KPMG

Advisory Services

Information Risk Management

Turning knowledge into value

IT-Risiko- und Sicherheitsmanagement

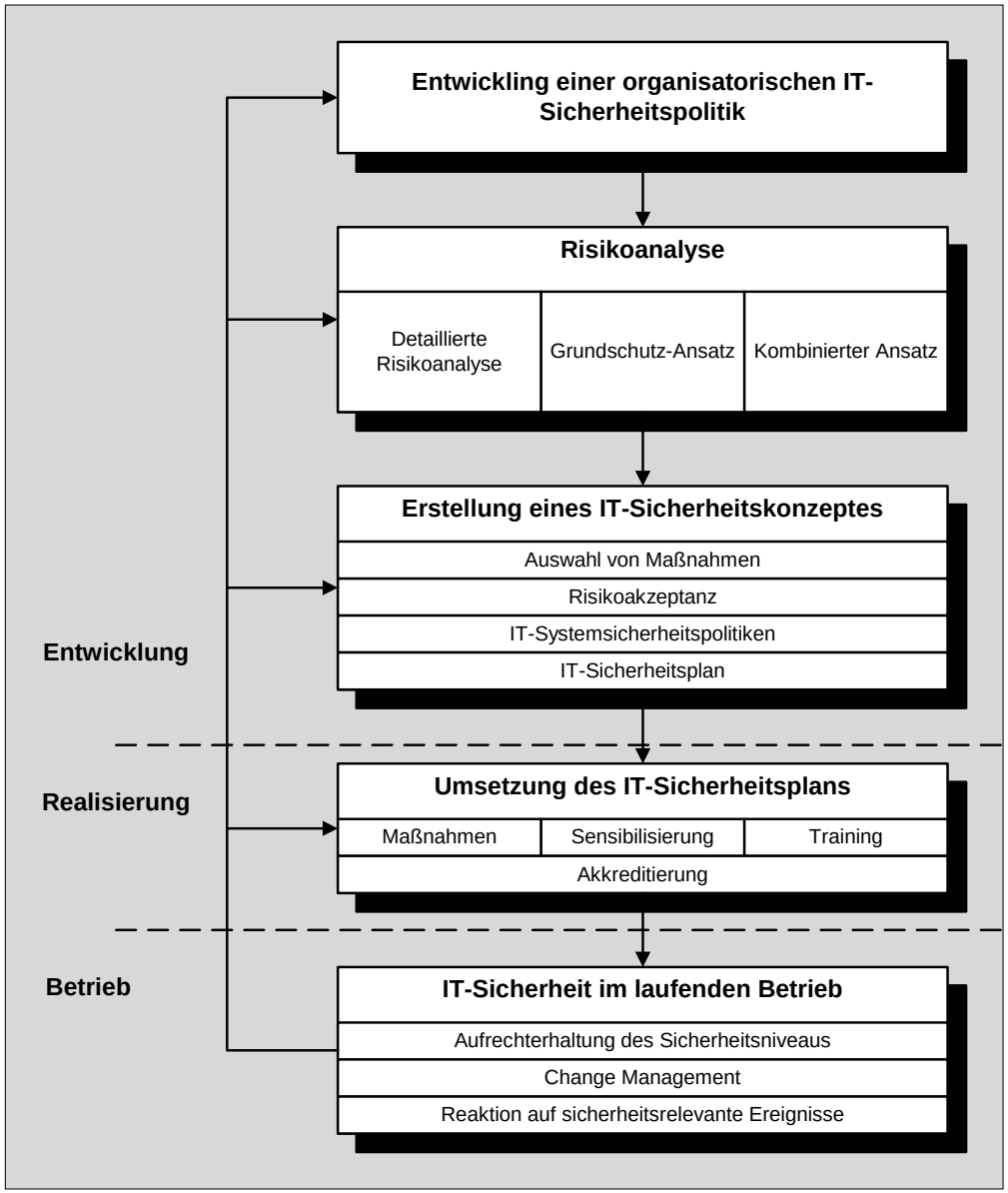
Workshop der GI Fachgruppe SECMGT am 28. Januar 2005 in Frankfurt/Main

Markus Gaulke
mgaulke@kpmg.com

IT- Sicherheitsmanagement

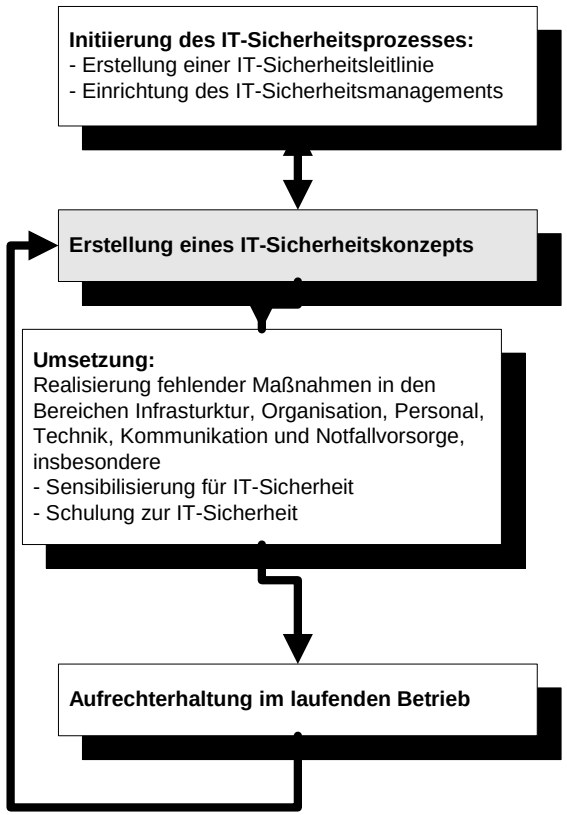
Aufgaben des IT-Sicherheitsmanagements

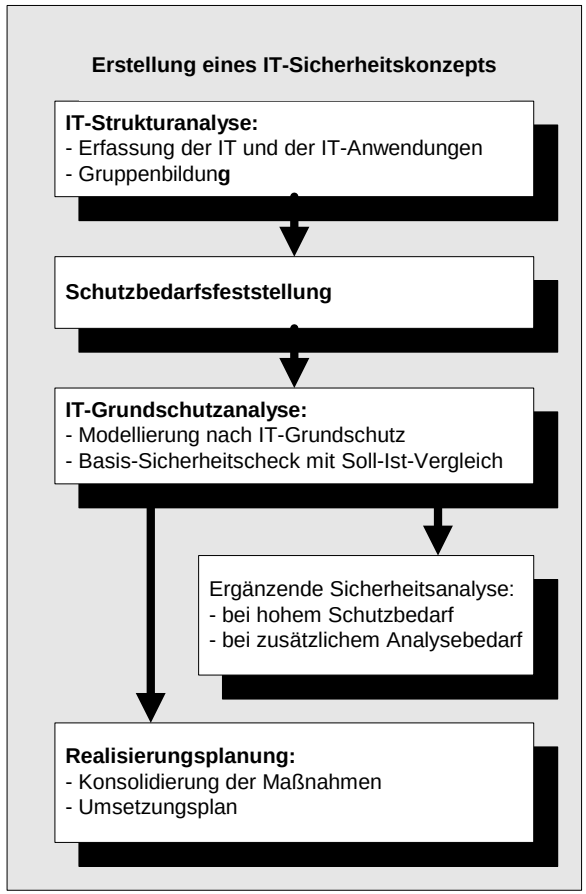
- Festlegung der IT-Sicherheitsziele, -strategien und –politiken der Organisation
- Festlegung der IT-Sicherheitsanforderungen
- Ermittlung und Analyse von Bedrohungen und Risiken
- Festlegung geeigneter Sicherheitsmaßnahmen
- Überwachung der Implementierung und des laufenden Betriebes der ausgewählten Maßnahmen
- Förderung des Sicherheitsbewusstseins innerhalb der Organisation
- Entdecken von und Reaktion auf sicherheitsrelevante Ereignisse



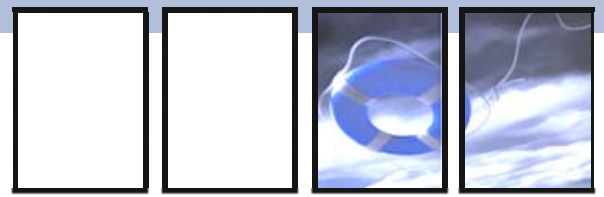
Rahmen des IT-Sicherheits-managements

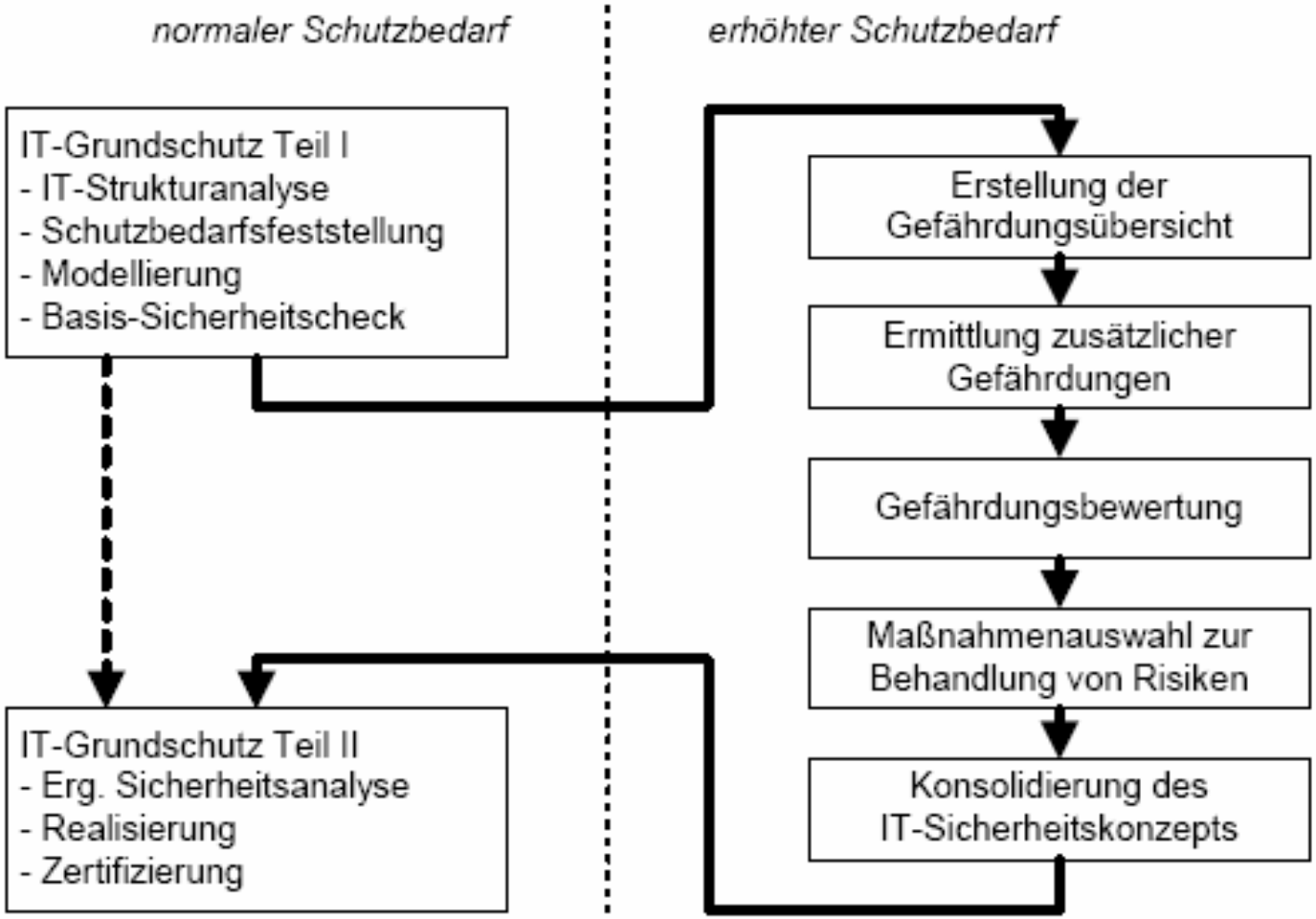
IT-Grundschutzhandbuch





Risikoanalyse auf Basis IT-Grundschutzhandbuch



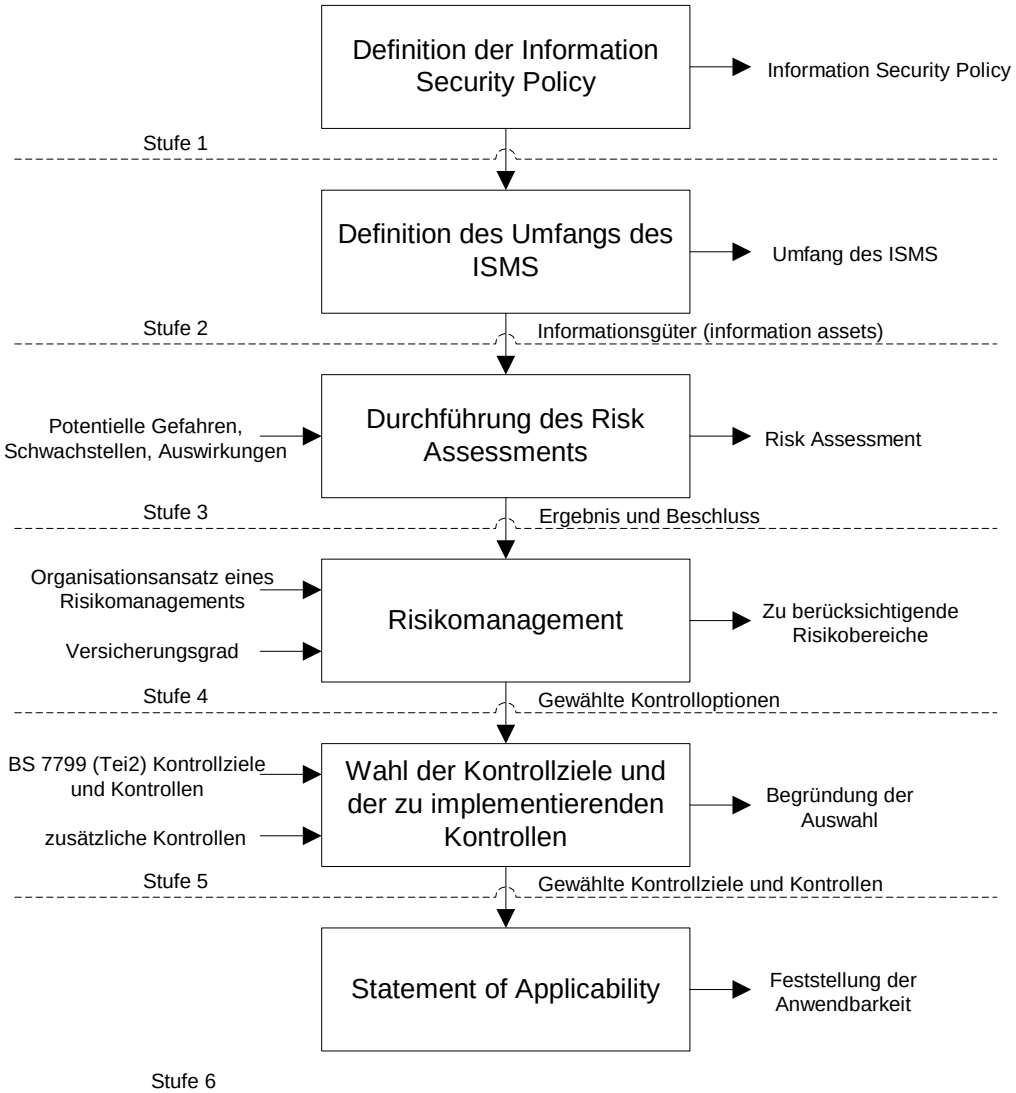


ISO/IEC 17799 (BS 7799)

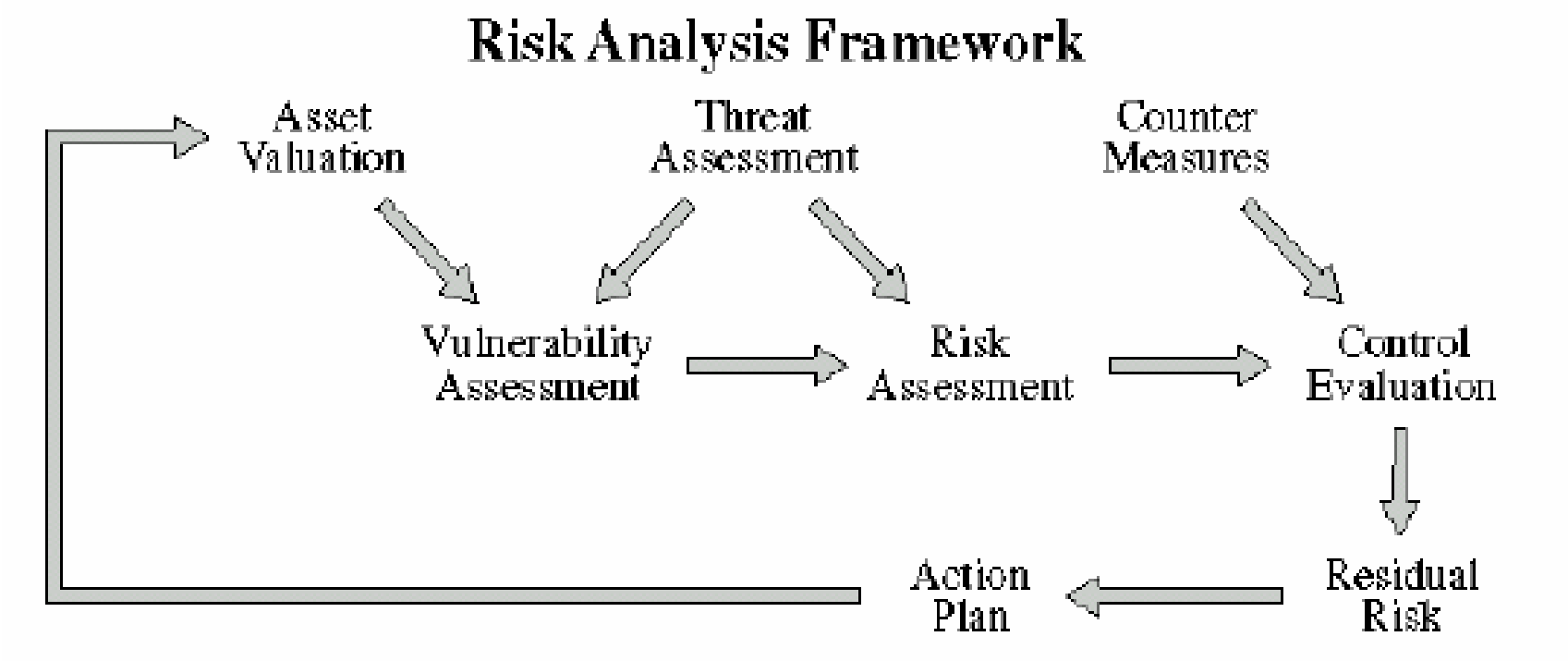
Vorgehensweise gemäß Teil 2 des BS 7799 zur Schaffung eines Managementrahmens für das ISMS:

- Definition der Informationssicherheitspolitik
- Bestimmung des Anwendungsbereichs des Managementsystems
- Durchführung einer angemessenen Risikoanalyse
- Identifizierung der Risikobereiche
- Auswahl der Sicherheitsziele und –maßnahmen
- Erklärung zur Anwendbarkeit der Maßnahmen

Information Security Management nach ISO/IEC 17799



COBIT – Risk Analysis Framework



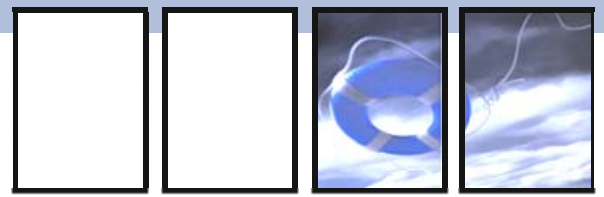
Risikoanalyse

Wertanalyse

Wert jedes einzelnen zu schützenden Objektes wird ermittelt. Folgende Schritte sind notwendig:

1. **Identifikation der zu schützenden Objekte**
2. **Festlegung der Bewertungsbasis für Sachwerte**
3. **Festlegung der Bewertungsbasis für immaterielle Werte**
4. **Ermittlung der Vermögenswerte**

Risikoanalyse



Beispiel: Schutzbedarfskategorisierung für Vertraulichkeit der Datenbestände

Klasse	Beschreibung	Schutzbedarf	Schutzanforderungen	Beispiele
0	Allgemein zugänglich	Keiner	Allgemein zugänglich (keine Maßnahmen)	■ Information die zur Veröffentlichung bestimmt ist ■ Presseartikel ■ Geschäftsberichte ■ Allgemeine Kundeninformationen
1	Zum internen Gebrauch	Normal	Zugang und Leseberechtigung auf Mitarbeiter beschränkt, die diese Informationen im Rahmen ihrer Aufgaben benötigen umfassende Analyse der Kundenbeziehungen oder Geschäftsaktivitäten ist nicht möglich	■ Einzeltransaktionen ■ Arbeitsanweisungen ■ Handbücher ■ Marktinformationen
2	Vertraulich	Erhöht	Zugang und Leseberechtigung auf vom Dateneigentümer benannte Mitarbeiter beschränkt Kundenbeziehungen oder Geschäftsaktivitäten können nicht durch Dritte beeinflusst werden	■ Kontoauszüge ■ Kundenstammdaten ■ Kreditakten ■ Rechnungswesen ■ Planungs- und Budgetdaten ■ Quartalsberichte

Risikoanalyse

Schutzbedarfskategorien

Kategorie 1 (niedrig-mittel)	Kategorie 2 (hoch)	Kategorie 3 (sehr hoch)
Grundschutz-betrachtungen	Grundschutz-betrachtungen	Grundschutz-betrachtungen
	Risikoanalyse	Risikoanalyse
		Individuelle Risikobetrachtung

Risikoanalyse

Bedrohungsanalyse

Die Gefährdungsbereiche sowie die potentiellen organisatorischen, technischen und benutzerbedingten Ursachen für Bedrohungen werden systematisch ermittelt. Folgende Schritte sind notwendig:

1. **Identifikation möglicher Bedrohungen / Gefährdungsbereiche**
2. **Identifikation möglicher Angreifer / Auslöser**
3. **Ermittlung der potentiellen Schadenshöhe**
4. **Ermittlung der Eintrittswahrscheinlichkeiten**

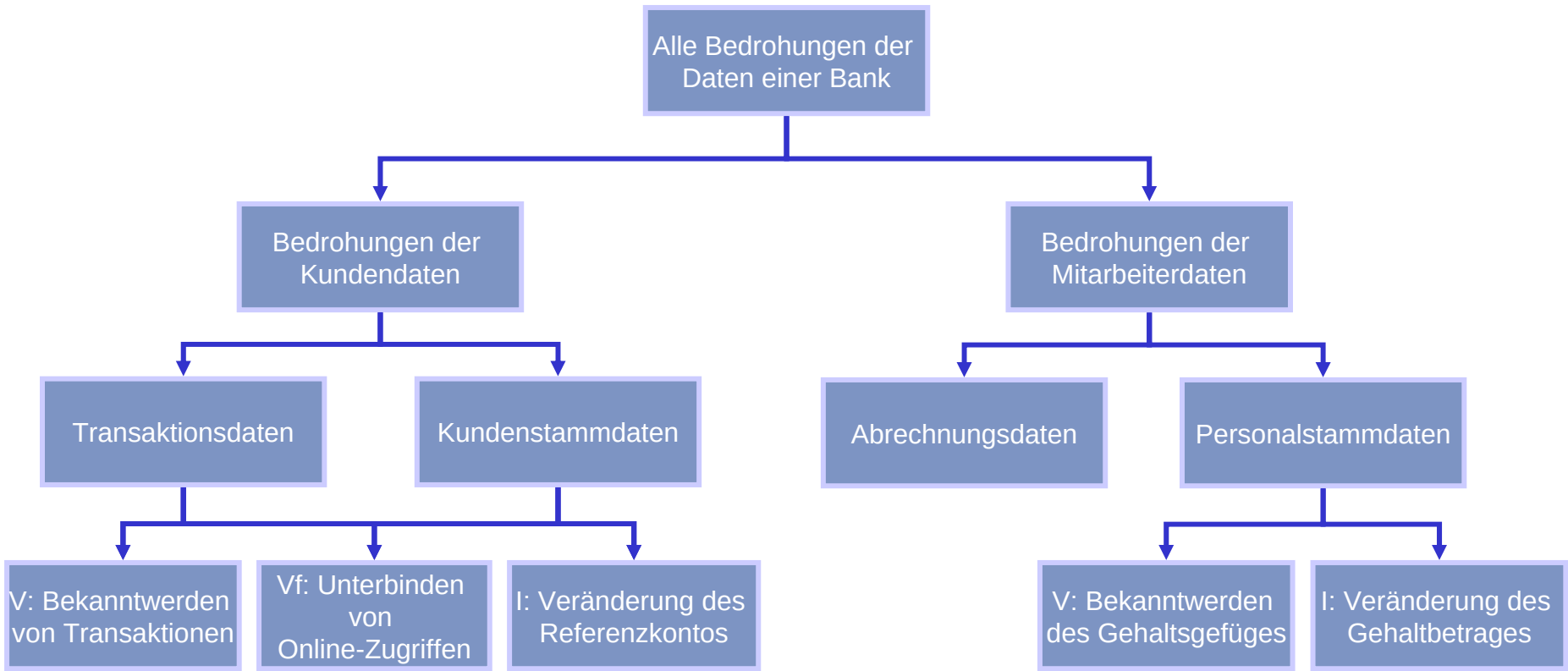
Risikoanalyse

Beispiel: Matrix für die Bedrohungsanalyse in der Softwareentwicklung

Auslöser / Bedrohung	Program-mierer	Interner Benutzer	Externer Benutzer	Mobiler Code	...
Externe Angriffe	Vandalismus	Erspähung von Passwörtern	Anschlag	–	
Integrität / Vertraulichkeit	Direkter Speicherzugriff	Logische Bomben	Passwortkom-promittierung	Viren	
Verfügbarkeit	Speicher belegen	Prozesse erzeugen	Netzlast erzeugen	Monopolisiere n der CPU	
Abstreiten	Abrechnungs-betrug	Abrechnungs-betrug	Abrechnungs-betrug	–	
Rechte-missbrauch	Programm-manipulation	Daten-manipulation	Daten-manipulation	Daten-manipulation	

Risikoanalyse

Beispiel: Bedrohungsbaum für Daten (Finanzinstitut)



Risikoanalyse

Beispiel: Schwachstellenanalyse (High-Level-Ebene)

- Ausfall wichtiger Systeme und ganzer Prozeßketten
- Hohe Abhängigkeit von Spezialisten oder Dritten
- Verlust oder Beschädigung sensitiver Daten

- Unzuzreichendes Projekt-Management
- Neue, unbekannte Technologien/Prozesse
- Fehlende Software-Konzepte/Pflichtenhefte

- Unangemessene IT-Organisation
- Keine IT-Steuerung & Controlling

- Know-how veraltet/lückenhaft
- Arbeitsbelastung
- Fehlbedienung

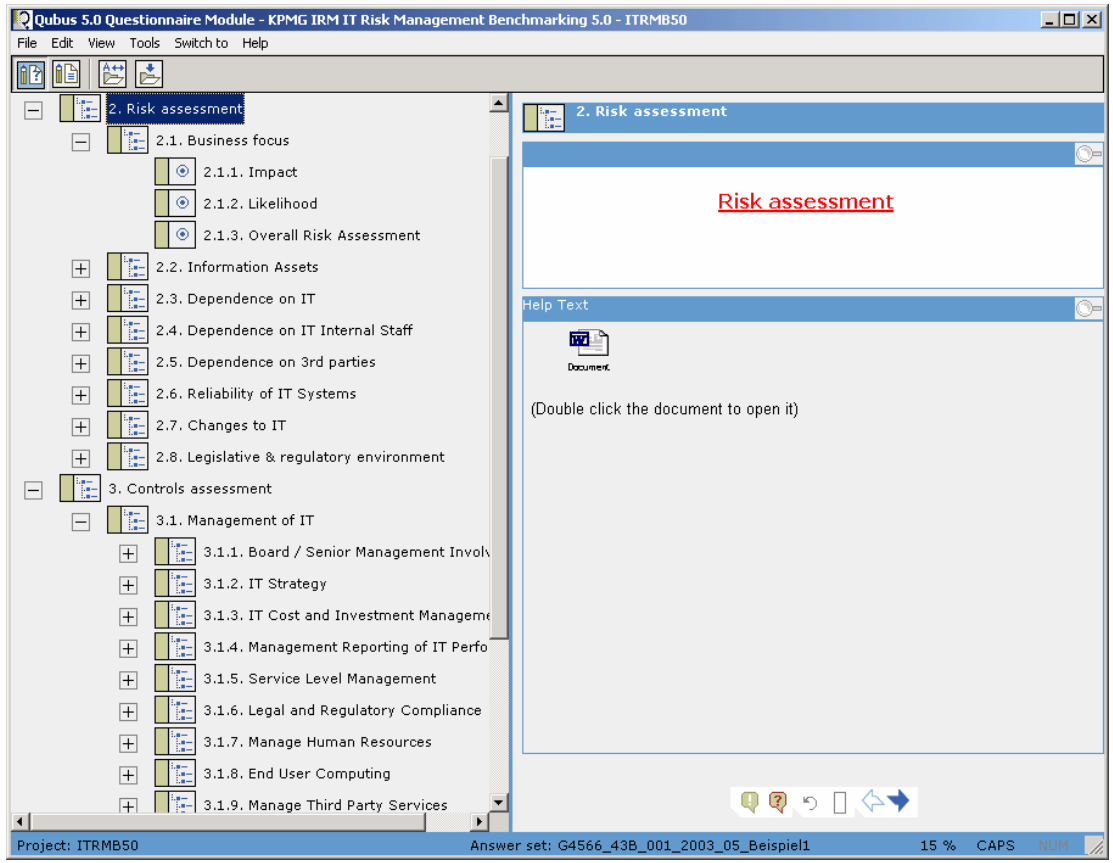
- Ineffizientes Trouble-Shooting ⇒ Qualität der Prozesse
- Unzureichender Schutz der Prozesse bzw. Daten
- Insellösungen / Überalterung
- Infrastruktur / techn. Ressourcen unzureichend

- fehlende IT-Strategie
- Unzureichende geschäft-liche Anforderungen
- Nicht-Berücksichtigung rechtlicher Rahmen-bedingungen

Tools für die Risikoanalyse

Unterstützung
der Risikoanalyse
und –bewertung
durch geeignete
Software-Tools

Bei KPMG IRM:
ITRMB
**(IT-Risk
Management
Benchmarking)**



Kontakt und Information

Diplom-Betriebswirt (BA)
Markus Gaulke
CISA, CISM
Senior Manager –Information Risk Management

Marie-Curie-Strasse 30
D-60439 Frankfurt/Main
MGaulke@kpmg.com

Tel. +49 (69) 95 87-2313
Fax +49 (69) 95 87-19 2313
Mobile +49 (172) 6767383

KPMG Deutsche Treuhand Gesellschaft Aktiengesellschaft
Wirtschaftsprüfungsgesellschaft – Member of KPMG International

Markus Gaulke: „Risikomanagement in IT-Projekten – IT-Governance für Projekte umsetzen“

Oldenbourg-Verlag, München, 2004

www.risikomanagement-in-IT-Projekten.de