Risikomanagement

Katharina Schroer
Mat. Nr.: 10997260

Ausarbeitung zum Vortrag Risikomanagement am 21.01.2014

Juristisches IT-Projektmanagement
WS 2013/14

INHALTSANGABE

ABBILDUNGSVERZEICHNIS

1. Einführung

1.1 Kurzerläuterung

Risiken gehen immer einher mit unternehmerischen Tätigkeiten und müssen daher hingenommen werden. Der Begriff Risiko beschreibt die Wahrscheinlichkeit, dass ein, vorwiegend als schlecht gesehenes Ereignis, eintritt. Meist liegt dieses Ereignis außerhalb der Planung und ist Resultat aus der Unsicherheit der zukünftigen Unternehmungen und deren meist auch unvollständiger Informationsstand.

„Diese Unvollkommenheit der Planung kann aber nicht nur zu einer negativen Planabweichung und damit zu einem sogenannten Risiko im engeren Sinne (= Verlustgefahr) führen; aus ihr ergibt sich zugleich die Möglichkeit, dass sich beispielsweise ein Geschäft besser entwickelt als angenommen. In diesem Fall spricht die Betriebswirtschaftslehre von einem Risiko im weiteren Sinne (= Chance). Daneben existieren ungewisse zukünftige Geschehnisse, die keine Chancen mit sich bringen. Das sind die sog. Schadensgefahren bzw. ‚reinen' Risiken."

(Hopp, K. U. (2001). *„GmbH-Risikomanagement zur Unternehmenssicherung und Haftungsbegrenzung"*. Bonn: VSRW-Verlag, S. 20.)

Bei nicht rechtzeitiger Erkennung der Risiken und Ergreifung entsprechender Maßnahmen drohen Schäden in unterschiedlichstem Ausmaß. Von kleinen, leicht verkraftbaren bis zu großen Unternehmen zerstörenden Schäden gibt es keine Grenzen.

Der systematische Prozess und deren Maßnahmen der Identifikation, Bewertung, Steuerung/Überwachung und Kontrolle dieser Risiken wird als Risikomanagement bezeichnet. Ein Geschäft, Unternehmen kann, sollte und ist sogar teilweise gesetzlich verpflichtet Risikomanagement zur qualifizierten Planung und Durchführung jeglicher Art von Projekten einzusetzen.

1.2 Anwendungsstand

„Während im Rahmen von (börsennotierten) Großunternehmungen von einem flächendeckenden Vorhandensein eines institutionalisierten Risikomanagements ausgegangen werden kann, erscheint im deutschen Mittelstand diesbezüglich noch erheblicher Nachholbedarf zu bestehen. So verfügen - nach einer Umfrage im Jahr 2011 - etwa 50% der mittelständischen Unternehmungen noch nicht über ein ausreichend institutionalisiertes Risikomanagementsystem und sehen den Aufbau sowie den Betrieb eines solchen Systems eher als eine Aufgabe der operativen Bereiche, weniger dagegen als eine Aufgabe der obersten Führung (Vorstand, Geschäftsführung). Eine Studie der DAX30-Unternehmen aus dem Jahr 2010 kommt hingegen zu dem Ergebnis, dass zwei Drittel der Unternehmungen dem zentralen Risikomanagement eine so große Bedeutung einräumen, dass Risikomanagementstellen oder Abteilungen existieren, die ausschließlich mit Risikomanagementaufgaben betraut sind und dabei überwiegend als Abteilung direkt unter dem Vorstand organisiert sind.“

(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])

1.3 Gefahrenquellen in der IT

Fehler im oder einfach nur schlecht durchgeführtes Risikomanagement wird meist im Zusammenhang mit Finanzen, Banken, etc. genannt. Doch ist es nicht nur die Finanzbranche die Risiken birgt. Jedes Projekt, jedes Unternehmen muss mit Risiken umgehen und Gegenmaßnahmen ergreifen. Doch wo genau lauern die Risiken in der IT?

Sicherheit, Verfügbarkeit, mangelnde Performance sind Begriffe, die zum Thema Risikomanagement in der IT oft zu hören sind. Allerdings decken sie nicht den gesamten Bereich der Gefahren in der IT ab.
Die nächste Grafik (Abb. 1) soll einen kleinen Überblick über die Gefahrenquellen in der IT-Branche geben.

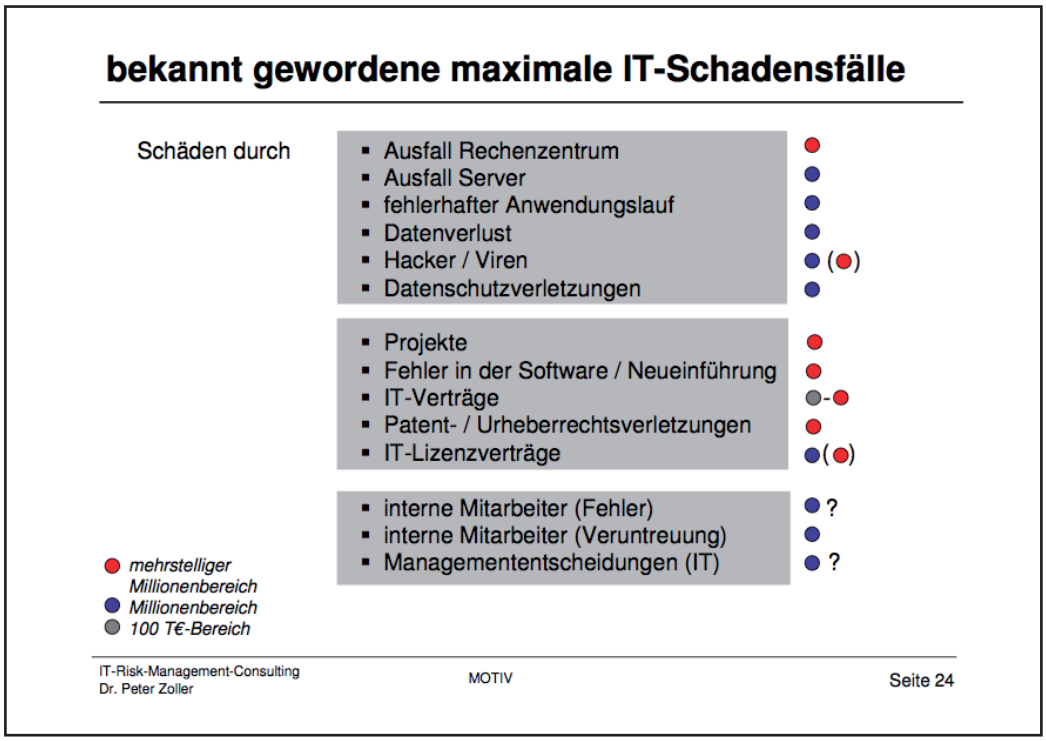

Abb. 1 Ursachen Schadensfälle in der IT
(Dr. Zoller, Peter (2013). *"Risikomanagement am Beispiel Projekt-Compliance & Projekt-Verträge"*. Foliensatz Gastvorlesung LMU Juristisches IT-Projektmanagement, Seite 24)

2. Juristische und formale Hintergründe speziell für die IT

Durch effizientes Risikomanagement lassen sich große Schäden abwenden. Das schließt auf ein natürliches Interesse aus Seite der Unternehmen an der Existenz eines qualitativen und funktionierenden Risikomanagements. Doch abgesehen von dem Eigeninteresse sind Unternehmen auch rechtlich dazu verpflichtet.

Risikomanagement ist eine juristische Pflicht!

Im folgenden möchte ich auf die gesetzlichen Richtlinien / Standards / Normen und Empfehlungen eingehen.
(Wichtig ist jedoch dabei in Erinnerung zu behalten, dass diese nur ein Bruchstück darstellen)
Die untenstehende Grafik (Abb. 2) zeigt eine Auswahl, von denen ich im Folgenden ein paar näher erläutern möchte.

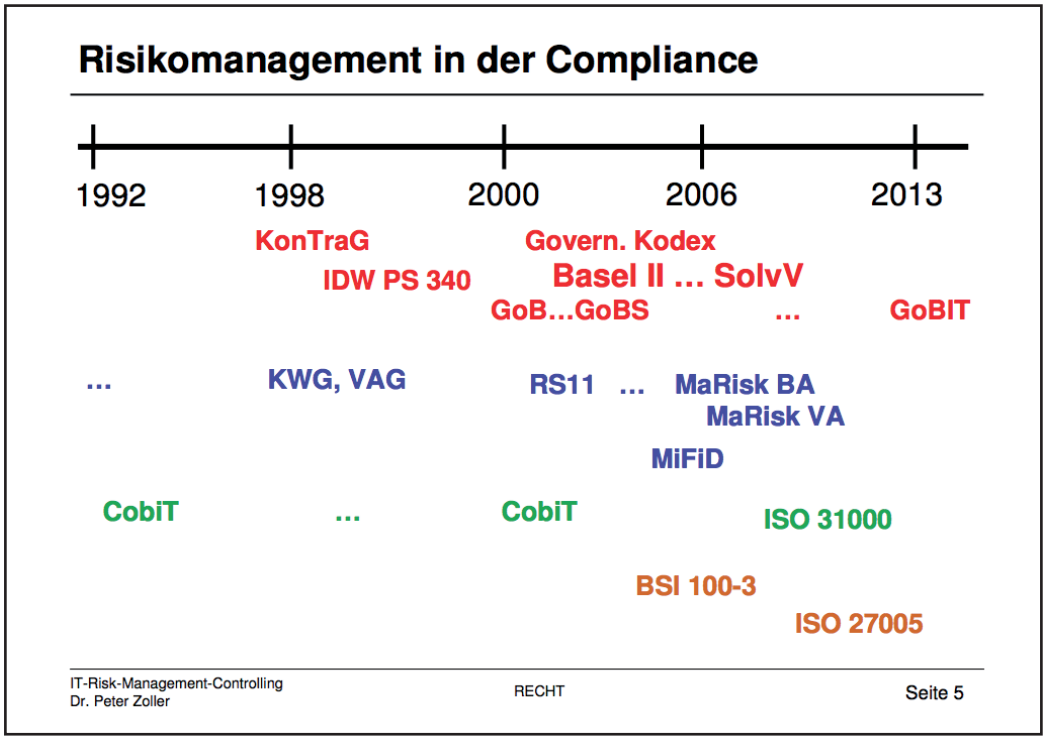

Abb. 2 Risikomanagement in der Compliance
(Dr. Zoller, Peter (2013). *"Risikomanagement am Beispiel Projekt-Compliance & Projekt-Verträge"*. Foliensatz Gastvorlesung LMU Juristisches IT-Projektmanagement, Seite 5)

2.1 Rechtliche Hintergründe

Es gibt im deutschen und internationalem Recht einige Gesetzgebungen, in denen das Risikomanagement verankert ist. Die wichtigsten für die IT Branche und deren Bedeutung möchte ich folgenden näher darstellen.

→ BSIG
Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik

„Der Gesetzgeber definiert IT-Sicherheit als die Einhaltung bestimmter Sicherheitsstandards, welche die Schutzgüter Verfügbarkeit, Unversehrtheit beziehungsweise Vertraulichkeit von Informationen durch Sicherheitsvorkehrungen in oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen betreffen. So nachzulesen in Paragraf 2 Absatz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG).“

(Dr. von Holleben, Kevin Max & Winters, Fabian (18.10.2013) *„Risiko-Management ist eine juristische Pflicht“*. URL: http://www.computerwoche.de/a/risiko-management-ist-eine-juristische-pflicht,2547615 [Stand: 14.01.2014])

§2 Absatz 2

„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.“

→ KonTraG
Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Durch das KonTraG, dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, am 01. Mai 1998 in Kraft getreten, obliegt den Vorständen von börsennotierten Aktiengesellschaften die Pflicht, ein Risikomanagementsystem zu installieren.
Es fordert die Einführung eines adäquaten Risikomanagements von börsennotierten Aktiengesellschaften. Vorgesehen ist, dass „der Vorstand geeignete Maßnahmen zu

treffen, insbesondere ein Überwachungssystem einzurichten hat, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“ (§ 91 Abs. 2 AktG).
Kern des KonTraG ist eine Vorschrift, die die Unternehmensleitungen dazu zwingt, ein unternehmensweites Früherkennungssystem für Risiken (Risikofrüherkennungssystem) einzuführen und zu betreiben, sowie Aussagen zu Risiken und zur Risikostruktur des Unternehmens im Lagebericht des Jahresabschlusses der Gesellschaft zu veröffentlichen.
Hinweis: Zu beachten ist, dass bei Nichterfüllung der Vorschriften des KonTraG Geschäftsleiter in die persönliche Haftung geraten können (OLG Düsseldorf, 26.4.01, 6 U 94/00).

Betroffene Rechtsformen:

Folgende Rechtsformen haben das KonTraG zu beachten:

- Aktiengesellschaft
- GmbH
- GmbH & Co. KG
- KG, wenn keine natürliche Person haftet und
- OHG, wenn keine natürliche Person haftet

Es ist zu beachten, dass Unternehmen dann unter die Vorschriften des KonTraG fallen, wenn neben den Rechtsformvorschriften zwei der drei nachstehenden Kriterien erfüllt sind:

- Bilanzsumme > 3,44 Mio. EUR
- Umsatz > 6,87 Mio. EUR
- Mitarbeiterzahl > 50

(vgl. Herke, Martin Dieter (Ausgabe 04/2005), Seite 99. *„Risikomanagement entsprechend dem KonTraG“*. URL: http://www.iww.de/bbp/archiv/gesetz-zur-kontrolle-und-transparenz-im-unternehmensbereich-risikomanagement-entsprechend-dem-kontrag-f24228 [Stand: 14.01.2014])

→ Deutscher Corporate Governance Kodex

Der Deutsche Corporate Governance Kodex (abgekürzt DCGK) ist ein von einer Regierungskommission der Bundesrepublik Deutschland erarbeitetes Regelwerk, das vor allem Empfehlungen und Anregungen für börsennotierte Unternehmen enthält, die auf eine gute Unternehmensführung zielen, also die Grundsätze guter Leitung und Kontrolle von großen Unternehmen.

„Empfehlungen des Kodex sind im Text durch die Verwendung des Wortes „soll" gekennzeichnet. Die Gesellschaften können hiervon abweichen, sind dann aber verpflichtet, dies jährlich offenzulegen und die Abweichungen zu begründen („comply or explain").[...]Ferner enthält der Kodex Anregungen, von denen ohne Offenlegung abgewichen werden kann; hierfür verwendet der Kodex den Begriff „sollte".[...]

Der Kodex richtet sich in erster Linie an börsennotierte Gesellschaften und Gesellschaften mit Kapitalmarktzugang im Sinne des § 161 Absatz 1 Satz 2 des Aktiengesetzes. Auch nicht kapitalmarktorientierten Gesellschaften wird die Beachtung des Kodex empfohlen.

3.4 Die ausreichende Informationsversorgung des Aufsichtsrats ist gemeinsame Aufgabe von Vorstand und Aufsichtsrat.
Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance. Er geht auf Abweichungen des Geschäftsverlaufs von den aufgestellten Plänen und Zielen unter Angabe von Gründen ein.[...]
Der Aufsichtsrat soll die Informations- und Berichtspflichten des Vorstands näher festlegen. Berichte des Vorstands an den Aufsichtsrat sind in der Regel in Textform zu erstatten. Entscheidungsnotwendige Unterlagen werden den Mitgliedern des Aufsichtsrats möglichst rechtzeitig vor der Sitzung zugeleitet.[...]

4.1.4 Der Vorstand sorgt für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen.[...]

5.2 Der Aufsichtsratsvorsitzende soll zwischen den Sitzungen mit dem Vorstand, insbesondere mit dem Vorsitzenden bzw. Sprecher des Vorstands, regelmäßig Kontakt halten und mit ihm Fragen der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance des Unternehmens beraten. [...]

5.3.2 Der Aufsichtsrat soll einen Prüfungsausschuss (Audit Committee) einrichten, der sich insbesondere mit der Überwachung [...] des Risikomanagementsystems [...] befasst. [...]“

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

2.2 Relevante Standards und Normen

Analog zu den Gesetzgebungen, gibt es einige Standards und Normen, die den Prozess und weitere Details des Risikomanagements darstellen. Im folgenden werden diese genannt und erklärt.

→ ISO 31000

ISO 31000 ist die erste weltweilt gültige ISO Norm (Standard) für Risikomanagement. Sie beinhaltet Definitionen und Begriffserklärungen. Weitere Inhalte sind Grundsätze des Risikomanagements, eine Beschreibung der Elemente des Risikomanagementsystems sowie eine Beschreibung des Risikomanagementprozesses.
Eine Zertifizierung nach der Norm ist allerdings nicht möglich.

Die ISO 31000 umfasst im Wesentlichen 5 Kapitel:

1. Anwendungsbereich
2. Begriffe und Definitionen
3. Grundsätze des Risikomanagements
4. Beschreibung des Risikomanagementsystems
5. Beschreibung des Risikomanagementprozesses

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

→ ISO/IEC 2700x

Im Bereich Informationssicherheitsmanagement ISMS (Information Security Management System) stellt die ISO 27005 eine genaue Anleitung zur IT Risikoanalyse und zum Risikomanagement im IT Bereich. Die ISO 27005 beinhaltet dabei einerseits eine Beschreibung des kompletten Risikomanagementprozesses als Ganzes und andererseits eine genaue Beschreibung der einzelnen Schritte des Risikomanagement und der Risikoanalyse. Die Anhänge der IEC 27005 liefern nützliche Informationen zur Etablierung eines Risikomanagement im Bereich Informationssicherheit und damit zur Erfüllung von Forderungen der ISMS Norm ISO 27001.

(*„ISO 27005 Einführung“.* URL: http://www.risikomanagement-wissen.de/ISO_27005_Einfuehrung.htm [Stand: 14.01.2014])

Der Sicherheits-Risikomanagement-Prozess orientiert sich an der ISO 31000 und ist nicht verpflichtend oder zertifizierbar.

→ BSI 100-3
Risikoanalyse auf der Basis von IT-Grundschutz

„Die IT-Grundschutz-Kataloge des BSI enthalten Standard-Sicherheitsmaßnahmen aus den Bereichen Organisation, Personal, Infrastruktur und Technik, die bei normalen Sicherheitsanforderungen in der Regel angemessen und ausreichend zur Absicherung von typischen Geschäftsprozessen und Informationsverbünden sind. Viele Anwender, die bereits erfolgreich mit dem IT-Grundschutz-Ansatz arbeiten, stehen vor der Frage, wie sie mit Bereichen umgehen sollen, deren Sicherheitsanforderungen deutlich über das normale Maß hinausgehen. Wichtig ist dabei, dass die zugrundeliegende Methodik möglichst wenig zusätzlichen Aufwand mit sich bringt und möglichst viele Ergebnisse aus der IT-Grundschutz-Vorgehensweise wiederverwendet. Vor diesem Hintergrund hat das BSI einen Standard zur Risikoanalyse auf der Basis von IT-Grundschutz erarbeitet. Diese Vorgehensweise bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit den IT-Grundschutz-Maßnahmen arbeiten und möglichst nahtlos eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten. Hierfür kann es verschiedene Gründe geben:

- Die Sicherheitsanforderungen des Unternehmens bzw. der Behörde gehen teilweise deutlich über das normale Maß hinaus (hoher oder sehr hoher Schutzbedarf).
- Die Institution betreibt wichtige Anwendungen oder Komponenten, die (noch) nicht in den IT-Grundschutz-Katalogen des BSI behandelt werden.
- Die Zielobjekte werden in Einsatzszenarien (Umgebung, Anwendung) betrieben, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Die Vorgehensweise richtet sich sowohl an Anwender der Informationstechnik (Sicherheitsverantwortliche und -beauftragte) als auch an Berater und Experten. Häufig ist es allerdings empfehlenswert, bei der Durchführung von Risikoanalysen auf Expertensachverstand zurückzugreifen."

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

→ **IDW PS 340**

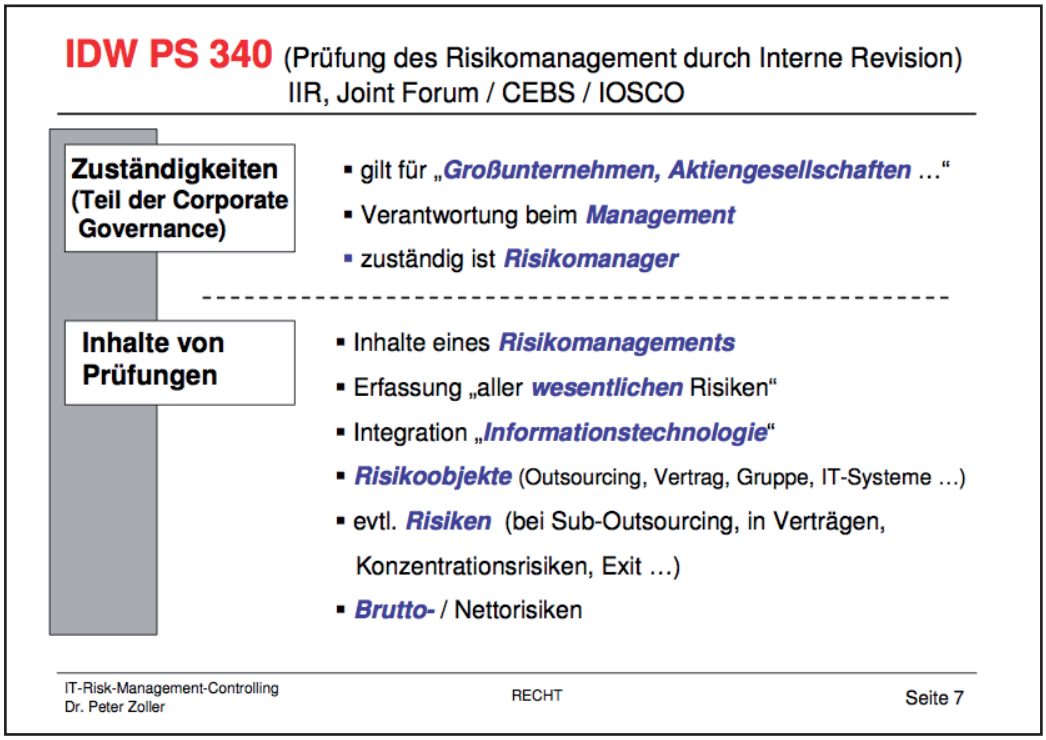

Abb. 3 Standard IDW PS 340
(Dr. Zoller, Peter (2013). *"Risikomanagement am Beispiel Projekt-Compliance & Projekt-Verträge"*. Foliensatz Gastvorlesung LMU Juristisches IT-Projektmanagement, Seite 7)

5.1 Frameworks

Frameworks bieten eine nicht rechtliche aber gute Orientierung für die Anwendung von Risikomanagement. Besonders ein, für die IT relevantes, möchte ich im folgenden vorstellen.

→ CobiT

„COBIT (Control Objectives for Information and Related Technology) ist das international anerkannte Framework zur IT-Governance und gliedert die Aufgaben der IT in Prozesse und Control Objectives (oft mit Kontrollziel übersetzt, eigentlich Steuerungsvorgaben, in der aktuellen deutschsprachigen Version wird der Begriff nicht mehr übersetzt). COBIT definiert hierbei nicht vorrangig wie die Anforderungen umzusetzen sind, sondern primär was umzusetzen ist. [...]
In Summe definiert das COBIT 5-Frameworks 37 IT-Prozesse, denen die Control Objectives zugeordnet sind.“

(*„COBIT“.* URL: http://de.wikipedia.org/wiki/COBIT [Stand: 19.01.2014])

6. Kerntätigkeiten und Methoden des Risikomanagements

6.1 Übergreifende Sicht

Der Prozess des Risikomanagements besteht primär aus 4 Kerntätigkeiten:
→ Risikoidentifikation
→ Risikobewertung
→ Risikosteuerung / Risikohandhabung
→ Risikokontrolle / Risikoüberwachung

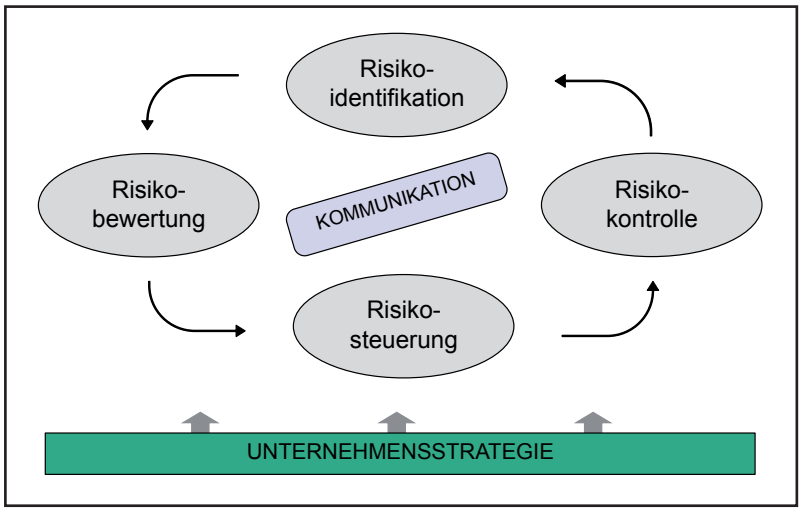

Abb. 4 Risikomanagement Zyklus

Diese vier Kerntätigkeiten bilden einen Kreis und können und müssen während eines Projektes beliebig oft wiederholt werden.
Üblich jedoch ist wie in der folgenden Grafik (Abb. 5) zu sehender Vorgang. Zu Beginn eines Projektes, noch in der Projektvorphase, eine ausführliche Risikoanalyse durchzuführen. Dies wird jedoch oft aufgrund dem mit einhergehenden hohen Extraaufwands von Vielzahl von Unternehmen gescheut. Der Nachteil aus einer nicht frühzeitig, sorgfältig durchgeführten Risikoanalyse zeigt sich allerdings leider meist erst, wenn der Schaden nicht mehr abwendbar ist.

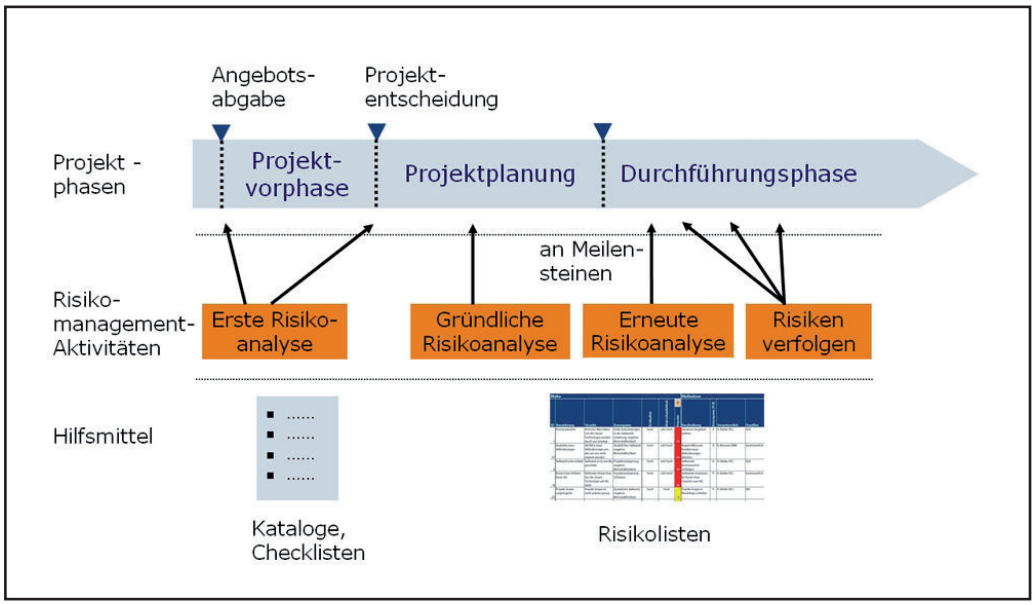

Abb. 5 Risikomanagement in den Projektphasen
(„Risikomanagement und Phasen des Projekts. Risikomanagement beginnt bereits in der Projektvorphase. (Method Park)“. URL: http://www.elektronikpraxis.vogel.de/themen/embeddedsoftwareengineering/management/articles/290447/ [Stand:10.01.2014])

Risiken, die aus einer ersten Analyse aufgedeckt wurden müssen über den Projektverlauf weiterhin gemonitort werden. Zudem ist es wichtig, weitere Iterationen durchzuführen um eventuell erst durch den Projektverlauf entstandene Risiken frühzeitig aufdecken und somit Schäden mindern oder ganz abwenden zu können und Potentiale zu erkennen.

Unternehmenspolitik

Eines der Ziele eines jedes Unternehmen ist unumstritten die Rentabilität. Eine Unternehmenspolitik bzw. Strategie gibt Klarheit über die Fragen: „Was? Wie? Wann?“. Sie zeigt auf, welche Vision erreicht werden soll. Sie umfasst die Maßnahmen und Entscheidungen die zu der Erfüllung der Vision verhelfen und setzt den zeitlichen Rahmen fest, häufig mit Zuhilfenahme von Meilensteinen.
Bereichsstrategien sowie die IT-Strategie und deren IT-Sicherheit arbeiten auf ein gemeinsames Ziel hin: Die Erfüllung der ganzheitlichen Unternehmensstrategie.

Ein sehr wichtiger und übergreifender Punkt im Risikomanagement stellt die diese Strategie dar. Sie sollte Anhaltspunkt und Ausgang zur Formulierung einer eigenen Risikopolitik sein. Eine Risikopolitik beinhaltet Grundsätze zum Umgang mit Risiken

und sie gibt Handlungsrichtungen und Prämissen zum Fällen von Entscheidungen vor. Sie zeigt zudem auf, was die maximale Risikoausprägung ist, die in Kauf genommen werden kann. Ein Ziel der Risikostrategie ist die Erfüllung der Unternehmensstrategie, daher sollte sie mit ihr in Übereinstimmung stehen.

Ein Widerspruch zwischen einer der erwähnten Strategien führt dazu, dass Bereiche, Teams oder Personen auf kontroverse Weise auf eine Vision oder verschiedene Visionen hinarbeiten.

6.2 Risikoidentifikation

Die Risikoidentifikation stellt die Sammlung aller aktueller und möglicher zukünftigen Risiken dar. Diese werden dabei in Form eines Szenarios dokumentiert. In diesem Prozess können die Risiken zudem geclustert werden, dies kann z.B. nach Fachbereichen, etc. geschehen.
Die Risikoidentifikation ist ein sehr wichtiger Prozess, da aufbauend auf dessen Ergebnis weitergearbeitet wird.

Eine gute und hilfreiche Methode zur Risikoidentifizierung, neben anderen Methoden, ist die SWOT-Analyse. Die Bezeichnung „SWOT“ basiert auf den englischen Begriffen Strengths (Stärken), Weaknesses (Schwächen), Opportunities (Chancen) und Threats (Gefahren).
In der Analyse werden die einzelnen Themen abgearbeitet und aus deren Matrix Situation gebildet. Die Analyse hilft dabei systematisch vorzugehen und auch Teilbereiche und Situationen zu betrachten, die auf den ersten Blick nicht sichtbar sind.

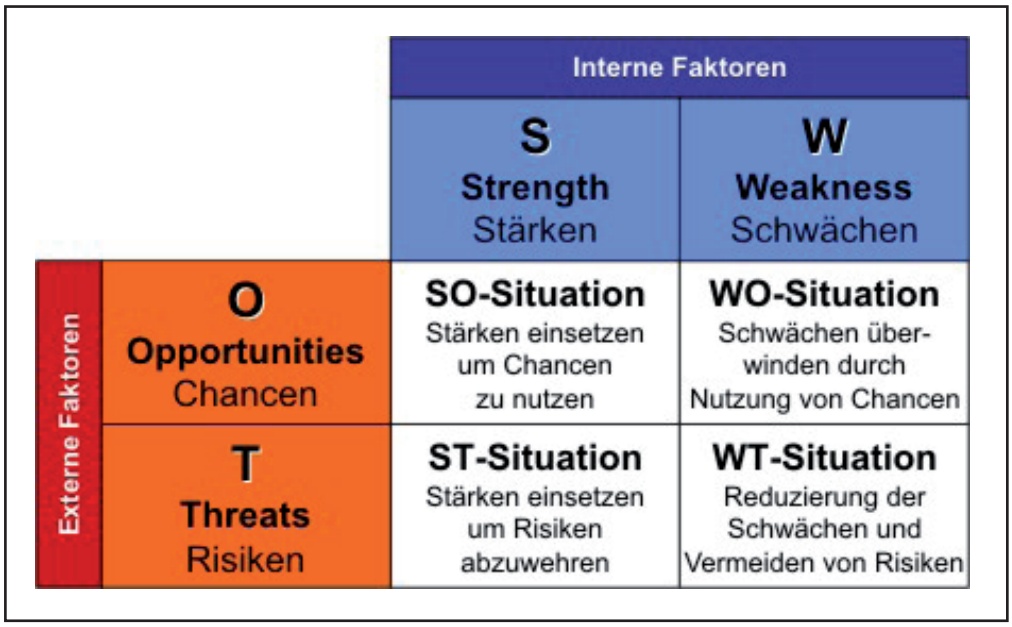

Abb. 6 SWOT-Analyse
(URL: http://www.thessenvitz.de/swot-analyse/ [Stand:12.01.2014])

In welchem Detail man die SWOT-Analyse durchführt ist je nach Projekt und Rahmenbedingungen variabel aber sich folgende Fragen zu stellen kann sehr hilfreich sein:

Strengths:	Was läuft gut? Was sind unsere Stärken? Worauf sind wir stolz? Wo stehen wir momentan?
Opportunities:	Was sind unsere Zukunftschancen? Was könnten wir ausbauen? Welche Verbesserungsmöglichkeiten haben wir? Was können wir in unserem Umfeld nutzen?
Weaknesses:	Was ist schwierig? Welche Störungen behindern uns? Was fehlt uns?
Threats:	Wo lauern künftig Gefahren? Was kommt an Schwierigkeiten auf uns zu? Was sind mögliche Risiken? Womit müssen wir rechnen?

Auf Basis einer sauberen SWOT-Analyse fällt es meist einfacher Risiken zu identifizieren. Sie bildet eine gute Grundlage und deckt alle Bereiche ab.

6.3 Risikobewertung

Die Risikobewertung beurteilt alle auf Grundlage der Risikoidentifikation gefundenen Risiken. Die Bewertung erfolgt üblicherweise in den Dimensionen **Eintrittswahrscheinlichkeit** des bestimmten Risikos und deren **Schadenshöhe** bei Eintritt. Häufig ist eine visuelle Darstellung der Risiken mit Hilfe einer Risikomatrix hilfreich.

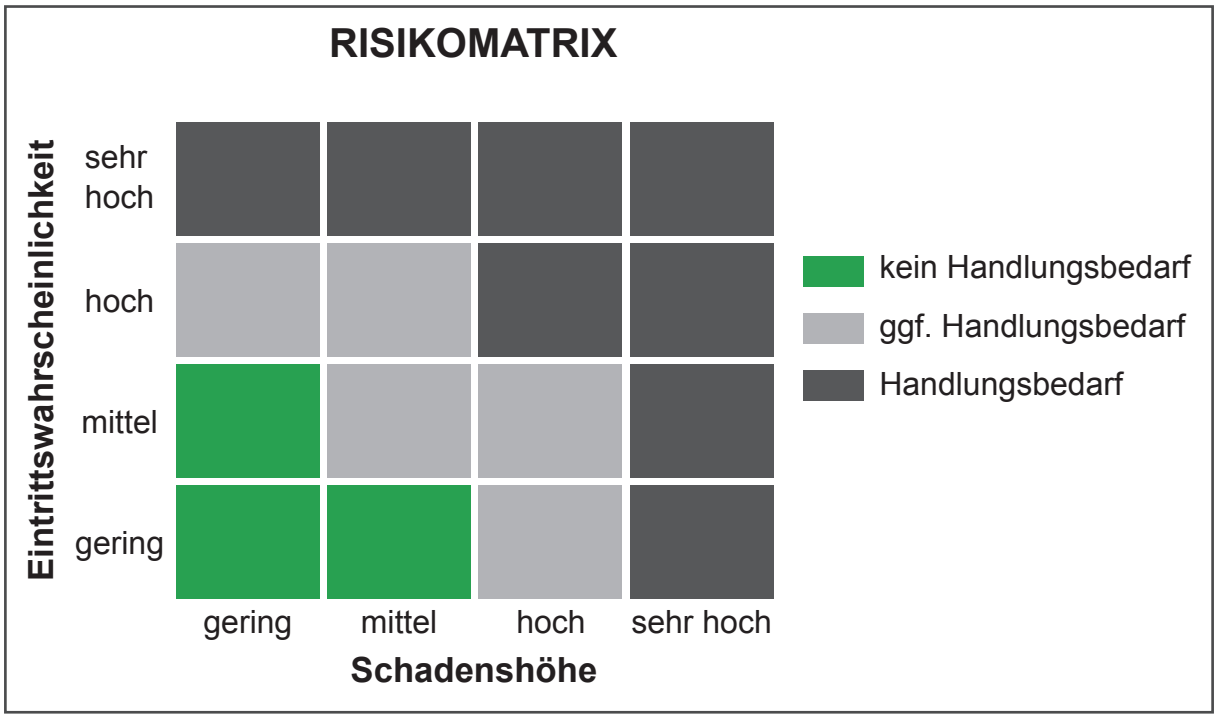

Abb. 7 Einfache Darstellung einer Risikomatrix

Diese Matrix kann an Komplexität durch die Zunahme der Anzahl der Unterteilungen von gering bis sehr hoch steigen. Die Matrix ist meist in drei Kategorien, veranschaulicht durch die drei Farben und deren Bedeutung „kein Handlungsbedarf“, „ggf. Handlungsbedarf“ und „Handlungsbedarf“ eingeteilt.
Die grüne Farbe stellt den Bereich „kein Handlungsbedarf“ dar. Diese Risiken können aufgrund ihrer geringen Eintrittswahrscheinlichkeit und deren geringen Schadensausmaß vernachlässigt werden. Im hellgrauen Bereich befinden sich die Risiken mit „ggf. Handlungsbedarf“. Diese Risiken müssen näher betrachtet werden, es bietet sich dort unter anderem die Verminderung oder Abwälzung (z.B. durch eine Versicherung) der Risiken. Risiken, die im dunkelgrauen Bereich platziert sind, sind durch akuten „Handlungsbedarf“ aufgrund der Höhe ihrer Eintrittswahrscheinlichkeit und ihres Schadensausmaßes gekennzeichnet.

Es empfiehlt sich zur Risikobewertung sowie auch zur Risikoidentifikation Workshops zu halten. Dabei sollten allen relevanten Fachstellen bzw. Arbeitsgruppen, auf die das Projekt eine Auswirkung hat, mit eingebunden werden.
Das Aufschreiben der Risiken auf kleine vorgefertigte Kärtchen bietet eine Möglichkeit diese im nächsten Schritt einfach und visuell in einer Matrix zu verorten bzw. von den Teilnehmern verorten zu lassen. Die Kärtchen können zudem Platz für Vorschläge für Maßnahmen, Verantwortliche etc. enthalten um Ideen gleich festzuhalten.

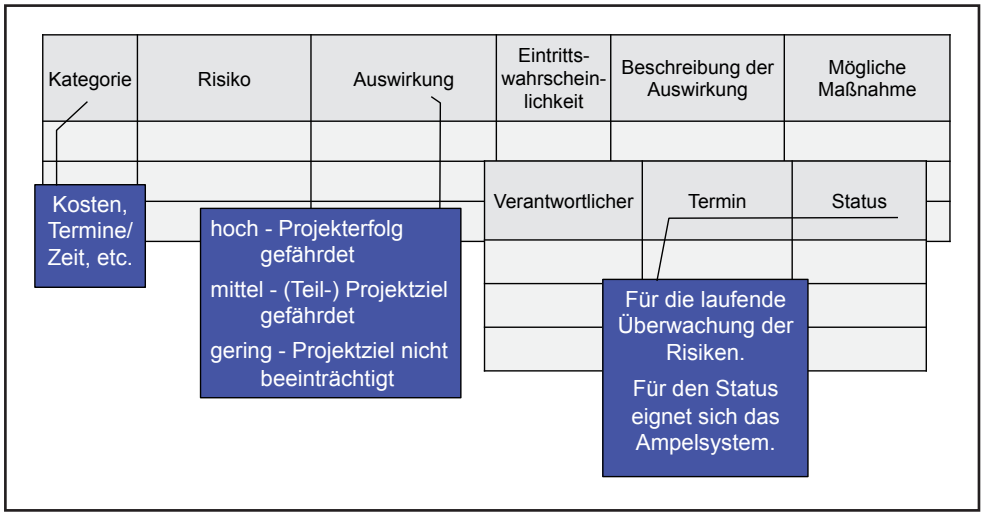

Abb. 8 Beispiel Risikoportfolio

Als Nacharbeit ist es empfehlenswert ein Risikoportfolio (Abb. 8) zu erstellen. Das ist ein Dokument (meist als Excel-Form) in dem die Ergebnisse festgehalten werden. Darunter fallen die Risiken, Auswirkungen, Eintrittswahrscheinlichkeit, verantwortliche Personen, etc. Dieses Portfolio kann auch, je nach Handhabung schon früher mit Lücken erstellt werden.

6.4 Risikosteuerung

Im Rahmen der Risikosteuerung müssen Möglichkeiten und Maßnahmen gefunden werden um mit dem Risiko umzugehen. Diese müssen immer im Einklang mit der Risikopolitik und der Unternehmensstrategie sein.
Dabei gibt es wie in der Risikobewertung schon angesprochen vier Hauptkriterien:

- **Vermeiden** – alle Gegenmaßnahmen, die das Risiko komplett abwenden

- **Mindern** – alle korrektiven und präventiven Maßnahmen, die ergriffen werden können, um bei einem eingetreten Risiko die Auswirkungen zu verringern beziehungsweise so gering wie möglich zu halten
- **Überwälzen** – z.B. Versicherung für das Projekt abschließen oder das Risiko an andere Projektmitglieder (z.B. Lieferanten) auslagern
- **Selbst tragen (Zuschläge und Reserven)** – das Risiko in Kauf nehmen, einkalkulieren für den Fall, dass es eintritt und Kosten selbst tragen

(vgl. *„Projektrisikomanagment“*. URL: http://www.kraus-und-partner.de/projektmanagement/grundlagen/projektrisikomanagement [Stand. 10.01.2014])

In der folgenden Grafik (Abb. 10) ist der Prozess nochmals sehr gut beschrieben. Es ist auch mit einer sehr guten Risikoidentifikation nie möglich sicherzustellen, dass alle Risiken erkannt wurden. Die Grafik teilt die Risiken und deren Handhabung auf.

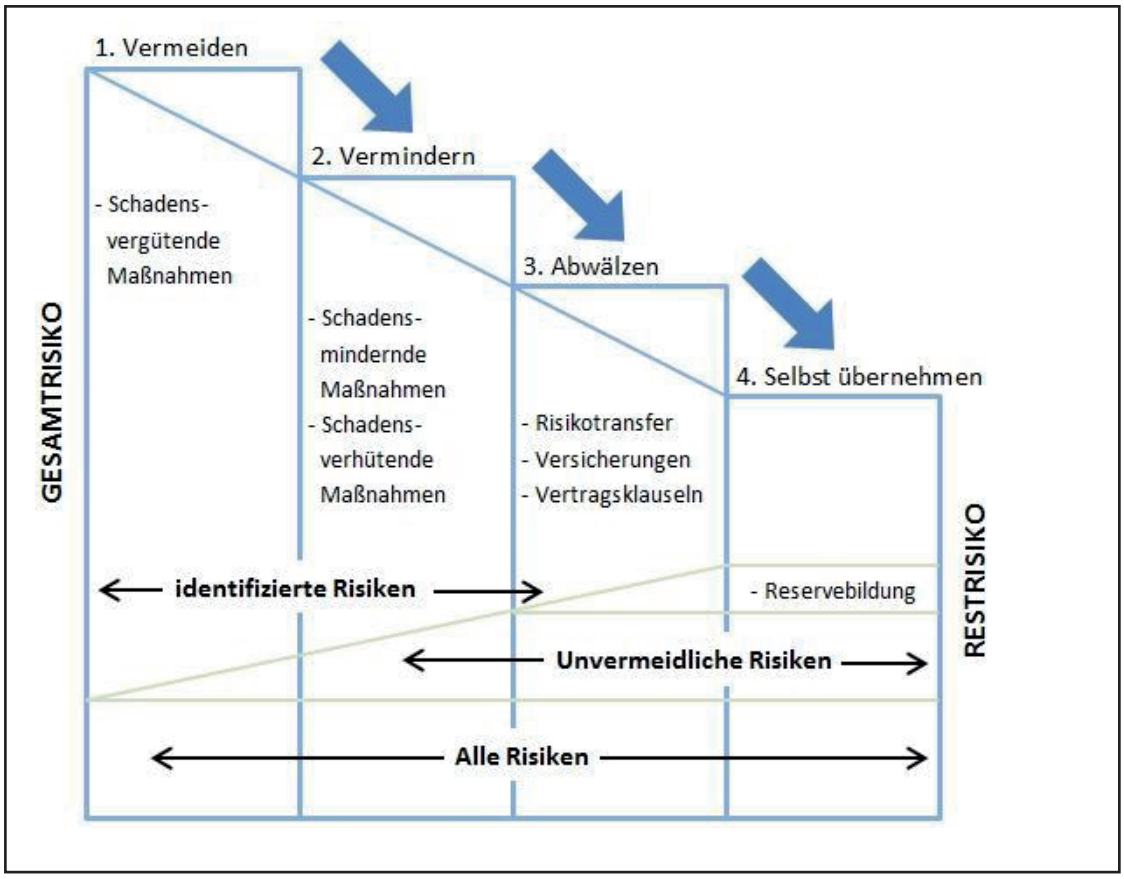

Abb. 9 Risikosteuerung
(Einerhand, Johanna (2011). *„Risikosteuerung – wie können Risiken in der Landwirtschaft gesteuert werden?“.* URL: http://web.altagenetics.com/germany/Article/Print/1083 [Stand: 13.01.2014])

6.5 Risikokontrolle

Die Risikokontrolle stellt eine laufende Tätigkeit des Risikomanagements dar. Sie stellt sicher, dass das erstellte Risikoprofil und deren Maßnahmen mit den laufenden Tätigkeit im Projekt bzw. im Unternehmen übereinstimmen. Von Vorteil ist es dabei einen Standard-Prozess bzw. ein Berichtswesen zu implementieren, dass die aktuelle Situation aufzeigt.

7. Fazit / Erkenntnisse

→ 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

QUELLEN

(Hopp, K. U. (2001). *„GmbH-Risikomanagement zur Unternehmenssicherung und Haftungsbegrenzung“*. Bonn: VSRW-Verlag, S. 20.)

(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])

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

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

(Dr. von Holleben, Kevin Max & Winters, Fabian (18.10.2013) *„Risiko-Management ist eine juristische Pflicht“*. URL: http://www.computerwoche.de/a/risiko-management-ist-eine-juristische-pflicht,2547615 [Stand: 14.01.2014])

(vgl. Herke, Martin Dieter (Ausgabe 04/2005), Seite 99. *„Risikomanagement entsprechend dem KonTraG“*. URL: http://www.iww.de/bbp/archiv/gesetz-zur-kontrolle-und-transparenz-im-unternehmensbereich-risikomanagement-entsprechend-dem-kontrag-f24228 [Stand: 14.01.2014])

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

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

(*„ISO 27005 Einführung“.* URL: http://www.risikomanagement-wissen.de/ISO_27005_Einfuehrung.htm [Stand: 14.01.2014])

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

(Dr. Zoller, Peter (2013). *“Risikomanagement am Beispiel Projekt-Compliance & Projekt-Verträge“*. Foliensatz Gastvorlesung LMU Juristisches IT-Projektmanagement, Seite 7)

(*„COBIT“.* URL: http://de.wikipedia.org/wiki/COBIT [Stand: 19.01.2014])

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

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

(vgl. *„Projektrisikomanagment“*. URL: http://www.kraus-und-partner.de/projektmanagement/grundlagen/projektrisikomanagement [Stand. 10.01.2014])

(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])