Risikomanagement

Ein Vortrag von Katharina Schroer

Juristisches IT-Projektmanagement
WS 2013/2014

Inhalt

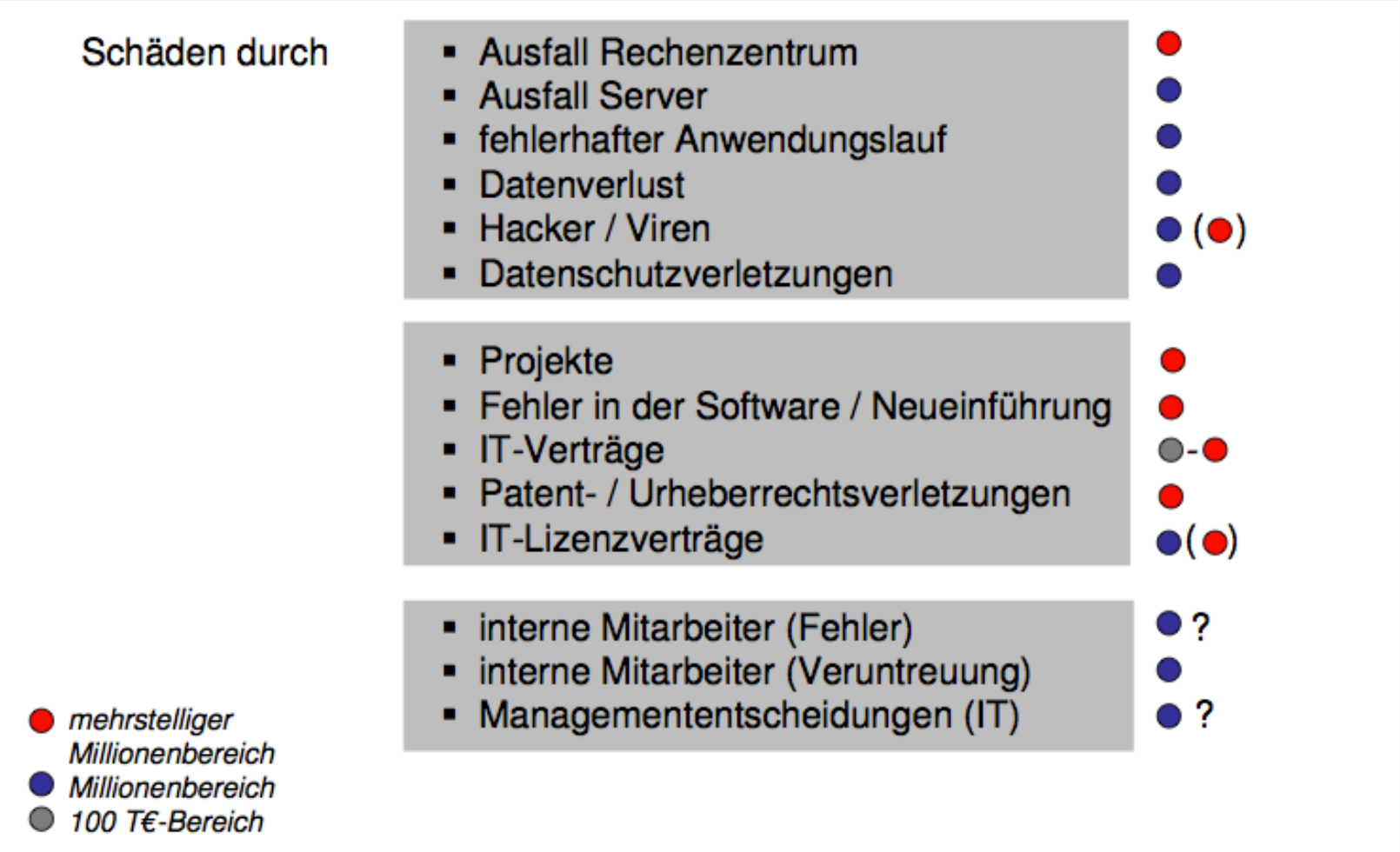
Was ist Risikomanagement?

DEFINITION RISIKO

Risiko beschreibt die Wahrscheinlichkeit, dass ein, vorwiegend als schlechtes gesehenes Ereignis, eintritt.

→ Der systematische Prozess und deren Maßnahmen zum Umgang mit diesen Risiken wird als **Risikomanagement** bezeichnet.

Schadensfälle in der IT



GRAFIK: Dr. Zoller, Peter (2013). “Risikomanagement am Beispiel Projekt-Compliance & Projekt-Verträge“. Foliensatz Gastvorlesung LMU Juristisches IT-Projektmanagement, Seite 24

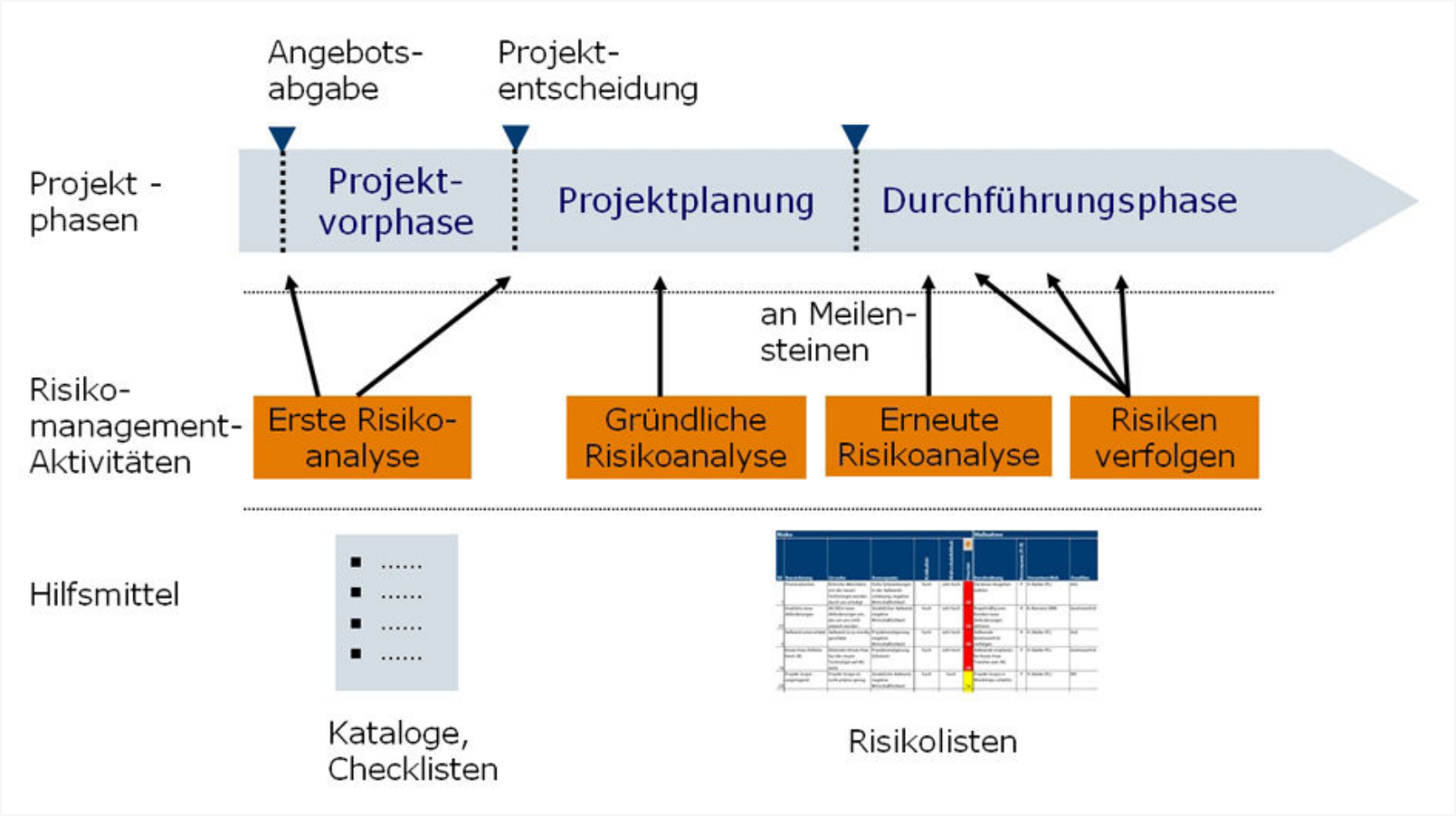
Können Risiken ganz vermieden werden?

RISIKEN = CHANCEN

→ Risiken sind notwendiger Bestandteil, ungeplant, nicht vermeidbar

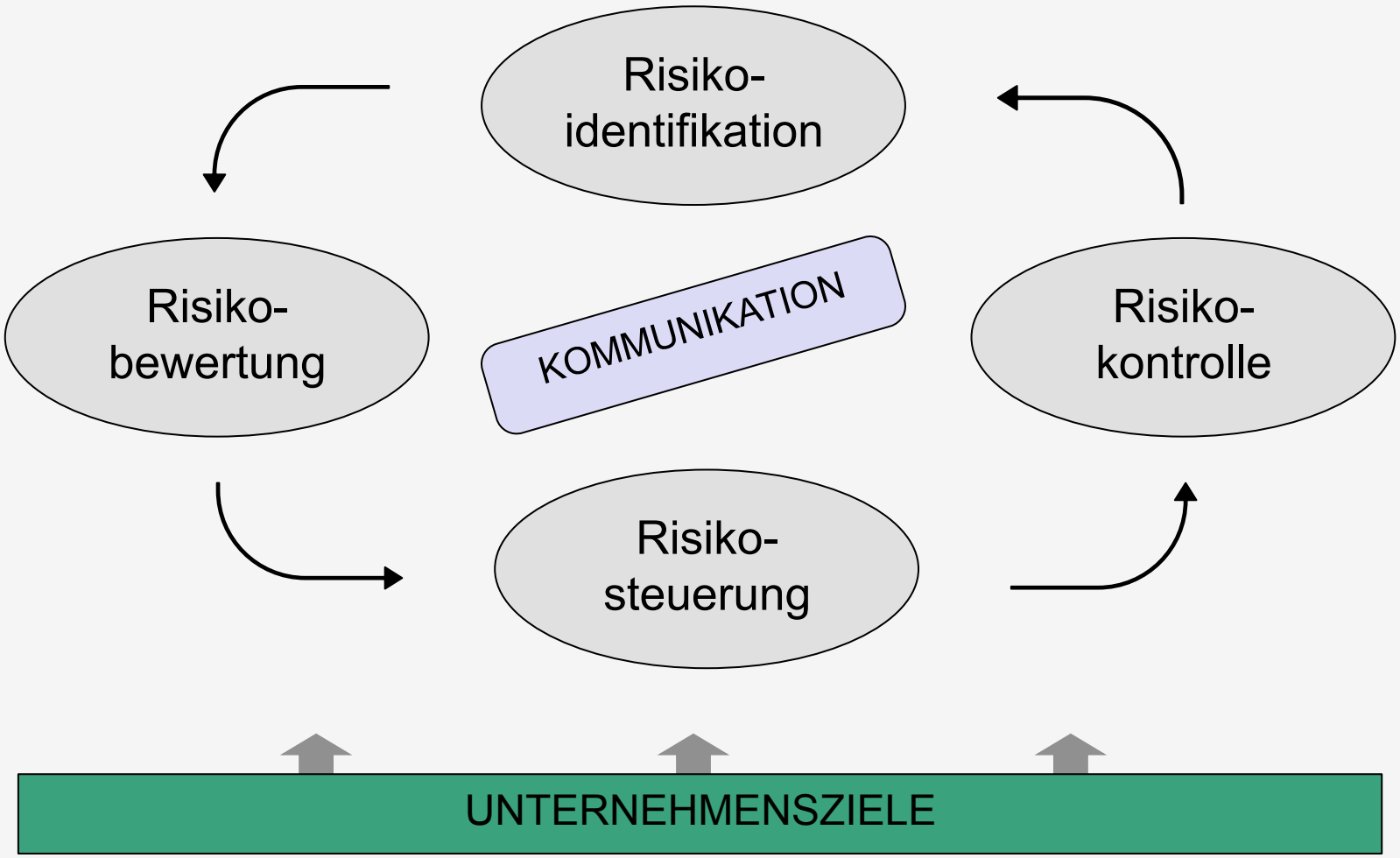
→ JEDOCH: gutes Risikomanagement schafft Abhilfe!

Wann ist der richtige Zeitpunkt?



GRAFIK: „Risikomanagement und Phasen des Projekts. Risikomanagement beginnt bereits in der Projektvorphase. (Method Park)“. URL: http://www.elektronikpraxis.vogel.de/the- men/embeddedsoftwareengineering/management/ articles/290447/ [Stand:10.01.2014]

Risikomanagementzyklus



UNTERNEHMENSZIELE

→ Vision des Unternehmens

→ Die Unternehmensstrategie klärt die Fragen „WAS sind unsere Ziele?“, „WIE wollen wir diese erreichen?“, „WANN wollen wir diese erreichen?“

→ Risikopolitik / IT-Risikopolitik baut auf der Unternehmensstrategie auf

→ Alle Maßnahmen des Risikomanagements müssen im Einklang mit der Unternehmensstrategie stehen

Risiko-identifikation

→ Sammlung aller aktueller und möglicher zukünftiger Risiken

→ Wichtiger Prozess!

METHODIK

SWOT - Analyse

		Interne Faktoren	
		S **Strength** Stärken	**W** **Weakness** Schwächen
Externe Faktoren	**O** **Opportunities** Chancen	**SO-Situation** Stärken einsetzen um Chancen zu nutzen	**WO-Situation** Schwächen überwinden durch Nutzung von Chancen
	T **Threats** Risiken	**ST-Situation** Stärken einsetzen um Risiken abzuwehren	**WT-Situation** Reduzierung der Schwächen und Vermeiden von Risiken

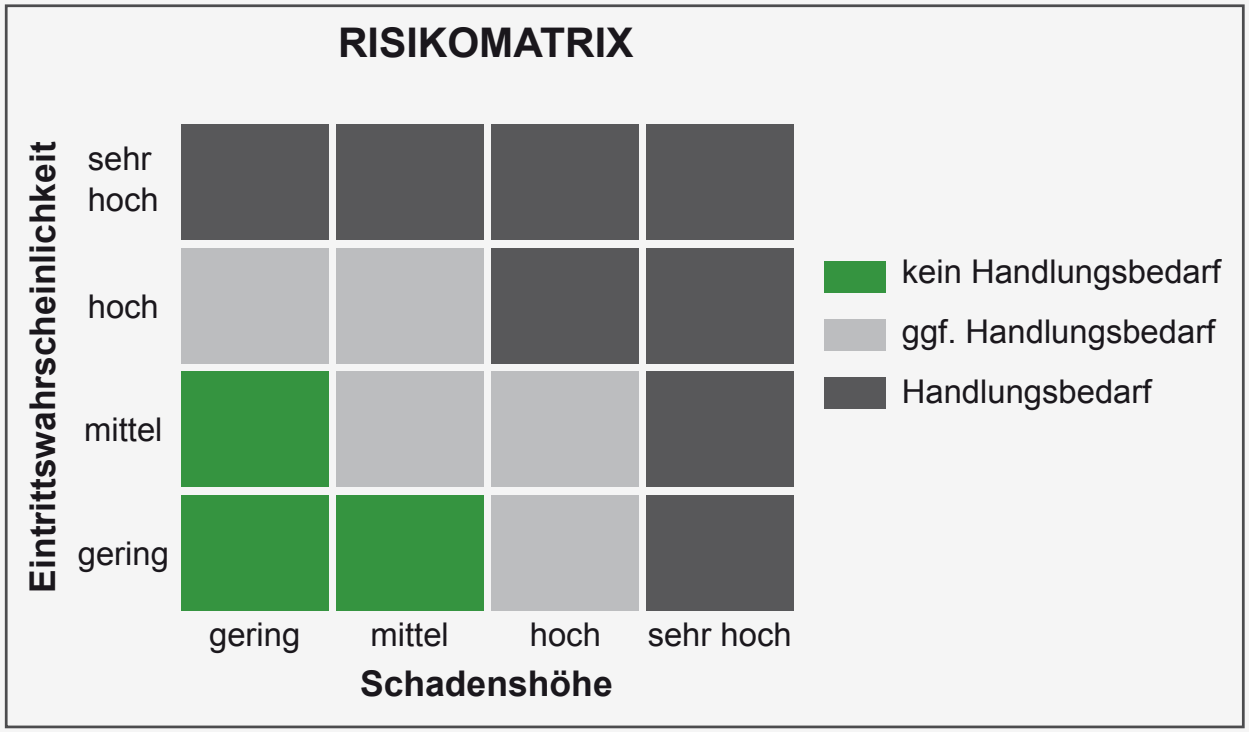
GRAFIK: URL: http://www.thessenvitz.de/swot-analyse/ [Stand:12.01.2014]

Risiko-bewertung

→ Beurteilt die gefundenen Risiken

→ Bewertung erfolgt in den Dimensionen **Eintrittswahrscheinlichkeit** und **Schadenshöhe**

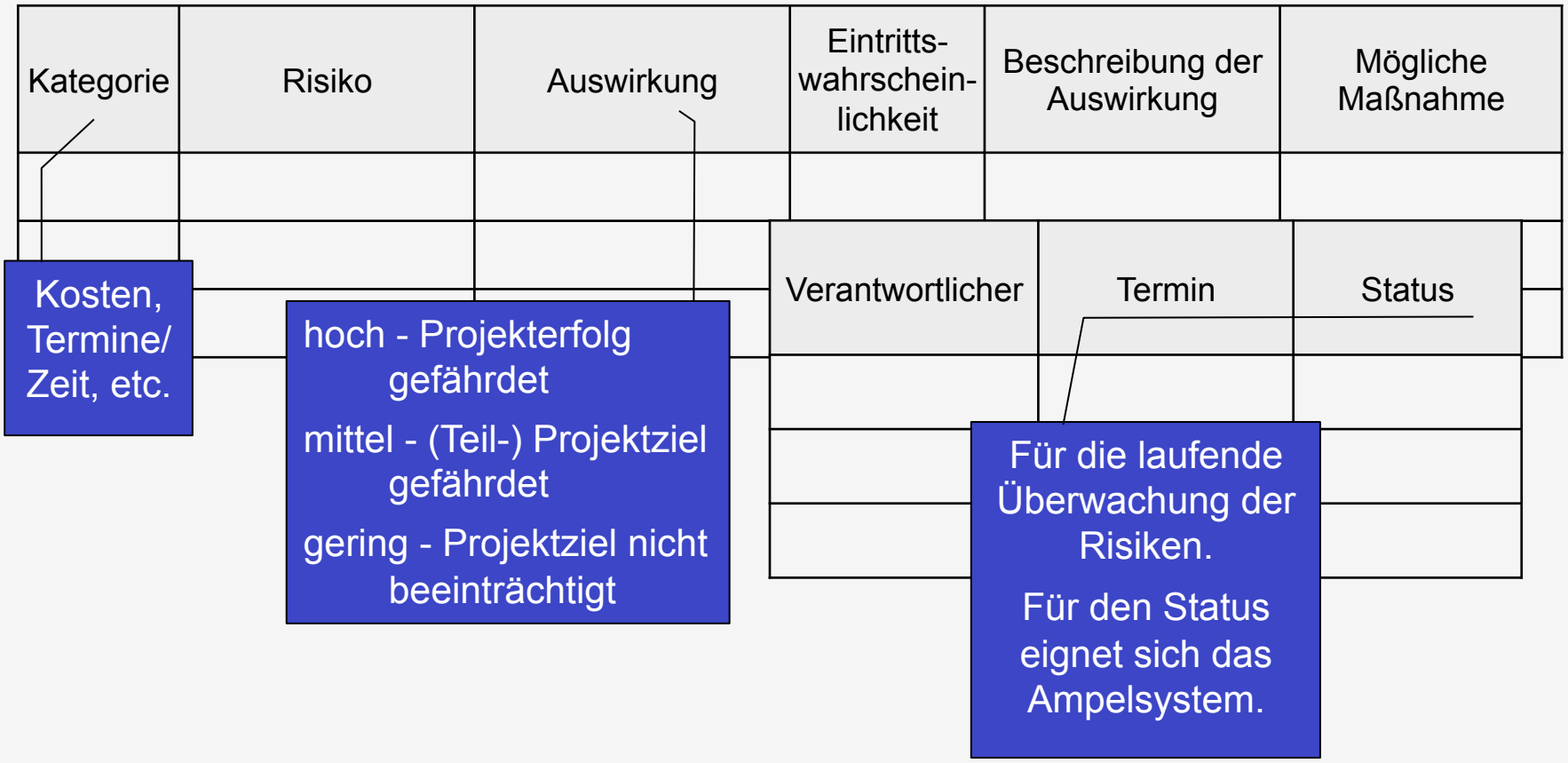
METHODIK



Risiko-bewertung

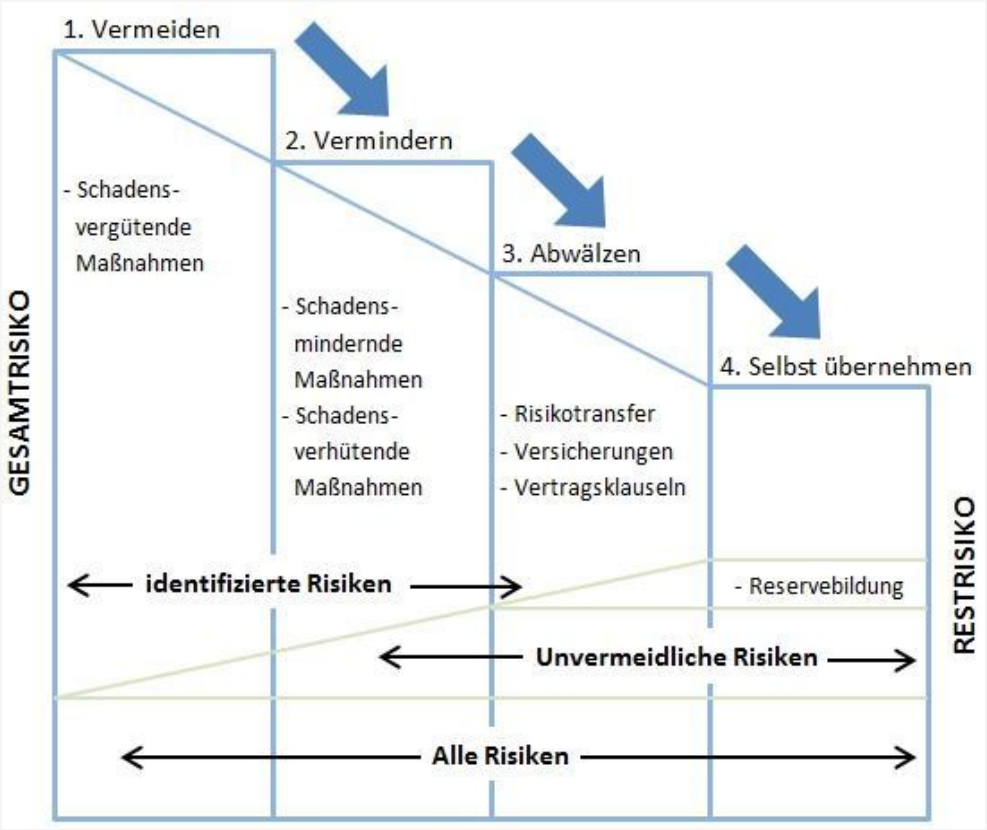
Zusatz: Risikoportfolio

→ Optimal zur Nachverfolgung / meist als Excel-Datei



Risiko-steuerung

→ Finden von Maßnahmen zum Umgang mit den Risiken



Vermeiden – Gegenmaßnahmen, die das Risiko komplett abwenden

Mindern – Maßnahmen, die die Auswirkungen verringern bzw. so gering wie möglich halten

Überwälzen – z.B. Versicherung abschließen oder Risiko an andere Projektmitglieder auslagern

Selbst tragen (Zuschläge und Reserven) – Risiko in Kauf nehmen, einkalkulieren, Kosten selbst tragen

GRAFI: Einerhand, Johanna (2011). „Risikosteuerung – wie können Risiken in der Landwirtschaft gesteuert werden?“. URL: http://web.altagenetics.com/germany/Article/Print/1083 [Stand: 13.01.2014]

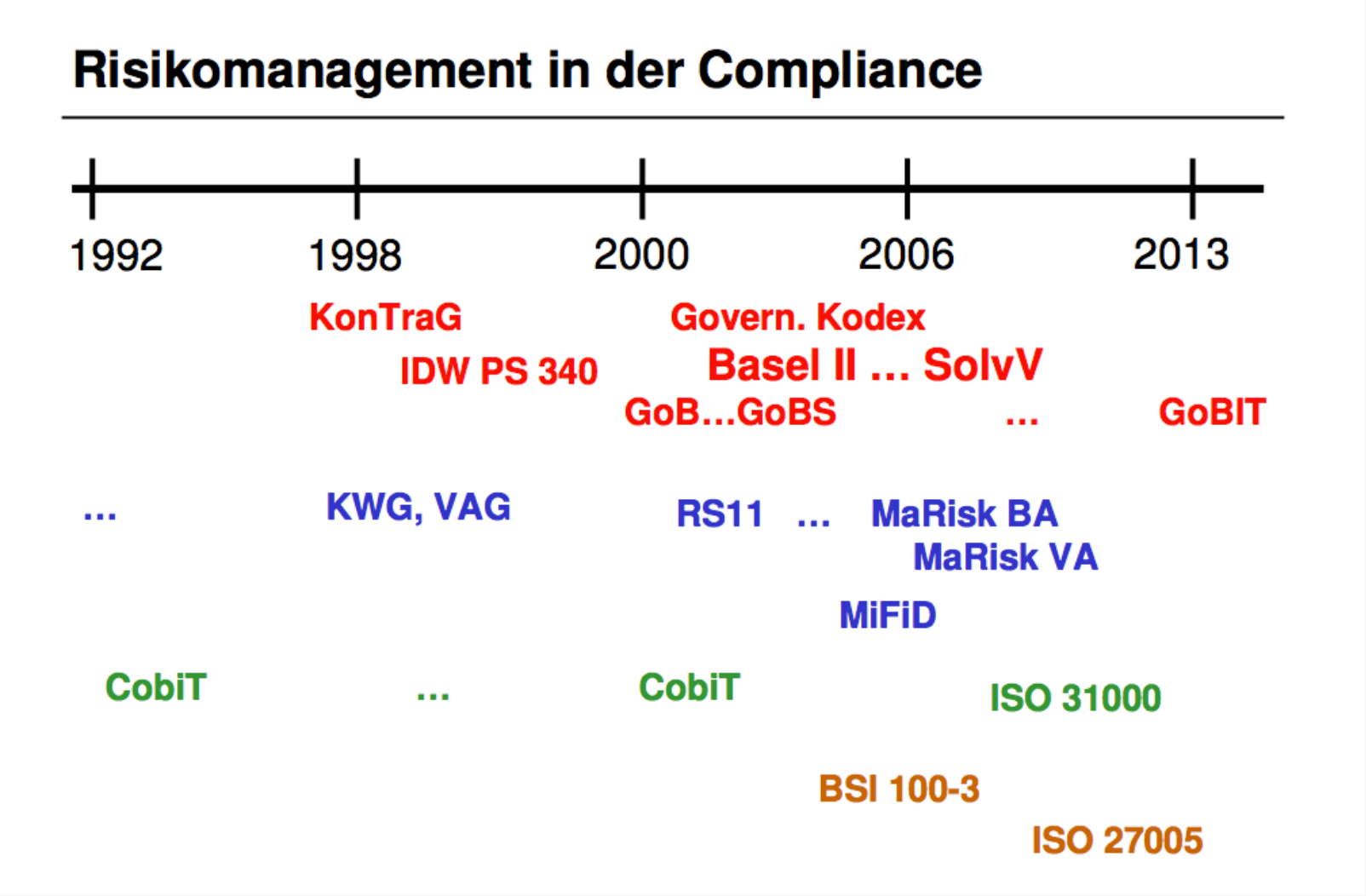
Risiko-kontrolle

→ Laufende Tätigkeit des Risikomanagements

→ Sicherstellung, dass „SOLL“ und „IST“ Situation übereinstimmen

→ Berichtswesen oder Standardprozess implementieren

Juristische Hintergründe



GRAFIK: Dr. Zoller, Peter (2013). “Risikomanagement am Beispiel Projekt-Compliance & Projekt-Verträge“. Foliensatz Gastvorlesung LMU Juristisches IT-Projektmanagement, Seite 5

BISIG

Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik

„Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder

2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.“

(§ 2 Abs. 2)

KonTraG

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“
(§ 91 Abs. 2 AktG)

→ Bei Nichterfüllung der Vorschriften des KonTraG können Geschäftsleiter in die persönliche Haftung geraten können
(OLG Düsseldorf, 26.4.01, 6 U 94/00)

→ Betroffene Rechtsformen:
Aktiengesellschaft, GmbH, GmbH & Co. KG, KG / OHG (wenn keine natürliche Person haftet)

Deutscher Corporate Governance Kodex

→ Regelwerk - von der Regierungskommission der Bundesrepublik Deutschland erarbeitet

→ Empfehlungen und Anregungen für börsennotierte Unternehmen, die auf eine gute Unternehmensführung zielen
(Grundsätze guter Leitung und Kontrolle von großen Unternehmen)

→ „soll“ - Abweichungen jährlich offen legen und begründen
„sollte“ - Anregungen von denen abgewichen werden kann

Eine von mehreren Stellen an denen das Risikomanagement angesprochen wird.

„Der Vorstand sorgt für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen.[...]“
(4.1.4)

ISO 31000

Erste weltweilt gültige ISO Norm (Standard) für Risikomanagement.

→ Beinhaltet Definitionen, Begriffserklärungen, Grundsätze des Risikomanagements, eine Beschreibung der Elemente des Risikomanagementsystems sowie eine Beschreibung des Risikomanagementprozesses

→ nicht zertifizierbar

ISO/IEC 2700x

Informationssicherheitsmanagement ISMS
(Information Security Management System)

→ Anleitung zur IT Risikoanalyse und zum Risikomanagement im IT Bereich

→ Der Prozess orientiert sich an der ISO 31000

→ nicht verpflichtend / zertifizierbar

BSI 100-3

Risikoanalyse auf der Basis von IT-Grundschutz

→ IT-Grundschutz-Kataloge des BSI enthalten Standard-Sicherheitsmaßnahmen aus den Bereichen Organisation, Personal, Infrastruktur und Technik

→ spezifiziert ergänzende, vereinfachte Risikoanalysen, falls die Sicherheitsanforderungen **deutlich** über das normale Maß hinausgehen ...

IDW PS 340

Prüfungsstandard –

Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB

→ Teil der Corporate Governance

→ Gilt für Großunternehmen, Aktiengesellschaften,...

→ Verantwortung beim Management

→ Zuständig ist Risikomanager

CobiT

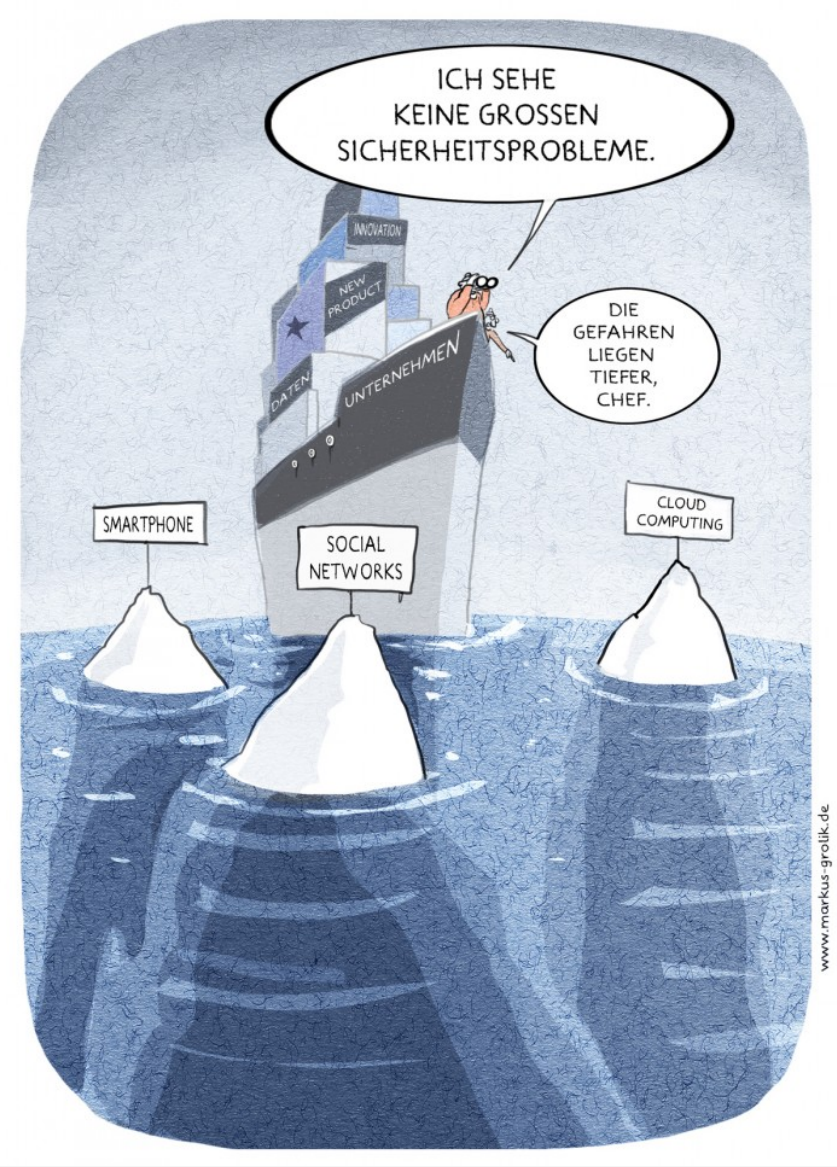
Control Objectives for Information and Related Technology

→ International anerkanntes Framework zur IT-Governance

→ COBIT definiert hierbei nicht vorrangig wie die Anforderungen umzusetzen sind, sondern primär WAS umzusetzen ist

→ In Summe definiert das COBIT 5-Frameworks und 37 IT-Prozesse

Bewusstsein für Risiken schaffen!



Fazit

- → Risikomanagement ist nicht nur empfehlenswert, es ist auch juristisch verpflichtend
- → Bewusstsein für Risiken schaffen
- → Risikomanagement ist Teil der Governance
- → Frühzeitiges und sauberes Risikomanagement ist von großer Bedeutung
- → Risikomanagement ist transparent
- → Es ist dynamisch, iterativ und reagiert auf Veränderungen

Quellenangabe / Literaturhinweis

- Dr. Zoller, Peter (2013). “Risikomanagement am Beispiel Projekt-Compliance & Projekt-Verträge“. Foliensatz Gastvorlesung LMU Juristisches IT-Projektmanagement

- „IT-Grundschutz-Standards“. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html [Stand:14.01.2014]

- Prof. Dr. Krystek, Ulrich & Prof. Dr. Fiege, Stefanie. „Gabler Wirtschaftslexikon, Stichwort: Risikomanagement„. Springer Gabler Verlag. URL: http://wirtschaftslexikon.gabler.de/Archiv/7669/risikomanagement-v9.html [Stand: 12.01.2014]

- Regierungskommission (2013). „Deutscher Corporate Governance - Kodex“. URL: http://www.corporate-governance-code.de/ger/kodex/index.html [Stand: 12.01.2014])

- URL: http://www.risikomanagement-iso-31000.de [Stand: 14.01.2014]