



# Risikomanagement

## Haken und Ösen in der Praxis



# Warum Risiko-Management?

## 1. Unternehmerisch-strategische Motivation

- Zur **Priorisierung von Prozessen** und Prozesszielen im Sinne der Sicherstellung des Unternehmenserfolgs.
- Im Rahmen des zukunftsorientierten **strategischen Controlling**.

## 2. Zielorientiert-kulturbildende Motivation

- Denken in Risiken als **intrapreneurische Erweiterung** der Management-Aufgabe.

## 3. Als Erweiterung des Sicherheitsmanagement-Prozesses

- Risikomanagement-Prozess als **integrative Funktion** zwischen Unternehmenssteuerung/Controlling und IT-Sicherheitsmanagement.

## 4. Weil's vom KonTraG/HGB so vorgeschrieben ist!!

- „Wir müssen uns mal wieder mit Risiko-Management beschäftigen, in zwei Monaten kommen die Wirtschaftsprüfer!“
- „Was muss ich tun? Mein Chef sagt, das Risikoinventar muss bis morgen Abend fertig sein, was immer das sein soll!“



# Gemeinsames Verständnis „Risikomanagement“

## Konzept „Risiko“

- **kalkulierte Prognose** eines möglichen Schadens bzw. Verlustes im negativen Fall oder eines möglichen Nutzens bzw. Gewinns im positiven Fall.
- Sicherheitsmanagement: Produkt von *Eintrittswahrscheinlichkeit* x *Ereignisschwere*
- Betriebswirtschaftslehre: Risiko als Wagnis -> **kalkulatorische Kosten**.
- Quantitative Risikobewertung: *Eintrittshäufigkeit* x *Schadensausmaß*
- Risiko ist **Antonym von Sicherheit!**
- *Hint: Risikomanagement kennt Kennzahlen!*

## Konzept „Management“

- Taylor: Planen, Organisieren, Koordinieren, Kontrollieren
  - *direktiv*
- Mintzberg, Stähle, et al.
  - Systematische Arten & Weisen der Informationsverteilung
  - Sonderbehandlung wichtiger Vorfälle (Priorisierung)
  - Verbindlichkeiten in Vorteile wandeln und Wünsche in Verbindlichkeiten wandeln (Explizite Information mit Handlungsrelevanz)
  - *prozessual*



## Fazit: „Ja was nun?“

- **Aus zwei Konzepten lässt sich weder Theorie noch Modell ableiten**
  - Risikomanagement als Menge von **Teilfunktionen der Management-Aufgabe**.
  - Risikomanagement ähnelt dem allgemeinen Management: *Es gibt wenig Informationen darüber, wie es gut funktioniert, aber unzählige Literatur dazu, was man tun sollte.*
- **Es existiert oft kein einheitliches Risikoverständnis im Unternehmen**
  - Als „neue“ Management-Aufgabe **per Definition, nicht per Konsens** herbeigeführt.
  - Priorisierung in schnellebigen Märkten, die hohen operativen Aufwandsanteil haben, auch ohne Risiko-Management schwierig genug.
  - Sicherheitsmanagement und Risikomanagement **behandeln Risiken nicht einheitlich**, obwohl der Sicherheitsmanagement-Prozess in den Risikomanagement-Prozess integriert sein sollte.
    - Sicherheitsmanagement: Gefährdung-/Maßnahme-Zusammenhang.
    - Risikomanagement: Risiko/Strategie-Zusammenhang.



# Fokussierung auf geschäftskritische Risiken

## Isolierte Betrachtung geschäftskritischer Risiken

- ist für direktive Unternehmenssteuerung **alleine nicht ausreichend**.
- bedingt jedenfalls ein **zweites Steuerungssystem** neben dem regulären Controlling-Instrumentarium.
- wirft eine weitere Frage auf: „*Was bitte ist geschäftskritisch?*“

## Gesamtbetrachtung geschäftskritischer Risiken fordern

- vorhandenes **business alignment** von operativen Prozessen und Geschäftsprozessen.
- operative **Prozessreifegrade** auf Stufe „**messbar**“.
- detailliertes **Verständnis der Geschäftsprozesse** durch das operative Management.

## Formalisierung des Risikomanagement

- Prozesse sind formalisierbar.
- Inhalte sind schwer formalisierbar. Unternehmerische Schwerpunkte sind in schnell wandelndem Umfeld ebenso volatil.
- Für spezielle Bereiche entstehen sehr unübersichtliche Risiko-Kataloge.



# Risiko-Erhebung (I)

## Probleme bei der Risiko-Erhebung

- Unklarheit der Begriffe **Risiko** <-> **Ursache** (Rekursivität der Risiken)
  - Umsatzziele nicht erreicht, weil Absatz zu gering.
  - Absatz zu gering, weil Verkaufssystem ausgefallen.
  - Verkaufssystem ausgefallen, weil Software-Fehler.
  - Software-Fehler, weil unzureichendes Qualitätsmanagement.

## Für Management unzureichend beantwortete Fragen

- Wie unterscheiden sich Risiko und zugehöriges Prozess-Ziel?
- Wie ordne ich Risikomanagement in eine Balanced Scorecard ein?
- Wie stehen Risikokennzahlen im Zusammenhang mit meiner Prozesskontrolle/Zielvereinbarung?
- Welcher „normale“ Bereichsleiter, der einen Bereich bzw. ein Produkt zu entwickeln hat, soll oder will das eigentlich noch alles verstehen??



## Risiko-Erhebung (II)

### Tätigkeiten des Managers (nach Mintzberg)

- **50%** aller Aktivitäten eines Managers dauern **weniger als 9 Minuten**
- Im Schnitt beschäftigten sich Manager nur **2 Mal pro Woche** länger als 30 Minuten mit einem Thema am Stück.
- Manager haben im Tagesgeschäft die Aufgabe, Störungen wichtiger Vorgänge zu priorisieren.
- Wie hoch ist dabei die Motivation des Managers für das langfristige Risiko-Management?

### Problem bei multinationalen Konzernen

- Risikoaggregation über Sprachbarrieren hinweg

### Problem auch bei nationalen Unternehmungen

- Zentrale „Übersetzung“ notwendig.
- Fähigkeit operativer Führungskräfte im geschäftsprozessrelevanten Sprachspiel treffend zu strukturieren und zu formulieren oft ungenügend ausgeprägt.



# Risikoklassifizierung

## Probleme bei der Risikoklassifizierung

- **Stark unterschiedliche Bewerter:**
  - Gruppe 1 bewertet alles übervorsichtig und überkritisch
  - Gruppe 2 bewertet alles vernachlässigend
  - Gruppe 3 bewertet alles „im Mittelmaß“
  - einheitliche Bewertung erst durch **zentrale Revision** sicherstellbar.
  - Hoher kommunikativer Aufwand!
- Vergleichbarkeit qualitativ bewerteter Risiken fast unmöglich
  - Auch semiquantitatives Modell schafft wenig Abhilfe, steht doch immer gleich der Gesamtwert des Bereiches zur Disposition.
- Risikoausmaß stark von **Prozess- u. Projektgestaltung** abhängig
  - Wenn einzelne Risiken den kompletten Bereich infrage stellen, dann ist das eher eine fragwürdige Produkt-/Unternehmensstrategie und **keine Missionsaufgabe des Risikomanagements!**
  - Risiko-Management ersetzt keinen mangelhaften Planungs- und Kontrollprozess!



# Risikokontrolle

## Systembruch zwischen Risikomanagement- und Projektssystem

- Risikomanagement erfindet das **Projekt-Rad** neu: Gängige Risikomanagement-Systeme bieten die Möglichkeit, Projekte zu erfassen und deren Risiken zu planen.
- Projekte werden so mit zugehörigen Risiken verwaltbar.
- Was man eigentlich will: **Verknüpfung eines Risikos mit einem externen Projekt.**
- Lediglich gute Controlling-Instrumentarien für diese projektbezogenen Risiken

## Controlling-Funktionalitäten in RM-Software sind

- überwiegend auf einer sehr rudimentären Entwicklungsstufe
- beschränken sich auf das zwingend notwendige Maß
- Fehlen:
  - Umfangreiches **Tagging**, **Gruppenbildung**, spezielles Controlling auf gruppierten Risiken (z.B. Status-Tracking speziell projektierter Risiken innerhalb des RM-Systems)
  - Soll-/Ist-Vergleiche beim Risiko-Controlling, z.B. über Projektfortschritt bzw. **operativer Zwang**

## Sehr wenige SW-Systeme für operative Risiken (Prozessrisiken)

- Mehrheit der SW-Systeme aus dem Versicherungs-/Anlagebereich.



# IT-Risikomanagement (I)

## Spezielle Probleme des IT-Risikomanagements

- Aus dem **Sicherheitsmanagement** stammende Gefährdungskataloge sind oft sehr **umfangreich** und **nicht verdichtet**.
- Geschäftskritische Risiken sind **kaum ermittelbar**, **selten bezifferbar**, deshalb teilweise **nicht mehr versicherbar**.
  - Eine einzelne preisgegebene Kreditkarteninformation kann im journalistischen Sommerloch verheerende Auswirkungen haben.
- IT-Risikomanagement u. Sicherheitsmanagement nehmen **sich häufig zu wichtig**
  - Aufgrund des o.g. Sachverhalts sind **nicht** automatisch **alle IT-Risiken geschäftskritisch**.
  - IT-Sicherheitsmanagement ist ebenfalls nur ein Patchwork und keine lückenlose Strategie!
  - Es gibt in Unternehmen bedeutendere Risiken als IT-Risiken. Umfangreiche IT-Risikokataloge verzerren aber mengenmäßig das Bild.
- **Risikoakzeptanz** ist im Sicherheitsmanagement **keine allgemein akzeptierte Strategie**
  - IT-Risikomanagement wird zum Kostentreiber
  - Es muss ein unternehmerisches Restrisiko bleiben, sonst würden nur Versicherungen an Unternehmen verdienen, auch wenn das Sicherheitspersonal das anders sieht.



# IT-Risikomanagement

## Spezielle Probleme des IT-Risikomanagements

- **Absolutismus-Denken** bei IT-Risiken
  - „*Dieser Fall darf unter keinen Umständen eintreffen!*“
  - Prüft man die tatsächliche Geschäftsprozessrelevanz so kommt man auf strategischer bzw. taktischer Ebene zu einem völlig anderen Schluss.
- **Business-Continuity-Management** hat seine Berechtigung!
  - Der Ernstfall wird eintreffen!
  - Manchmal ist es besser, eine Strategie für den Ernstfall zu haben, anstatt Millionen in dessen Vermeidung zu stecken.
  - Angst ist eine Folge der **Trennung von Eigentümerschaft und Management**.  
Eigentümer sind als Unternehmer oft risikobereiter, da sie an potentiellen Erfolgen stärker partizipieren.
- Patches, Workarounds, **Bugs**
  - Risiken, deren Eintreffen 1 x im Monat fest geplant wird, sind kein Fall für das Risikomanagement.
  - Sie sind Bugs, um die sich das Qualitätsmanagement kümmern sollte!



# Zusammenfassung

**Es gibt viel zu tun!**

**Packen wir's an!**

**Vielen Dank für Ihre Aufmerksamkeit!**