GI, Fachgruppe

Management der Informationssicherheit

Operational Risk- und IT-Security-Management – Gemeinsamkeiten und Unterschiede

Möglichkeit der Identifikation und Bewertung von IT-Sicherheitsrisiken im Rahmen der operationellen Risiken nach Basel II?

Vorstellung

über mich

Stefan Kronschnabl, Dipl. W-Inf. Univ.

Wissenschaftlicher Mitarbeiter ibi research

Forschungsschwerpunkt IT-Security Management, Leitung: Professor Dr. Erhard Petzel

über das ibi research

Einrichtung zur Forschung und Umsetzung der Forschungsergebnisse in die Finanzwirtschaft

Gemäß Satzung fließen die Ergebnisse der ibi research unmittelbar in die Lehre der Universität ein

Umgekehrt stützen sich die Arbeiten im ibi research auf die Forschung des Lehrstuhls

Gesellschafter: MLP, Sparkassenverband Bayern und Prof. Bartmann

Inhalt

1. Motivation und Einführung

2. Risiko und Risikomanagement

2.1 Zielsetzung des Risikomanagements

2.2 Risikobegriff und Risikoarten

2.3 Risikomanagementkreislauf

3. Operationelle Risiken in Basel II

3.1 Basel II Kompakt

3.2 Kategorisierung operationeller Risiken in Basel II

3.3 Bewertungsverfahren operationeller Risiken nach Basel II

4. IT-Sicherheitsrisiken

4.1 Definition und Standards

4.2 Kategorisierung von IT-Sicherheitsrisiken

4.3 Problematik beim IT-Sicherheitsmanagement

5. IT-Sicherheitsrisiken und operationelle Risiken im Vergleich

5.1 Kategorisierung – Gemeinsamkeiten und Unterschiede

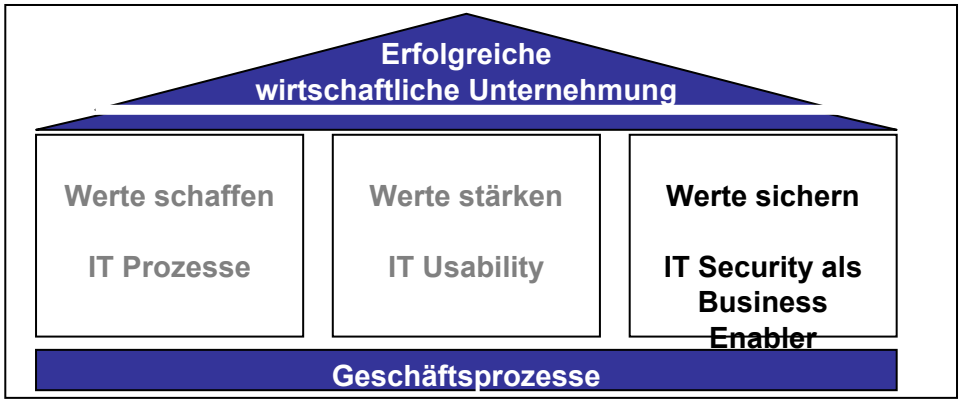
5.2 Management Modelle – Gemeinsamkeiten und Unterschiede

5.3 Ableitung eines Verfahrens zur Bewertung von IT-Sicherheitsrisken nach Basel II

6. Fazit und Ausblick

1. Motivation und Einführung

- Zunehmende Bedeutung der IT
  - Ohne funktionierenden IT keine Bankgeschäfte möglich (Überlebensfähigkeit ohne IT: 2-3 Tage [Schamberger])
  - Bedrohungen durch IT-Risiken nehmen zu [CERT, CSI]



- §25a Abs.1 KWG: IT-Sicherheit liegt in der Verantwortung des Managements - nach einem Sicherheits-Vorfall wird ex-ante geprüft!

  → Notwendigkeit der Etablierung eines geeigneten ISMS mit konkreten Verfahren

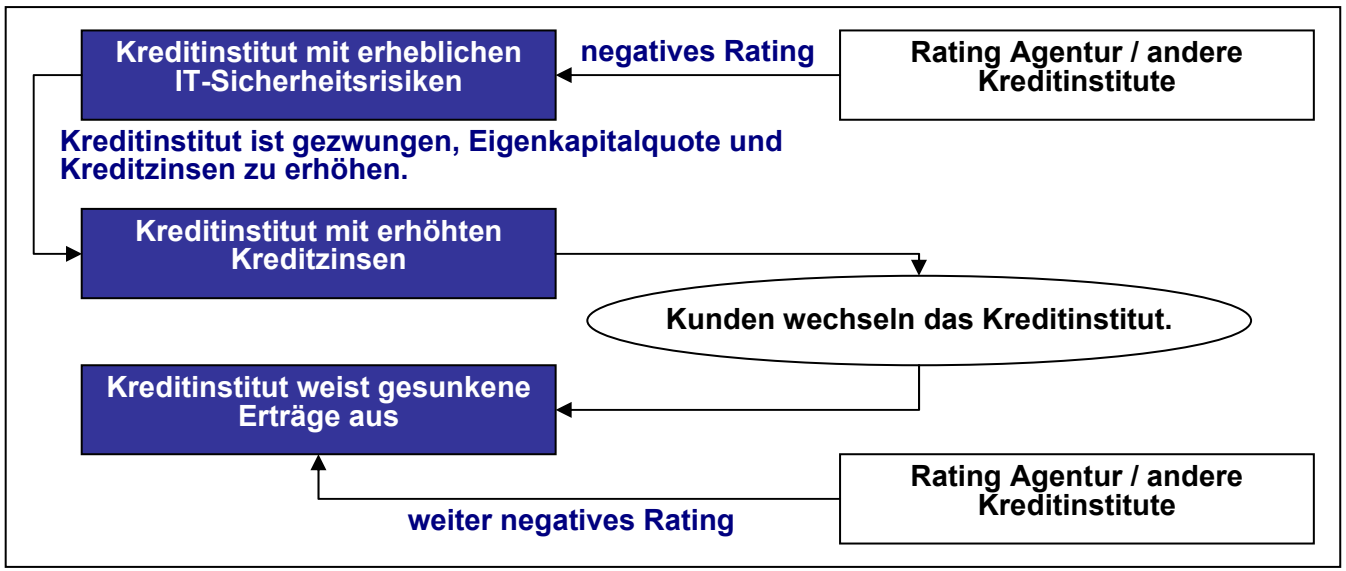
  → in Wissenschaft und Praxis kaum erforscht und manifestiert

1. Motivation und Einführung

- Das mit dem Betrieb von IT-Systemen verbundene Risiko ist Teil des operationellen Risikos in Banken
  - Die IT-Sicherheitsrisiken sind Teil des Betriebsrisikos
  - Sicherheitsziele: **Verfügbarkeit, Vertraulichkeit oder Integrität**
- Baseler Ausschuss weist der IT-Sicherheit wesentliche Bedeutung bei der Verminderung der operationellen Risiken zu [vgl. Sound Practices]
- Maßnahmenorientiert wird das Thema IT-Sicherheit zudem in den „Risk Management Principles for Electronic Banking“ behandelt

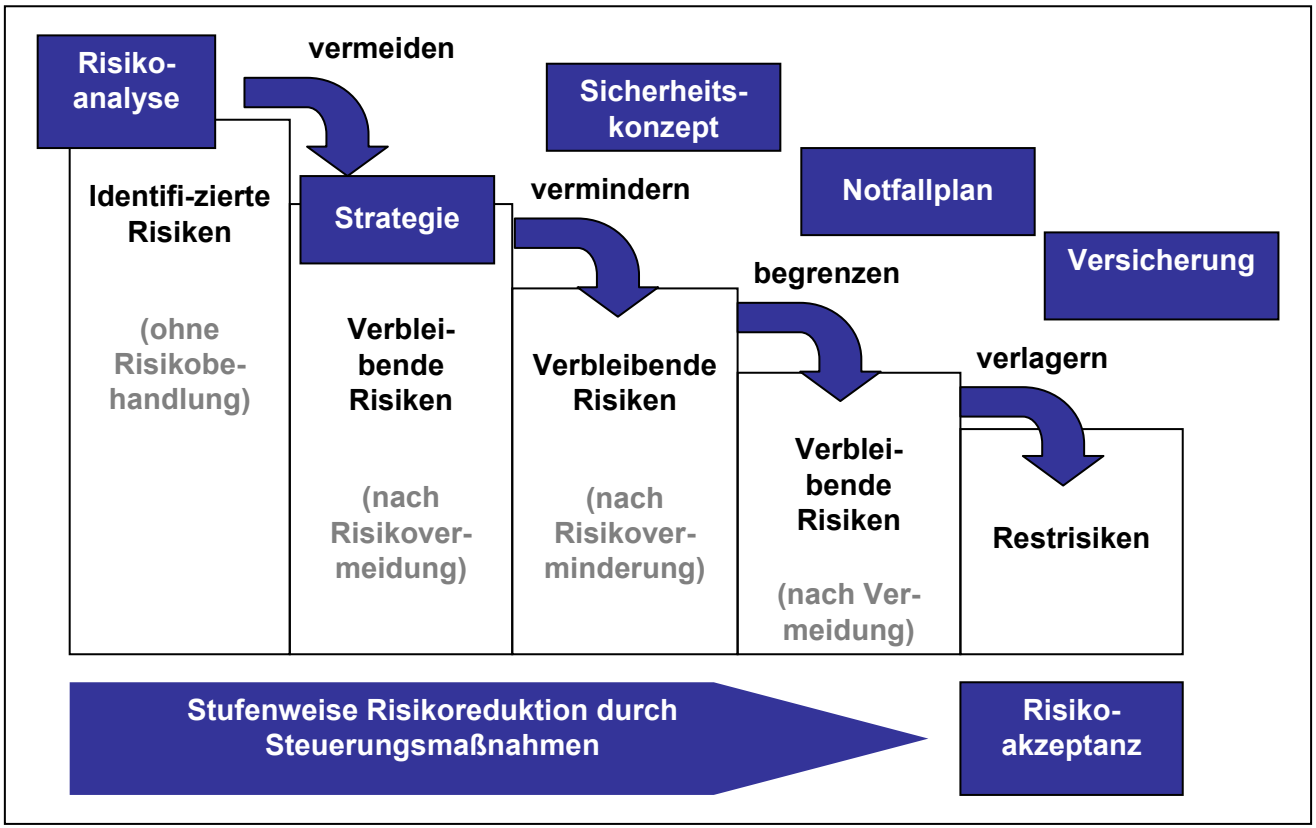
1. Motivation und Einführung

- Mögl. negative Ratings aufgrund von IT-Risiken
  - Mögl. Kundenwechsel aufgrund mangelnden Vertrauens
  - Notwendiges EK für chancenbehaftete Geschäfte fehlt



2. Risiko und Risikomanagement

- Zielsetzung: Risikominimierung durch aktives Risikomanagement



In Anlehnung an [Gaulke 2003]

2. Risiko und Risikomanagement

- Definition
  - „Risiko als die Möglichkeit einer negativen Abweichung zwischen dem tatsächlich erreichten Ergebnis und dem erwarteten Ergebnis." [Romeike 2004, S. 44]
  - Risiko als „Wagnis, eine Gefahr oder auch eine Verlustmöglichkeit bei einer unsicheren Unternehmung." [DUDEN 1983]
  - Risiko lat. Ris(i)co, eigentlich Klippe, die zu umschiffen ist

Definition

Risiko bezeichnet den möglichen Eintritt eines Schadensereignisses, und ergibt sich als Summe der möglichen Schäden multipliziert mit den jeweiligen Eintrittswahrscheinlichkeiten.

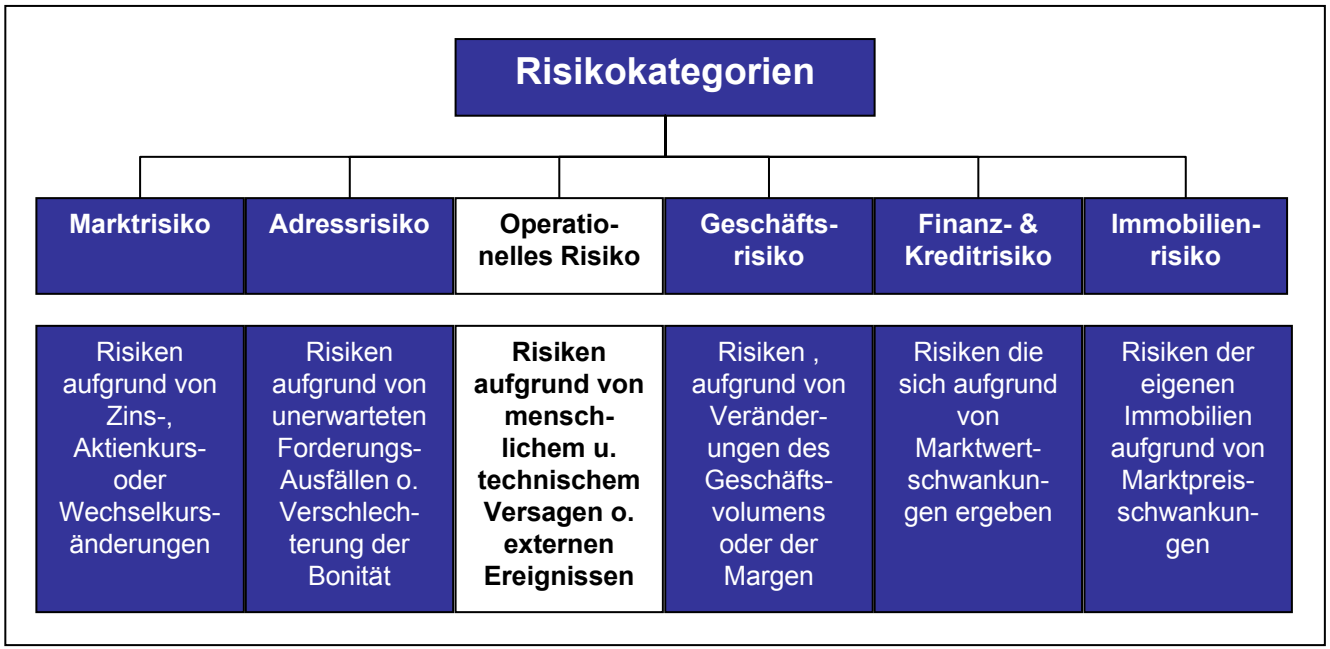
$$Risiko = \sum_{i=1}^{n} (LGE_i \times PE_i)$$

PE = Probability of Loss Event (Schadenseintrittswahrscheinlichkeit)

LGE = Loss Given Event (Verlust bei Schadenseintritt)

2. Risiko und Risikomanagement

- Risikokategorien



- Abhängigkeiten zwischen den dargestellten Risikoarten
  - Unzureichende Sicherung der IT kann Manipulationen möglich machen
  - Folge: finanzielle Schäden / Reputationsschäden

3. Operationelle Risiken in Basel II

- Basel II - Grundlagen und Überblick
  - Steuerungsinstrumente zur Schaffung eines Gleichgewichts zw. ökonomisch benötigtem EK und regulatorischen Vorgaben
  - Gründung 1975 von den Zentralratspräsidenten der G-10 Staaten, sowie Luxemburg; 1984 Beitritt der Schweiz
  - Konsultationspapiere als Grundlage der europäischen Gesetzgebung
    - Umsetzung durch nationale Gesetze und Durchführungsverordnungen
    - Institute haben die Möglichkeit gezielt Einfluss zu nehmen; Unterstützung mit methodischem Know-how durch Auswirkungsstudien
    - Umsetzungs- und Steuerungsvorschriften als „lebendem Prozess“ [Bieg 2003]

3. Operationelle Risiken in Basel II

- Einführung und Definition
  - „*…the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."* [BIS 2001c, S.2]

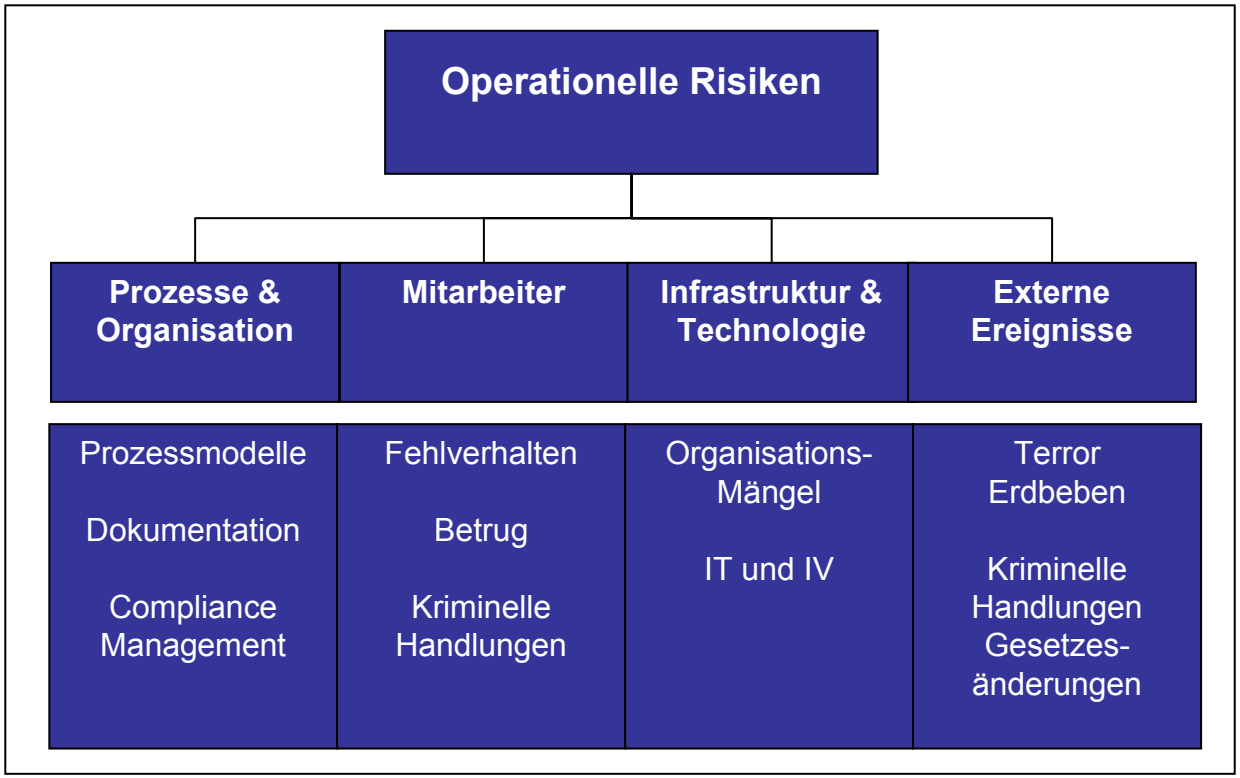
Definition (4.1)

„Operationelles Risiko = die Gefahr von unmittelbaren oder mittelbaren Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder von externen Ereignissen eintreten."

  - „Rechtliche Risiken werden durch diese Definition folglich mit eingeschlossen, die Gruppe der strategischen Risiken, sowie Reputations- und Geschäftsrisiken dagegen nicht." [BIS 2001a, S.103]

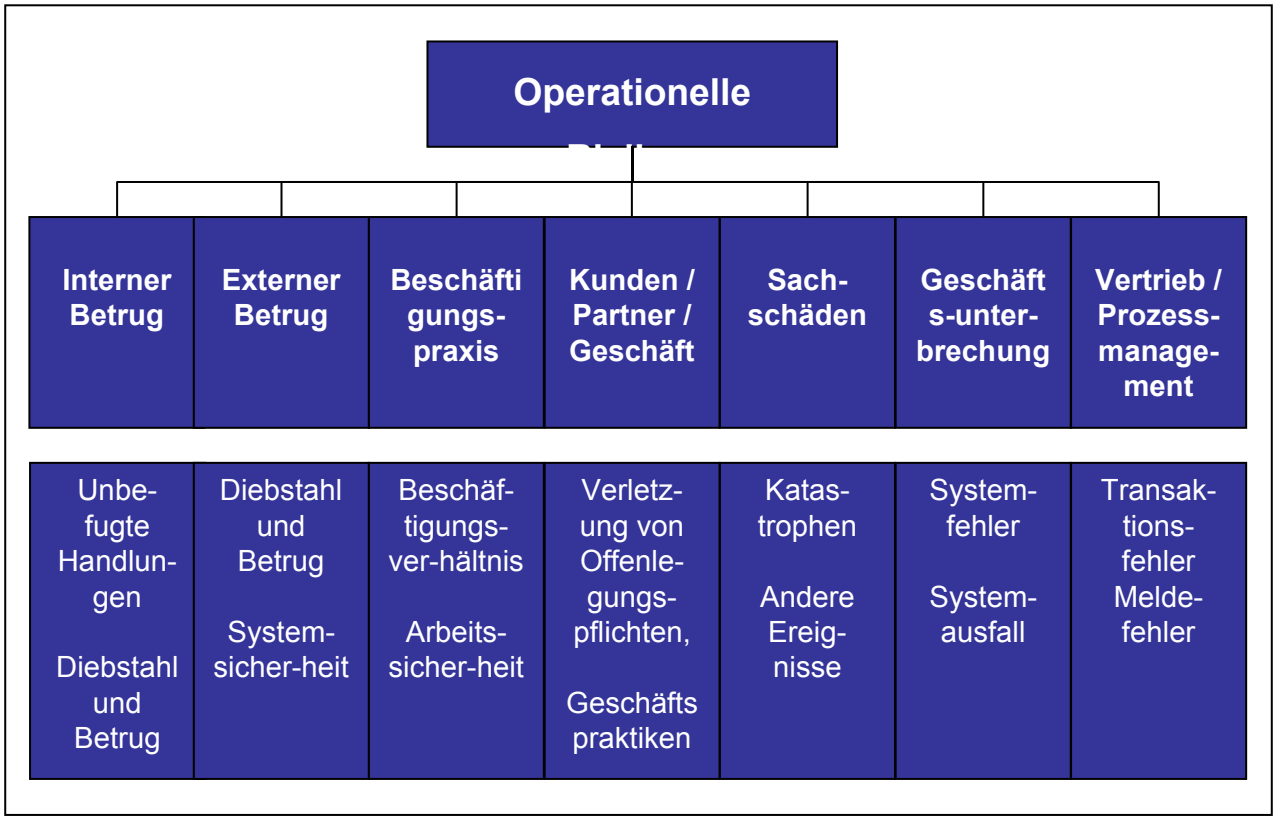
3. Operationelle Risiken in Basel II

- Ursachenkategorisierung



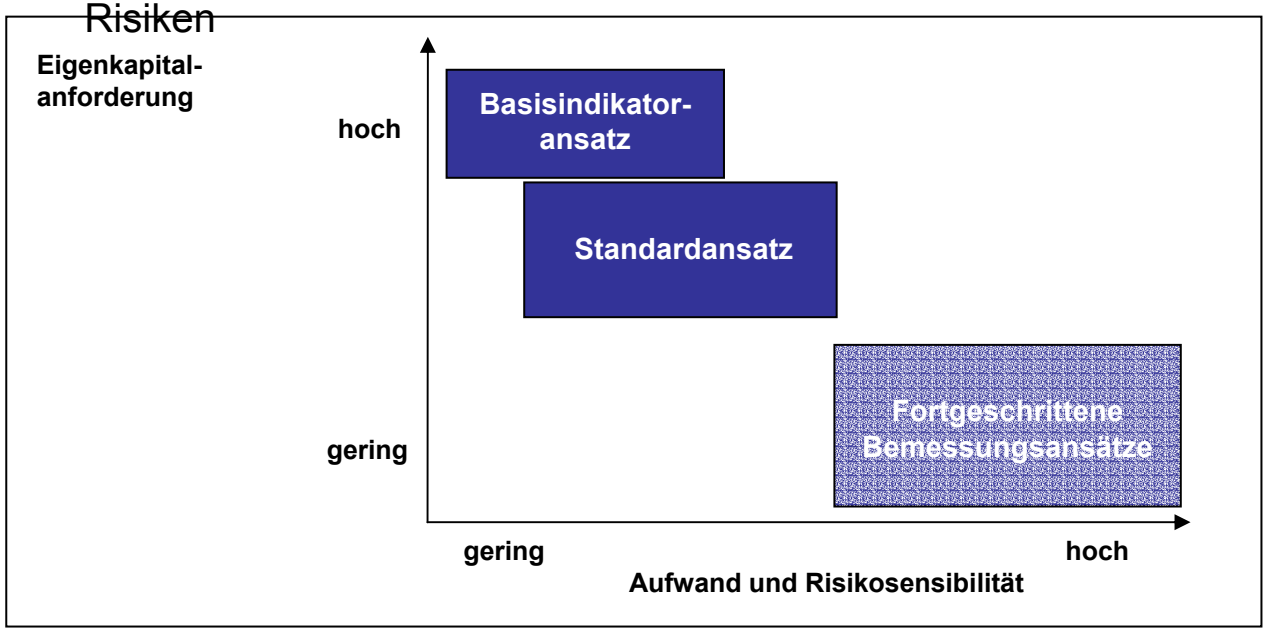
3. Operationelle Risiken in Basel II

- Ereigniskategorisierung



3. Operationelle Risiken in Basel II

- Überblick über die einzelnen Bewertungsmodelle
  - Drei verschiedenen Methoden zur Bestimmung der Risiken
  - Methoden bauen stufenweise aufeinander auf
  - Unterschied: Komplexität, Sensitivität und Messgenauigkeit der Risiken



Fortgeschrittene Bemessungsansätze -> geringere EK-Hinterlegung -> Anreiz zur Verbesserung des RM

[BearingPoint 2003]

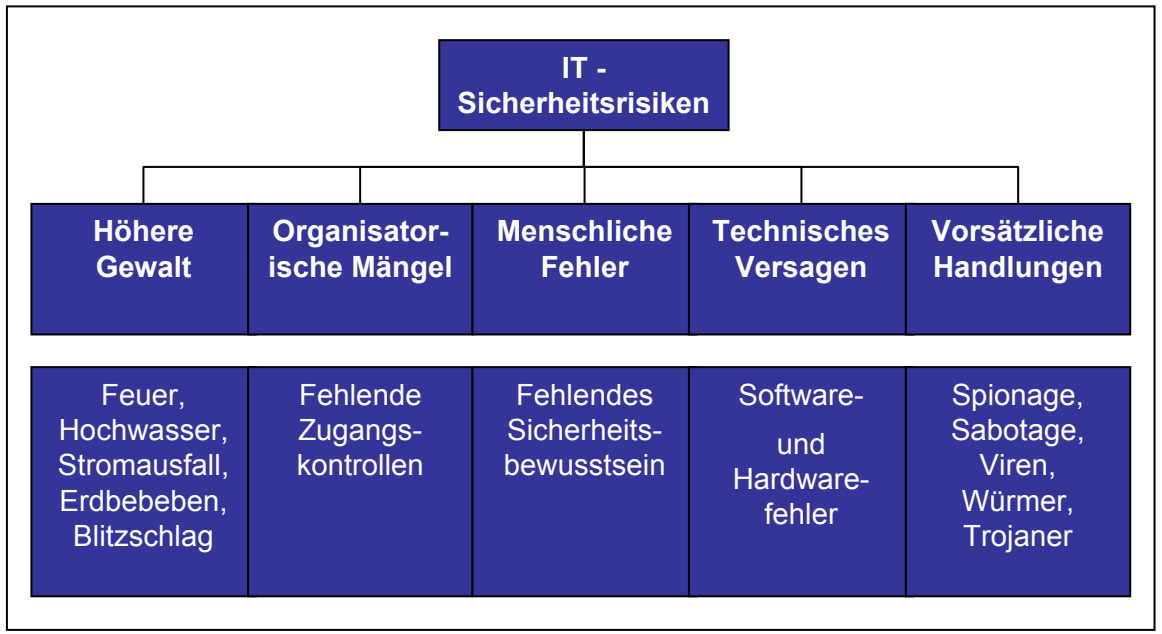
4. IT-Sicherheit und IT-Sicherheitsrisiken

- Die klassischen Schutzziele der IT-Sicherheit

Die Schutzziele der IT-Sicherheit	
Vertraulichkeit (Geheimhaltung)	• **Schutz vor unberechtigter Kenntnisnahme** • **Inhalt einer Nachricht ist nur Absender und Empfänger bekannt** • **Kenntnisnahme der Inhalte einer Nachricht durch unberechtigte Dritte wird verhindert**
Verfügbarkeit	• **Schutz vor unbefugter Beeinträchtigung der Funktionalität eines Systems oder einer Anwendung** • **Daten und Informationen müssen im Rahmen der vereinbarten Betriebszeit jederzeit verfügbar und funktionsbereit sein**
Integrität (Vollständigkeit)	• **Sicherstellung der Korrektheit (Unversehrtheit) der Daten (Datenintegrität) bzw. der korrekten Funktionsweise von Systemen (Systemintegrität)** • **Verhinderung unbefugter oder unabsichtlicher Veränderung**

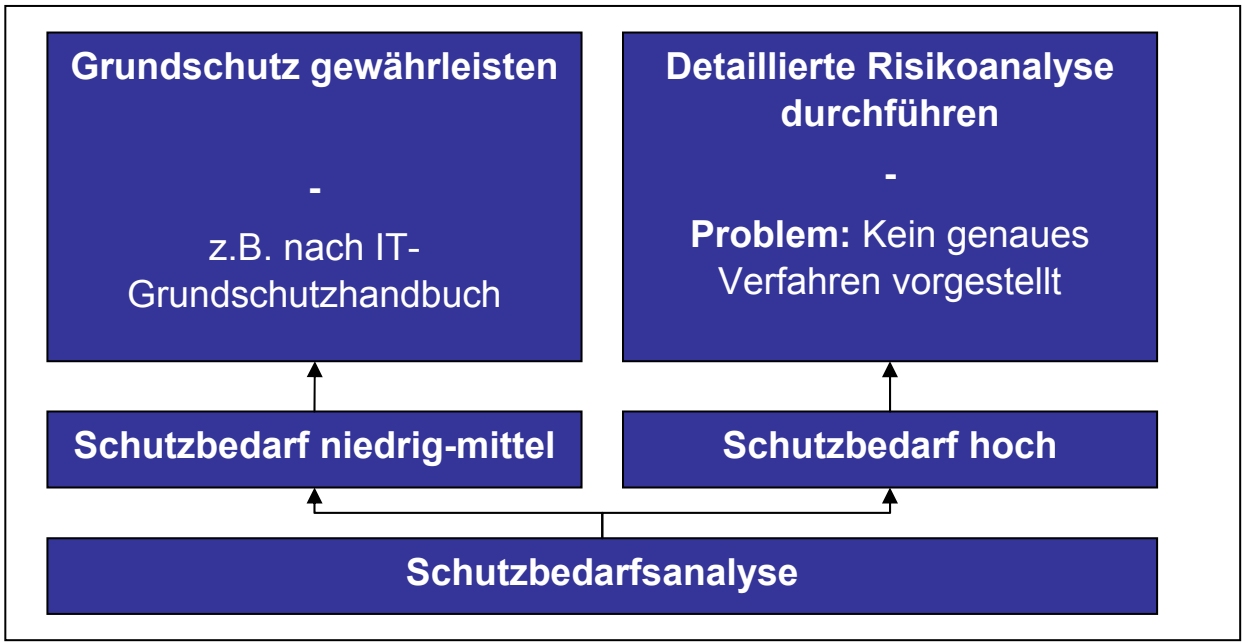
4. IT-Sicherheit und IT-Sicherheitsrisiken

- Kategorisierung von IT-Sicherherheitsrisiken / IT-GSHB
  - Kategorisierung von IT-Sicherheitsrisiken durch Gefährdungskategorien
  - Darstellung gemäß des Gefahrenkatalogs des BSI



4. IT-Sicherheit und IT-Sicherheitsrisiken

- Risikoanalyse nach IT-GSHB
  - Zunächst Durchführung einer Schutzbedarfsanalyse
  - Identifizierung kann sich dabei nach [IDW 2003] grundsätzlich auf wesentliche Elemente des IT-Systems beschränken



4. IT-Sicherheit und IT-Sicherheitsrisiken

- Erstellung eines Konzepts zur Schutzbedarfsanalyse
  - Klarheit über Notwendigkeit von Verfügbarkeit, Integrität und Vertraulichkeit
  - Einteilung in vordefinierte Stufen (gering – mittel – hoch)
  - Aufführung unterstützender Fragen und Beispiele zur Einstufung

	Gering Stufe 0				Mittel Stufe 1				Hoch Stufe 2			
Vertraulichkeit												
Integrität												
Verfügbarkeit												

- Risikoanalyse bei hohem Schutzbedarf
  - **Problem: Kein Verfahren vorgegeben - Idee: Kombination mit Basel II**

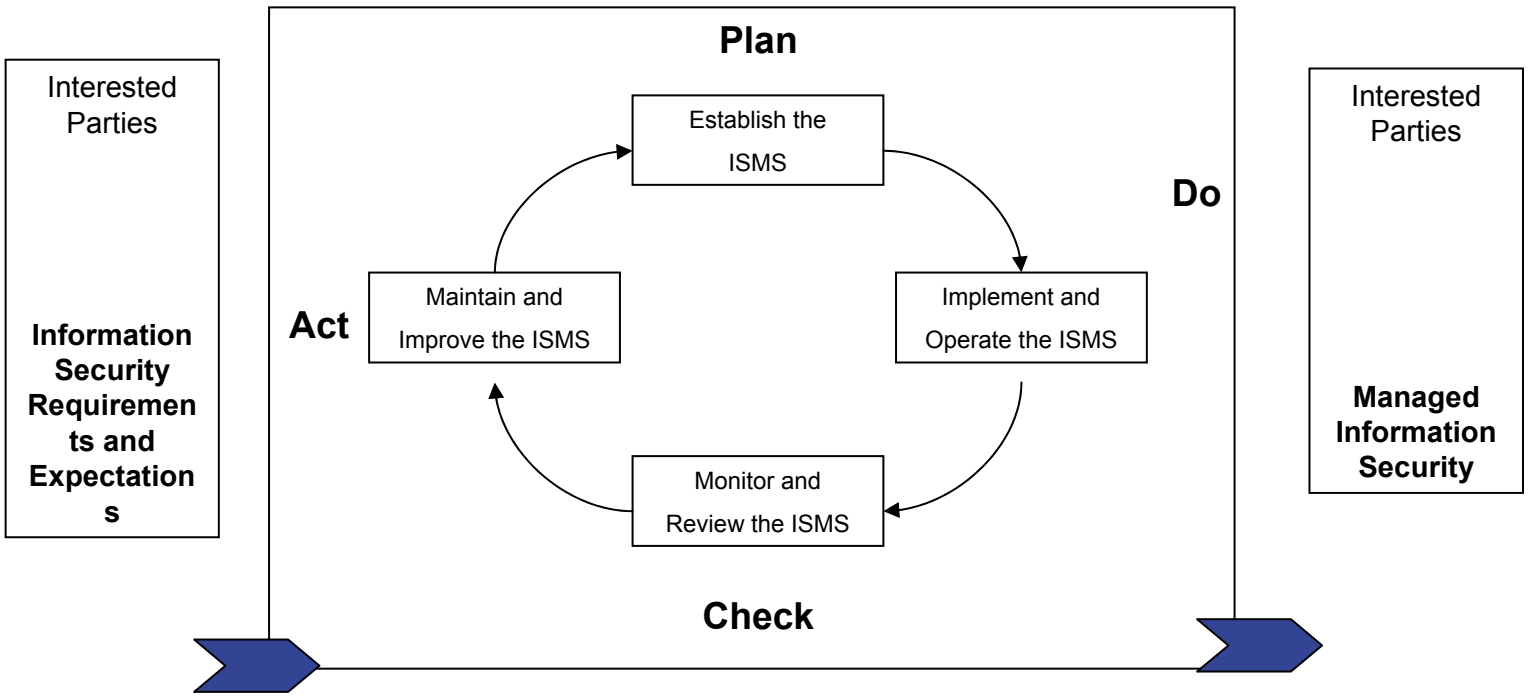
5. IT-Sicherheitsrisiken und operationelle Risiken

- Die Herausforderung liegt darin, das ORM und das klassische ISMS besser zu integrieren.
  - Probleme vor allem auf der Prozess- und Organisationsebene
  - Einbindung von IT-Sicherheitsrisiken in die operationellen Risiken
  - Bewertung von IT-Sicherheitsrisiken nach der Methodik von Basel II

- Vorgehensweise
  - Überblick über den Managementkreislauf
  - Erarbeitung eines Basel II und BSI konformen Kategorisierungsmodells
  - Überprüfung und Sicherstellung der Vollständigkeit
  - Entwicklung eines Modells zur Risikoanalyse von IT-Sicherheitsrisiken

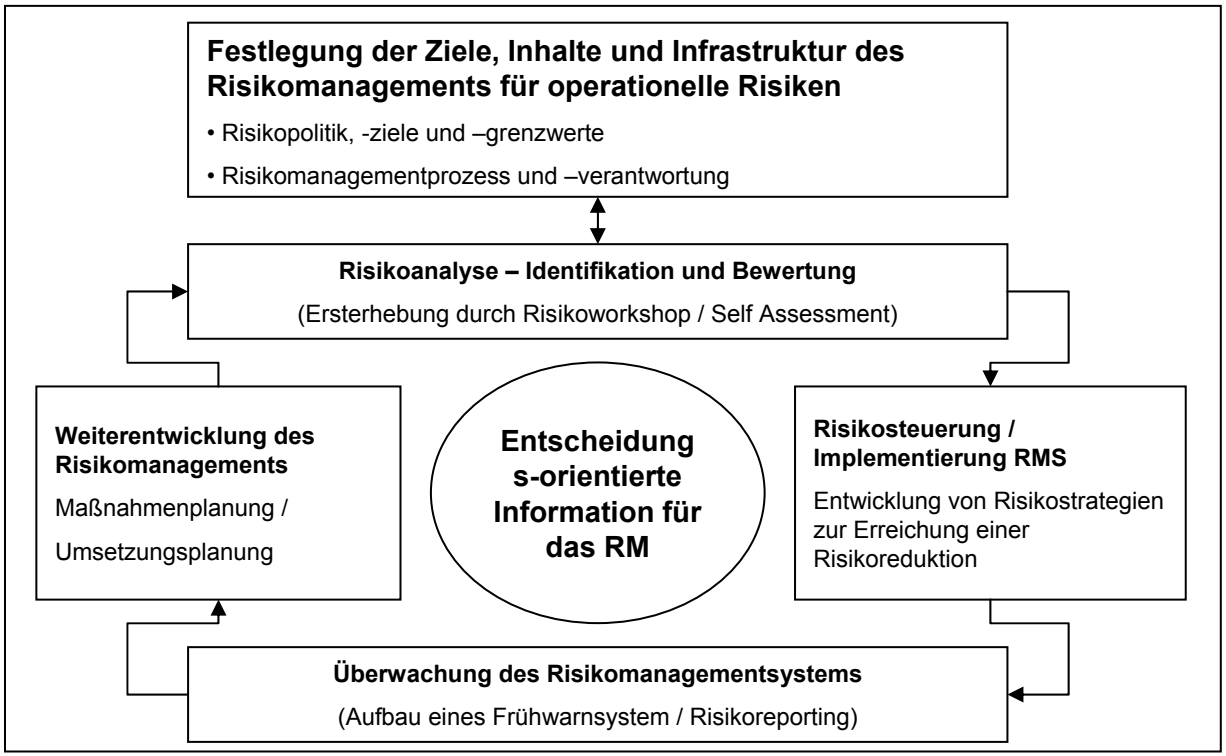
5. IT-Sicherheitsrisiken und operationelle Risiken

- Risikomanagement Kreislauf – Beispiel BS 7799-2



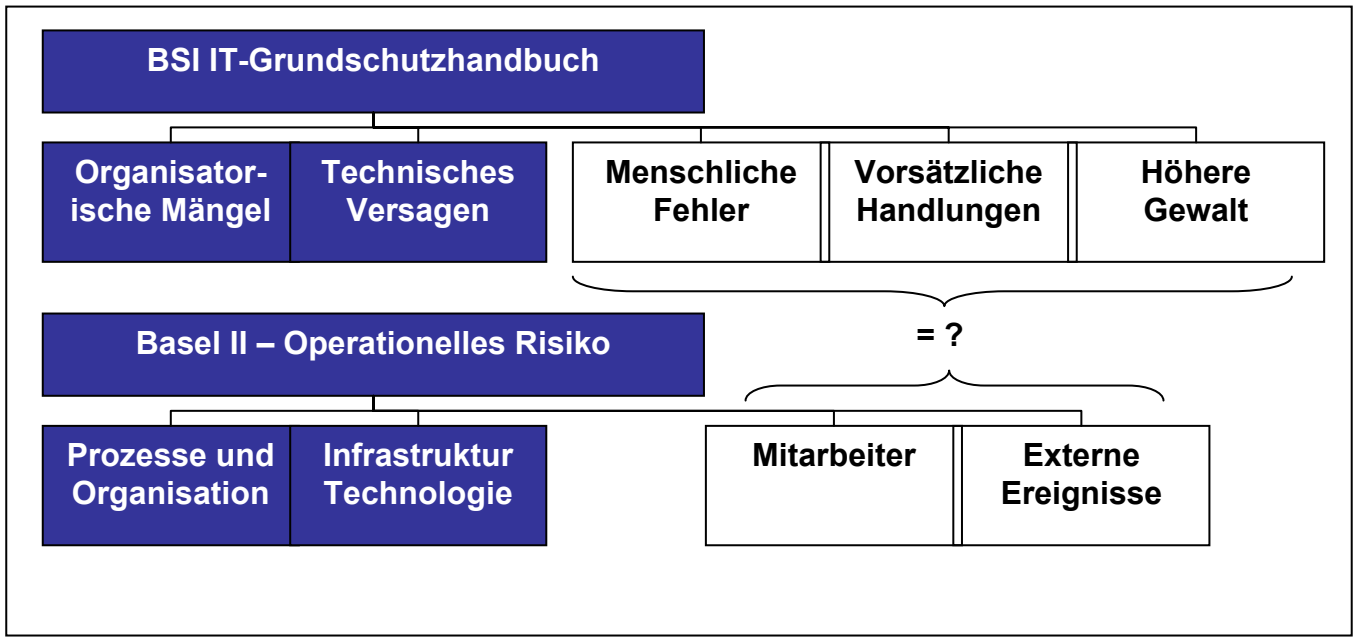
5. IT-Sicherheitsrisiken und operationelle Risiken

- Risikomanagement Kreislauf – Beispiel OpRisk



5. IT-Sicherheitsrisiken und operationelle Risiken

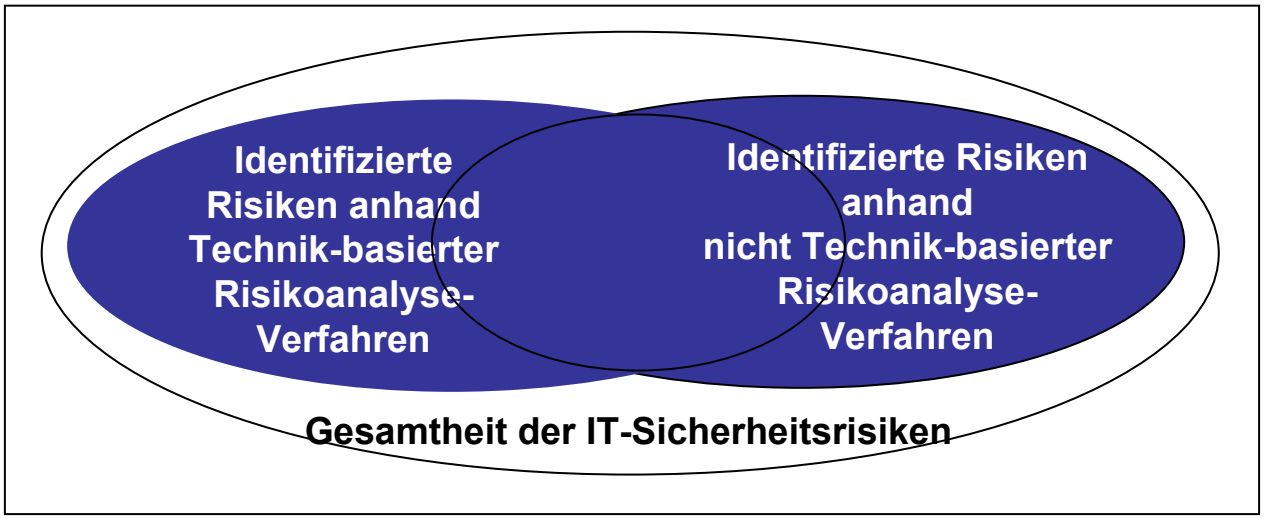
- Vergleich der Ursachenkategorisierungen nach Basel II und BSI
- Vergleich verdeutlicht gewisse Überschneidung



Fazit: Die beiden Kategorisierungsmodelle sind über die unteren Ebenen inhaltlich deckungsgleich

5. IT-Sicherheitsrisiken und operationelle Risiken

- Idee: Risikoanalyse durch zwei komplementäre Verfahren
  - Technik-basierte Risikoanalyse-Verfahren
  - Nicht Technik-basierte Risikoanalyse-Verfahren



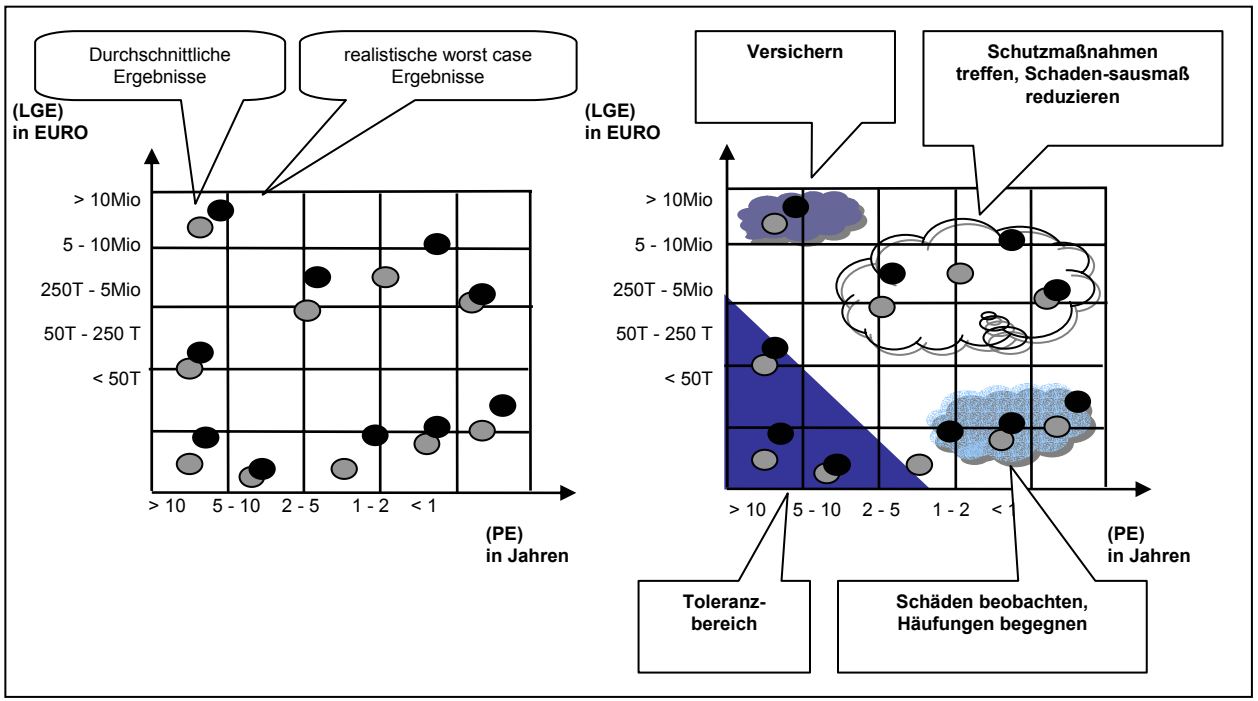
  - Damit: Erreichung eines mögl. vollständigen und realitätsnahen Risikoabbilds
  - Erfüllung der spezifischen Anforderungen von IT-Sicherheitsrisiken

5. IT-Sicherheitsrisiken und operationelle Risiken

- Verfahren zur Technik basierten Risikoanalyse:
  - Penetrationstests
  - Security Scanner
- Verfahren zur Nicht Technik basierten Risikoanalyse:
  - Self-Assessment anhand des Kriterienkatalog nach Basel II
    - Risikolisten zur Gewährleistung der Vollständigkeit
    - Einsatz numerischer Größen bei der Bewertung
    - Bewertung des primären/sekundären Schadenspotenzials
    - Ermittlung der jeweiligen Durchschnittswerte für PE und LGE
    - Ermittlung der Werte für den realistisch gesehen „schlimmsten Fall“ für PE und LGE je Einzelrisiko [Schuppenhauer 1998]

5. IT-Sicherheitsrisiken und operationelle Risiken

- Ergebniss-Darstellung - Abbildung in Form einer Risikomatrix
  - Möglichkeit der Darstellung individueller Akzeptanzlinie
  - Visualisierung von Schwellenwerten / Handlungsbedarfen



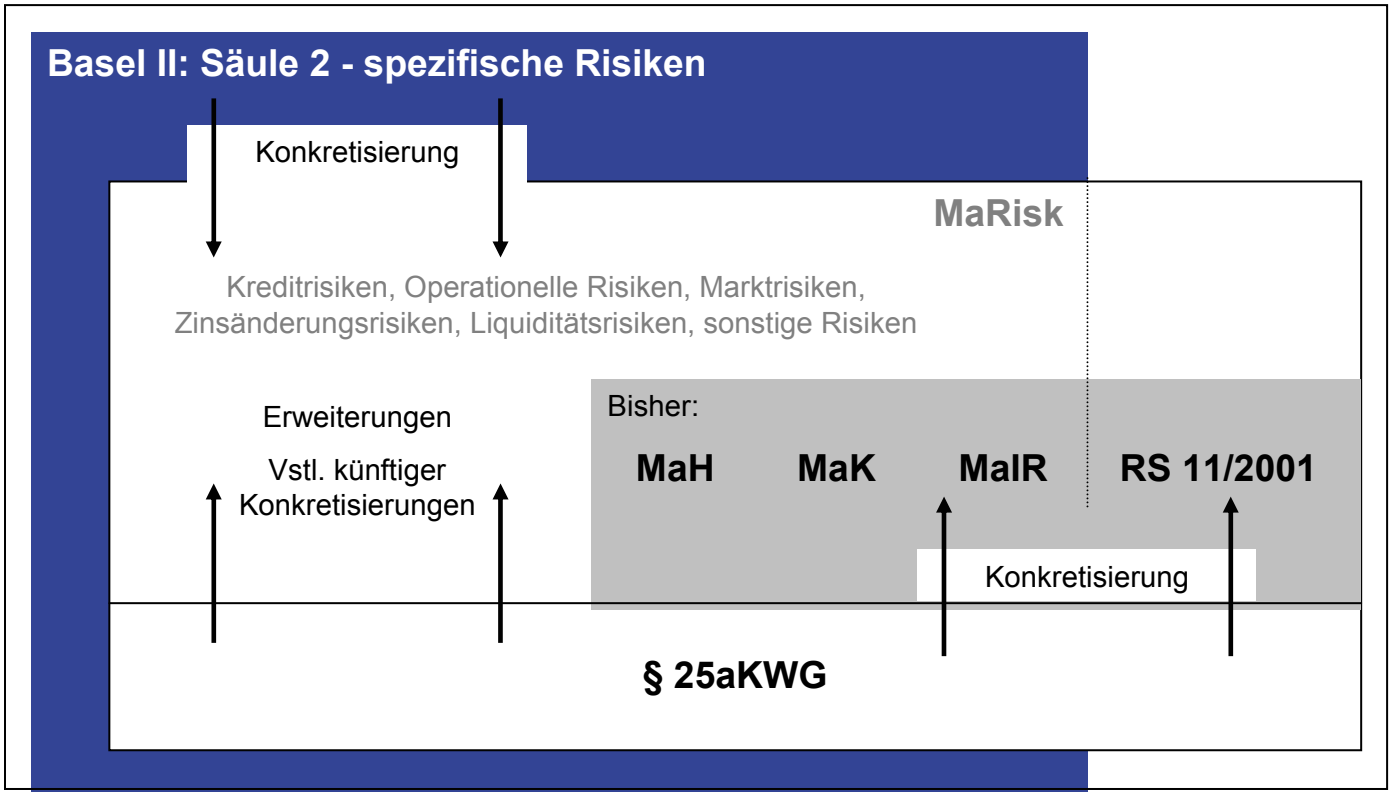
In Anlehnung an Secaron AG

6. Fazit und Ausblick

- OpRisk- und IT-Security-Management in den Management Grundkonzepten identisch
- OpRisk- und IT-Security-Management sind vergleichbar kategorisiert
- OpRisk- und IT-Security-Management erfahren Motivationsschub durch Basel II und MaRisk
- Kommunizieren der Vorteile ist ausschlaggebend für den Erfolg
  - Etablierung einer offenen Risikokultur
  - Akzeptanz durch den Vorstand
  - Kommunikation des Themas im Unternehmen - Sensibilisierung der Mitarbeiter
  - Risikomanagement bleibt auf der Strecke, wenn der ***„Risikofaktor Mensch“*** [Schneier 2003] nicht mitspielt

6. Fazit und Ausblick

- BaFin hat Entwicklung der MaRisk angekündigt - Zusammenführung bisher geltender Regelungen



6. Fazit und Ausblick

- Next Steps to do:
  - Anwendung des Verfahrens in der Praxis
  - Analyse der Integrationsmöglichkeit in ein gesamtheitliches Management Modell (z.B. in Anlehnung an das ISMS nach BS7799)
  - Möglichkeiten der Kosten-Nutzen-Berechnung evaluieren / ROSI

Sicherheit kostet Zeit und Geld – fehlende Sicherheit die Zukunft!

Vielen Dank für Ihre Aufmerksamkeit