaden in der IT erzeugt.**

Restrisiken gehören zum allgemeinen Lebensrisiko, das der Unternehmer bei der Gründung eingeht.



# IT-Risikomanagement

## Bewertung der Bedrohungen

- Im IT-Umfeld fehlen **historische Statistiken**, mit denen sich die Bedrohungslage hieb- und stichfest plausibilisieren liesse
- ⇒ Einschätzung der Eintrittswahrscheinlichkeiten subjektiv und damit ungenau
- Abhilfe schaffen Kriterien zur Abschätzung bei **vorsätzlichen Handlungen**:
  - Vorwissen
  - Spezialwissen
  - Hilfsmittel/Ausrüstung
  - Gelegenheit

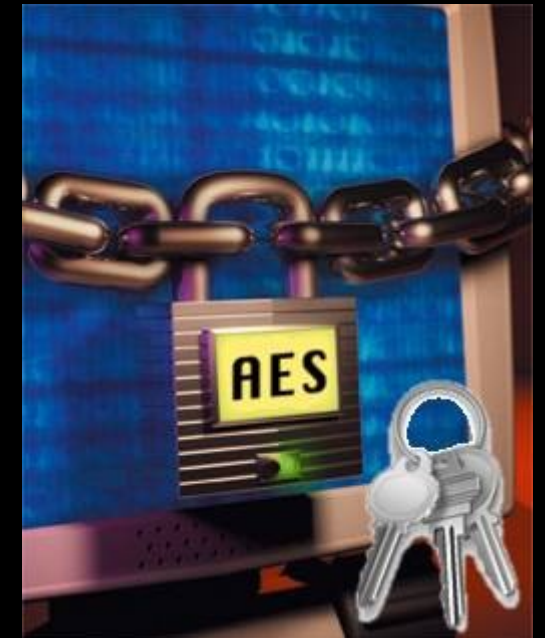


⇒ Erfahrung bei der Einschätzung dringend notwendig!

# IT-Risikomanagement

## Bewertung der Maßnahmenwirksamkeit

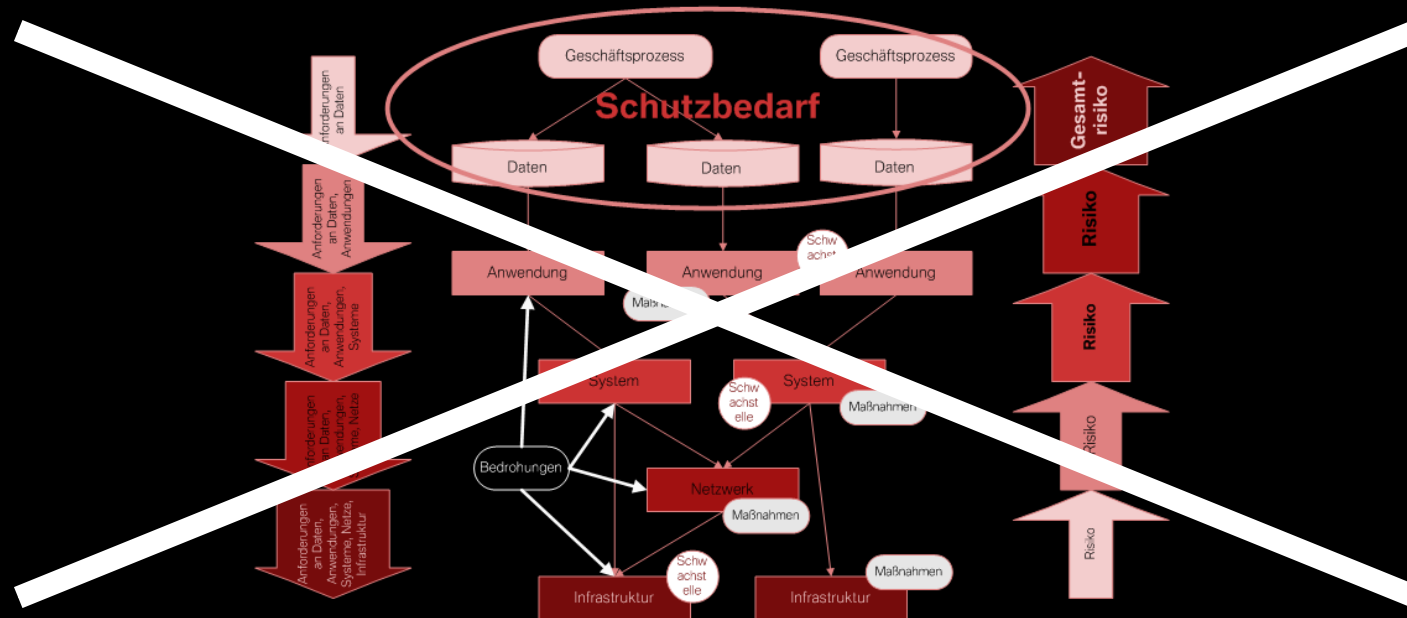
- Welche Maßnahmen sind im Einzelfall **notwendig** und welche **entbehrlich**?
  - Wie verhalten sich verschiedene Maßnahmen im **Vergleich**?
  - Das Fehlen welcher Maßnahmen bedeutet eine **Schwachstelle** – und damit ein Risiko?
- ⇒ Einschätzung der **Maßnahmenwirksamkeit** subjektiv und damit ungenau
- ⇒ Erfahrung bei der Einschätzung dringend notwendig!



# IT-Risikomanagement

## Risiko-Aggregation

- In großen Unternehmen bestehen vielfältige **Verflechtungen** und **gewachsene Strukturen** (auch abteilungs- und bereichsübergreifend), die keine exakte Aggregation der Risiken mit vertretbarem Aufwand mehr zulassen.

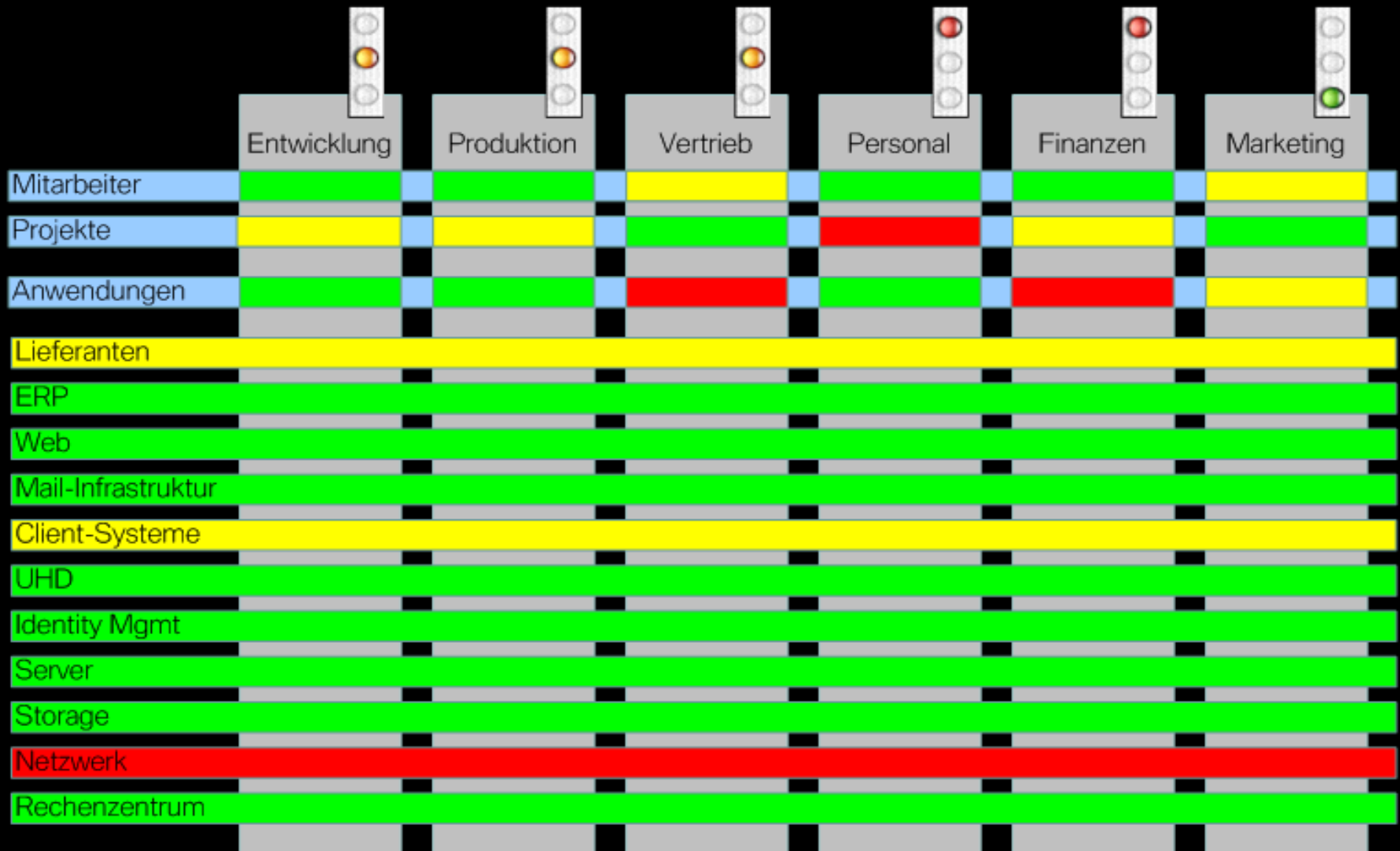


⇒ Ergebnisse der Risiko-Ermittlung sind **nicht 100% belastbar** für betriebswirtschaftliche Rechnungen (Business Case, Kosten/Nutzen, Wertbeitrag für das Unternehmen)

# IT-Risikomanagement

## Pragmatischer Ansatz zur Aggregation

### Risiko-Landkarte



# IT-Risikomanagement

## Beispiel für Risiko-Aggregation

Abhängigkeitsgrad	Vertraulichkeit	Integrität	Verfügbarkeit		Gesamt (max)	Risiko allgemein	Risiko speziell
Schutzbedarf	3	3	4				
	↓	↓	↓				
Mitarbeiter			4	→	4	1	4
Projekte			0	→	0	0	0
Anwendungen	3	3	4	→	4	2	8
Lieferanten			4	→	4	1	4
ERP	3	3	4	→	4	0	0
Web			4	→	4	0	0
Mail-Infrastruktur			2	→	2	0	0
Client-Systeme			4	→	4	1	4
UHD			1	→	1	0	0
Identity Management			2	→	2	0	0
Server			4	→	4	0	0
Storage			4	→	4	0	0
Netzwerk			4	→	4	2	8
Rechenzentrum			4	→	4	0	0
<b>Gesamtrisikowert</b>						<b>28</b>	

# IT-Risikomanagement

## Fazit zum schwachstellenorientierten Vorgehen

- weniger **Ressourcenaufwand** (Zeit, Geld, Personal)
- mehr **Vergleichbarkeit** und ggf. annähernde Vollständigkeit, da einzelne Risiko-Manager mehr Analysen schaffen
- keine Doppelzählung von Risiken aufgrund von **Aggregation**
- die notwendigen **Maßnahmen** liegen auf der Hand: Beseitigung der identifizierten Schwachstellen

### **ABER:**

- Bewertungen basieren auch hier auf Einschätzungen und sind deswegen nicht 100% belastbar

# IT-Risikomanagement

## Fazit zum IT-Risikomanagement

- Ergebnisse des Risikomanagements sind nicht 100% belastbar für betriebswirtschaftliche Rechnungen (Business Case, Kosten/Nutzen, Wertbeitrag für das Unternehmen)
- ⇒ Risiken eignen sich nicht besonders gut, **Ziele** davon abzuleiten.
- ⇒ Risiken eignen sich nicht besonders gut, um zentgenaue **Kosten-Nutzen-Betrachtungen** zu begründen
- ⇒ Ein "**Forecast**" auf die Risikolage multipliziert den Unsicherheitsfaktor derartig, dass praktisch kein Sinn mehr enthalten ist

# IT-Risikomanagement

## Offene Fragen

Michael Haack  
haack@informatik.org  
089/3822 9712

**"IT Security is an art - not a science."**