

31. Risiko-Management

Prof. Dr. rer. nat. Uwe Aßmann
Lehrstuhl Softwaretechnologie
Fakultät Informatik
Technische Universität Dresden
[http://st.inf.tu-
dresden.de/teaching/swm](http://st.inf.tu-dresden.de/teaching/swm)
2016-0.3, 13/06/16

- 1) Grundlagen
- 2) Risikomanagement-Prozess
- 3) Risiko-Handhabung
 - 1) Primäre Maßnahmen, hier IT-Sicherheitskonzept
 - 2) Sekundäre Maßnahmen, Risikoversicherung
- 4) Krisenmanagement bei Entwicklungsrisiken



- ▶ Dieter Köhnlein, Thomas Willert, Thomas Rauschen. Aktuarielle Software für Risikomanagement und Unternehmenssteuerung. Versicherungswirtschaft Heft 20/2006.
 - http://www.risknet.de/typo3conf/ext/bx_elibrary/elibrarydownload.php?&downloaddata=3
- ▶ Werner Gleißner, Frank Romeike. Anforderungen an die Softwareunterstützung für das Risikomanagement. ZfCM – Zeitschrift für Controlling & Management, Gabler Verlag / GWV Fachverlage, Wiesbaden
 - http://www.risknet.de/typo3conf/ext/bx_elibrary/elibrarydownload.php?&downloaddata=190

Referenzierte Literatur

- ▶ Balzert, H. : Lehrbuch der SW-Technik; Bd 2 Spektrum- Verlag 2001
- ▶ Wallmüller, E.: Risikomanagement für IT- und Software-Projekte; Hanser Verlag 2004
- ▶ <http://www.bsi.bund.de/>
- ▶ <http://www.risknet.de>
- ▶ <http://www.ecc-handel.de>
- ▶ <http://www.ec-net.de> Netzwerk elektronischer Geschäftsverkehr
- ▶ <http://www.internet-sicherheit.de/>
- ▶ <http://www.sageg.de/> Kompetenzzentrum für Sicherheit im elektronischen Geschäftsverkehr in Chemnitz



31.1 Grundlagen



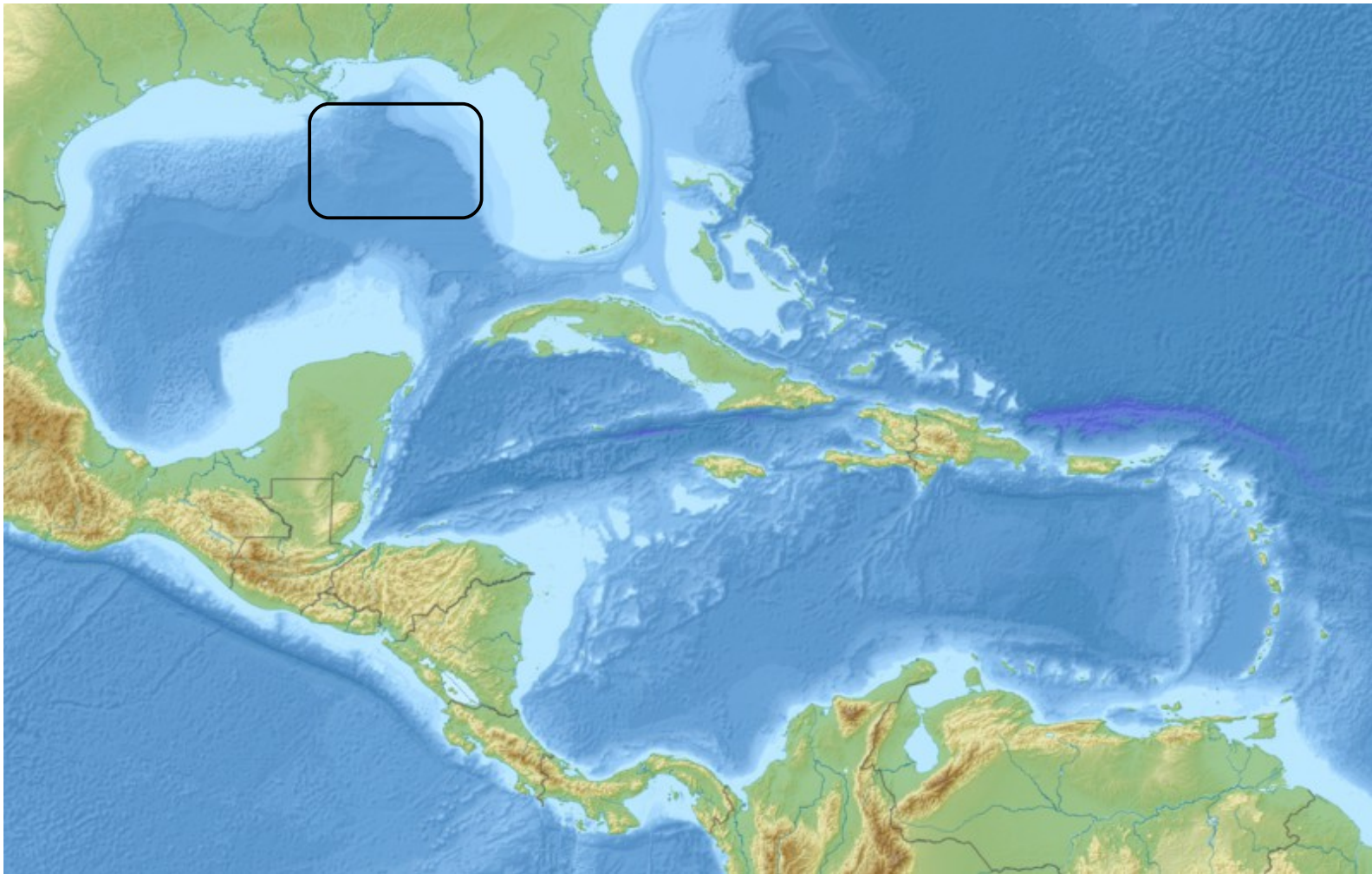
Misserfolge internationaler Großprojekte

Projekt	Verspätung	Verlust
Deutsches Mautsystem „Toll Collect“	2 Jahre	rd. € 2,2 Milliarden
„YOU“-Projekt von Bank Vontobel	Abbruch nach 2 Jahren	CHF 256 Millionen
California PKW-Zulassung	3 Jahre	\$ 54 Millionen
American Airlines Autovermietung	7 Jahre	\$ 165 Millionen
Denver Flughafen Gepäckverteilung	2 Jahre	\$ 750 Millionen
US Bundesfinanzamt Steuer	8 Jahre	\$ 1600 Millionen
London, Elektronische Börse	12 Jahre	£ 800 Millionen
London, Krankenwagenleitsystem	5 Jahre	£ 12 Millionen und der
		Verlust von 46 Leben

Quelle: [Wallmüller, E.]

Tiber-Ölfeld

- ▶ 5-6 Mrd Barrel (riesig) (Nordsee: 2,1 Mrd Barrel)



Deepwater Horizon

- ▶ 2.9.2009, Tiber-Ölfeld vor dem Mississippi-Delta: Meerestiefe 1250m, Tiefe 10685m
 - Oft Gaseinbrüche während der Bohrungen
 - BP-Manager bestanden darauf, einen zweiten Zement-Verschlussstopfens gegen Wasser zu tauschen (Kosten)
- ▶ 20.4.2010: Explosion beim Zementieren des Bohrloches, kurz vor Verschuß
 - Während einer Party für das 7jährige sichere Betreiben
 - Methangasexplosion aus eisförmigem Methanhydrat stammend, das im Ölfeld und auf dem Meeresgrund vorhanden ist
 - Angeblich 40% des Öls waren Methan (normal: 5%)
- ▶ Der Blow-out Preventer (BOP) versagte (7 min nach Explosion)
 - Dichtgummi beschädigt, leere Batterien
 - Kontrollsystem außer Kraft gesetzt
- ▶ kein Verschußsystem vorhanden

Menschliches Versagen



Fukushima Nuclear Disaster



Fehler: Wälle waren nur 7m hoch, Tsunami 13m



http://en.wikipedia.org/wiki/2011_T%C5%8Dhoku_earthquake_and_tsunami

http://en.wikipedia.org/wiki/Fukushima_Daiichi_nuclear_disaster

Die Grenze des Menschen

- ▶ Atomenergie ist billig, solange man die Unfälle und die Abfälle nicht betrachtet
 - Unfall Fukushima wegen verkehrter Einschätzung der Natur
 - Unfall Tschernobyl wegen Leichtsinns
 - Müll: Mehrere 1000 Jahre Halbwertszeit
 - Wie den Müll lagern und sichern?
- ▶ Schadenshöhe:
 - Tschernobyl: ?? etliche Tote bei der Rettung
 - 1 Mrd. \$ bei Kernschmelze in Harrisburg Three Mile Island, 1979, keine Tote
 - Fukushima sicher mehr als 25 Mrd, keine Tote
- ▶ Eintrittswahrscheinlichkeit:
 - Deutschland kehrt sich von der Kernenergie ab, weil die Eintrittswahrscheinlichkeit für Unfälle verkehrt eingeschätzt wurde (Kanzlerin Merkel, März 2011)

- ▶ Software Engineering Code of Ethics and Professional Practice (Version 5.2)
- ▶ <http://www.acm.org/about/se-code>
- ▶ Principle 1: **PUBLIC**
- ▶ Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:
 - ▶ 1.01. Accept full responsibility for their own work.
 - ▶ 1.02. Moderate the interests of the software engineer, the employer, the client and the users with the public good.
 - ▶ 1.03. Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and **does not diminish quality of life, diminish privacy or harm the environment**. The ultimate effect of the work should be to the public good.
 - ▶ 1.04. **Disclose** to appropriate persons or authorities **any actual or potential danger** to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.
 - ▶ 1.05. Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.

- ▶ Principle 3: **PRODUCT**
- ▶ Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. In particular, software engineers shall, as appropriate:
 - ▶ 3.02. **Ensure** proper and **achievable goals** and objectives for any project on which they work or propose.
 - ▶ 3.03. **Identify**, define and address ethical, economic, cultural, legal and **environmental issues** related to work projects.
 - ▶ 3.04. Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.
 - ▶ 3.05. Ensure **an appropriate method is used** for any project on which they work or propose to work.
 - ▶ 3.06. **Work to follow professional standards**, when available, that are most appropriate for the task at hand, departing from these only when ethically or technically justified.

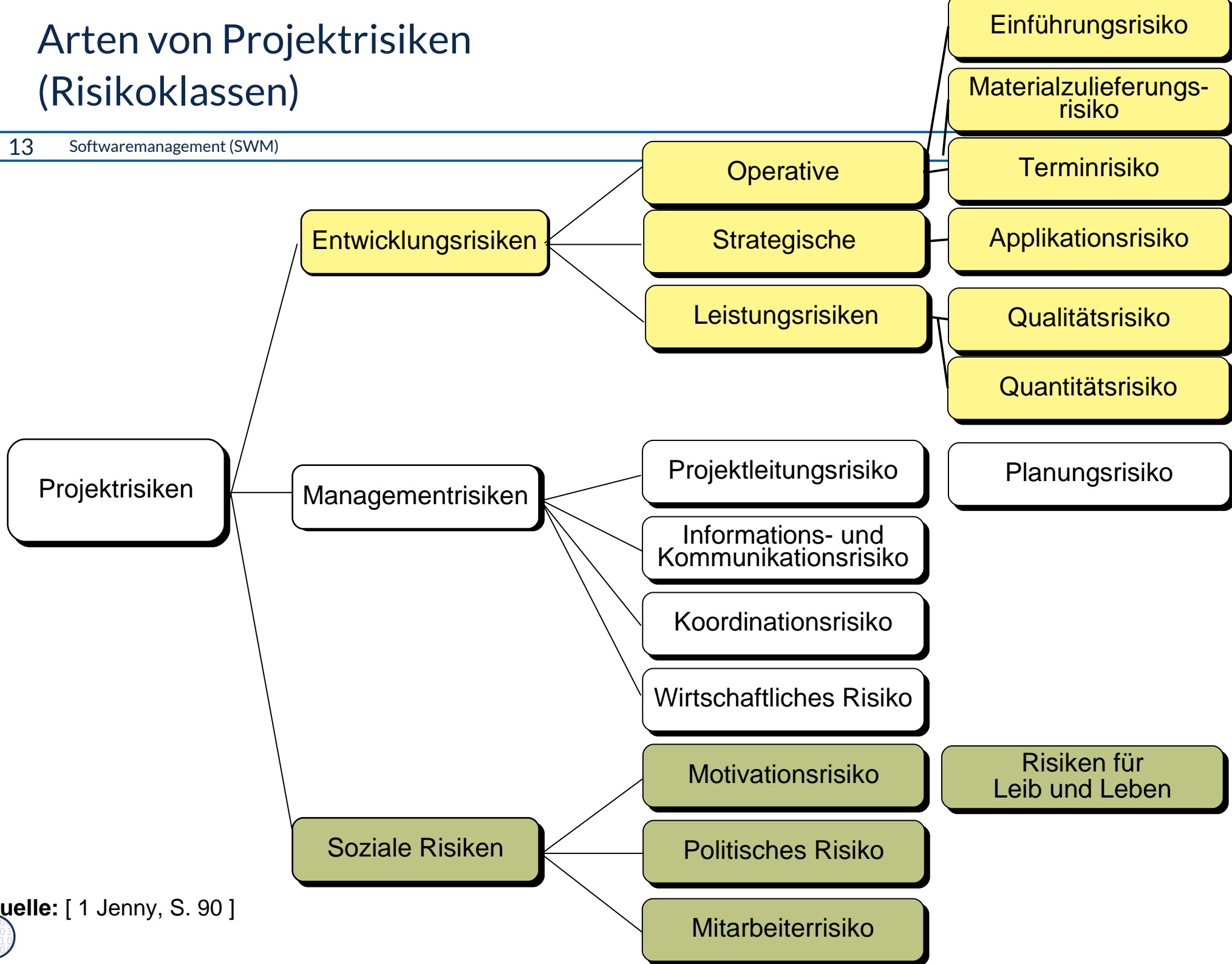
Unter dem **Projektrisiko** wird die Höhe des Schadens verstanden, den ein Unternehmen erleidet, wenn die **Projektziele nicht erreicht** werden.

Das **Gesamtrisiko** lässt sich in Teilrisiken zerlegen. **Risikoklassen:**

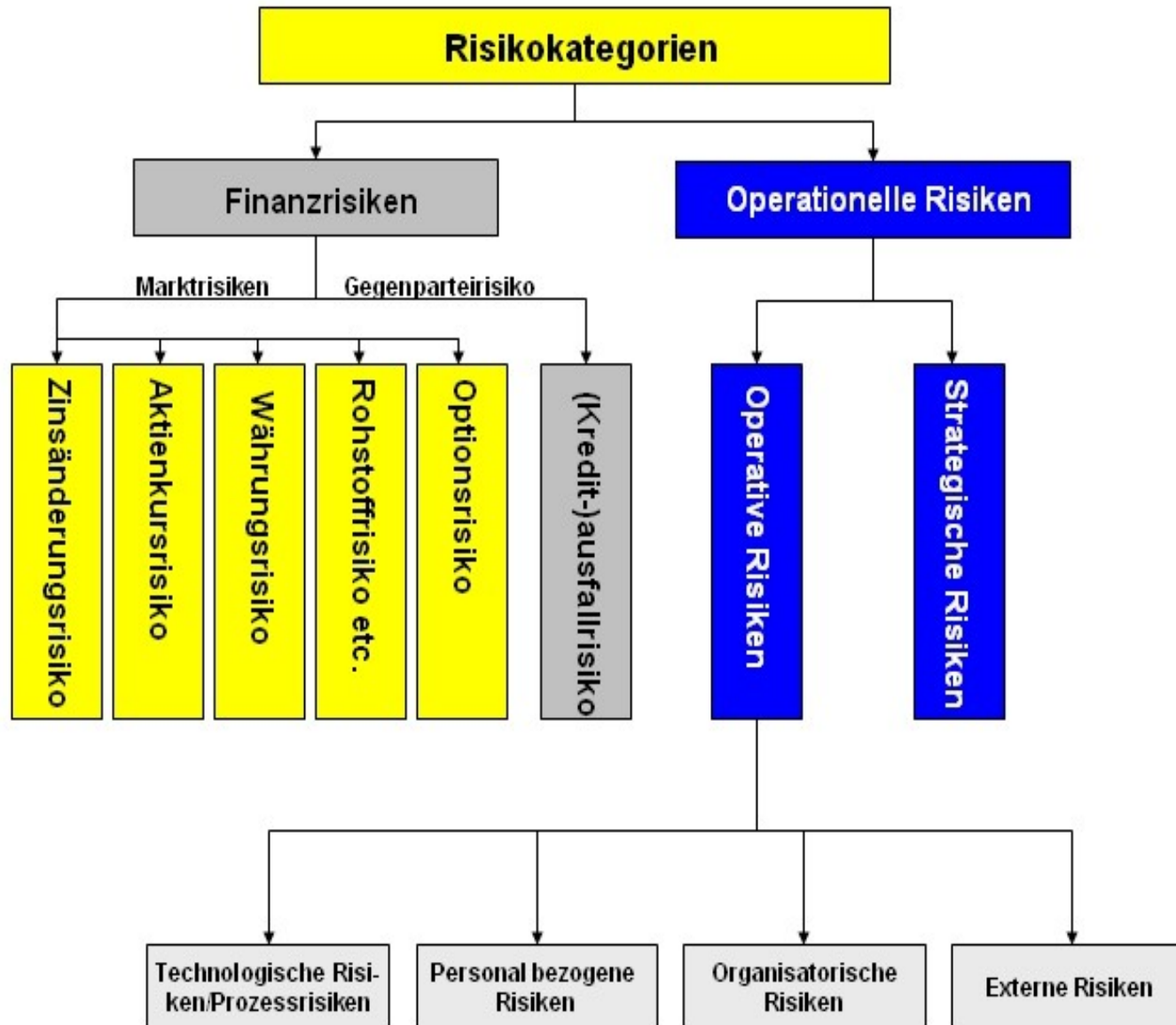
- **Entwicklungsrisiken:**
 - Operationelle Risiken
 - Operative Risiken
 - Es werden zusätzliche Ressourcen benötigt,
 - Termine (Zeitplanung) nicht einzuhalten (Zeitrisko!),
 - Strategische Risiken
 - Leistungsrisiken:
 - Qualitätsrisiken: Das Produkt weist Mängel auf
 - Quantitätsrisiken
- **Managementrisiken:**
 - Finanzrisiken/Wirtschaftlichkeitsrisiken: Die Wirtschaftlichkeit erweist sich niedriger als erwartet (Nutzen zu gering, Kosten höher),
- **Soziale Risiken (Stakeholder-Risiken):**
 - Kundenunzufriedenheit: Der Auftraggeber oder der Kunde ist nicht zufrieden,
 - Die Motivation der Mitarbeiter sinkt.

Quelle: [1 Jenny, S. 88ff]

Arten von Projektrisiken (Risikoklassen)



Verfeinerung von Risikoklassen



Def.: Ziel des **Risikomanagements** ist es, die Wechselbeziehungen zwischen Risiken und Erfolg zu formalisieren und in anwendbare Prinzipien und Praktiken umzusetzen.

Aufgabe des Risikomanagements ist es demzufolge

- Risiken zu identifizieren,
- sie zu analysieren,
- sie zu bewerten,
- sie anzusprechen,
- ihre Handhabung zu planen,
- sie zu beseitigen, bevor sie zur Gefahr oder zur Hauptquelle für Überarbeitung werden
- etwaige Schäden zu begrenzen oder beseitigen (Krisenmanagement).

Ein Risiko beschreibt die Möglichkeit, dass eine Aktivität oder ein Objekt einen Schaden haben könnte, dessen Folgen ungewiss sind.

Quelle: [Balzert, S. 176 – 185]

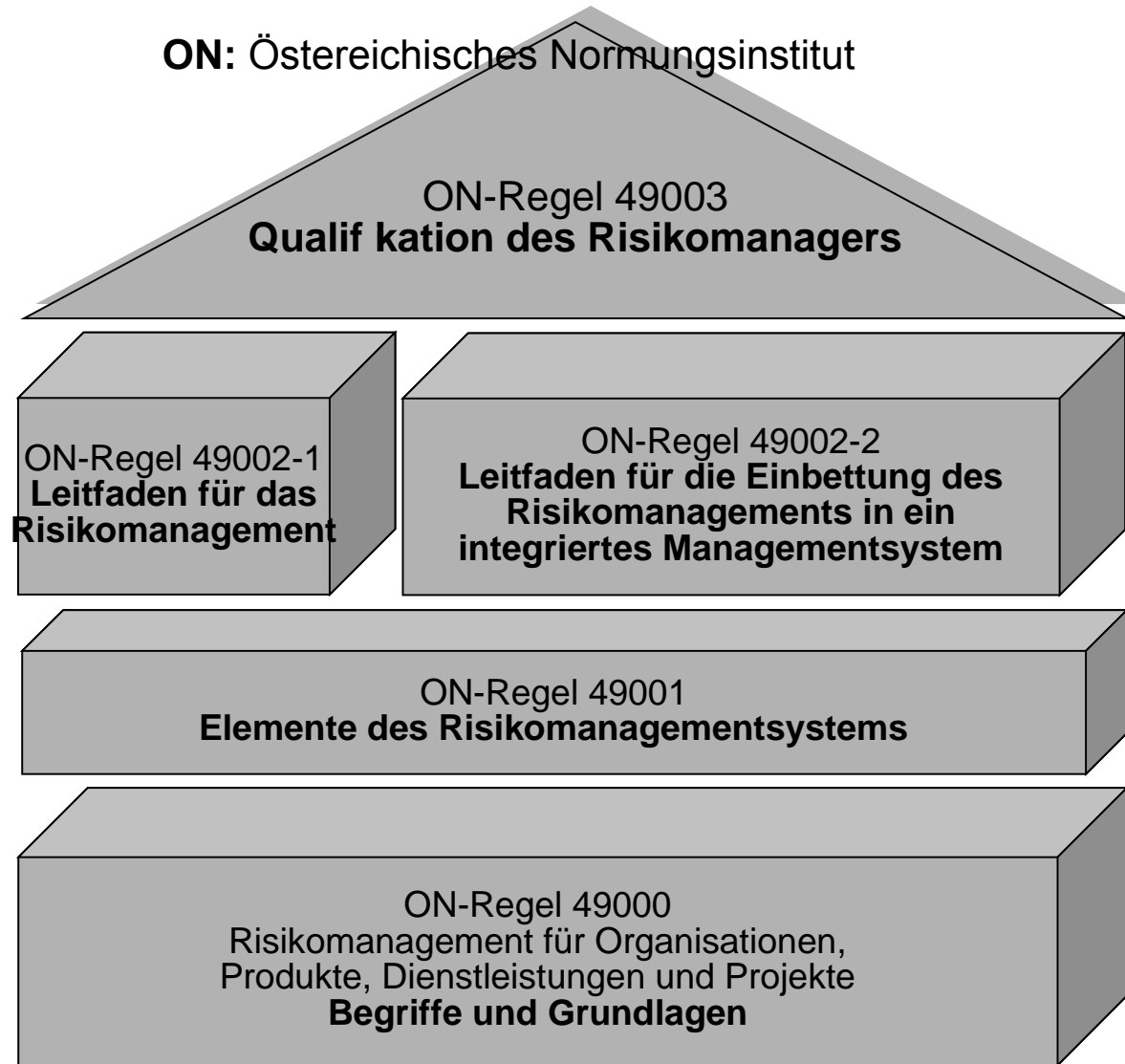
Probleme des Risiko-Managements

- ▶ Probleme:
 - Risikoverbergung: Risiken werden unter den Teppich gekehrt
 - Informalität: Risikomanagement basiert häufig auf der Intuition der Betroffenen
 - Konzepte der Geschäftsführung sind selten mit gezieltem Risikomanagement auf der operativen Ebene in Projekten oder Organisationen verbunden.
 - Unpopularität: Der Überbringer schlechter Nachrichten wird zwar nicht mehr, wie im alten Griechenland, umgebracht, aber immer noch nicht ernst genommen.
- ▶ Notwendig: Schaffung eines effizienten internen Kontrollsystems einschließlich notwendiger Optimierungen
 - Risikobewusstsein und Risikotransparenz verbessern
- ▶ Risikomanagement setzt in der Praxis meist erst ein, wenn Risiken aufgrund verursachter Schäden augenfällig werden, d.h. materialisiert sind.
 - Wir sprechen im Falle der eigentlichen Intervention (Schadenbegrenzung, Schaden behebung) von Problem- bzw. Krisenmanagement

Ziele des Risiko-Managements

- ▶ Analyse
 - Risiken sichtbar machen: systematisch Risikoursachen identifizieren;
 - Potenzielle Gefährdungssituationen möglichst frühzeitig erkennen und erfassen;
- ▶ Bewertung
 - wo Risiken sind, sind auch Chancen;
 - Risiken einschätzen und bewerten, um geeignetes Umgehen mit Risiken festzulegen
- ▶ Behandlung bzw. Risikoreduktion
 - Risiken kommunizieren und allen Beteiligten bewusst machen;
 - Risikobehandlung durchführen
- ▶ Kontrolle
 - Risiken in ihrer Entwicklung verfolgen;
 - Risiken eingrenzen und als bewusste Steuerungsgröße des Managements verwenden;
 - Hilfsmittel zur Erkennung, Bewertung und Steuerung der Risiken bereitstellen und nutzen.

Bsp.: ON-Normenwerk des Risiko-Managements

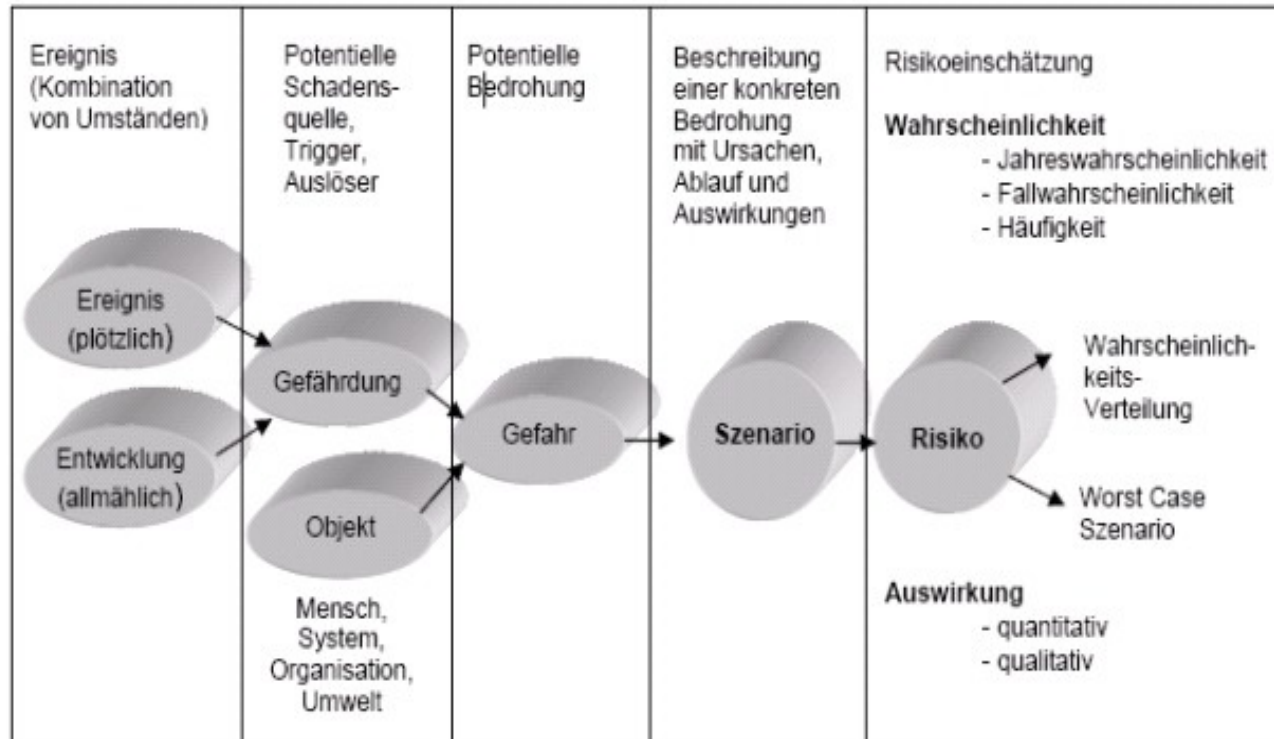


Quelle: [Wallmüller, E. S.9]

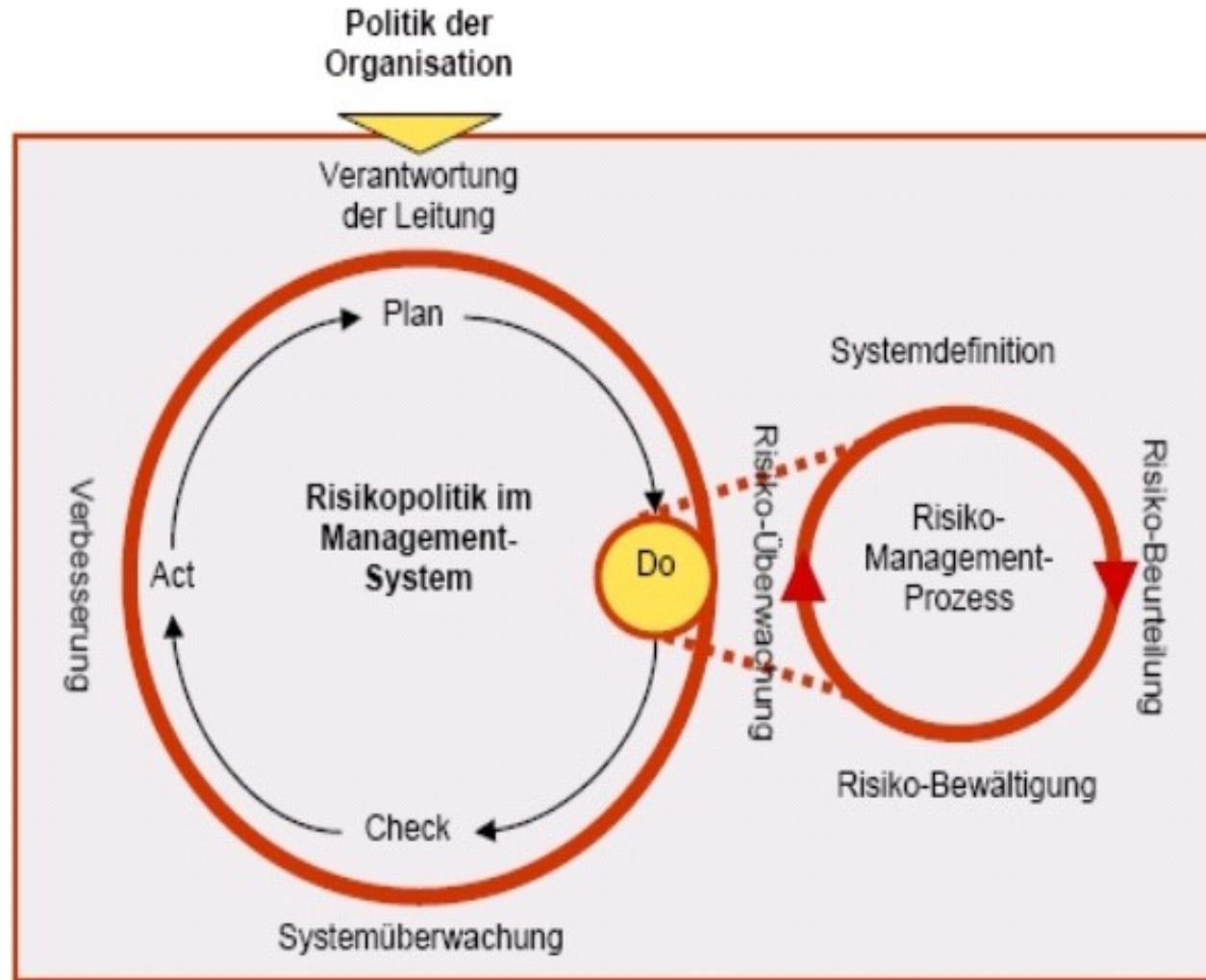
<http://www.risknet.de/wissen/grundlagen/risk-management-standards/on-regelwerk-risikomanagement-des-oesterreichischen-normungsinstituts/>

Kriterium	Risikoportfolio, Risikolandschaft	FMEA	Fehlerbaum- Analyse	Auswirkungs- Analyse	HAZOP	HACCP
Ansatz, Prinzip	Gesamtsicht der Risiken einer Organisation oder eines Systems (Top-down-Ansatz)	Fehlfunktionen eines technischen Systems oder Prozesses	Top Event wird auf Ursachen und Vorereignisse untersucht	Top Event wird auf Folgeereignisse bis zu den Endzuständen untersucht	Fehlfunktionen eines technischen Systems oder Prozesses	Kritische Punkte des Prozesses werden ermittelt und überwacht
Anwendung	Organisationen und Systeme	Automobilindustrie, komplexe technische Systeme	Störfallanalyse, komplexe technische Systeme	Störfallanalyse, komplexe technische Systeme	Chemie, Petrochemie Pharma, Nuklearanlagen	Nahrungsmittel- und Getränkeindustrie
Bedeutung des Risikobegriffes	Schadensereignis, Fehlentwicklung	Fehlfunktion	Schadensereignis	Schadensereignis	Fehlfunktion	Toleranzwert überschritten
Definition	$R = f(W; A)$ $R = W \cdot A$	$RPZ = A \cdot B \cdot E$	Wahrscheinlichkeit	Wahrscheinlichkeit	Leitwörter	Kontrollpunkte

http://www.risknet.de/fileadmin/template_risknet/images_content/RM-Standards/online-regel-05.jpg



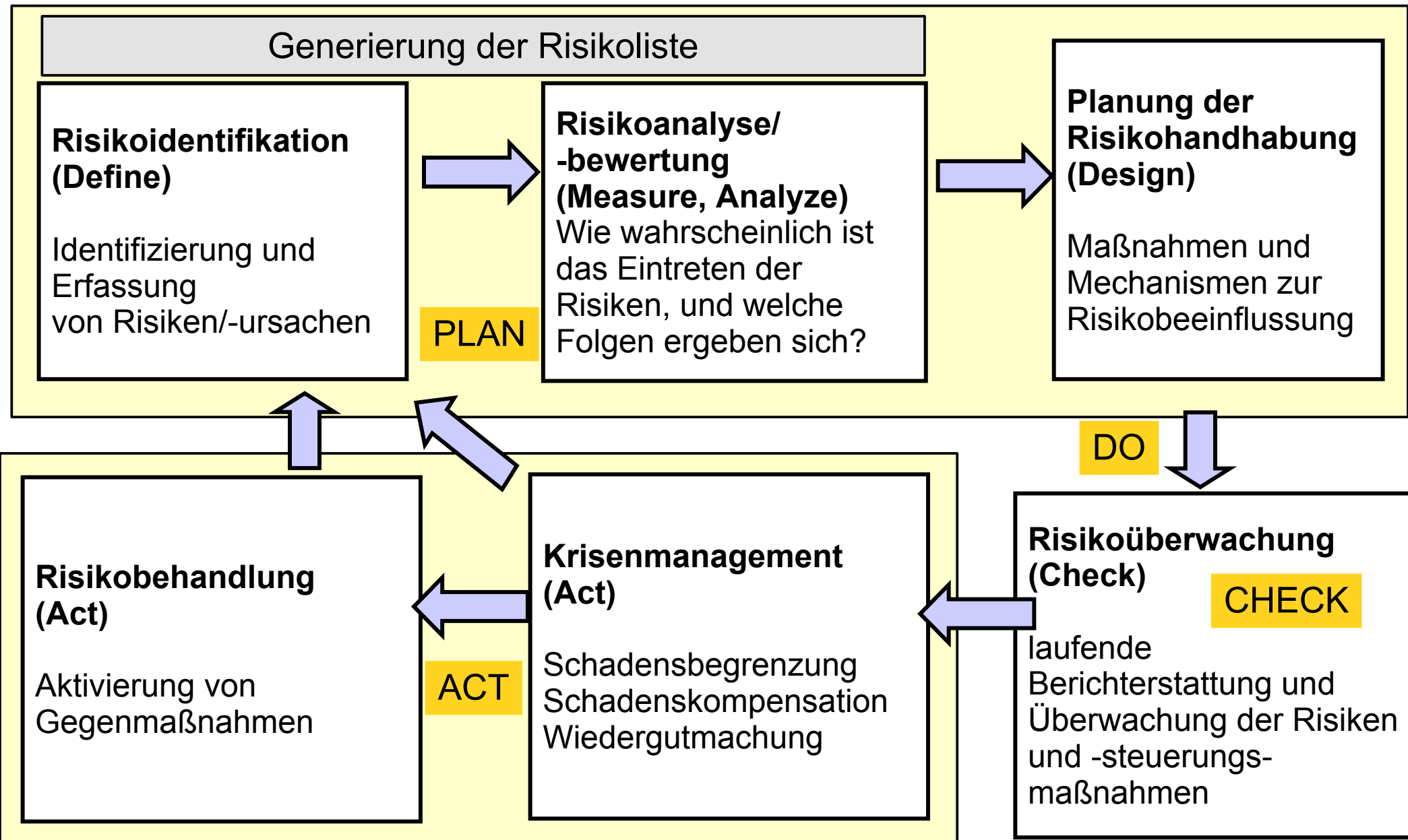
http://www.risknet.de/fileadmin/template_risknet/images_content/RM-Standards/on-regel-03.jpg



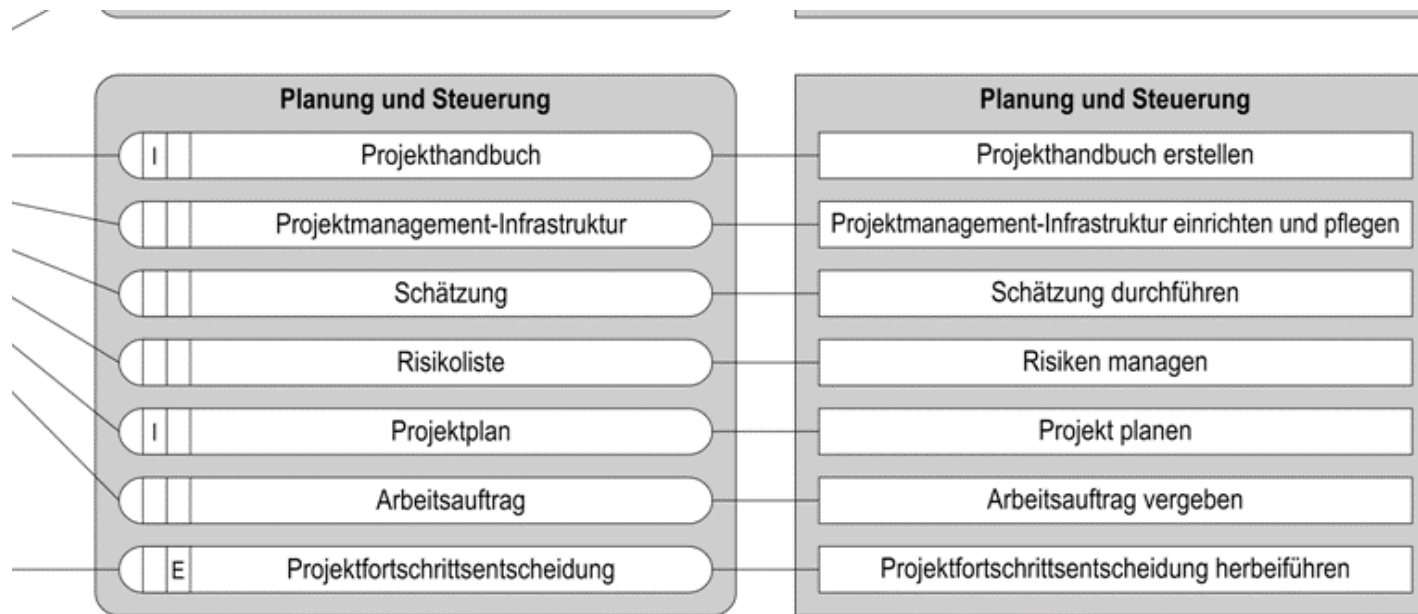
31.2 Risikomanagement-Prozess



Unternehmensweiter RM-Prozess als PDCA



Vorgehensbaustein Projektmanagement



Aktivität **Risiken managen**

vorbeugend, in periodisch kurzen Schritten

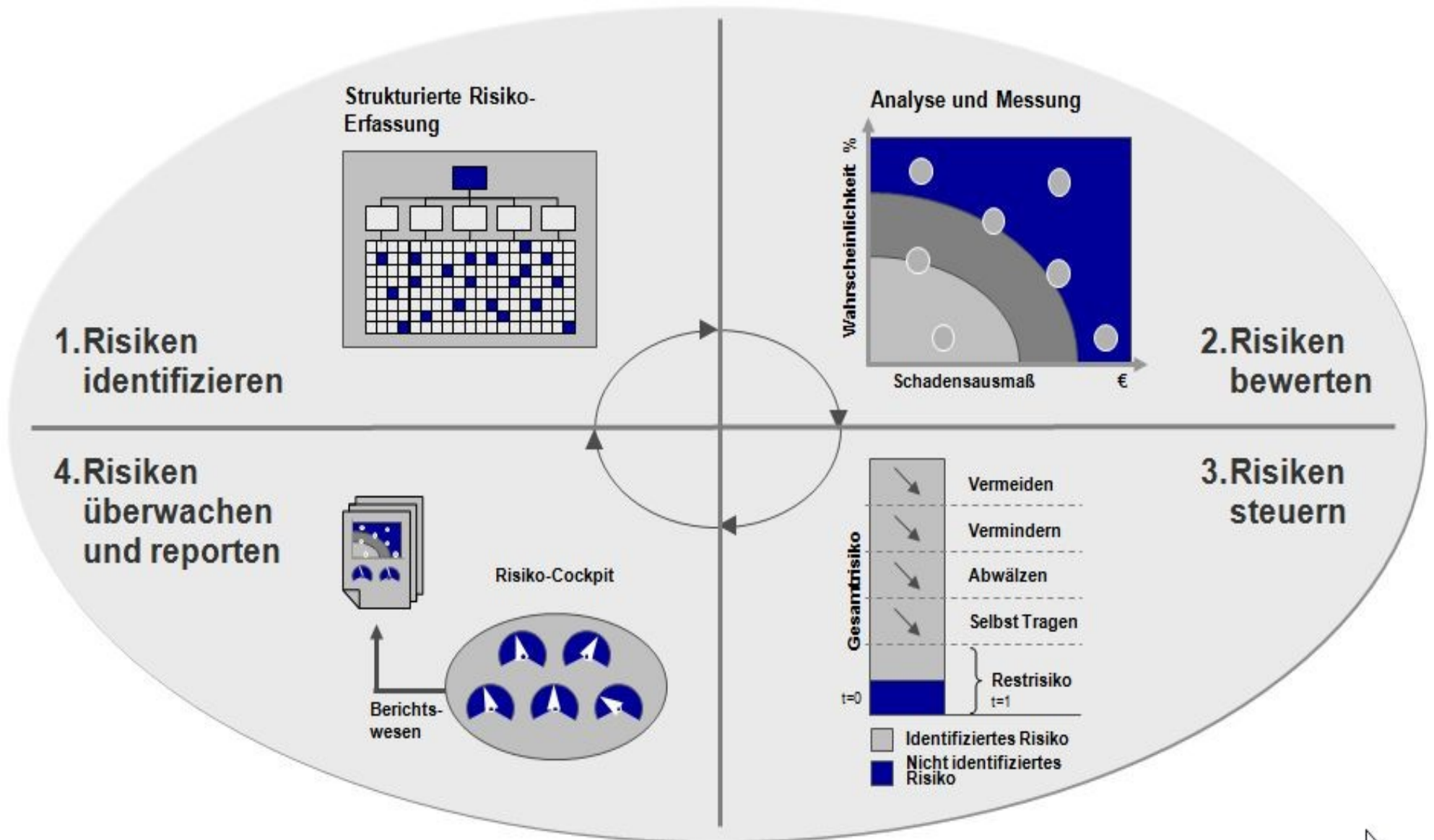
- Risiken identifizieren, bewerten, Maßnahmen planen,
- Risiken überwachen und Wirksamkeit der Maßnahmen verfolgen.

Produkt **Risikoliste**

Es werden

- die identifizierten Risiken ermittelt
- sie werden fortgeschrieben und verwaltet
- die geplanten Gegenmaßn. festgehalten.

Quelle: V-Modell XT Dokumentation; URL: <http://ftp.uni-kl.de/pub/v-model-xt/Release-1.1/Dokumentation/html/>



31.2.1) Risikoidentifikation

Mögliche Techniken und Vorgehensweisen der Risikoidentifikation sind:

▶ Informell

- Szenariotechnik (Use Case, CRC-Karten)
- Brainstorming
- Strukturierte Interviews/Umfragen
- Workshops (Reviews)
- Checklisten
- Fragebögen

▶ Formell

- Fehlerbaumanalyse (fault trees)
- Auswertung Planungs- und Controlling-Unterlagen
- Analyse von Prozessabläufen mit Flussdiagrammen, Sequenzdiagrammen u. ä.
- Fehlermöglichkeits- und Einflussanalyse (FMEA)
- Benchmarking

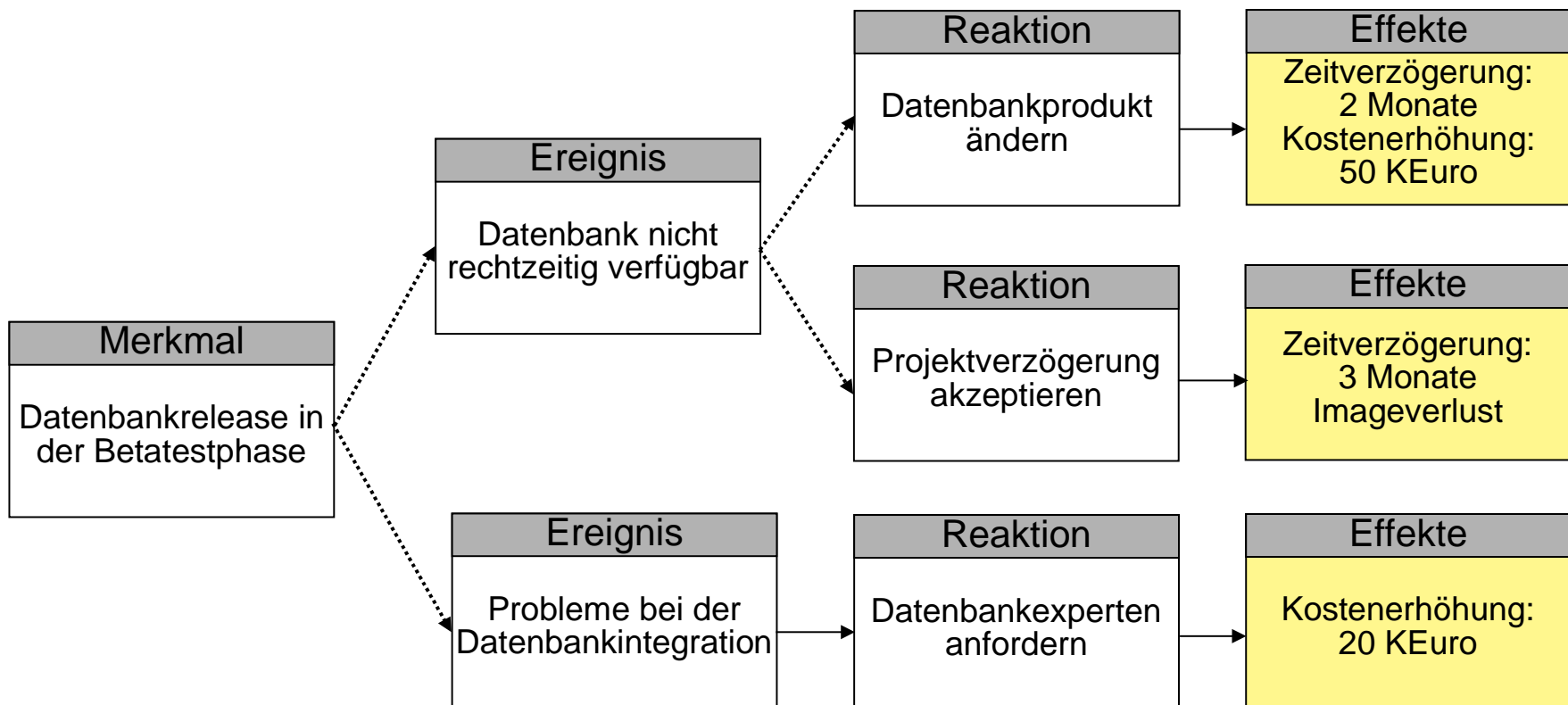


- ▶ **Risikodokumentation mit Risikolisten, -katalogen oder -datenbanken:**
 - Kurzbeschreibung
 - Risikomerkmale
 - mögliche technische Ausprägungen
 - Alternativen
 - zeitliche Lage des Risikos im Projekt

- ▶ **Zusätzlich: Risiko-Szenario mit Ursache-Wirkungs-Graph:**
 - Randbedingungen, die zum Eintreten des Risikos führen können
 - Auswirkungen auf andere Bereiche des Projektes
 - terminliche Auswirkungen

Ein Risikoszenario stellt einen ereignisbasierten Ursache-Wirkungsgraph auf:

- ▶ **Risikomerkmale:** Merkmal mit Wahrscheinlichkeit für negatives Eintreten des Ereignisses
- ▶ **Risikoereignis** repräsentiert das Eintreten des negativen Vorfalls
- ▶ **Risikoreaktion:** Aktion, die bei Eintreten des Ereignisses ausgeführt wird
- ▶ **Risikoeffekt** beschreibt Auswirkungen des Risikoereignisses



Quelle: [Wallmüller, E. S. 9]

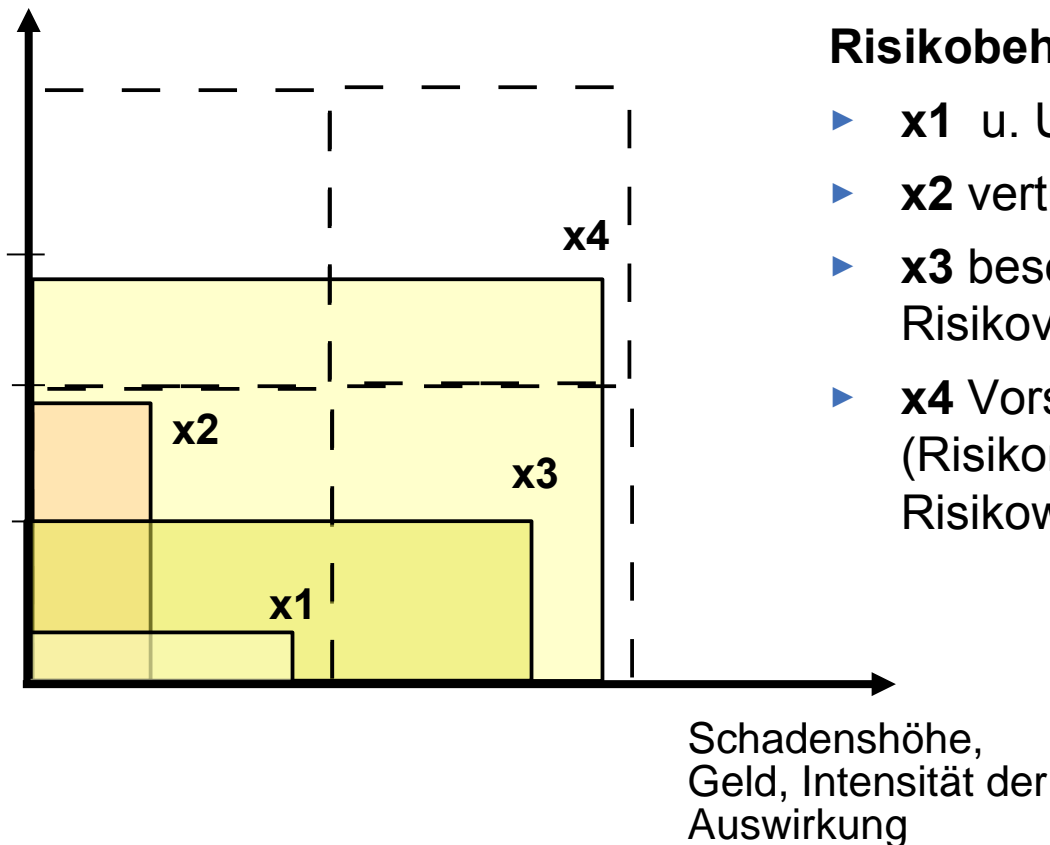
31.2.2) Risikoanalyse/-bewertung

- ▶ Ziel: Priorisierung der Risikoliste
- ▶ Expertenbefragung: Risikodefinition + Risikodiskussion + Risikobewertung (Zeit, Kosten)
- ▶ **Eintrittswahrscheinlichkeit** in % gibt an, wie wahrscheinlich ein Risikofall eintritt
- ▶ Die **Schadenshöhe** ist Bewertung in Geld: (welchen Schaden wird das Risiko verursachen?)
- ▶ **Risikopriorität** ergibt sich aus **Risikofaktor** = Eintrittswkt. x Schadenshöhe
- ▶ **Risikoreduktionskosten** bilden die Kosten der Risikobehandlung
- ▶ **Risikoreduktionsnutzen** beurteilt, ob Risikobehandlung sich lohnt

Risikoselektion mit Portfolio-Analyse

- ▶ Risikoselektion erfolgt mit Hilfe einem Portfolio aus Eintrittswahrscheinlichkeit und Schadenshöhe
- ▶ Der **Risikofaktor** ist die Fläche zwischen dem Ursprung und dem Punkt

Eintrittswahrscheinlichkeit

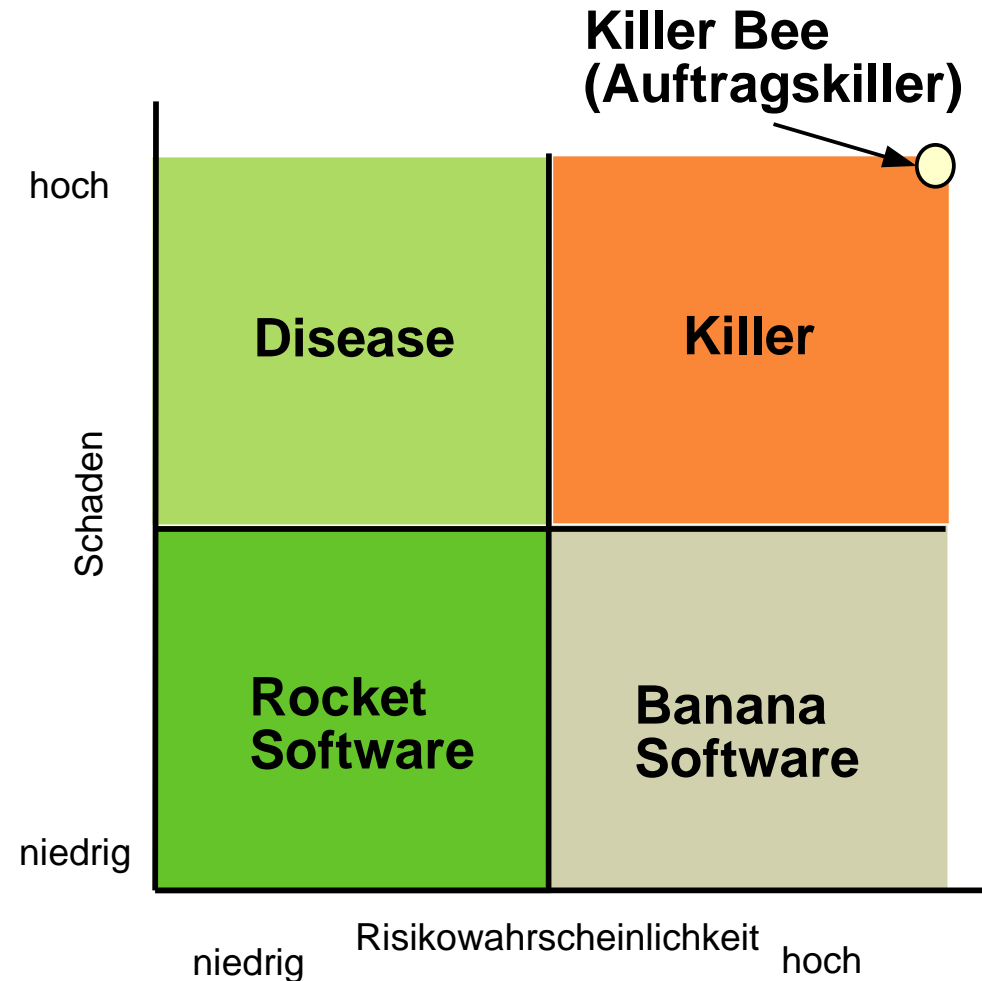


Risikobehandlungsplanung:

- ▶ **x1** u. U. Vernachlässigen
- ▶ **x2** vertraglich vorsorgen
- ▶ **x3** besonders beachten, z.B. mit Risikoversicherung
- ▶ **x4** Vorsorge treffen (Risikorückstellung); Risikowahrscheinlichkeit reduzieren

Auftragkiller-Projekte als Klassifikation der Produktrisiken

- Die “Auftragkiller”-Analyse analysiert die Menge der Projekte nach **Produktrisiken**



Kritikalitätsklassen für Risiken

Kritikalität

hoch

Art des Fehlverhaltens (für Informationssysteme)

Fehlverhalten macht sensitive Daten für unberechtigte Personen zugänglich oder verhindert administrative Vorgänge (z. B. Gehaltsauszahlung, Mittelzuweisung) oder führt zu Fehlentscheidungen infolge fehlerhafter Daten

niedrig

Fehlverhalten verhindert Zugang zu Informationen, die regelmäßig benötigt werden

keine

Fehlverhalten beeinträchtigt die zugesicherten Eigenschaften nicht wesentlich

Kritikalität

hoch

Art des Fehlverhaltens (für eingebettete Systeme)

Fehlverhalten kann zum Verlust von Menschenleben führen

mittel

Fehlverhalten kann die Gesundheit von Menschen gefährden oder zur Zerstörung von Sachgütern führen

niedrig

Fehlverhalten kann zur Beschädigung von Sachgütern führen, ohne jedoch Menschen zu gefährden

keine

Fehlverhalten gefährdet weder die Gesundheit von Menschen noch Sachgüter

Beispiel einer projektspezifischen Kritikalitätseinstufung für eine
Realzeitanwendung (z. B. Flugsicherung, fly-by-wire, drive-by-wire)

Kritikalität

Art des Fehlverhaltens

hoch

Fehlverhalten, das zu fehlerhaften Positionsangaben der Flugobjekte am Kontrollschirm führen kann

niedrig

Fehlverhalten, das zum Ausfall von Plandaten und damit zu Abflugverzögerungen führen kann

keine

alle übrigen Arten von Fehlverhalten

Maßnahmen zur Abwehr der Auswirkung von Fehlverhalten

Konstruktive Maßnahmen:

Entwicklung von eigensicheren bzw. fehlertoleranten Funktionseinheiten,
Konfigurierung von redundanten oder diversitären Funktionseinheiten
(unter diversitär wird in diesem Zusammenhang die Realisierung redundanter
Funktionseinheiten durch unterschiedliche Algorithmen oder physische Prinzipien
verstanden)

Analytische Maßnahmen:

Durchführung umfangreicher Verifikation und Validation bis zur
Zertifikationsreife

- ▶ Der **Risiko-Reduktions-Nutzen (RRN)** charakterisiert die Verbesserung des Risikofaktors im Verhältnis zu den Reduktionskosten

$$RRN := \frac{(RF' \text{ pre} - RF' \text{ post})}{RRK}$$

RF'pre: Risikofaktor vor den Maßnahmen zur Reduzierung

RF'post: Risikofaktor nach diesen Maßnahmen

RRK: Risiko-Reduktionskosten

Beispiel: Schnittstellenfehler mit 30% Wahrscheinlichkeit würde Kosten von 1 M€ verursachen
Behandlung a) Senkung der Wahrscheinlichkeit auf 10% durch ein SS-Prüfprogramm von 20 000 €
Behandlung b) Senkung auf 5% durch ausgiebigen Test der Schnittstelle, Kosten = 200 000 €

$$RRN(a) = (1 \text{ M€} * 0,3 - 1 \text{ M€} * 0,1) : 20\,000 \text{ €} = 10$$

$$RRN(b) = (1 \text{ M€} * 0,3 - 1 \text{ M€} * 0,05) : 200\,000 \text{ €} = 1,25$$

3-D Portfolio Schadenshöhe, Wahrscheinlichkeit, Reduktionsnutzen

Top 10 Elemente der Risiko-Analyse (1)

Risikoelement	Risikomanagement-Techniken
1 Personelle Defizite	<ul style="list-style-type: none">▪ Hochtalentierte Mitarbeiter einstellen▪ Teams zusammenstellen
2 Unrealistische Termin- und Kostenvorgaben	<ul style="list-style-type: none">▪ Detaillierte Kosten- und Zeitschätzung mit mehreren Methoden▪ Produkt an Kostenvorgaben orientieren▪ Inkrementelle Entwicklung▪ Wiederverwendung von Software▪ Anforderungen streichen
3 Entwicklung von falschen Funktionen und Eigenschaften	<ul style="list-style-type: none">▪ Benutzerbeteiligung▪ Prototypen▪ Frühzeitiges Benutzerhandbuch
4 Entwicklung der falschen Benutzungsschnittstelle	<ul style="list-style-type: none">▪ Prototypen▪ Aufgabenanalyse▪ Benutzerbeteiligung
5 Vergolden (über das Ziel hinausschießen)	<ul style="list-style-type: none">▪ Anforderungen streichen▪ Prototypen▪ Kosten/Nutzen-Analyse▪ Entwicklung an den Kosten orientieren

Quellen: [Mayr, S.172], [Balzert, S. 179]

Top 10 Elemente der Risiko-Analyse (2)

Risikoelement	Risikomanagement-Techniken
6 Kontinuierliche Anforderungsänderungen	<ul style="list-style-type: none">▪ Hohe Änderungsschwelle▪ Inkrementelle Entwicklung (Änderungen auf spätere Erweiterungen verschieben)
7 Defizite bei extern gelieferten Komponenten	<ul style="list-style-type: none">▪ Leistungstest▪ Inspektionen▪ Kompatibilitätsanalyse
8 Defizite bei extern erledigten Aufträgen	<ul style="list-style-type: none">▪ Prototypen▪ Frühzeitige Überprüfung▪ Verträge auf Erfolgsbasis
9 Defizite in der Echtzeitleistung	<ul style="list-style-type: none">▪ Simulation▪ Leistungstest▪ Modellierung▪ Prototypen▪ Instrumentierung▪ Tuning
10 Überfordern der Softwaretechnik	<ul style="list-style-type: none">▪ Technische Analyse▪ Kosten/Nutzen-Analyse▪ Prototypen

31.2.3) Planung der Risikohandhabung

- ▶ **Risikohandhabung** gliedert sich in primäre und sekundäre Maßnahmen
- ▶ **Primäre Maßnahmen** sind **echte Vorbeugungs-Maßnahmen** zur Behandlung der Risikowahrscheinlichkeit bzw. Risikoeintritts
 - **Risikovermeidung** ist kostenintensiv und wird nur praktiziert, wenn bei anderen Vorgehensweisen inakzeptables Gefahrenpotential verbleiben würde.
 - **Risikoverminderung** beabsichtigt eine geringe Eintrittswahrscheinlichkeit und/oder einen geringen Schadensumfang im Eintrittsfall.
- ▶ **Sekundäre Maßnahmen** sind **Maßnahmen zur Schadensbehandlung** bzw. **Kompensation**:
 - **Risikostreuung** bedeutet eine Verteilung der Risiken, z.B. eine Verteilung von Aktien auf unterschiedliche Unternehmen bei Kapitalanlagen.
 - **Risikoverlagerung (-ausschluss)** kann durch Vertragsbedingungen, z.B. Verlagerung der Risiken auf Lieferanten, Unterauftragnehmer usw. erreicht werden
 - **Risikoversicherung** ist eine sichere aber auch sehr teure Form der Risikohandhabung (Kosten-/ Nutzenanalyse), u.u. mit Selbstbeteiligung
 - Risiken, für die **Risikovorsorgen** (Rücklagen) bilden sind (bewusst eingegangen)
 - **Risikoübernahme/Risikoakzeptanz** heißt, das Unternehmen akzeptiert das bestehende Risiko und trägt die Schäden der verbleibenden Risiken im

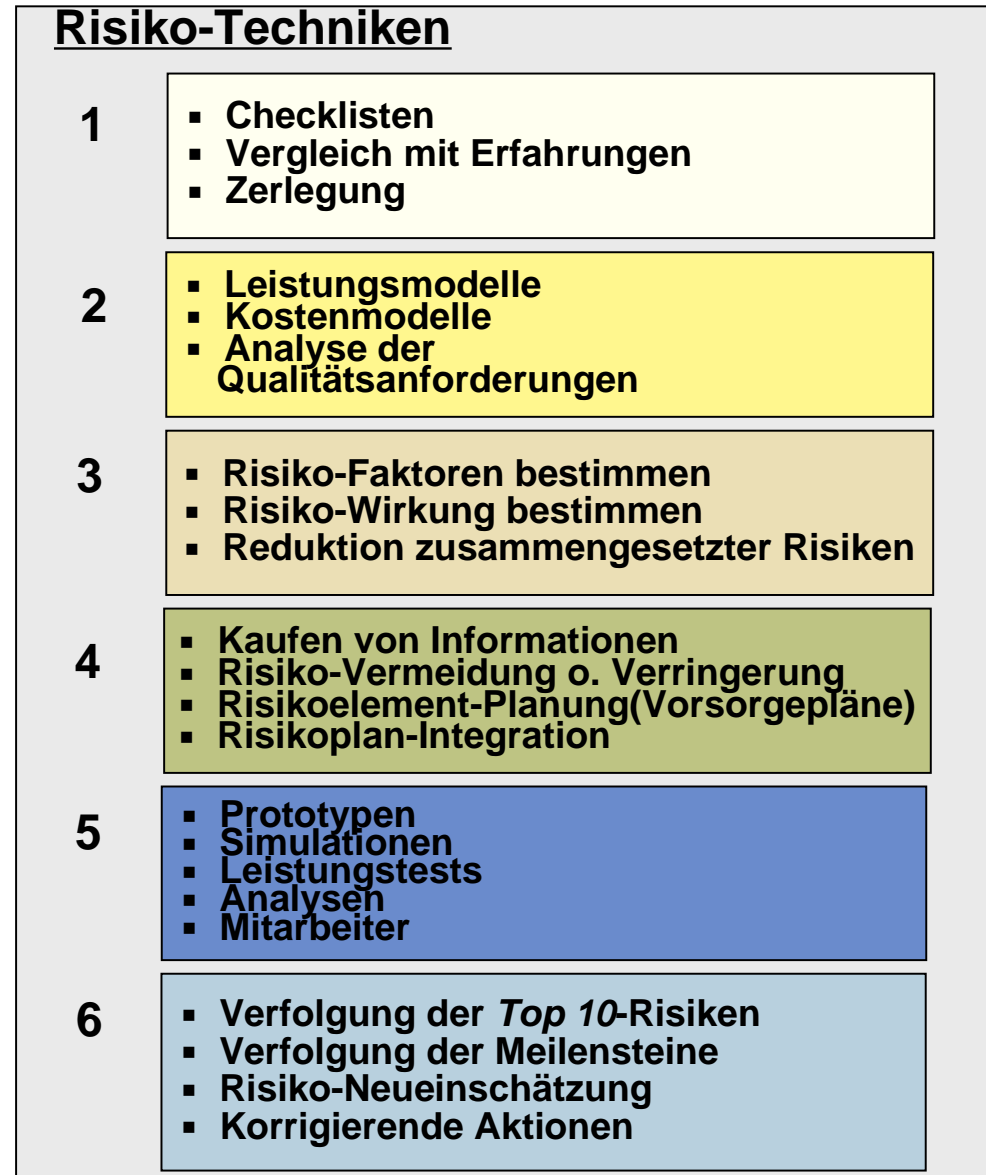
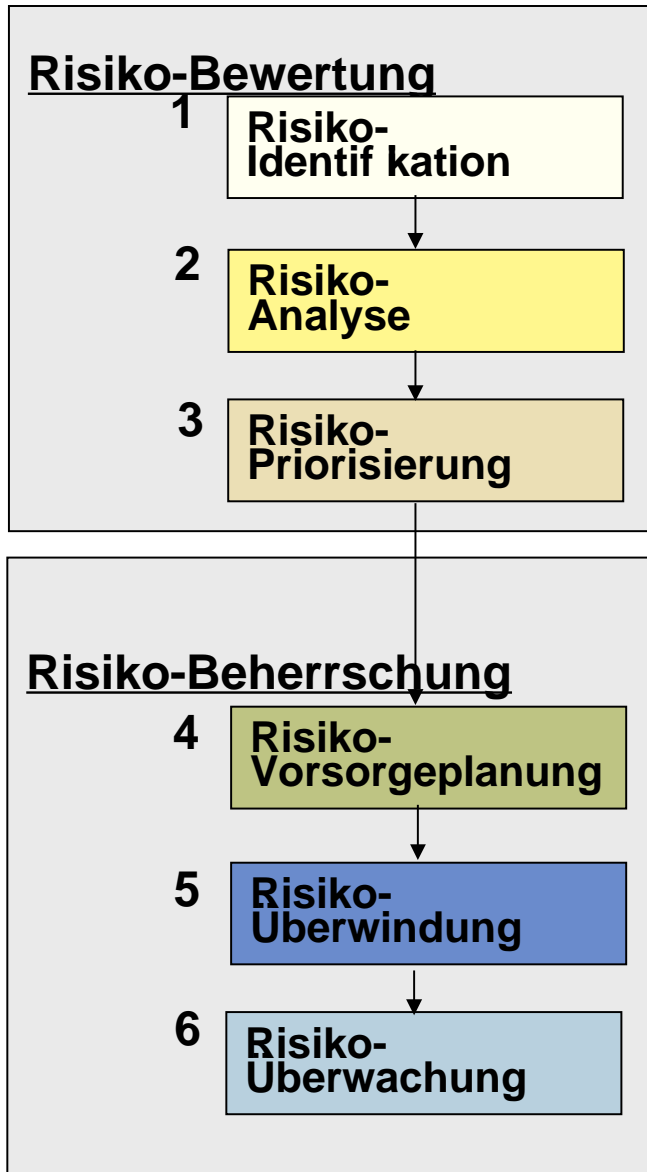
31.2.4) Risikoüberwachung

- ▶ Kontrollmaßnahmen:
 - regelmäßige Verfolgung des Projektfortschritts (Terminüberwachung) zu festgelegten Zeitpunkten
 - Fortschritts- und Abweichungsberichte
 - personelle und finanzielle Aufwandskontrolle
 - regelmäßige Berichterstattung der für die Maßnahme Verantwortlichen
 - Erkennen möglicher Veränderungen von Risikosituationen
 - Aufzeigen von Sachverhalten, die Schadenshöhe und Eintrittswahrscheinlichkeit verändern

31.2.5) Risikobehandlung

- ▶ Risikobehandlung durch die geplanten sekundären Maßnahmen (Gegenmaßnahmen):
 - Initiieren von Notfallmaßnahmen
 - Risikoversicherung: Information von Versicherungen
 - Dokumentation von Schäden
 - Risikoverlagerung: Formulierung von Regressansprüchen
- ▶ Krisenmanagement
 - Begrenzung von Schäden
 - Wiedergutmachung von Schäden

Schritte des Risikomanagements nach Balzert





31.3 Risikohandhabung



Werkzeuge zur Risikobehandlung

- ▶ Die meisten Werkzeuge haben sich aus firmeninternen Vorgehensweisen zur Behandlung des Risikomanagements entwickelt
- ▶ Werkzeuge sind ähnlich zu Anforderungsmanagementsystemen oder Bugtracking-Systemen zu sehen
 - Risikopläne (einfache Dokumente)
 - Risikodatenbanken (verteiltetes Risikomanagement)
 - Erweiterung von Projektmanagement-Werkzeugen um Komponenten zur Risikoanalyse und -überwachung
 - z.B. Microsoft Project erweitert um Add-In @RISK <http://www.palisade-europe.com/riskproject/>
 - Weitere sind enthalten in der Übersicht:
<http://www.risknet.de/Loesungsanbieter.52.0.html>

Paradoxon der Risikobehandlung

- ▶ Risiken unterschätzt: Schaden tritt ein ==> Frust
- ▶ Risiken überschätzt: Vermeidbare Kosten; Verlust von Chancen ==> Frust
- ▶ Risiken richtig eingeschätzt: Nutzen nicht beweisbar, nachlassendes Risikobewusstsein ==> Frust

31.3. Primäre Risikobehandlung - Risikoverminderung am Beispiel eines IT- Sicherheitskonzeptes

BSI = Bundesamt für Sicherheit in der Informationstechnik (BSI)

IT-Grundschutzhandbuch

zur Erstellung von IT-Sicherheitskonzepten

<http://www.bsi.bund.de>

<http://www.bsi.bund.de/gshb>



DRESDEN
concept
Exzellenz aus
Wissenschaft
und Kultur

Schritte einer IT-Sicherheitskonzeption (Sicherheitsrichtlinie)

- 1) Ermittlung der **Schutzbedürftigkeit** des Unternehmens (Schadensanalyse)
 - 1) Möglichen Schaden für das Unternehmen durch Vertraulichkeits- und Integritätsverlust
- 2) **Bedrohungsanalyse**
 - 1) Hardware, Software, Datenträger ==> Szenarien durchspielen,
 - 2) Sicherheitslücken im **Schwachstellenkatalog** beschreiben
 - 3) **Mis-Use-Diagramme** aufstellen (siehe Softwaretechnologie-II)
 - 4) **Attacker-Models** erstellen
- 3) **Risikoanalyse**
 - 1) Risikoidentifikation: Mängel ermitteln in der Absicherung wie Internetzugänge, Standleitungen usw.
 - 1) Abschottungen definieren zwischen Unternehmenszweigen bzw. kritischen Bereichen wie Geschäftsführung, Forschungsabteilungen, Buchhaltung oder Personalwesen
 - 2) Risikofaktoren ermitteln
- 4) Erstellung des **IT-Sicherheitskonzeptes** als Risikovorsorgeplanung
 - 1) Bedrohungspotentiale unterteilen in **tragbare** und **nicht tragbare** Risiken
 - 2) technische und organisatorische **Risiko-Behandlungsmaßnahmen**, die die Risiken auf ein tolerierbares Niveau reduzieren, Aufhebung von Restrisiken

2) Bedrohungsanalyse: Grundbedrohungen

- ▶ a) Verlust der **Verfügbarkeit** (des IT-Systems, von Inf. bzw. Daten)
- ▶ b) Verlust der **Integrität** (Modifizierung von Programmen und Daten nur durch Befugte, ordnungsgemäße Verarbeitung und Übertragung)
- ▶ c) Verlust der **Vertraulichkeit** (von Informationen/Daten, Programmen, z. B. bei geheimzuhaltenden Verfahren)
- ▶ Bedrohungen setzen an Objekten an und können über Objekte Schaden anrichten, also Schutz der Objekte gegen Bedrohungen.

Sicherheitsgrundfunktionen zur Sicherung gegen Grundbedrohungen

- ▶ **Identifikation und Authentisierung**
- ▶ **Rechteverwaltung und -prüfung**
- ▶ **Beweissicherung** durch Aufzeichnung
- ▶ **Fehlerüberbrückung** und Gewährleistung der Funktionalität (Verfügbarkeit des Systems oder spezieller Funktionen, z. B. bei Gefährdung von Menschen: Luftverkehr, Kraftwerke, ...)
- ▶ **Übertragungssicherung** (Anforderungen an Kommunikationspartner, Übertragungswege, Vorgang der Übertragung, ...)

- ▶ Tool zur Analyse des IT-Grundschatzes
 - https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/gstool_node.html

Objektgruppen, die Risiken auslösen

Infrastruktur		IT-Räume, Aufbewahrungsräume
		Stromversorgung, Klima,
		Zutrittskontrolle, Feuerschutz, ...
Materielle Objekte	Hardware	Benutzerterminal, wechselbare Speicher
	Datenträger	Nutzerzugang, ...
	Paperware	Ur-Versionen, Anwendungs-Software,
		Sicherungskopien, ...
	Software	Bedienungsanleitungen, Betriebsvorschr.
	Software	für Normalbetrieb und Notfall, Protokoll-
Logische Objekte	Software	ausdruck, Anw.-Ausdruck
	Anw.-Daten	Anw.-Software, Betriebssystem-SW,
	Anw.-Daten	Zusatz-Software
	Kommunikation	Eingabe, Verarbeitung, Speicherung,
	Kommunikation	Ausgabe, Aufbewahrung
Personelle Objekte	Personen	Dienstleistungsdaten (Nutzer-),
	Personen	Netzsteuerungsdaten
		betriebsnotwendige Personen,
		überwachende Personen, Hilfspersonal

4) Erstellung IT-Sicherheitskonzept

- ▶ Ziel: IT-Sicherheitskonzept mit
 - Ordnung der Maßnahmen mit Prioritäten
 - personeller Verantwortung
 - Zeitplan zur Realisierung der Maßnahmen
 - Hinweisen zur Überprüfung auf Einhaltung der Maßnahmen
 - Zeitpunkt zur Überprüfung des IT-Sicherheitskonzepts

- ▶ Schritte zur Erstellung des Sicherheitskonzeptes
 - **a) Auswahl von Maßnahmen**
 - **b) Bewertung der Maßnahmen**
 - **c) Kosten-/Nutzen-Analyse**
 - **d) Restrisikoanalyse**

4) Erstellung IT-Sicherheitskonzept

4a) Maßnahmenbereiche strukturieren sich anhand der Objektgruppen:

- **Infrastruktur:** Bauliche und infrastrukturelle Maßnahmen
(Gelände, Gebäude, Fenster, Türen, Decken, ...)
- **Organisation:** Regelung von Abläufen und Verfahren
Einsatz eines IT-Sicherheitsbeauftragten
- **Personal:** Schulung, Motivation, Sanktionen, ...
- **Hardware/Software:** Identifikation, Authentisierung, Zugriffskontrolle, Beweissicherung
Wiederaufbereitung, Übertragungssicherheit
- **Kommunikationstechnik:** z. B. Verschlüsselungsverfahren zur
Wahrung von Integrität und Vertraulichkeit
Virenschutz-Software, Firewalls
Wahl von sicheren Passwörtern
Verschlüsselung von Datenträgern
Digitale Signaturen, Digitaler Personalausweis
- **Abstrahlschutz:** gegen missbräuchlichen Gewinn von Informationen
- **Notfallvorsorge:** Wiederherstellung der Betriebsfähigkeit nach Ausfall
- **Versicherungen:**
 - von Hardware (Elektronik-Sachversicherung), für Datenträger
 - gegen Folgeschäden von Betriebsunterbrechungen
 - für die betriebliche Haftpflicht
 - für den Rechtsschutz u. a.

- ▶ **4b) Bewertung der Maßnahmen:**
 - Beschreibung des Zusammenwirkens der Maßnahmen mit Ursache-Wirkungsanalyse
 - Überprüfung der Auswirkungen auf den Betrieb des IT-Systems
 - Überprüfung auf Vereinbarkeit mit Vorschriften (A-Recht, Datenschutz)
 - Bewertung der Wirksamkeit der Maßnahmen

- ▶ **4c) Kosten/Nutzen-Analyse:**
 - Kosten der Maßnahmen (Risikoreduktionskosten)
 - Verhältnis Kosten/Nutzen (Risikoreduktionsnutzen feststellen)

- ▶ **4d) Restrisikoanalyse:**
 - sind die Restrisiken tragbar?

- ▶ evtl. zurück zu a)

Referenzen

- ▶ Datensicherung
http://www2.ec-kom.de/ec-net/20100804_Flyer_10_Praxistipps_Sicherheit.pdf
- ▶ Laptop-Sicherheit
- ▶ http://www2.ec-kom.de/ec-net/20100728_WLAN-Sicherheit.pdf
- ▶ http://www2.ec-kom.de/ec-net/20100804_Flyer_10_Praxistipps_Sicherheit.pdf
- ▶ Umfrage Computer-Spionage
- ▶ <http://www.ec-net.de/EC-Net/Navigation/root,did=372400.html>

IT-Sicherheitsprozess

Beispiel zur Organisation in einer kleinen und einer mittelgroßen Organisation

IT-Sicherheitsniveaus laut BSI

Maximal:

Schutz vertraulicher Informationen
Informationen im höchsten Maße korrekt
Zentrale Aufgaben ohne IT-Einsatz nicht durchführbar.

Knappe Reaktionszeiten für kritische Entscheidungen
Ausfallzeiten sind nicht akzeptabel.

Hoch:

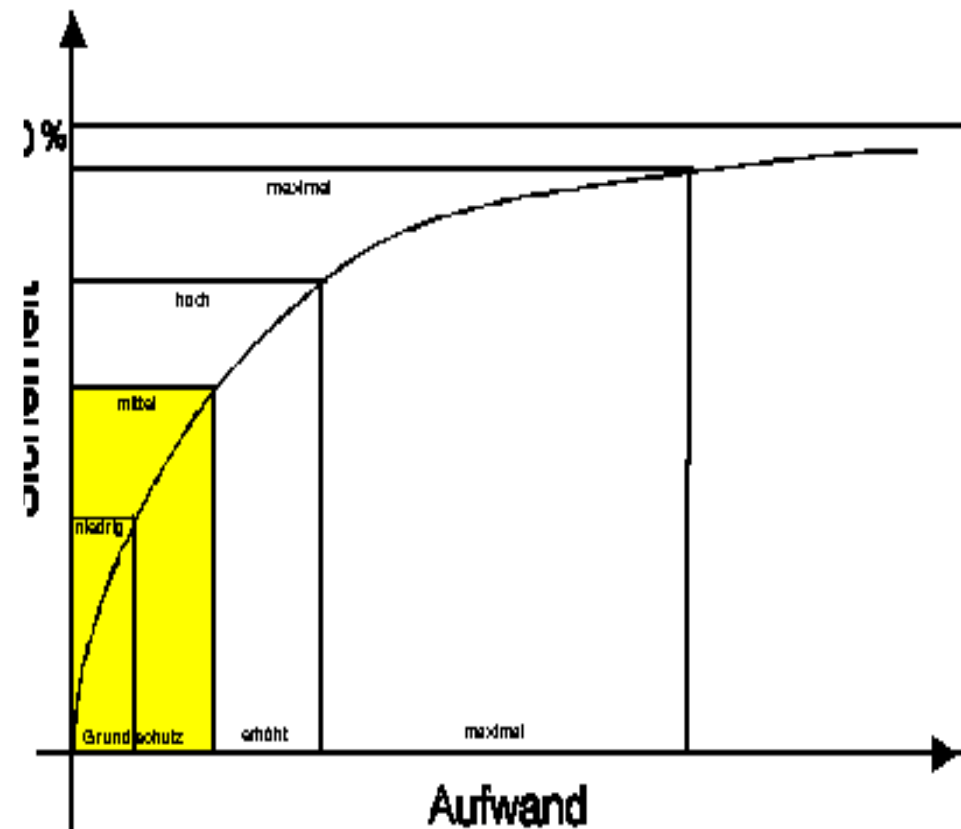
Der Schutz in sicherheitskritischen Bereichen stärker
Die verarbeiteten Informationen müssen korrekt sein
Fehler erkennbar und vermeidbar
In zentralen Bereichen laufen zeitkritische Vorgänge
oder es werden dort Massenaufgaben bearbeitet
es können nur kurze Ausfallzeiten toleriert werden.

Mittel:

Kleinere Fehler können toleriert werden, Fehler,
die die Aufgabenerfüllung erheblich beeinträchtigen,
müssen jedoch erkenn- oder vermeidbar sein.
Längere Ausfallzeiten sind nicht zu tolerieren.

Niedrig:

Vertraulichkeit von Informationen ist nicht gefordert.
Fehler können toleriert werden, solange sie die
Erledigung der Aufgaben nicht unmöglich machen;
längere Ausfallzeiten sind jedoch hinnehmbar.



Quelle: <http://www.bsi.bund.de/>

Durch technisches Versagen, versehentliches Löschen oder Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen.

- Entmagnetisierung von magnetischen Datenträgern durch Alterung oder durch ungeeignete Umfeldbedingungen (Temperatur, Luftfeuchte),
- Störung magnetischer Datenträger durch äußere Magnetfelder,
- Zerstörung von Datenträgern durch höhere Gewalt wie Feuer oder Wasser,
- versehentliches Löschen oder Überschreiben von Dateien,
- technisches Versagen von Peripheriespeichern (Headcrash),
- fehlerhafte Datenträger,
- unkontrollierte Veränderungen gespeicherter Daten (Integritätsverlust),
- vorsätzliche Datenzerstörung durch Computer-Viren

Ziel: kurzfristige Wiederaufnahme des IT-Betriebes durch redundanten Datenbestand

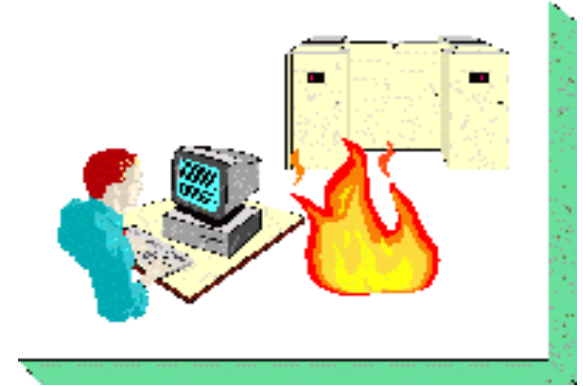
- ▶ **Maßnahmebündel für den IT-Grundschutz:**
 - Organisation
 - Personal (Verpflichtung, Vertretung, Schulung, Verfahren beim Ausscheiden usw.)
 - Gebäude, Verkabelung,
 - Büroraum (Fenster, Türen, Schlüssel, Zutrittsregelung, Kontrollgänge, . . .)
 - Datenträgerarchiv
- ▶ **Beispiel Minimaldatensicherungskonzept:**
 - **Software:** erworben oder selbst erstellt, einmalig Vollsicherung
 - **Systemdaten:** sind mindestens einmal monatlich mit einer Generation zu sichern.
 - **Anwendungsdaten:** mindestens monatlich Vollsicherung im Drei-Generationen-Prinzip
 - **Protokolldaten:** mindestens monatlich Vollsicherung im Drei-Generationen-Prinzip
- ▶ **Ergänzende Kontrollfragen:**
 - Werden sämtliche Mitarbeiter, auch neu eingestellte, auf ein Datensicherungskonzept oder ersatzweise auf das

Krisenmanagement bei Notfall

(Maßnahmen zur Wiederherstellung der Betriebsfähigkeit)

Phase 1: Planung der Notfallvorsorge

- Maßnahmen während des Betriebes (z. B. Rauchverbot, Stromversorgung, Wartung, Datensicherung)
- Notfallpläne (Teile eines Notfallhandbuchs) mit Maßnahmen bei Eintreten eines Notfalls.



Phase 2: Umsetzung der Notfallvorsorgemaßnahmen

- Ziel: Eintrittswahrscheinlichkeit eines Notfalls verringern sowie zügige und wirtschaftliche Wiederherstellung der Betriebsfähigkeit.

Phase 3: Durchführung von Notfallübungen

- Umsetzung der im Notfall-Handbuch aufgeführten Maßnahmen einüben und Steigerung deren Effizienz.

Phase 4: Umsetzung geplanter Maßnahmen nach Eintreten eines Notfalls

Notfallvorsorge: u. a.:

M 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen

M 6.2 Notfall-Definition, Notfall-Verantwortlicher

M 6.3 Erstellung eines Notfall-Handbuchs

M 6.5 Definition des eingeschränkten IT-Betriebs

M 6.6 Untersuchung interner und externer Ausweichmöglichkeiten

M 6.11 Erstellung eines Wiederanlaufplans

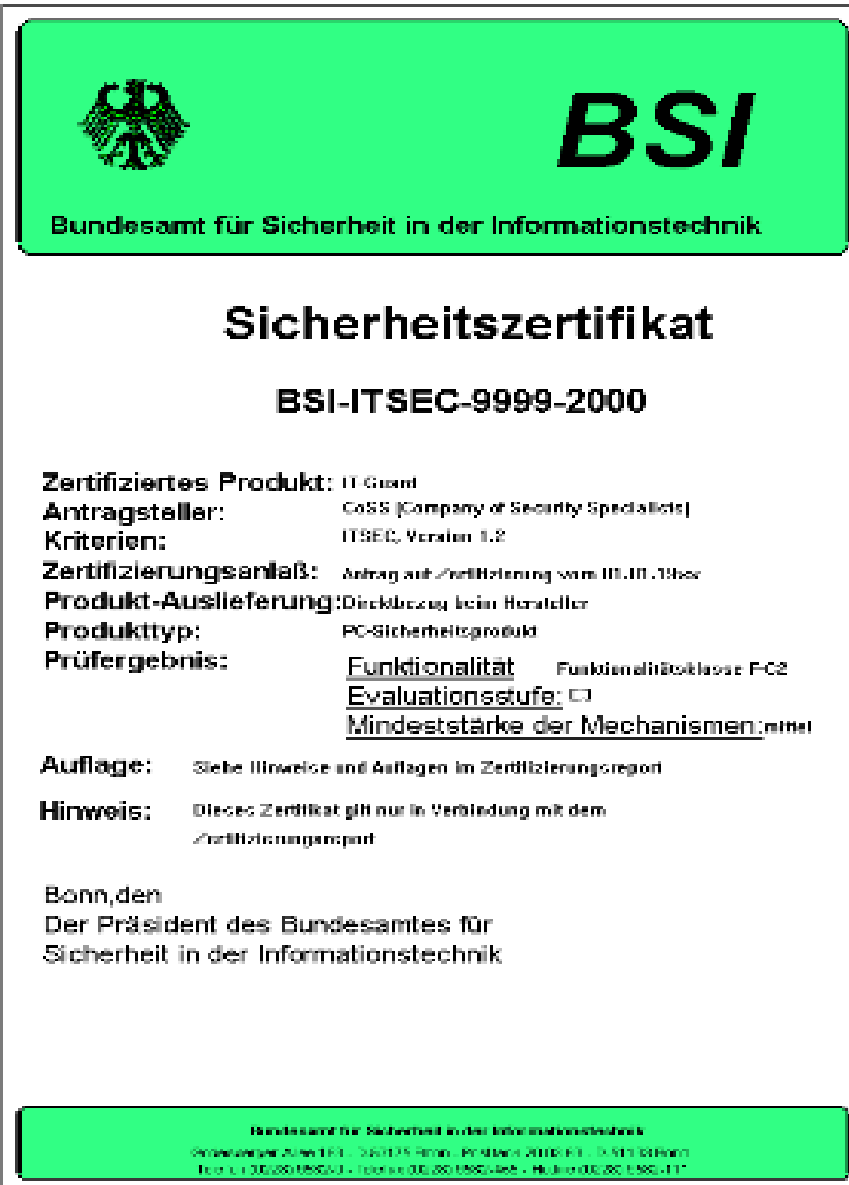
M 6.8 Alarmierungsplan

M 6.12 Notfallübungen

M 6.16 Versicherungen

M 6.14 Ersatzbeschaff.-plan

BSI-Sicherheitszertifikat



Die europäischen Sicherheitskriterien (**I**nformation **T**echnology **S**ecurity **E**valuation **C**riteria **ITSEC**) = Grundlage für die Prüfung der Vertrauenswürdigkeit von IT-Produkten (Korrektheit u. Wirksamkeit der Sicherheitsfunktionen wie Authentisierung, Zugriffskontrolle und Übertragungssicherung). Die Sicherheitsfunktionen wirken gegen folgende drei **Grundbedrohungen**:
Verlust der Vertraulichkeit
Integrität
Verfügbarkeit

Der **Zertifizierungsreport** enthält neben dem Sicherheitszertifikat einen **Bericht**, in dem Details der Prüfung und Zertifizierung veröffentlicht werden. (Sicherheitseigenschaften des IT-Produkts, abzuwehrende Bedrohungen, Anforderungen an Installation und Einsatzumgebung, Maßnahmen gegen inhärente Schwachstellen.)



(Prüfung und Bewertung der Sicherheit von Informationstechnik)

- Standard **Common Criteria for Information Technology Security Evaluation (CC)**, Version 2.0 , 5/1998 unter Beteiligung Deutschlands, Frankreichs, Großbritanniens, Kanadas, der Niederlande und der USA

Version 3.1, 9/2006

⇒ für die **Bewertung** der Sicherheitseigenschaften der informationstechnischen Produkte und Systeme

- **CC-Dokumentation gegliedert:**

Teil 1: Einführung und allgemeines Modell

Teil 2: Funktionale Sicherheitsanforderungen

Teil 2: Anhang

Teil 3: Anforderungen an die Vertrauenswürdigkeit

Quelle: <http://www.bsi.bund.de/cc/>
<http://www.commoncriteriaportal.org/cc/>

31.3.2 Sekundäre Maßnahmen (Gegenmaßnahmen), hier Risiko-Versicherung



Eine **Datenträger-Versicherung (DTV)** versichert das Nichtfunktionieren der Datensicherung

- Wiedereingabe der Daten, z. B. 5 000 € für Wiedereingabe von 1MByte
 - Wiederbeschaffung der Software und Daten
 - Folgeschäden sind nicht versichert
- ▶ Folgende Schäden werden ersetzt:
- falsches oder zerstörtes Backup
 - Störung oder Ausfall der DV-Anlage, der DFÜ, Stromvers., Klimaanlage.
 - Bedienungsfehler (falsche DT, falsche Befehlseingabe)
 - Vorsatz Dritter (Sabotage, Progr.- oder Datenmanipulation, Hacker, Viren, Einbruch)
 - Über- oder Unterspannung, elektrost. Aufladung, elektromagn. Störung
 - höhere Gewalt (Blitz, Hochwasser, Brand, ...)
- ▶ Anbieter: Versicherungskonzerne wie
- Unister GELD.de GmbH Leipzig <http://www.geld.de/risiko-versicherung.html>
 - Gerling-Konzern (Versich.-Beteiligungsgesellschaft (Holding) in > 30 Ländern) <http://www.gerling.de>

- ▶ Produkthaftung: der Hersteller ist für das Versagen seiner Produkte verantwortlich
 - Personenschäden (können bei eingebetteter Software entstehen, wie Auto, Flugzeug, Bahn, U-Bahn)
 - Sachschäden
 - Ausfälle oder entgangene Gewinne (falls Produkt nicht rechtzeitig fertig wird)

Versicherungsarten (1)

Elektronikversicherung am Bsp. einer großen Versicherung (500 MA, 18 Standorte)

Versicherungsarten:

1. Sachträgerversicherung

Ersatz zum Nennwert der Anlage (Schaden durch Einwirkung von außen)
Erweiterung: Leihgerät während Reparatur

2. Datenträgervers. DTV

wie bei 1., ohne "auswechselbare" DT
hier: Materialwert + Rekonstruktion der Daten u. Progr. ==> versichert ist nur das Nichtfunktionieren der eigenen Datensicherung

3. Softwarevers. SWV

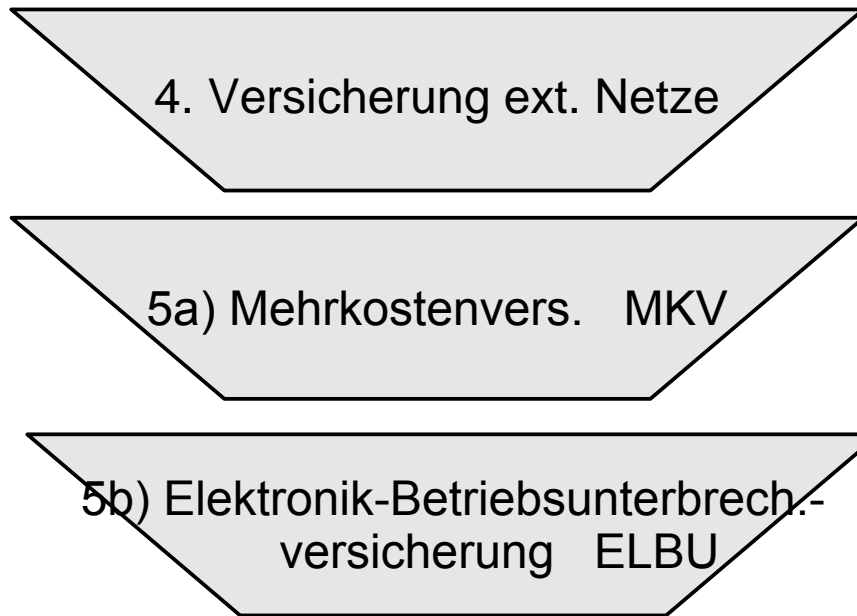
Bei Verlust /Veränderung auch ohne Sachschaden. Bsp.: DFÜ, Bedienfehler, Viren, Manipulation Dritter.

Leistung: Kosten der Wiederherstellung
DT-Versicherung ist in Softwareversicherung enthalten

ABE = Allg. Bedingungen für Elektronikvers.

Beispiel Versicherungsarten (2)

noch: Elektronikversicherung am Bsp. einer großen Versicherung



Mehrkosten für ein Ausweichkonzept
(Anmietung, Gebäude, Personal u.a.),
max. 1 Jahr

für Folgeschäden
eines sachschadenbedingten Ausfalls
=>wenn Ausweichmaßn. nicht möglich,
für entgangenen Gewinn u. fortl. Kosten

31.5 Krisenmanagement, hier bei Entwicklungsrisiken



- ▶ Operative Risiken: Planabweichung (Terminverzögerung, Kostensteigerung, Qualitätsmängel)
 - Setze mehr Personal und andere Ressourcen ein (Vorsicht, keine Proportionalität!)
 - Delegiere an Unteraufträge
 - Nehme finanziellen Verlust in Kauf und kompensiere im Multiprojektmanagement
 - Nehme nach Gummitwist-Quadrat Reduktion der Leistung in Kauf
 - Spreche mit Kunden

The End

- ▶ Explain the process of risk management
- ▶ How are risks analysed? How are they prioritized?
- ▶ Explain the risk reduction formula
- ▶ Explain the difference of primary and secondary risk mitigation