Willkommen zur Vorlesung

Modellbasierte Softwaretechniken für sichere Systeme

im Sommersemester 2012

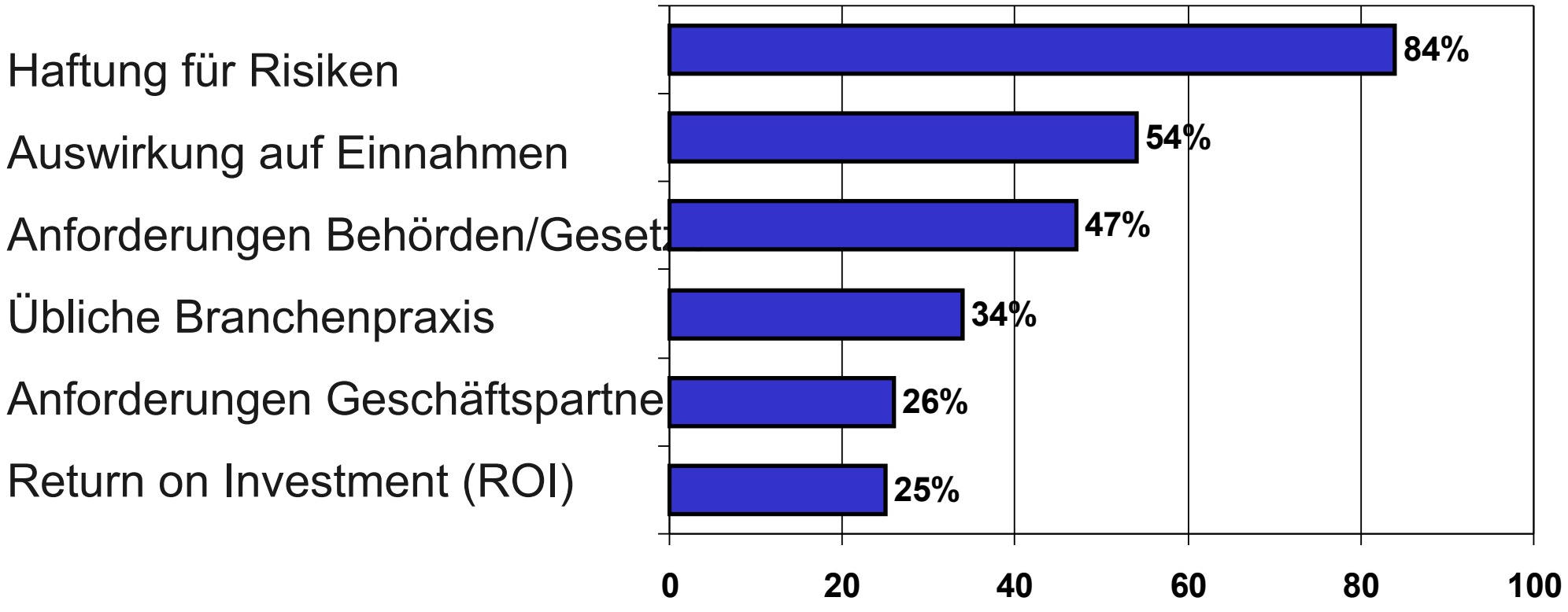
Prof. Dr. Jan Jürjens

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

14. Wirtschaftliche Steuerung der IT-Sicherheit

Basierend auf dem Foliensatz
„Wirtschaftliche Steuerung der IT-Sicherheit“
von Prof. Dr. Erhard Petzel (ibi Research an der Universität Regensburg)
(mit freundlicher Genehmigung)

Wie werden Investitionen in IT-Sicherheit gerechtfertigt?



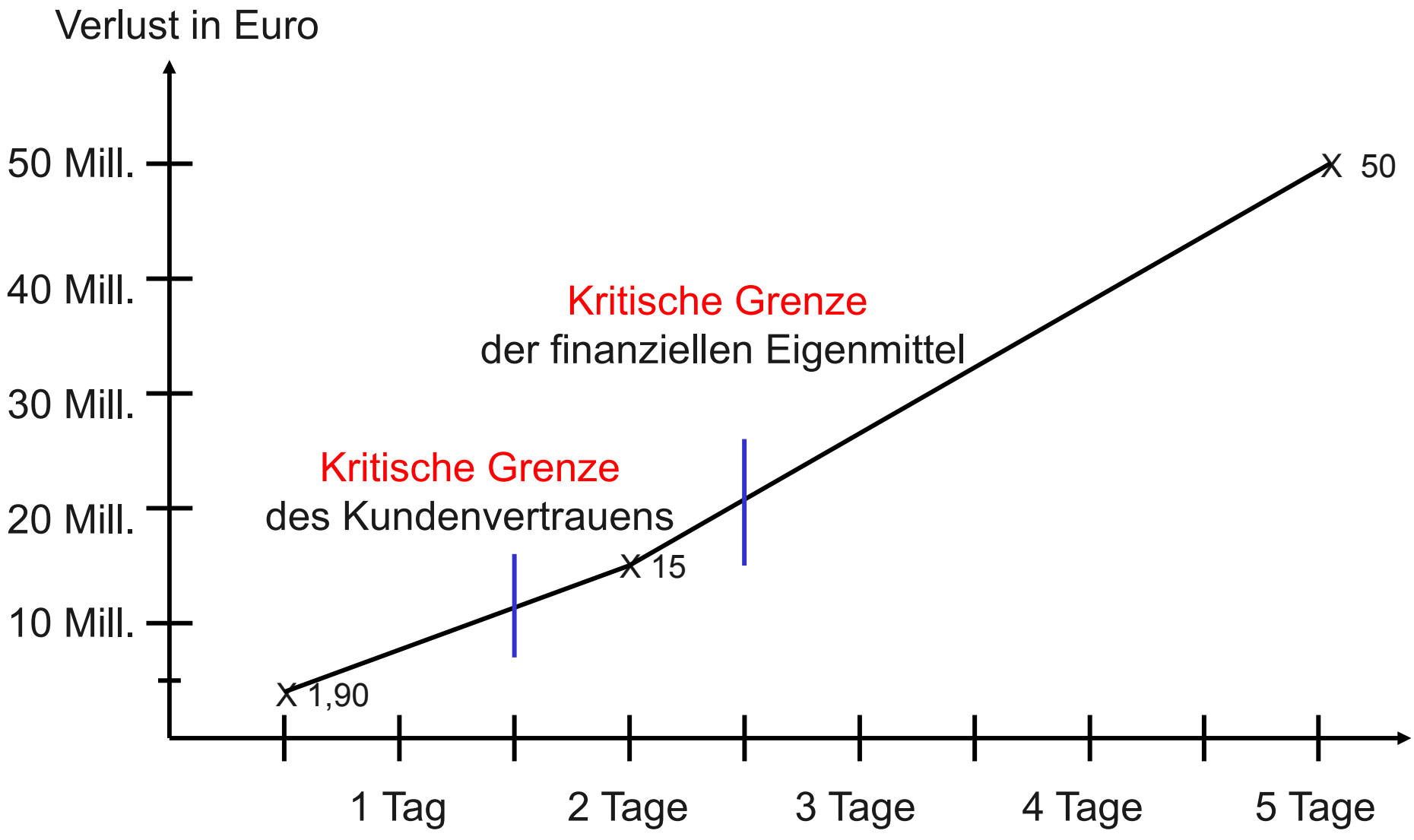
Quelle: Studie von silicon.de: IT-Security 2004

Was bedeutet wirtschaftlich ?
(Aus Sicht eines Informatikers ;-)

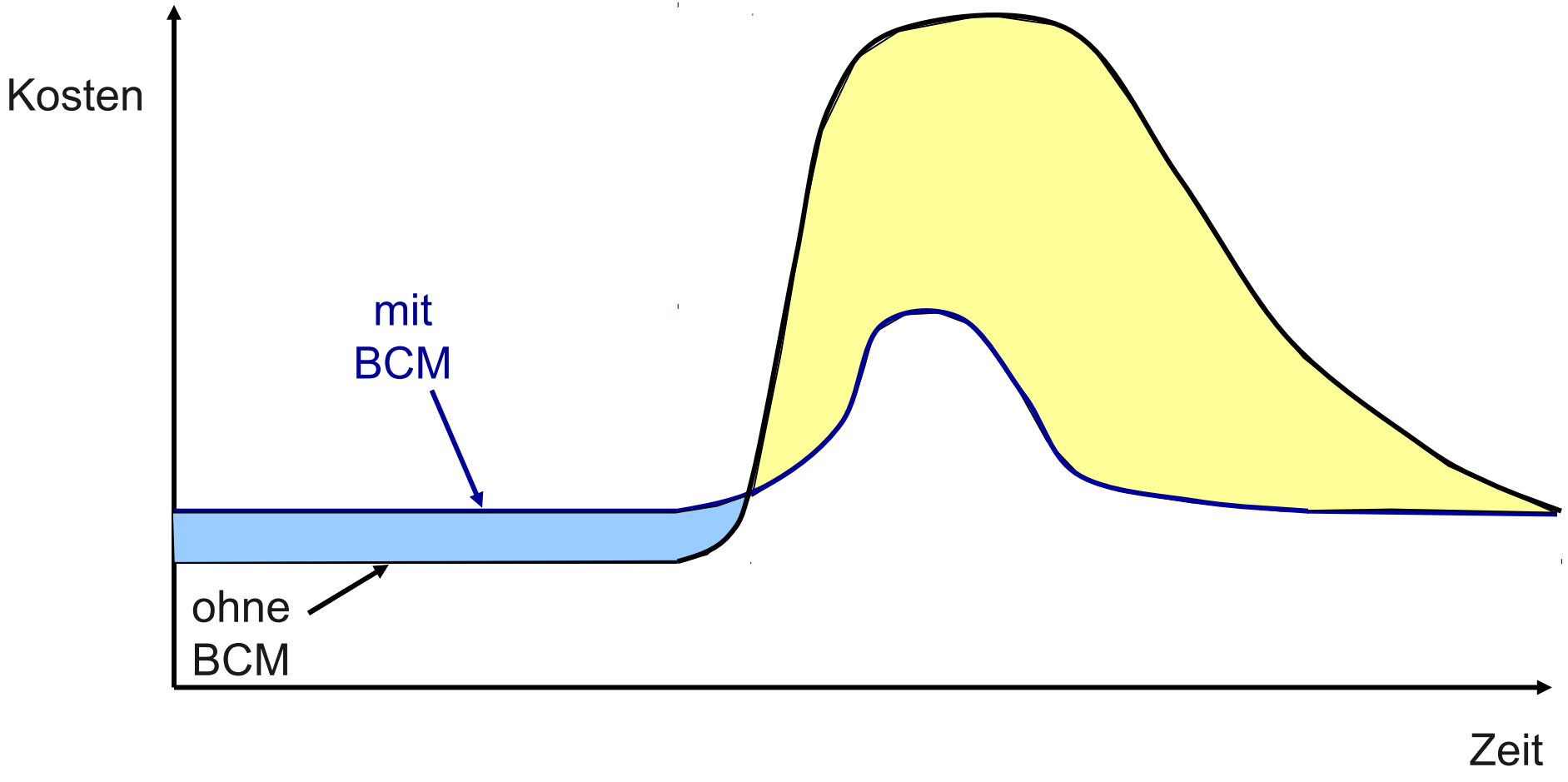
- **Wirtschaftlichkeitsprinzip:** Ein bestimmter Erfolg soll mit geringst-möglichen Mitteln (Minimalprinzip) bzw. mit gegebenen Mitteln der größtmögliche Erfolg erzielt werden (Maximalprinzip).
- **Absolute Wirtschaftlichkeit:** Bewertung einer einzelnen Investition: Das Projekt ist dann wirtschaftlich, wenn sein Kapitalwert positiv ist.
- **Relative Wirtschaftlichkeit:** Eine Investition A ist dann relativ wirtschaftlich gegenüber eine Alternative B, wenn sein Kapitalwert größer ist, unabhängig davon, ob er positiv ist oder nicht.

Um im Unternehmen insgesamt wirtschaftlich optimal zu handeln, muss insbesondere auch in einer optimalen Höhe in die IT-Sicherheit investiert werden.

Verlustverlauf bei einem Katastrophenfall



Wirtschaftlichkeit des Business Continuity Managements



Anforderungen an die Beurteilung der Wirtschaftlichkeit

Wirkungen der Sicherheitsprojekte sind vollständig zu erfassen - direkte und indirekte:

- Wirkungen können quantifizierbar, schwer quantifizierbar oder qualitativer Natur sein - möglichst viele Wirkungen sind zu erfassen
- Es müssen Negativwirkungen der Projekte berücksichtigt werden - z.B. kann eine mehrfache Benutzerauthentisierung die Arbeitsleistung negativ beeinflussen
- Struktur-/ Organisationsveränderungen sind zu berücksichtigen (Kontrollen)
- Um Investitionen zu beurteilen ist eine Lebenszyklusbetrachtung (TCO) erforderlich

Klassische BWL-Methoden der Wirtschaftlichkeitsanalyse

Methoden für einfache Situationen

- **Kostenvergleichsrechnung**
- **Amortisationsrechnung**
- **Rentabilitätsrechnung**

Methoden für komplexe Situationen

- **Nutzwertanalyse**
- **Kosten-/Wirksamkeits-Analyse**
- **Kosten-/Nutzen-Analyse**
- **Simulationen**

Sicherheit: Indirekte Wirtschaftliche Bewertung

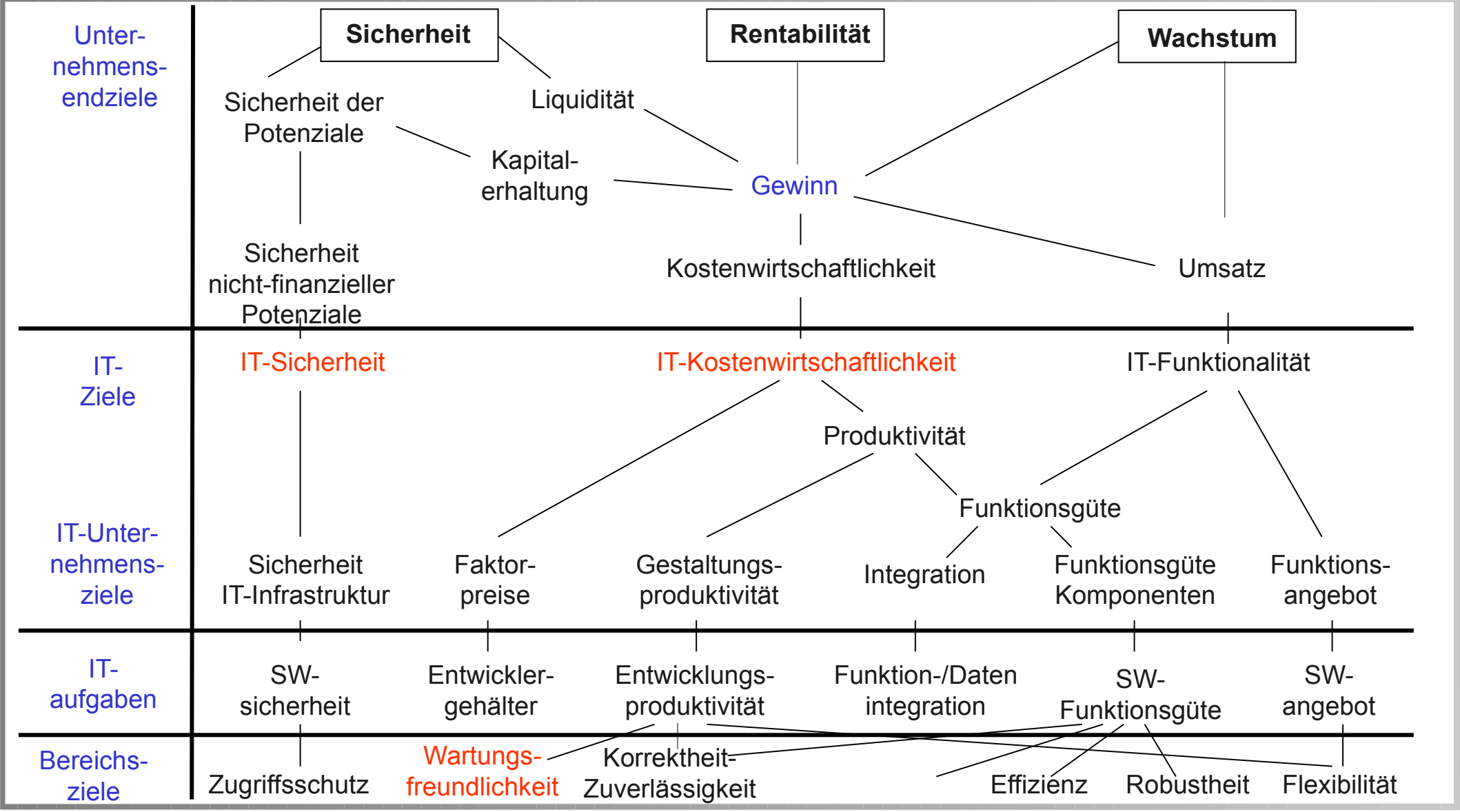
Sicherheit ist kein monetär bewertbares Wirtschaftsgut

bewertbar sind die eingesparten Kosten

Einsparungen von:
- ➔Ressourcen
- ➔externen Leistungen
- ➔billanzieller Werte
- ➔Schadensersatz

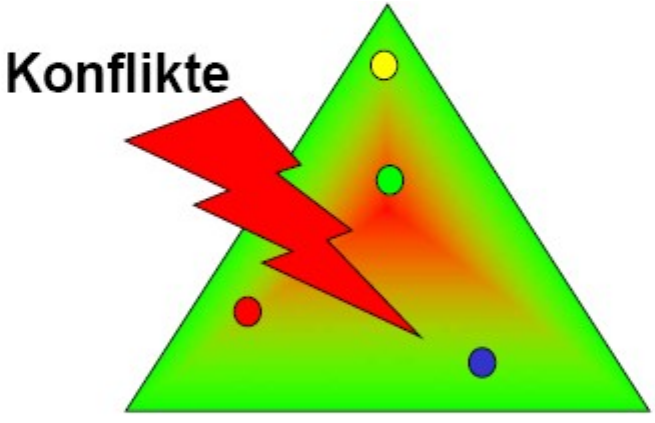
Vermeidung von Zeitverlusten

Sicherheit im Zielsystem des Unternehmens



(Bermuda-)Dreieck des IT-Managements

Kostenwirtschaftlichkeit



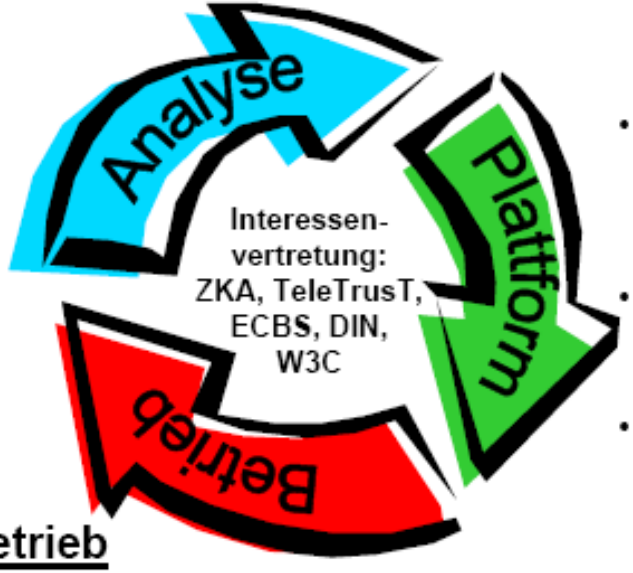
Benutzbarkeit (Usability)
Wartungsfreundlichkeit

IT-Sicherheit
Datenschutz

State of the art im Bankbereich: Sparkassen Informatik Zentrum

Aktive Sicherheit

- Ist die Konformität mit internen oder externen Anforderungen gegeben?
- Wird die Aufrechterhaltung des Sicherheitsniveaus gewährleistet?



Sichere IT-Plattform

- Sind die Komponenten der Infrastruktur herstellerseitig technisch sicher gestaltet?
- Ist die systemtechnische und kommunikationstechnische Infrastruktur miteinander sicher verknüpft und konfiguriert?
- Wird eine angemessene Sourcing-Strategie verfolgt und sind Rahmenverträge verfügbar?
- Entspricht die genutzte IT-Umgebung nationalem und internationalem Sicherheitsrecht?

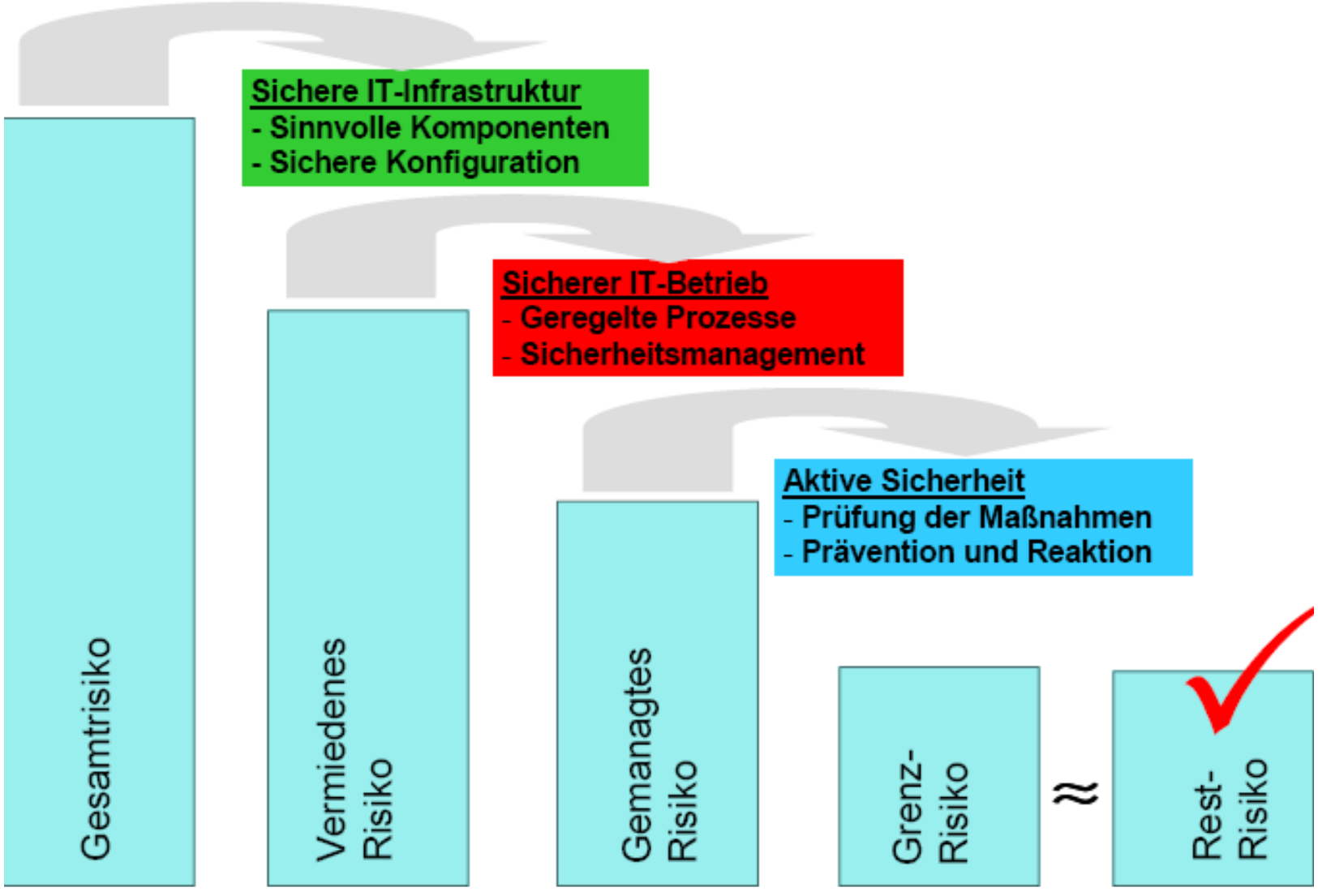
Sicherer IT-Betrieb

Sicherheit – Verfügbarkeit – Betrieb

- Wird die IT gemäß der Unternehmensziele und -strategie betrieben?
- Sind die definierten Service Level anforderungskonform (KWG § 25a, etc.)?
- Werden Prüfungs- und Revisionsanforderungen eingehalten (BaFin, IDW, OPDV)?
- Werden Potenziale zur Betriebskostenoptimierung (Angemessenheit) und zur aktiven Steuerung operationeller IT-Risiken genutzt (Basel II)?

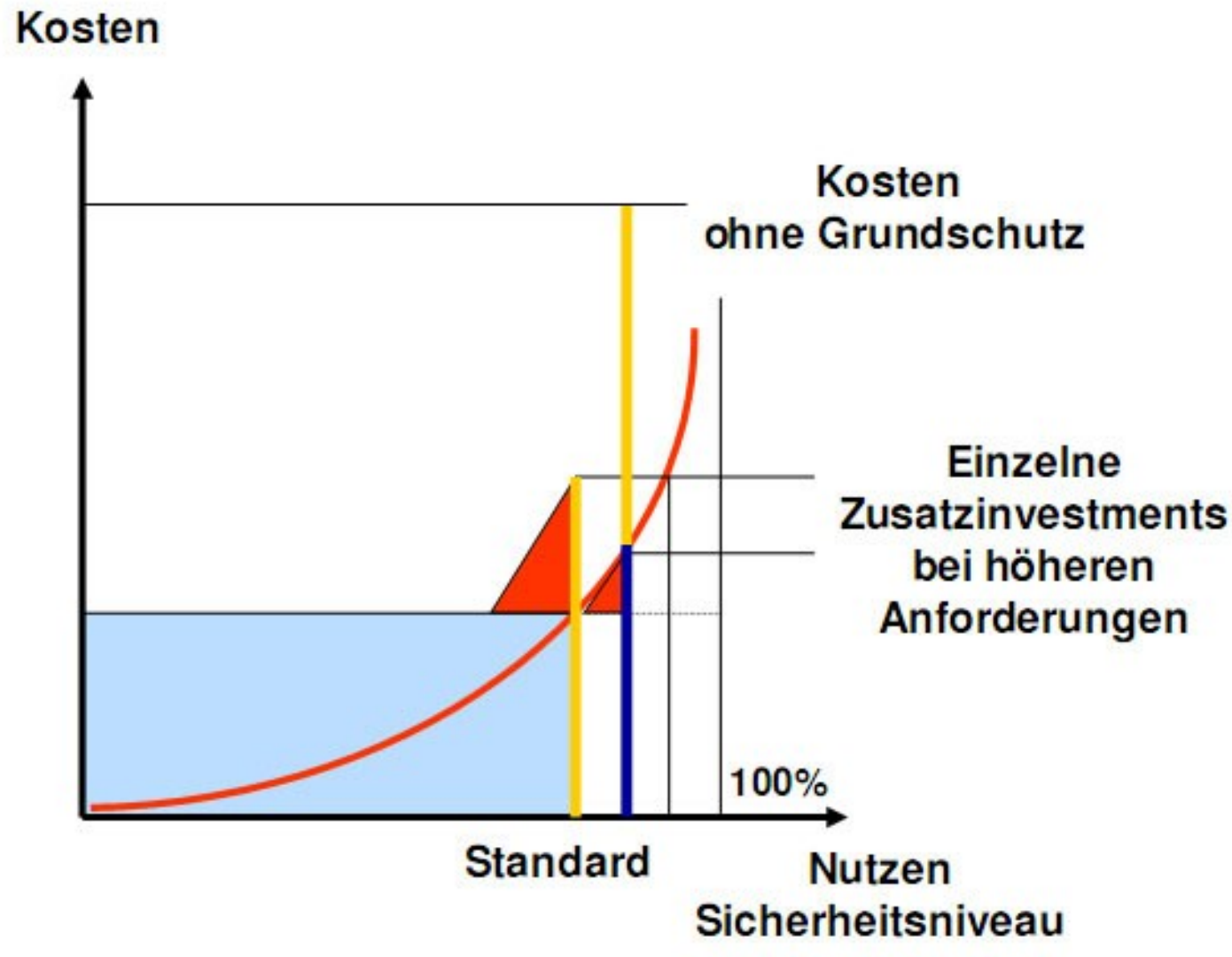
Quelle: Informatikzentrum der Sparkassenorganisation GmbH

Zusammenhang Risiko – IT-Sicherheit

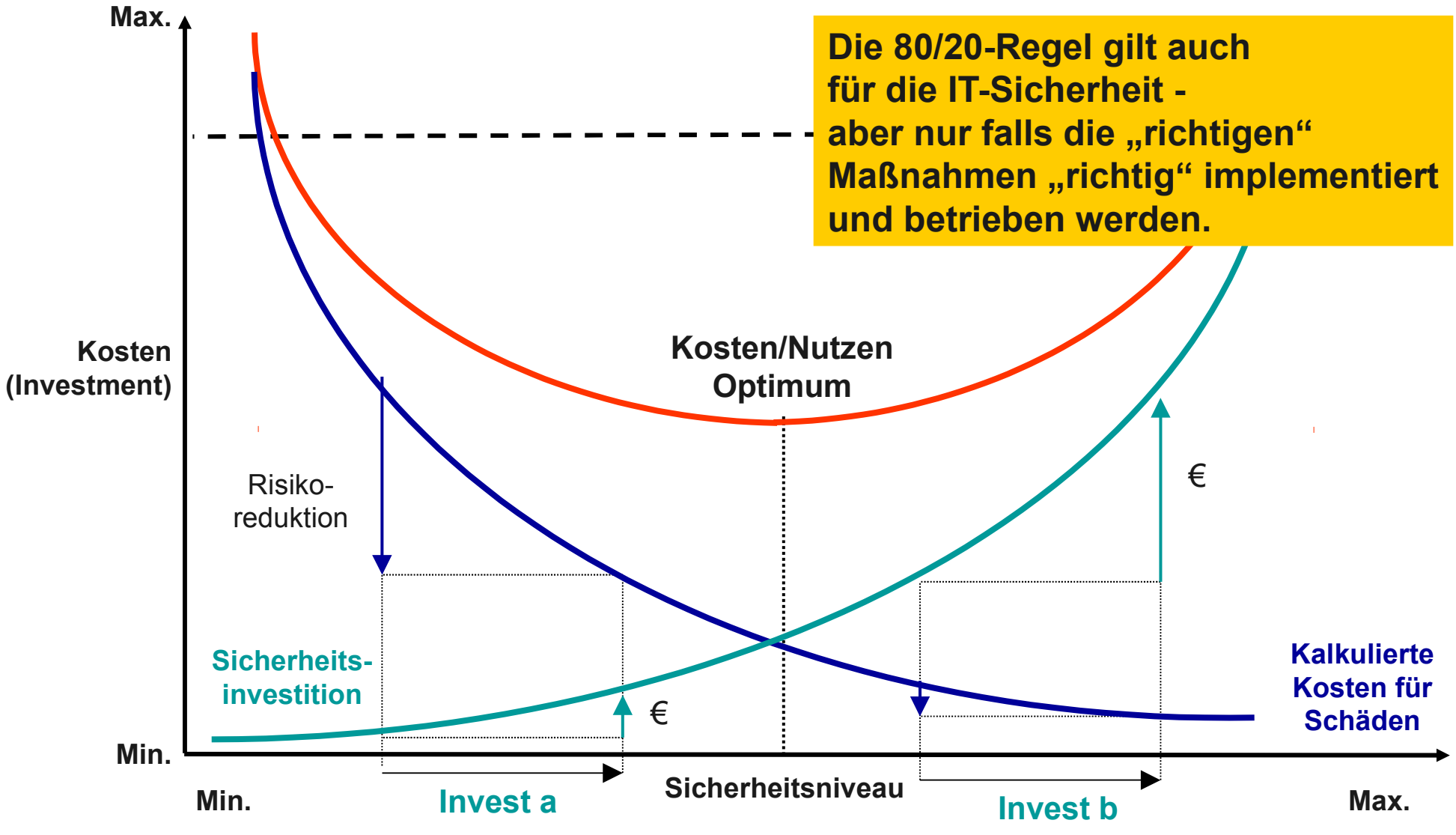


Quelle: Informatikzentrum der Sparkassenorganisation GmbH

Die Idee des Grundschutzes

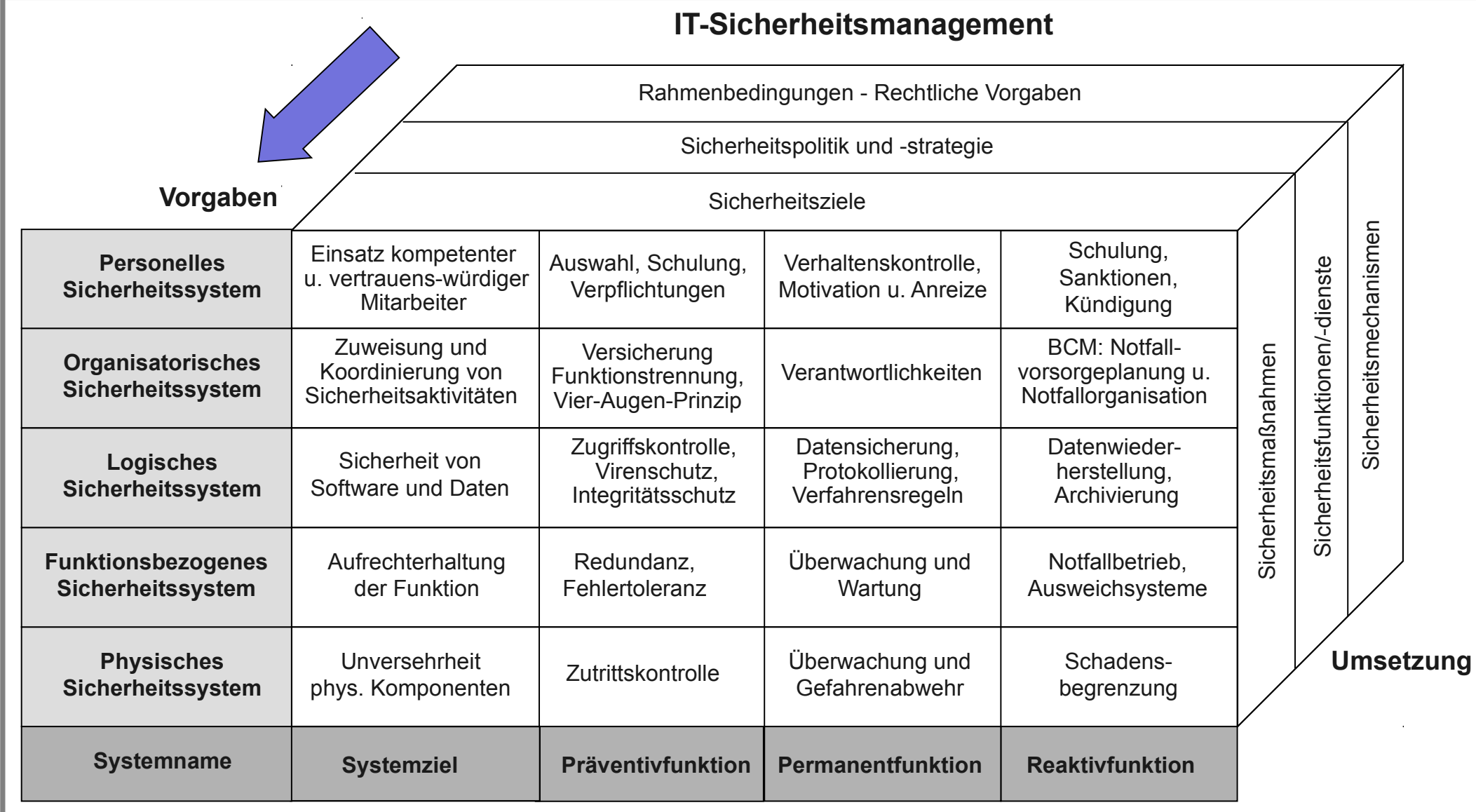


Kosten/Nutzen-Optimum von Sicherheitsinvestitionen



Die 80/20-Regel gilt auch für die IT-Sicherheit - aber nur falls die „richtigen“ Maßnahmen „richtig“ implementiert und betrieben werden.

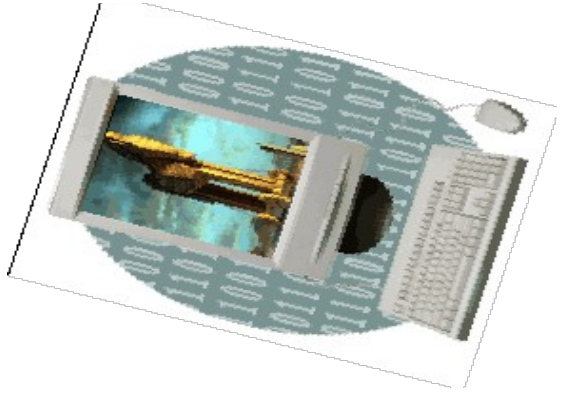
Generisches Modell einer Sicherheitsinfrastruktur



Personelles Sicherheitssystem	Einsatz kompetenter u. vertrauens-würdiger Mitarbeiter	Auswahl, Schulung, Verpflichtungen	Verhaltenskontrolle, Motivation u. Anreize	Schulung, Sanktionen, Kündigung
Organisatorisches Sicherheitssystem	Zuweisung und Koordinierung von Sicherheitsaktivitäten	Versicherung Funktionstrennung, Vier-Augen-Prinzip	Verantwortlichkeiten	BCM: Notfall-vorsorgeplanung u. Notfallorganisation
Logisches Sicherheitssystem	Sicherheit von Software und Daten	Zugriffskontrolle, Virenschutz, Integritätsschutz	Datensicherung, Protokollierung, Verfahrensregeln	Datenwieder-herstellung, Archivierung
Funktionsbezogenes Sicherheitssystem	Aufrechterhaltung der Funktion	Redundanz, Fehlertoleranz	Überwachung und Wartung	Notfallbetrieb, Ausweichsysteme
Physisches Sicherheitssystem	Unversehrheit phys. Komponenten	Zutrittskontrolle	Überwachung und Gefahrenabwehr	Schadens-begrenzung
Systemname	**Systemziel**	**Präventivfunktion**	**Permanentfunktion**	**Reaktivfunktion**

Kostenbetrachtung einer Maßnahme

- Für alle Maßnahmen sind die einmaligen und wiederkehrenden Kosten zu berücksichtigen
- Diesen Kosten wird der Nutzen gegenübergestellt, der sich durch die Risikoreduktion ergibt Überprüfung der Angemessenheit (Beispiel)
- Maßnahme: Beschaffung eines Programms zur Überwachung des Rechnerzugriffs
  - Kosten: € 300,- pro PC
  - Nutzen ?
- Maßnahme: Verantwortliche für die Datensicherung benennen
  - Kosten: Keine
- Maßnahme: Festlegung der Intervalle zur Datensicherung
  - Kosten: Ca. 1 Arbeitsstunde pro Woche
  - Nutzen ?



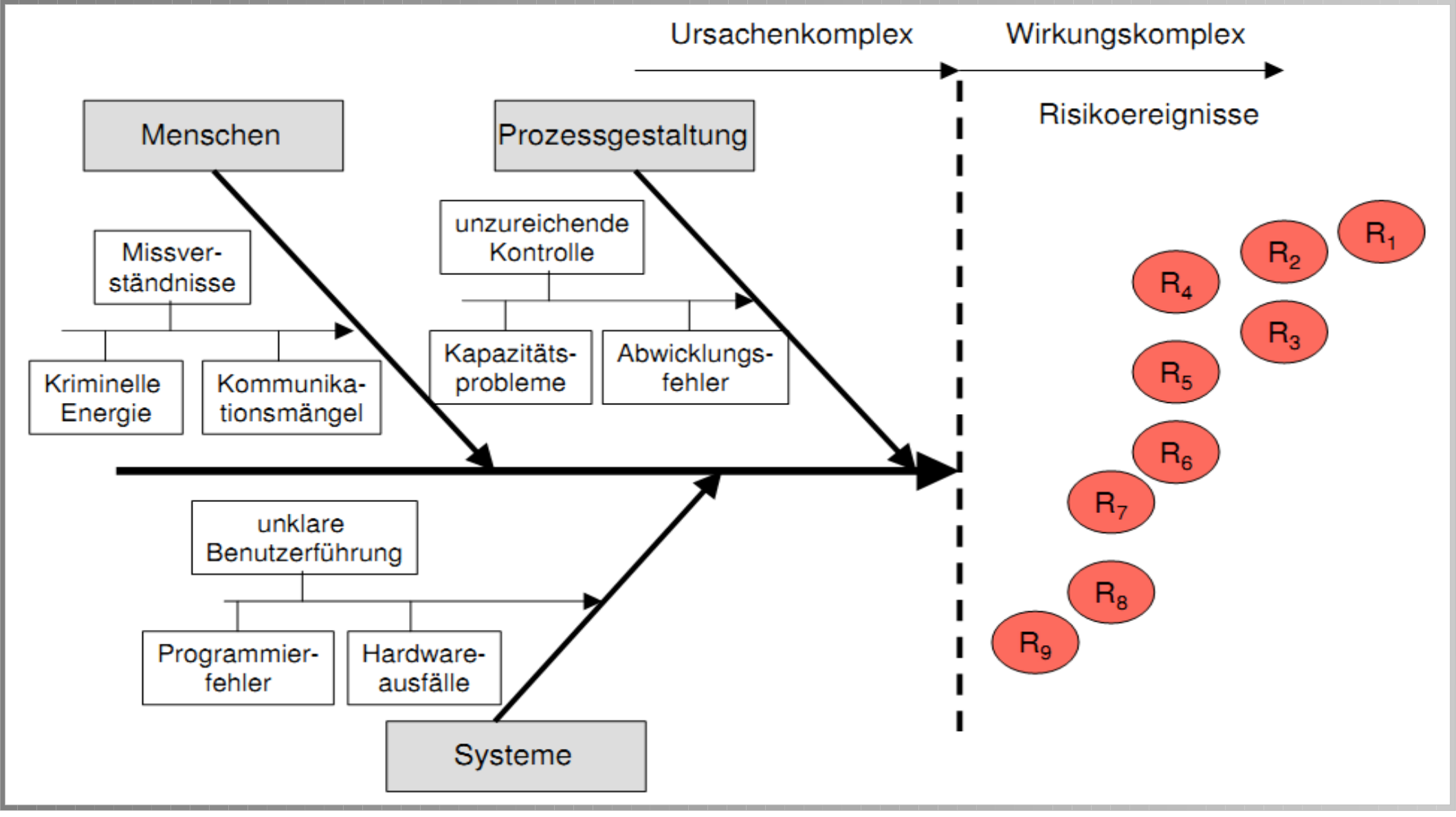
Beispiel: Total Cost of Ownership für Firewall-System (1/2)

Beschaffungsphase	**Zeitaufwand**	**Min. Kosten (€)**	**Max. Kosten (€)**
Sicherheitspolitik	2 Wo bis 3 Monate	7.500	45.000
Produktauswahl	2 Wo bis 3 Monate	7.500	45.000
Ergänzende Maßnahmen (Infrastruktur, Personal, Organisation)	1 Wo bis 4 Wo	3.750	15.000
Produktkosten		5.000	75.000
Installationsphase			
Installation	2 bis 5 Tage	1.500	3.750
Inbetriebnahme	3 bis 10 Tage	2.250	7.500
Sonstige Maßnahmen (Schulung)	3 Wo bis 3 Monate	11.250	45.000
Summe		**38.750**	**236.250**

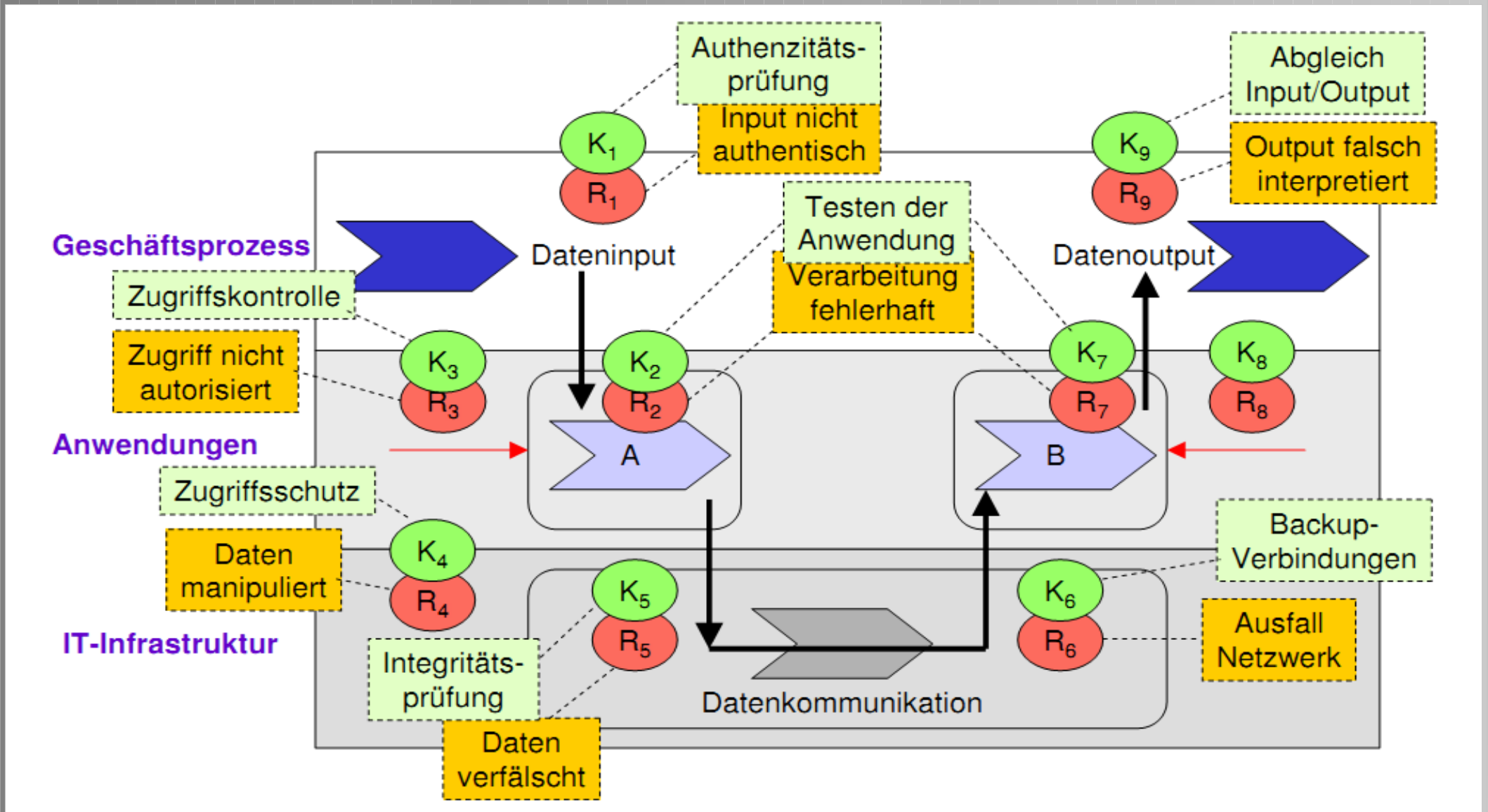
Beispiel: Total Cost of Ownership für Firewall-System (2/2)

Betriebsphase	**Aufwand**
Regelmäßige Überprüfung der umgesetzten Sicherheitsmaßnahmen	
Techn. Maßnahmen (Tests)	4 Tage pro Jahr
Infrastrukturelle Maßnahmen (Zugangskontrolle, Leitungsführung, etc.)	4 Tage pro Jahr
Organisatorische Maßnahmen (Logbuchauswertungen, Verbindungsüberprüfung – Common Point of Trust)	4 Tage pro Jahr
Personelle Sicherheitsmaßnahmen (Schulungen, Awareness-Bildung)	12 Tage pro Jahr
Aufrechterhaltung des Betriebs	
Rechteverwaltung	18 Tage pro Jahr
Analyse der Logbuchdaten	24 Tage pro Jahr
Einrichtung neuer Dienste	6 Tage pro Jahr
Genereller Admin-Aufwand	24 Tage pro Jahr
Summe	96 Tage pro Jahr = 75.000 Euro/Jahr
Bei 1000 Benutzern ergibt sich ein Aufwand von 75 € /Benutzer	

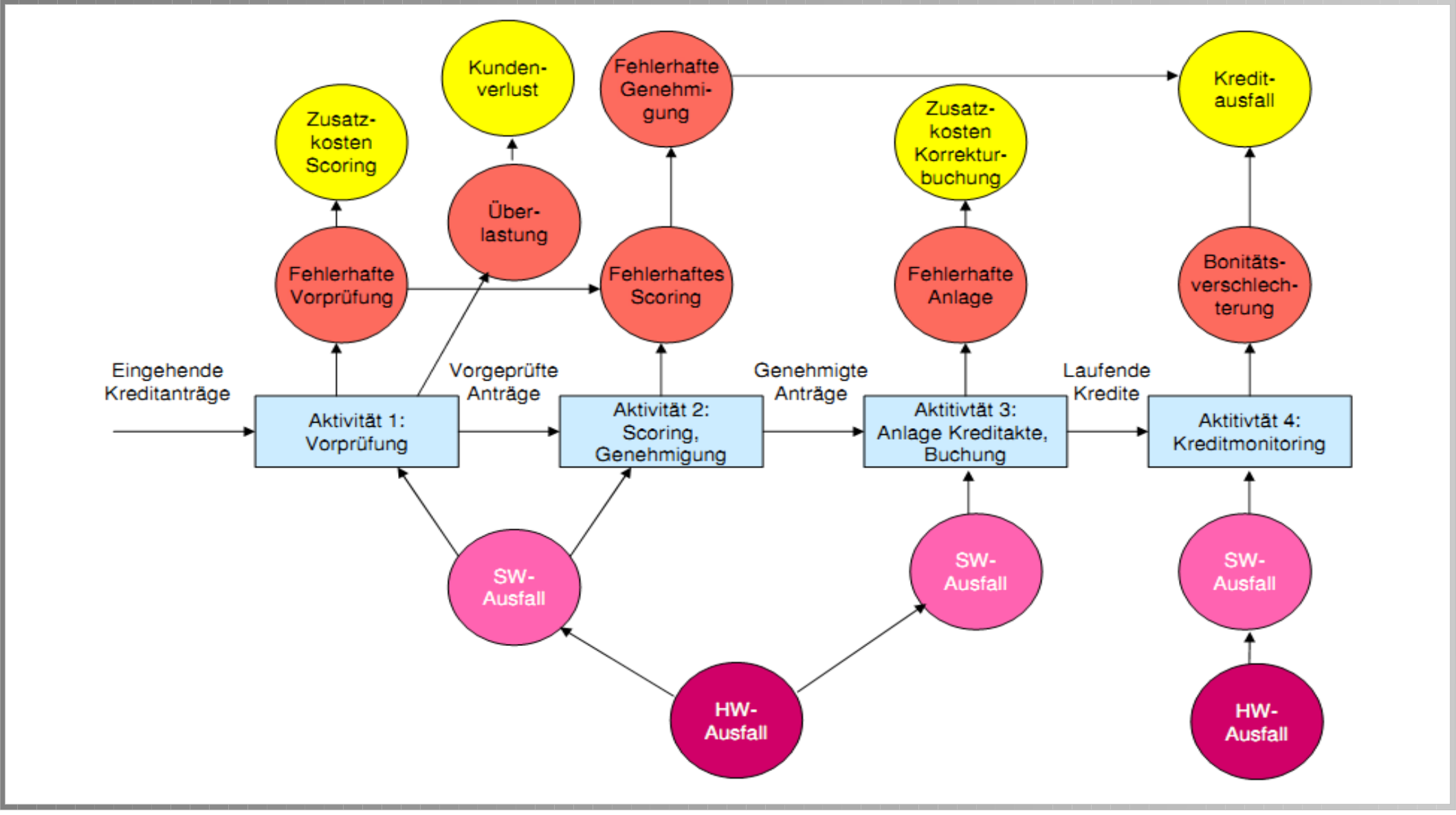
Ursachenanalyse ist bei Risiken von Geschäftsprozessen entscheidend !



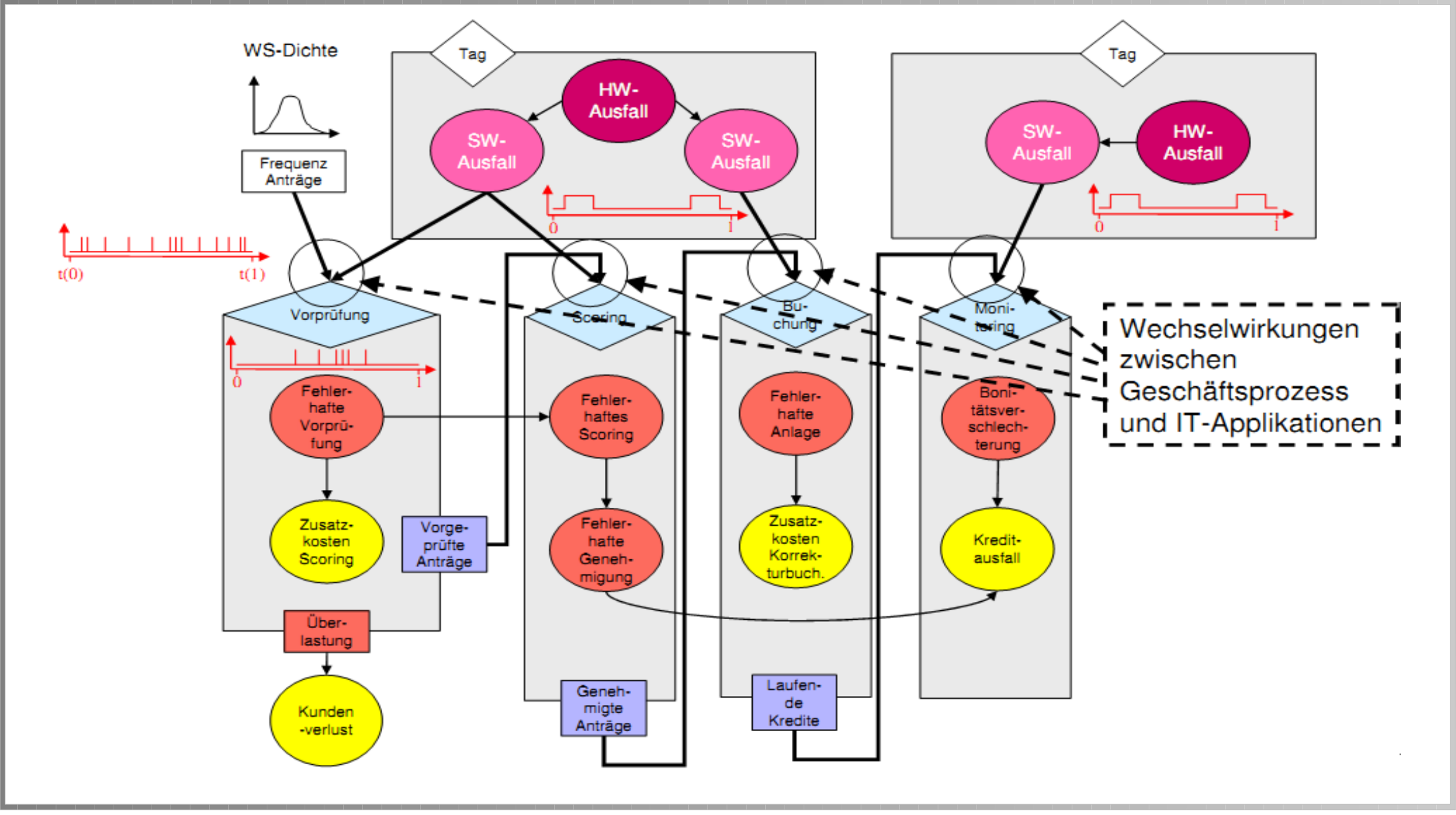
Ursachen-Wirkungs-Zusammenhänge erfordern Prozesssicht



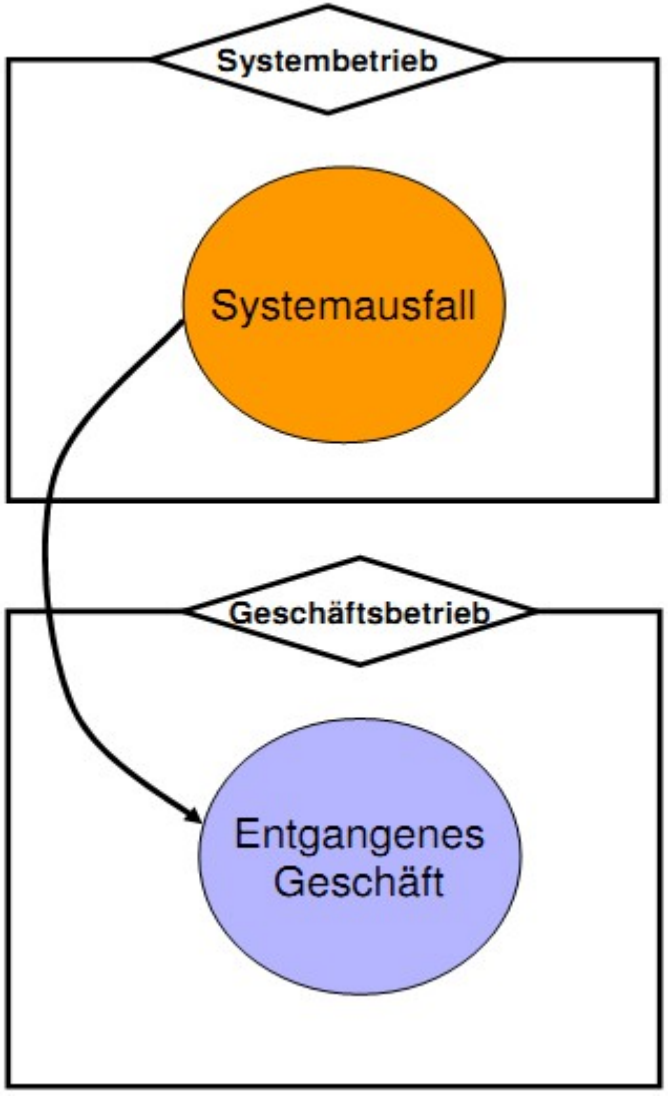
Prozessbasiertes OpRisk-Management: Beispiel Kreditbearbeitung

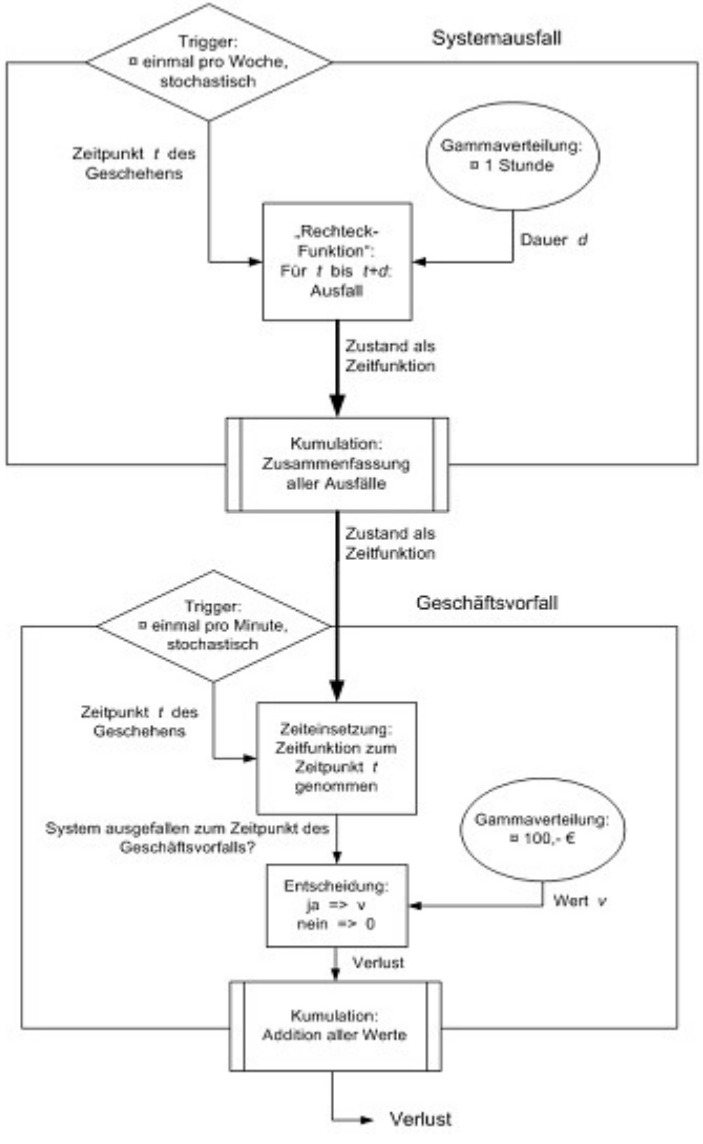


Prozessbasiertes Simulationsmodell Kreditbearbeitung

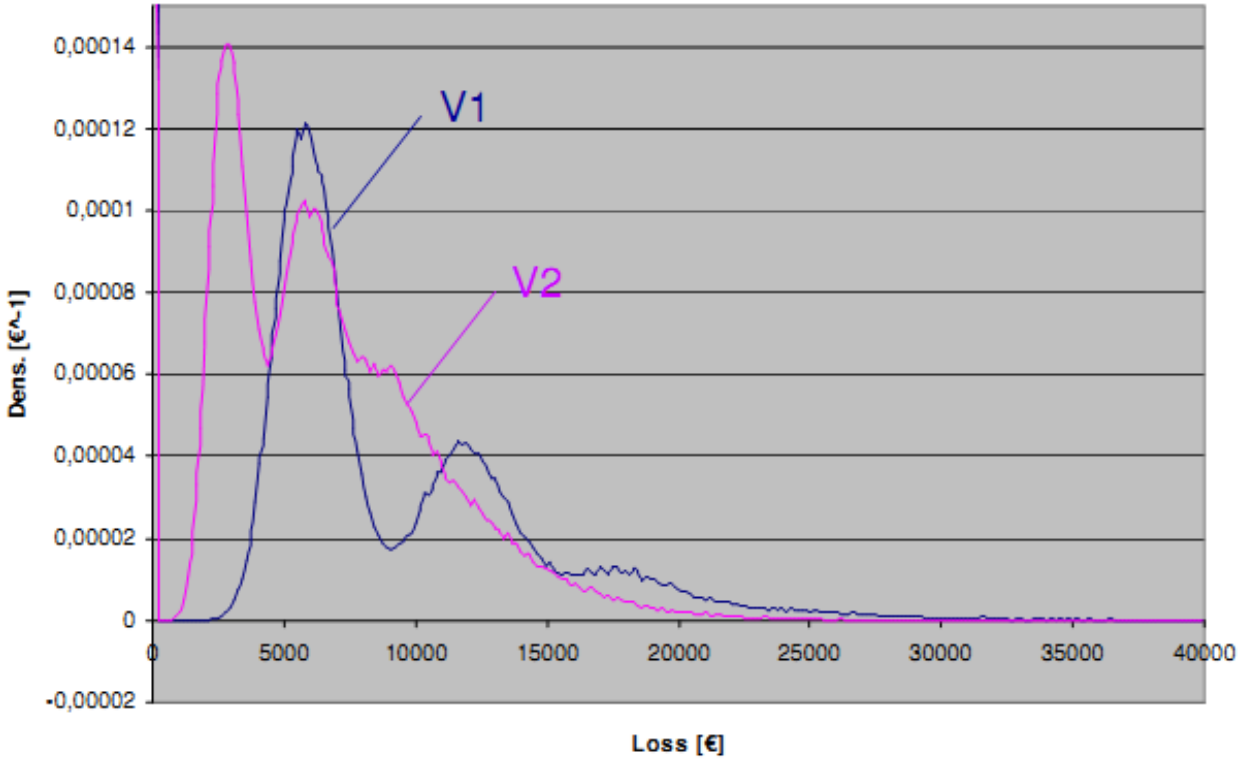


Wechselwirkung von IT-Applikationen und Geschäftsprozess





Simulationsergebnisse



Version 1:
IT-Ausfall Ø pro Woche 1x für Ø 1 Std.
Geschäftsvorfall (Wert Ø 100 €),
Ø einmal pro Minute (24 h).
Referenzzeitraum 1 Woche.

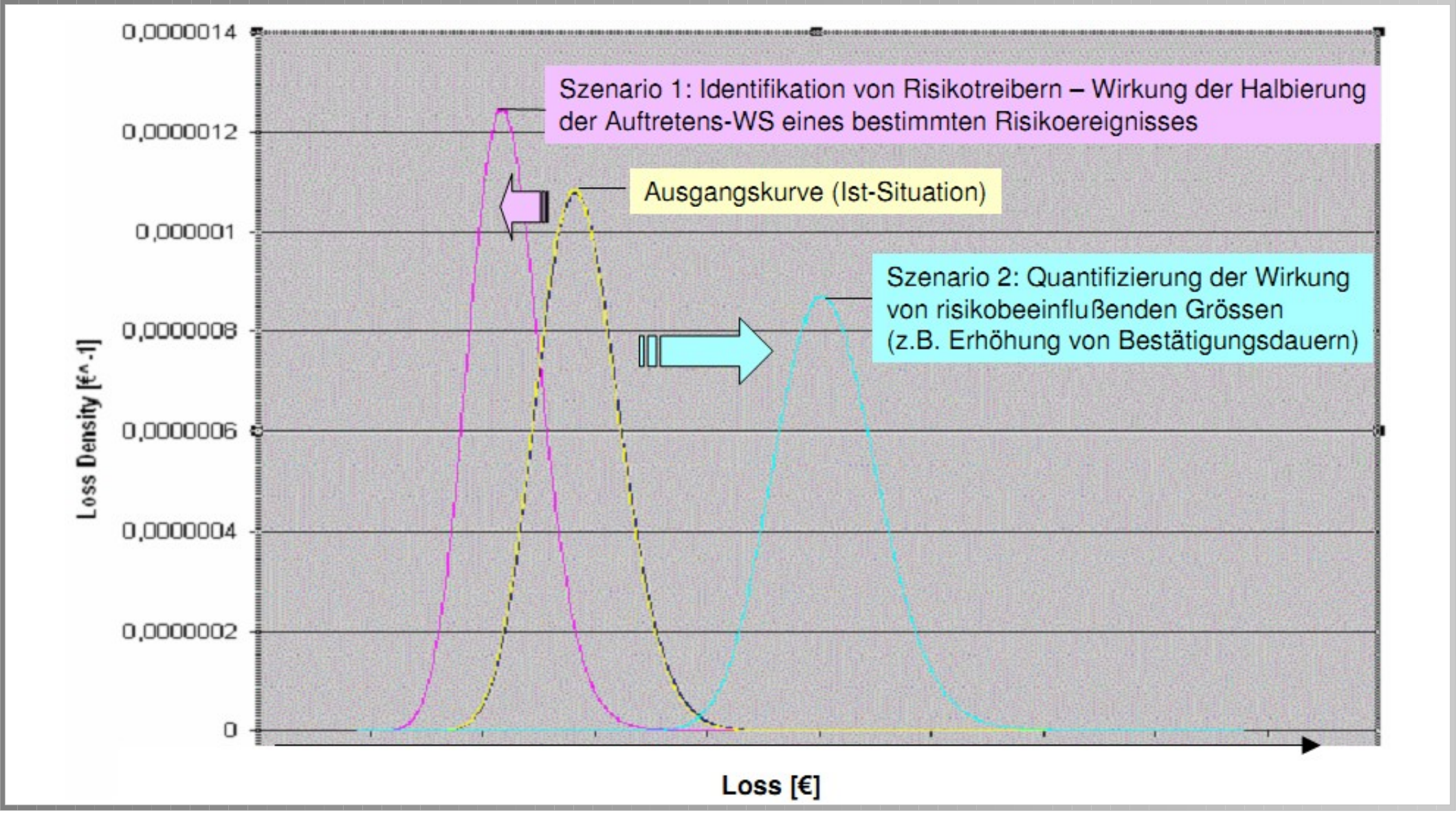
Ergebnisse:
Erwarteter Verlust = 6000 €/Woche
VaR = 24.400 € (0,99-Quantil)

Version 2:
IT-Ausfallrate wurde verdoppelt
(Ø 2x pro Woche).
Mittlere Ausfalldauer wurde halbiert
auf ½ Std.

Ergebnisse:
Erwarteter Verlust = 6000 €/Woche
VaR = 18.320 € (0,99-Quantil).

Wechselwirkungen zwischen Geschäftsprozess und IT beeinflussen VaR signifikant!

Analysemöglichkeiten durch Simulation



Aktuelles Forschungsprojekt: Seconomics

Aktuelles Projekt: Seconomics (EU).

Ziel: Unterstützung für Analysen hinsichtlich Rentabilität von Sicherheitsinvestitionen auf Basis von vorhandenen Artefakten (z.B. Geschäftsprozess-Modelle).