Themenfeld 8

Risikoanalyse

Exkurs

IT-Risikomanagement

Motivation

Ziele eines Unternehmens

- Gewinnoptimierung, Marktetablierung, Existenzsicherung, ...

Betrachtung von Risiken

- essenzieller Bestandteil unternehmerischen Handelns

Risiken nicht nur als Gefahr ansehen

- Chance und notwendige Voraussetzung für die Zielerreichung

Risiken nicht rein negativ beurteilen

- mit Risiken richtig umgehen
- Risiken in Chancen umwandeln

Unternehmen muss jederzeit in der Lage sein

- unternehmensweit konsistente Ertrags- und Risikoinformationen zu ermitteln

Effizientes Risikomanagement von strategischer Bedeutung

- wenn Risiken gesteuert und kontrolliert werden, trägt dies positiv und langfristig zu Unternehmenserfolg und Wachstum bei

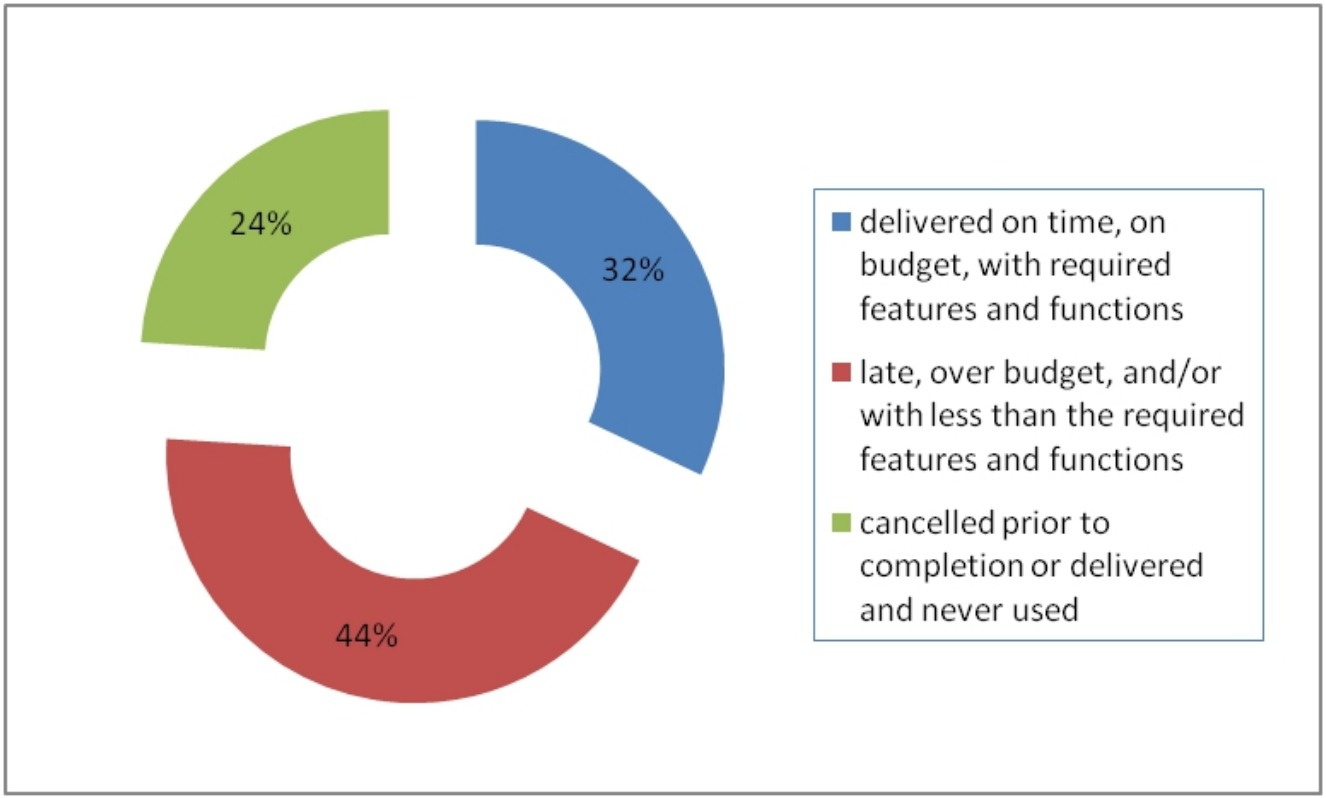
Doppelrolle der Informationstechnologie

- Voraussetzungen für die Aggregation von Daten zu aussagefähigen Ertrags- und Risikoinformationen
- Erzeugt selbst Risiken

Motivation

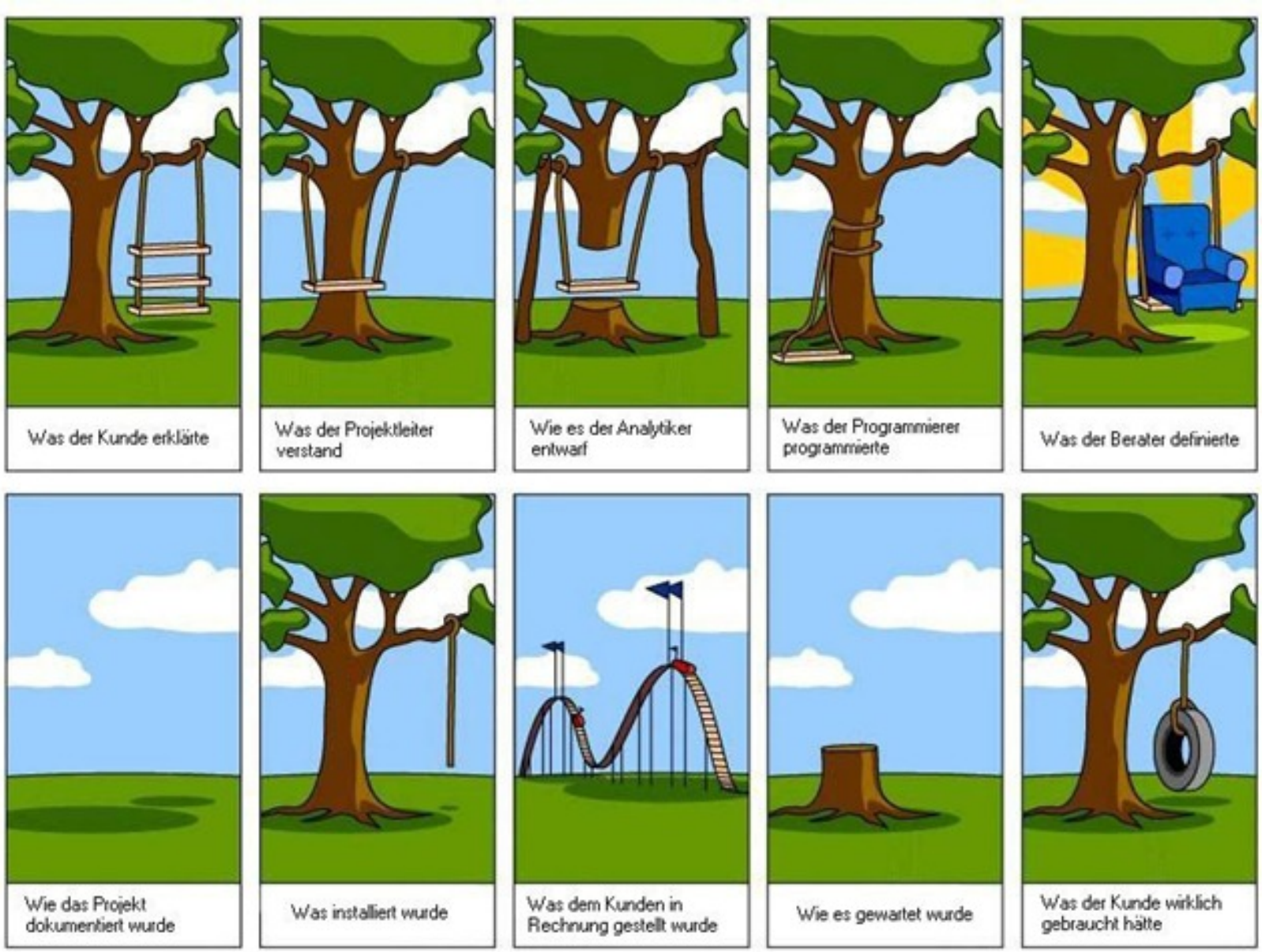
Standish Group im Jahre 2009 Umfrage

- Nur ein Drittel aller IT-Projekte werden im geplanten Zeit- und Budgetrahmen beendet
- fast die Hälfte diese Vorgaben nicht erfüllen
- der Rest wird abgebrochen



Motivation

IT-Projekte



Risikobegriff

„Risiko“ wird unterschiedlich beschrieben

- je nach Betrachtungsweise

Entscheidungsorientiert

- Abweichung/Varianz von Zielgrößen und Erwartungsgrößen
- Abweichung kann positiv oder negativ sein
- Je höher die Standardabweichung, umso größer das Risiko

Ausfallorientiert

- negative Abweichung des realisierten Ergebnisses vom Erwartungswert

Risiko = Eintrittswahrscheinlichkeit x Auswirkungen

- Einfache Gleichung für das Risiko
- Je geringer die Eintrittswahrscheinlichkeit, umso seltener
  - die Gefahr
  - die Chance
- Auswirkungen sind ungünstige Effekte, sollte das Risiko eintreten

Risiken sind Teil des Geschäftes

- Einige der Risiken spielen dabei nie eine Rolle, andere können bedrohlich werden.
- Risikomanagement hilft, Risiken zu erkennen, zu analysieren, zu bewerten und mit den entsprechenden Techniken abzuschwächen.

Methoden

- BSI-Standard 200-3
  - Risikoanalyse auf der Basis von IT-Grundschutz
- klassische Risikoanalyse
  - ISO 27001, 27005, 31000, 31010
- Penetrationstest
- Differenz-Sicherheitsanalyse

Risikomanagement
Bedeutung

Risikomanagement gewinnt an Bedeutung

- strategischen Bedeutung von IT-Projekten
- IT-Projekte werden anspruchsvoller und komplexer

Gründe

- Expansion / Globalisierung der Geschäftstätigkeit
- Automatisierung von Geschäftsprozessen
- Steigende Abhängigkeit von Verfügbarkeit und Sicherheit der Datenverarbeitung
- Neuartige Geschäftsprozesse aufgrund steigender Marktdynamik durch neue Technologien
- Inhärenten Risiken bei IT-Projekten im Vergleich zu anderen Projekten

Beispiel Softwareentwicklung

- technologisches komplexes und dynamische Umfeld
- Software als ein immaterielles Gut
  - Fertigstellungsgrad und Qualität können durch menschliche Sinne nur schlecht erfasst werden
- Aufwandsschätzung schwierig
  - fehlende Erfahrungswerte
    - technologischer Wandels
    - spezifischen Erfordernissen
  - Entwicklungsschritte sind schwer messbar
    - bestimmte Anforderungen werden erst in der Testphase erkannt
    - nicht schon in der Design- oder Entwicklungsphase
- hohe Einarbeitungszeit und sich ändernden Anforderungen während der Projektlaufzeit
  - Wegen komplexer Technologien kurzfristige Einarbeitung neuer Mitarbeiter nur schwer möglich
  - Anforderungen ändern sich aufgrund gesammelter Erfahrungen während der Projektlaufzeit

Risikomanagement umfasst

Festlegungen von Zielen auf Basis der Definition einer Strategie

- ggf. auch Visionen der das Risikomanagement anwendenden Stelle
- Ohne konkrete Ziele lassen sich keine Abweichungen messen

Definition von Werttreibern oder kritischen Erfolgsfaktoren zur Erreichung von Zielen

Festlegung einer Risikomanagement-Strategie

- abhängig von der Risikobereitschaft
- risikoavers, risikoneutral oder risikofreudig

Identifikation von Risiken

Bewertung/Messung von Risiken

Bewältigung von Risiken

Steuerung der Risikoabwehr

Monitoring, also Früherkennung

Strukturierung und Dokumentation in einem Risikomanagementsystem

Prozesse im Risikomanagement

Risikomanagementprozess

Phasen

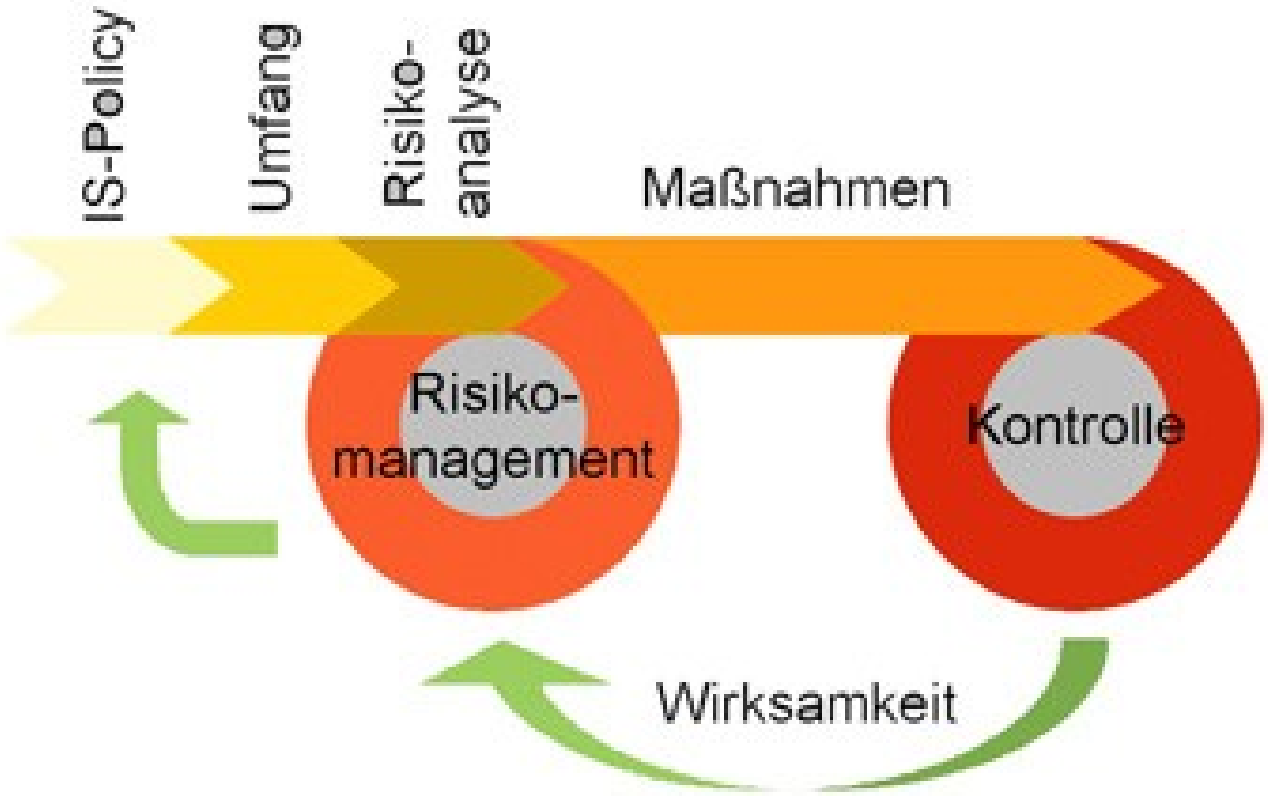
Risikoanalyse

Risikobewertung

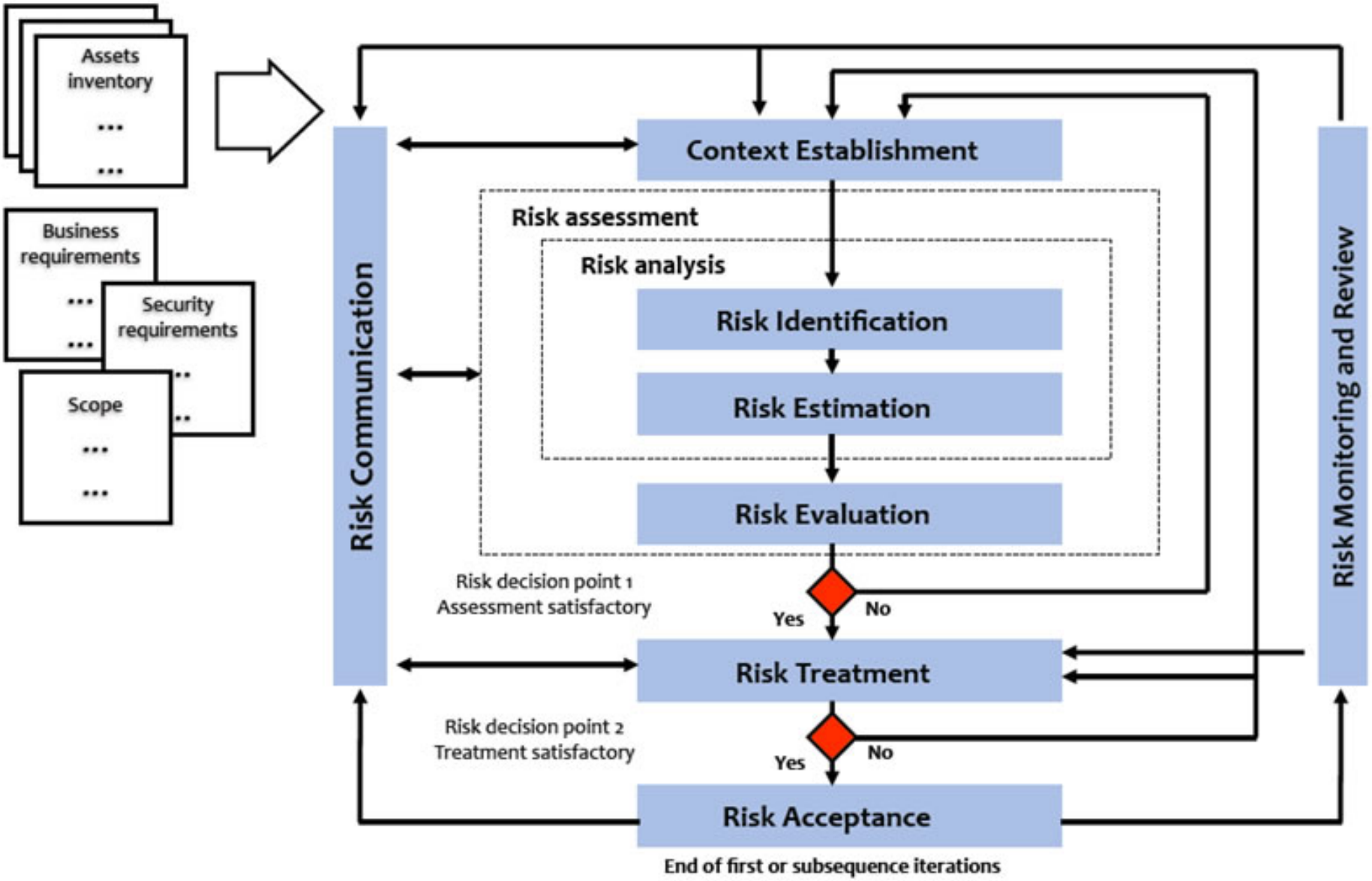
Risikominimierung

Risikokontrolle

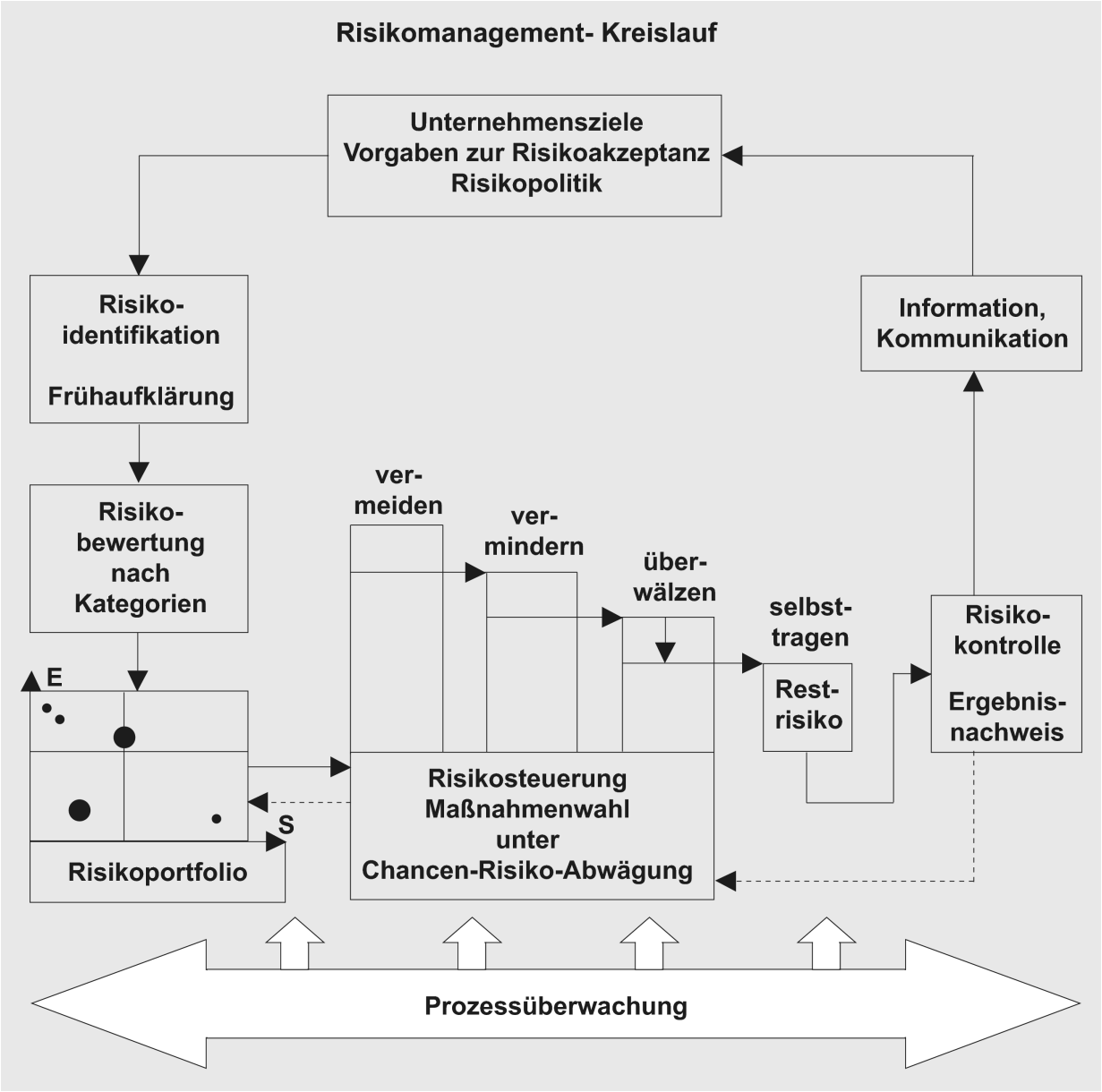
Risikoverfolgung



Informationssicherheit-Risikomanagement-Prozess



Informationssicherheit-Risikomanagement-Prozess



Risikomanagement

Teile des Risikomanagements

Erkennung und Bewertung von Risiken

Erarbeitung und Umsetzung von Maßnahmen

- optimale Lösung finden
- Risiken auf akzeptable Restrisiken reduzieren
- wichtigste Gefahrenquellen erkennen und abschwächen

Für jeden dieser Prozesse gilt

- In Abhängigkeit der Bedürfnisse
  - wird der Aufwand einer oder mehrerer Personen gefordert
- Jeder Prozess wird mindestens einmal durchlaufen
- Jeder Prozess tritt in einer oder mehreren Projektphasen auf
- Überschneidung der Prozesse ist möglich

Risikomanagement

Risikomanagement-Prozesse

Risikomanagementplanung

- Wie wird das Risikomanagement organisiert?
- Wie viel Risikomanagement ist nötig?
- Haben wir Erfahrungswerte in dieser Projektart?
- Zuständigkeiten
- Checklisten

Risikoidentifikation

- Identifizierung potenzieller Risiken
- Dokumentenanalyse
- Brainstorming
- SWOT-Analyse
- Ursache-Wirkungs-Analysen

Qualitative Risikoanalyse

- Eintrittswahrscheinlichkeit sowie Auswirkung
- Priorisierung (z.B. A, B und C-Risiken)

Quantitative Risikoanaylse

- i.d.R. bei hoch priorisierten Risiken
- Erweiterte Spezifizierung von Risiken
- Szenariensimulation

Risikobewältigunsplanung

- Gegenmaßnahmen

Risikoüberwachung und -steuerung

- Identifizierung/Lösung potenzieller oder eingetretener Risiken
- während dem gesamten Lebenszyklus

Weitere Risiken

IT-Operations (Risiken aus dem laufenden Betrieb)

- Administrative Fehler
- Systemausfall

IT-Security (Sicherheitsrisiken)

- Unzureichende Sicherheits- und Schutzmaßnahmen für IT-Systeme
- Fehlende Autorisierung und Authentifizierung für Datenzugriff und -austausch
- Nicht näher spezifizierte Risiken
  - Fehlende Akzeptanz / Ablehnung der Anwender gegenüber neuer Software
  - Konzeptionierungsfehler

Aufgrund der beschriebenen Problematik ist erkennbar, dass das Risikomanagement fester Bestandteil aller IT-Projekte sein sollte.

Prozesse im Risikomanagement

Risikomanagementplanung

Wie sollen die Aktivitäten des Risikomanagement durchgeführt werden?

- Risikomanagementplanung legt Vorgehensweise fest

Planung soll sicherstellen

- Risikomanagement ist in Bezug auf Risiken und der Bedeutung des Projektes angemessen
- Es stehen ausreichende Ressourcen für die Aktivitäten zur Verfügung

Erfolgschancen erhöhen

- gut strukturierte und sorgfältig vorbereitete Planung
- erleichtert Durchführung der anderen Risikomanagement-Prozesse

Erstellung eines Risikomanagementplans

Zusammenarbeit mit

- Projektleitern und -mitgliedern
- Stakeholdern
- für das Risikomanagement im Unternehmen zuständige Mitarbeiter

Auswirkungen haben dabei Risikobereitschaft und Risikotoleranz

- des Unternehmens und
- der Projektbeteiligten

Hilfreich zur Erstellung

- bereits definierte Ansätze und Konzepte für das Risikomanagement im Unternehmen
- allgemein oder aus vorangegangenen Projekten

Inhalte

Methodologie

- Ansätze, Werkzeuge und Datenquellen für das Risikomanagement

Rollen und Verantwortlichkeiten

- Organisation des Projektteams, Hierarchien

Budgetierung

- Kostenschätzung, benötigte Einsatzmittel

Zeitliche Planung

- Festlegung von Terminen für die Ausführung des Risikomanagement-Prozesses während der Projektlaufzeit

Risikokategorien

- Strukturen für die Risikoidentifikation festlegen

Definition der Risikowahrscheinlichkeiten und -auswirkungen

- als Unterstützung der Risikoanalyse

Prozesse im Risikomanagement

Risikoidentifikation

Für eine Beherrschung der Risiken, muss man diese zunächst kennen

- Bestimmung von Risiken unterschiedlicher Art

Kontinuierliche Durchführung und Bestimmung

- einzelne Risiken sind zu Beginn nicht absehbar
- es entwickeln sich neue oder übersehene Risiken
- Projektteam sollte in den Prozess einbezogen werden, damit es sich für die Risiken und die entsprechenden Risikobewältigungs-maßnahmen zuständig und verantwortlich fühlt.

Nach Identifizierung von Risiken

- Priorisierung mit Hilfe der Risikoanalyse

Risikokategorien

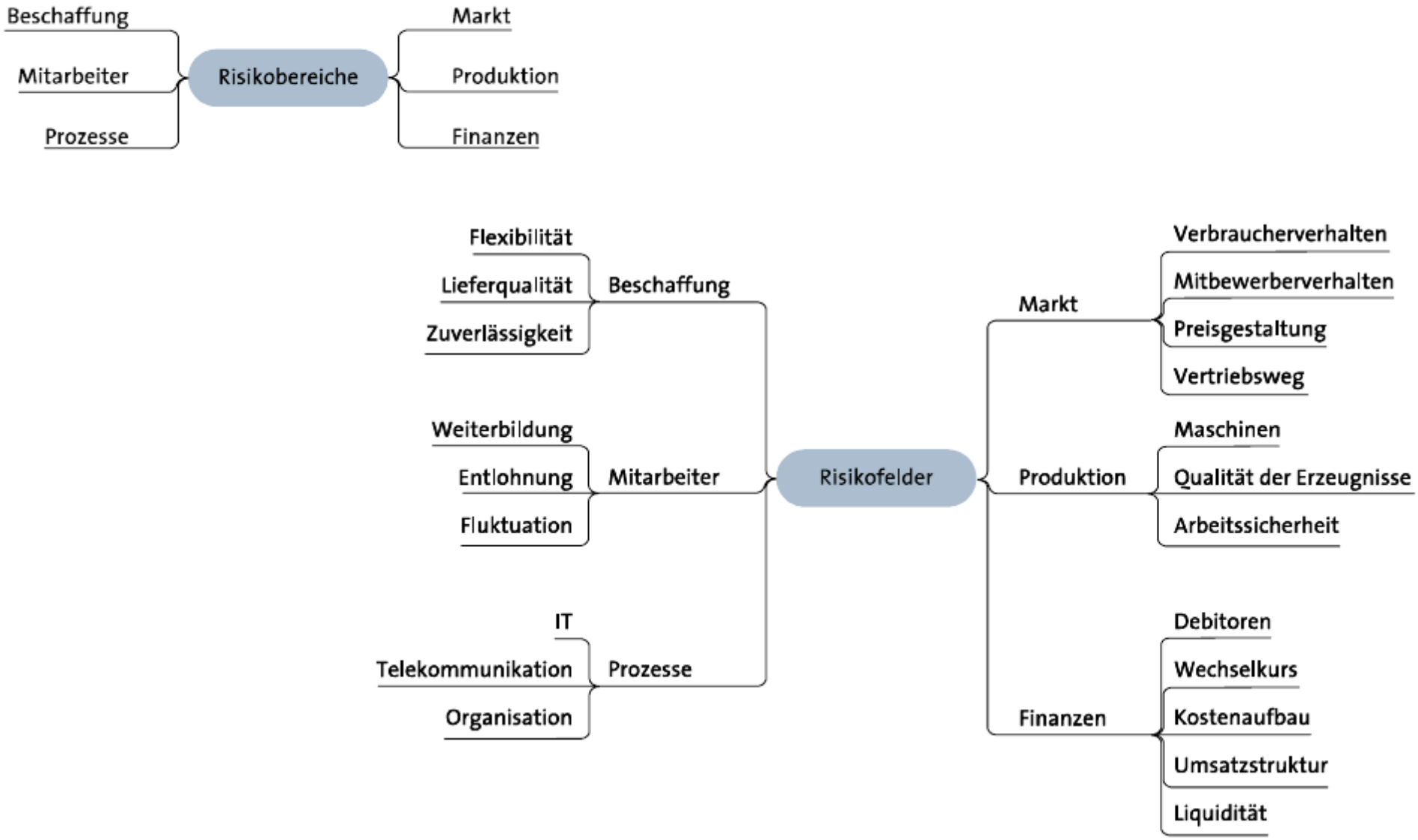
- Für eine systematische Identifizierung der Risiken ist es wichtig, die verschiedenen Kategorien von Risiken zu kennen
- Die Unterteilung kann dabei je nach Verständnis, Betrachtungsweise und Kontext unterschiedlich sein.
- Im betriebswirtschaftlichen Sinne gibt es z.B. die Unterscheidung von externen, internen, finanziellen und operativen Risiken.

Klassifizierung von Risiken

- Marktrisiken
  - z.B. schlechte Absatzzahlen, Kundenverlust, Portfolio nicht marktgerecht
- Geschäftsrisiken
  - z.B. falsche Produktstrategie, Kostenstrukturrisiken, Budgetengpässe, zu geringe Eigenkapitalquote
- Projektrisiken
  - z.B. unzureichende Planung, Terminverschiebungen, Anforderungen ändern sich
- Technische Risiken
  - z.B. Lösung lässt sich nicht integrieren, falsche Architekturen, Entwicklungswerkzeuge funktionieren nicht

Prozesse im Risikomanagement

Risikoidentifikation



Prozesse im Risikomanagement

Methoden der Risikoidentifikation

Brainstorming

- Innerhalb einer Arbeitsgruppe Ideen sammeln
- ermöglicht die Identifikation von Risiken in kurzer Zeit
- Quantität geht (zunächst) vor Qualität
  - wie im Brainstorming üblich, ohne Äußerung von Kritik
- Auswertungsphase
  - anschließend werden die Vorschläge bewertet und genauer definiert

Delphi-Methode

- Befragungstechnik um eine von Experten erstellte Prognose zu erhalten
- Mit Hilfe eines Fragebogens
  - Ideen der Teilnehmer basierend auf Ihrem fachlichen Know-how zusammengefasst
- Direkter Austausch der Experten untereinander muss unterbunden werden
  - Antworten sollen frei von Beeinflussungen sein
- Antworten werden zur Kommentierung an die anderen Experten weitergereicht
- Nach einigen Durchläufen liegt ein aussagekräftiges Ergebnis vor, welches frei von Voreingenommenheiten sein sollte

Post-Mortem-Analyse

- Analyse vorangegangener Projekte
  - Analyse vorangegangener Projekte, welche die Ziele oder Erwartungen nicht erfüllt haben
- systematische Erhebung aller möglichen Ausfall- und Ursachenkombinationen
- daraus können potenzielle Risiken für das Projekt sichtbar werden

Fehlermöglichkeits- und Einflussanalyse (FMEA)

- Ein System wird in einzelne Betrachtungseinheiten/Funktionsbereiche zerlegt
- Auf Basis der einzelnen Funktionen werden Schwachstellen herausgebildet
  - potentielle Fehlermöglichkeiten erkennen
- Ursachen und Auswirkungen werden systematisch anhand der Funktionsbereiche ermittelt

Szenariotechnik

- künftige Entwicklungen bzw. Szenarien anhand von definierten Risiken durchspielen
- Auswirkungen bestimmter Konstellationen von Einzelrisiken auf das Gesamtrisiko betrachten und ausgewerten
- Ziel: Ermittlung möglicher Worst-Case Szenarien bzw. das Finden neuer möglicher Risiken

SWOT-Analyse

- Projekt wird unter jedem der SWOT-Aspekte betrachtet
- erhöht die Bandbreite der betrachteten Risiken
- SWOT-Analyse ist ganzheitlicher und auch positiver ausgerichtet als andere Methoden
- Risiken werden nicht nur als negativer Aspekt betrachtet werden, sondern ebenso die Stärken und Chancen
  - ermöglicht eine direkte Umsetzung von Stärken und Chancen auf strategische oder operative Vorteile
- Schnittstellenrisiken zwischen Projekten und dem Unternehmen können identifiziert werden

Prozesse im Risikomanagement

Risikoidentifikation: Aufbereitung identifizierter Risiken

Identifizierte Risiken müssen aufbereitet werden

- damit diese den anderen Prozesse des Risikomanagement zur Verfügung stehen
- Hierfür eignet sich die Erstellung folgender Komponenten

Risikoregister

- Ursprungswerte aus der Risikoidentifikation
  - später gefüllt mit den Ergebnissen der anderen Prozesse
- Liste identifizierter Risiken und mögliche Folgen
- Liste der möglichen Bewältigungsmaßnahmen, sofern bereits identifiziert
- Liste der Grundursachen identifizierter Risiken
- Liste der Risikokategorien

Prozesse im Risikomanagement

Risikoanalyse: Qualitative Risikoanalyse

Schnelle und kosteneffektive Vorgehensweise

- Methoden zur Priorisierung der identifizierten Risiken
- Grundstein für die quantitative Risikoanalyse
  - trägt zur Risikobewältigungsplanung bei
- bezieht Informationen aus der Risikomanagementplanung und der Risikoidentifikation

Konzentration auf Risiken mit hoher Priorität

Prioritäten identifizierter Risiken bewerten

- Anhand der Eintrittswahrscheinlichkeit
- daraus resultierenden Auswirkungen auf die gesteckten Ziele
  - Zeitrahmen
  - Risikotoleranz
  - Budgetkosten
  - Umfang und Qualität

Bedeutung eines Risikos besser zu verstehen

- qualitative Bewertung der verfügbaren Informationen
- Risikobezogene Maßnahmen sind oftmals sehr zeitkritisch und können somit die Bedeutung oder Auswirkung eines Risikos stark erhöhen.

Laufender Prozess

- Die qualitative Risikoanalyse sollte im Laufe des Projektes ständig wiederholt werden, da sich Änderungen an den Projektrisiken ergeben können.

Prozesse im Risikomanagement

Risikoanalyse: Quantitative Risikoanalyse

Aufbauend auf qualitativer Risikoanalyse

- durchgeführte Priorisierung der Risiken
- einige Risikomanager führen sie gerne direkt nach der Risikoidentifikation durch

Auswirkungen werden analysiert

- numerische Einstufung der Risiken
- Somit wird gleichzeitig ein erster Ansatz für die Entscheidungsfindung erstellt

Methoden

- Monte-Carlo-Simulation (Szenariotechnik)
- Entscheidungsbaum-Analyse(Fehleranalyse)

Ziele

- Wahrscheinlichkeitsbestimmung von möglichen Ergebnissen
- Identifizierung von Risiken mit der höchsten Aufmerksamkeit
- Realistischen Bestimmung von Kosten, Terminen und Umfangszielen
- Bestimmung der besten Managemententscheidung, sollten einige Faktoren unbekannt sein

Quantitative Analyse nicht immer erforderlich

- Für eine effektive Risikobewältigung
- Zeit und das Budget bestimmen die Wahl zwischen qualitativer oder quantitativer Risikoanalyse

Aktiver Prozess

- quantitative Risikoanalyse sollte ein aktiver Prozess bis zum Abschluss des Projektes bleiben
- Wiederholung sinnvoll
  - Nach Risikobewältigungsplanung und als Teil der Risikoüberwachung und -steuerung
  - herausfinden, ob das Projektrisiko auf ein Mindestmaß reduziert werden konnte
  - Hieraus lässt sich ableiten, ob Risikomanagementmaßnahmen reduziert oder verstärkt werden sollten

Prozesse im Risikomanagement

Risikobewältigungsplanung

Vorgehensweisen und Verfahren

- Erreichen von Projektzielen
- Gefahren vermeiden

Aufbauend auf Risikoanalyse

- qualitativ und /oder quantitativ
- Risikoverantwortliche bestimmen
  - welche Maßnahmen zur Risikobewältigung übernehmen

Orientiert sich an ermittelten priorisierten Risiken

- Budget, Terminplan, Einsatzmittel und Maßnahmen

Vor der Bewältigung müssen Bedeutung und Umfang eines Risikos klar sein

- Folgende Punkte muss jeder Beteiligte verinnerlicht haben
  - kosteneffektiv
  - termingerecht
  - realistisch

Vorgaben an das Risikomanagement

- von betriebsinternen Projektmitgliedern
- von Vertragspartnern, Behörden, Gesetzgeber
  - Vertragspartner (meist zeitliche, aber auch Qualitätsvorgaben)
  - Gesetzgeber (Auflagen bzgl. des Datenschutzes und der Aufbewahrung von z.B E-Mails)
  - Behörden (häufig sind dies Vorgaben bzgl. des Budgets, da bei Verzögerungen oder Mehrkosten diese erst genehmigt werden müssen)

Prozesse im Risikomanagement

Risikobewältigungsplanung

Wie gehen wir Risiko um?

Vermeiden/Minimieren

- z.B durch Verbesserung der Kommunikation innerhalb des Projektteams und den Vertragspartnern

Vermindern

- z.B durch Änderungen an der Organisation um Projektziele oder Meilensteine nicht zu gefährden

Abwälzen/Übertragen

- z.B an den Auftraggeber oder Lieferanten durch entsprechende Vertragsklauseln etc.

Selbstübernehmen/Akzeptieren

- meist nur bei eher unbedeutenden Risiken/Bildung von Reserven

Maßnahmen/Anforderungen

Changemanagement

- Wer, Wie, Was?

Anforderungsmanagement

- Priorisierung / Kosten –Nutzen

Stakeholdermanagement

- Interessensanalyse

Beziehungsmanagement

- Beziehung zu den Anspruchsgruppen pflegen

Vertragsgestaltung

- gegenüber Auftraggebern und Lieferanten

Projektplan

- Puffer für Ressourcen

Kommunikation

Prozesse im Risikomanagement

Risikocontrolling: Risikoinventur

Risikoinventur

- erfasst Schäden durch Risiken
- Hierbei spielen Eintrittswahrscheinlichkeit sowie Ursachen eine Rolle

Grundlagen zur strukturierten Darstellung

- Vollständigkeit
  - alle Risiken
  - die erfolgreichen Abschluss eines Projektes gefährden können
- Abhängigkeiten (Interdependenzen)
  - Viele Risiken verstärken sich extrem bei ihrem Eintritt

Beispiel

- Es kommt in einem Serverraum zu einem Brand, durch ein defektes Netzteil
- Der Schaden steigt erheblich
  - überfällige Wartung des Brandbekämpfungssystems
  - langanhaltende Betriebsunterbrechung
  - Hardware muss getauscht und ein Backup eingespielt werden
- Eine Gefährdung für die gesamte Produktion ist die Folge
- Der Schaden entsteht nicht durch Verlust der Hardware oder deren (Brandschutzversicherung)
- eigentlicher kaum messbare Schaden: Betriebsunterbrechung (keine Versicherung)

Prozesse im Risikomanagement

Risikocontrolling: Risikoinventur

Quantifizierung

- Schadensausmaß richtet sich nach Eintrittswahrscheinlichkeit (starker Bezug)

Rechtzeitigkeit

- Risiken müssen so früh wie nur irgendwie möglich erkannt werden
- damit noch genügend Reaktionszeit bleibt
- Schaden möglichst gering zu halten

Kommunikation

- Während der Bewältigungsplanung sind Akzeptanzbereiche zu bilden
- durch die die jeweiligen Risikoträger bei Eintritt informiert werden

Verantwortung

- Risiken müssen entsprechend ihrer Art, den jeweiligen Zuständigkeitsbereichen zugeordnet sein
- nach Eintritt des Risikos muss der Zuständige dann die geplanten Maßnahmen ergreifen

Überwachung und Training

- Überwachungsverantwortlichen haben dafür zu sorgen, dass
  - Prozesse, Verantwortlichkeiten und Maßnahmen
  - in den Phasen des Eintritts ordnungsgemäß ablaufen
- Trainings und Tests für den Ernstfall nötig

Dokumentation

- Dokumentation während des ganzen Projektlebenszyklus ist Pflicht
- Dies nicht zu tun ist extrem fahrlässig
- Jeder Beteiligte muss stets Zugriff auf die Dokumentation haben
  - wann immer dies erforderlich ist

Zwei Phasen

Bruttobewertung

- grundsätzlichen Bedrohungspotenziale werden betrachtet
- wo liegen Schwerpunkte der Risikosteuerung

Nettobewertung

- Risiken bereits bestehenden Steuerungs- und Kontrollmaßnahmen gegenüberstellen

Aktuelle Risikolage

- Wir ermittelt
- Eignung und Angemessenheit bestehender Maßnahmen festgestellen

Maßstäbe eingrenzen

- Vor einer Bewertung der Risiken
- Maßstab für Schadensausmaß und Eintrittswahrscheinlichkeit eingrenzen
- Schätzungen oder Erfahrungswerten durch die Verantwortlichen
- Worst-Case-Szenario
- klare Grenzen zwischen den einzelnen Gefahrenstufen

Ampelmodell

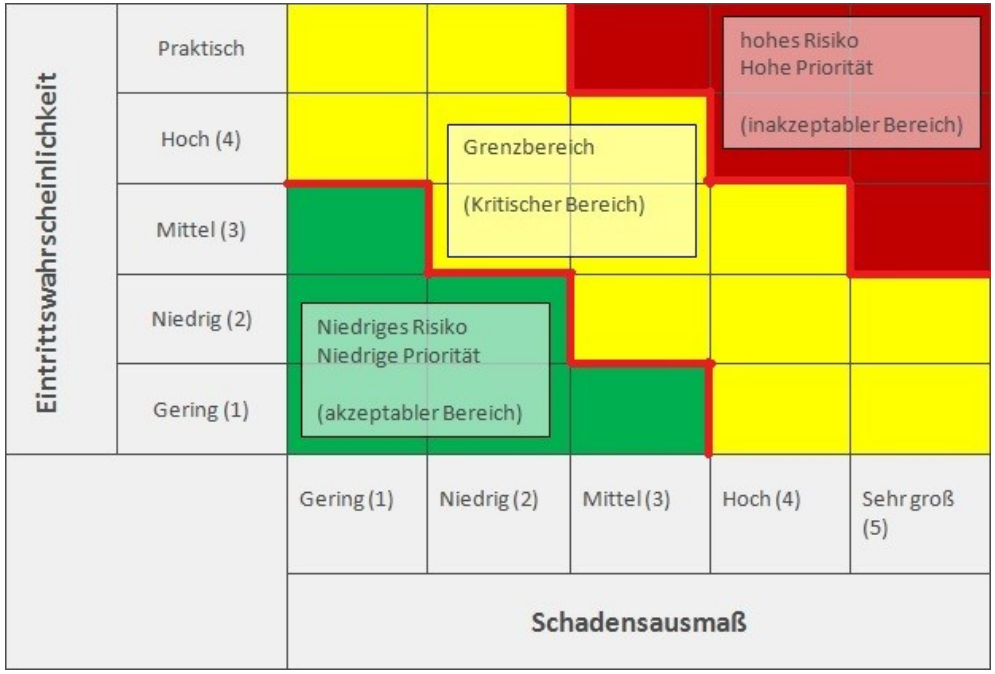
- besonders geeignet

Akzeptanzlinie

- Rote Linie zwischen akzeptablen und kritischem Bereich

Toleranzgrenze

- Rote Linie zwischen Grenzbereich und inakzeptablem Bereich
- Risiken, unterhalb dieser Linie, gelten als tolerierbar
- wenn es möglich ist
  - durch Maßnahmen diese unter Kontrolle zu halten
  - oder sogar in den akzeptablen Bereich zu bringen
- Festlegung der Grenzen wird durch Verantwortliche vorgenommen



Bewertung und Messung von Risiken

Kriterien

- Ungewissheit
  - Unsicherheit
  - Abschätzungssicherheit
  - Ahnungslosigkeit
- Ausbreitungsgrad des potenziellen Schadens
- zeitlicher Ausdehnungsgrad nach Eintritt
- Möglichkeit den Ursprungszustand wiederherzustellen
  - z.B durch einspielen eines Backups
- Verzögernde Wirkung des Schadens
  - evtl. nicht direkt sichtbar
- Mobilisierungspotenzial der beteiligten Mitarbeiter
  - nach einem Schaden weiter zu machen

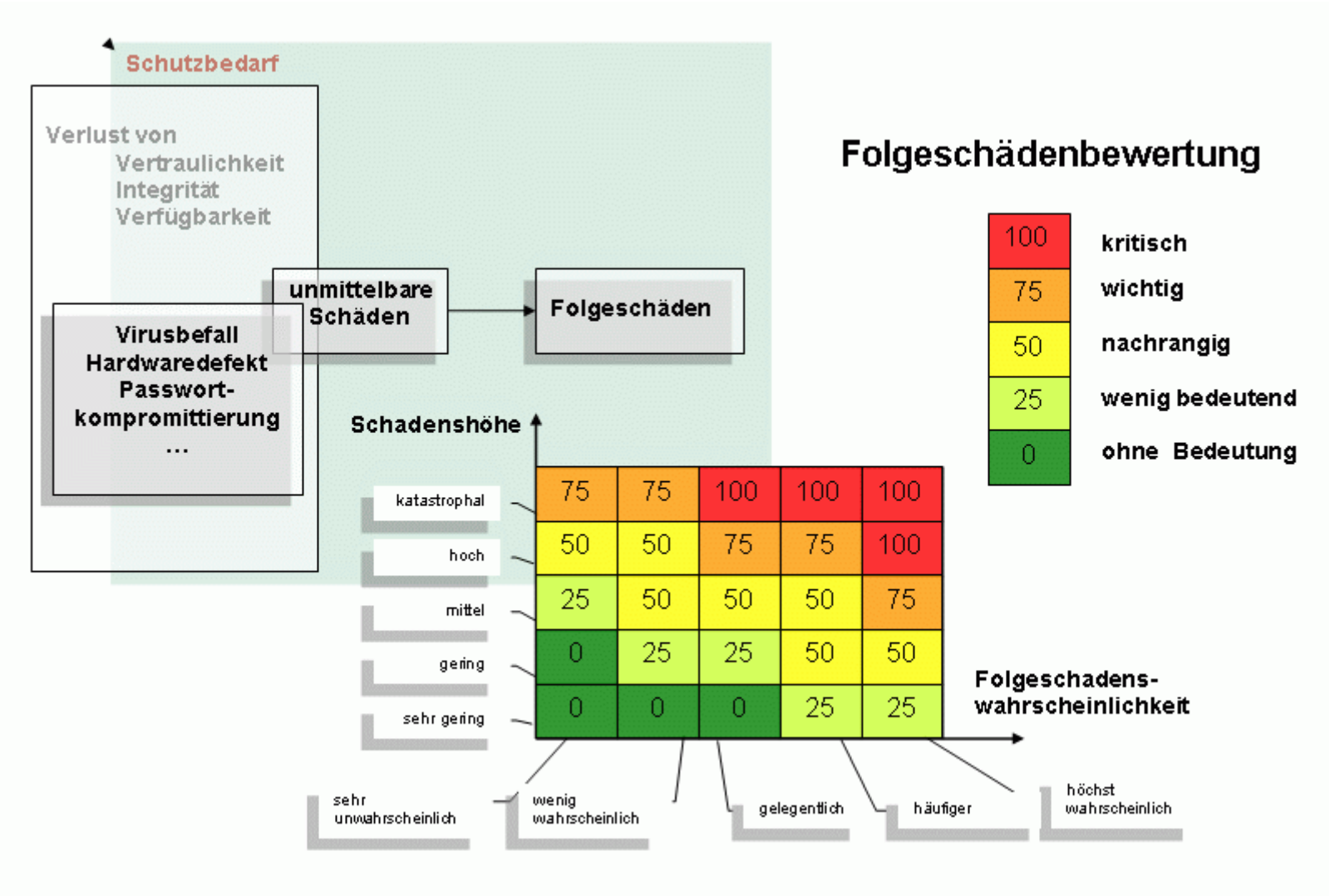
Ergebnis: qualitative und quantitative Bewertung von Risiken

- quantitativen Bewertung
  - Schadenshöhe/Intensität der Auswirkung
  - Eintrittswahrscheinlichkeit
- qualitative Bewertung
  - Aggregation (Zusammenlegung) von Risiken im Hinblick auf die Erreichung von Zielen

Monetäre und nicht-monetäre Größen

- Monetär
  - Umsatzausfall
    - z.B. Verzögerungen bei der Inbetriebnahme eines neuen ERP Systems
  - Mehrkosten
    - z.B. höhere Personalkosten durch Zeitliche Verzögerung
- Nicht-Monetär
  - Angestellten- / Kundenzufriedenheit
    - Probleme mit dem Umgang der neuen Software etc.
  - Marktanteil
    - Kunden können nicht schnell genug bedient werden
    - dadurch evtl. Verlagerung der Einkäufe bei der Konkurrenz

Bewertung und Messung von Risiken



Bewertung und Messung von Risiken

Berechnung des Faktors eines Risikos

Eintrittswahrscheinlichkeit * Schadenshöhe = Risikofaktor

- Berechnung des Faktors eines Risikos

Risikobewertung am Beispiel „Changemanagement“

- Erfahrungen bei vorrangegangenen Projekten:
  - Änderungen während des Projekts
  - z.B. Änderung der Meilensteinen
  - oder im schlimmsten Fall am eigentlichen Projektziel
- Dies sind Risiken, die komplette Projekte bedrohen oder sogar stoppen können
- Ein Risiko beeinträchtigt hierbei meist nicht nur eine Säule des gesamten Projekts
- Oft ist die Rede von einem Dreieck in dem sich ein Projektmanager bewegt
- Umso mehr dieser sich auf einen Punkt fokussiert, umso mehr entfernt er sich andererseits von einem anderen

Changemanagement hat großen Einfluss auf zeitlichen Rahmen und das Projektbudget

- Warum besteht das Risiko?
  - Kein klar definiertes Ziel
  - Mangelhaftes Anforderungsmanagement während des Planungsprozesses, ergeben stetig neue Projektänderungen
  - Oftmals wird der Benutzer nicht in die Planung mit einbezogen
- Wie wahrscheinlich ist das Risiko?
  - Eintrittswahrscheinlichkeit 5 – sehr hoch
  - Schadenswirkung 4 – hoch
- Risikofaktor
  - Wahrscheinlichkeit (5) * Schadenswirkung (4) = Risikofaktor (20)

Mit dem errechneten Risikofaktor landet dieses Risiko im nicht tolerierbaren Bereich (Stern Abb.).

Beispiele für weitere Risiken (Gefahrenbereiche)

Einsatz neuer Technologien
- W(4) * S(5) = RF(20)

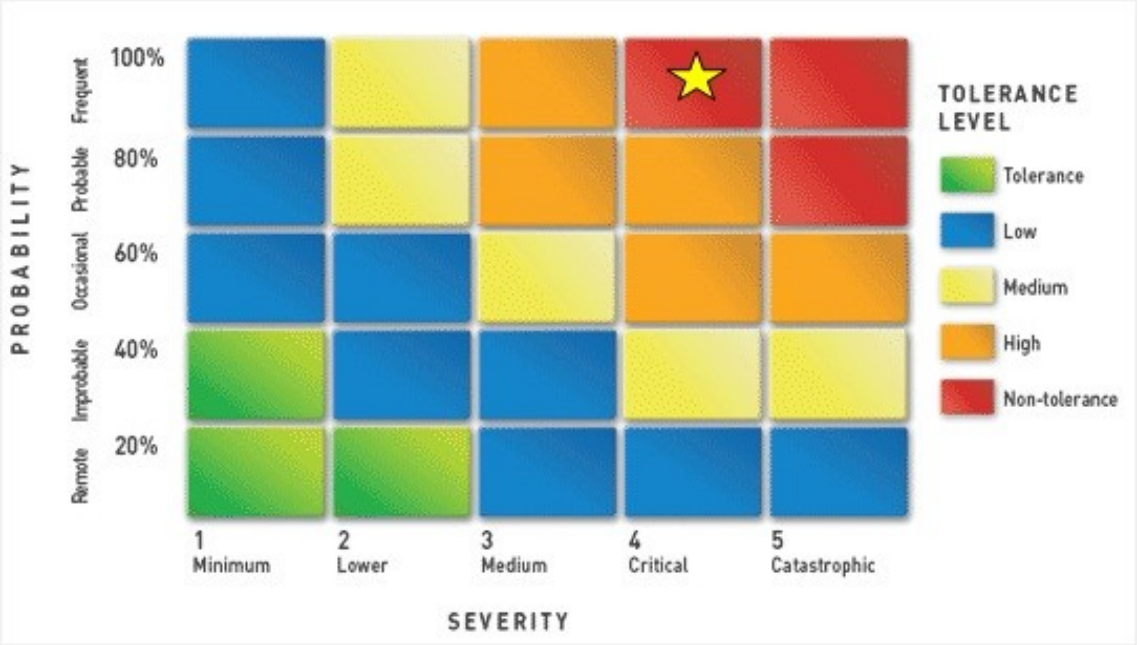
Implementierungen ohne Entwurf
- W(4) * S(4) = RF(16)

Unmotivierte Mitarbeiter
- W(3) * S(5) = RF(15)

Mitarbeiterfluktuation
- W(2) * S(4) = RF(8)

Machtkämpfe
- W(1) * S(2) = RF(2)

Unzureichende Reviews
- W(3) * S(4) = RF(12)



Legende:
W = Wahrscheinlichkeit S = Schadenswirkung RF = Risikofaktor

Qualität des IT-Managements

Kernpunkte

Planung und Organisation

- Sind IT-Strategie und Geschäftsstrategie aufeinander abgestimmt?
- Kann das Unternehmen seine IT-Ressourcen optimal nutzen?
- Sind die Ziele der IT von allen Mitarbeitern verstanden?
- Sind die IT-Risiken erkannt, verstanden und unter Kontrolle?
- Ist die Qualität der IT-Systeme angemessen für die geschäftlichen Anforderungen?

Beschaffung und Einführung neuer Systeme

- Liefern neue Projekte voraussichtlich Lösungen, die den geschäftlichen Anforderungen genügen?
- Werden neue Projekte voraussichtlich im vorgesehenen Zeit- und Kostenrahmen abgeschlossen?
- Können neue Systeme eine ordnungsgemäße Verarbeitung nach der Einführung sicherstellen?
- Können Änderungen an IT-Systemen durchgeführt werden ohne die Geschäftsprozesse zu behindern?

Betrieb und Unterstützung

- Werden IT-Dienstleistungen entsprechend der geschäftlichen Prioritäten ausgeführt?
- Sind die Kosten optimiert?
- Können die Mitarbeiter mit den IT-Systemen effektiv und sicher umgehen?
- Ist eine angemessene Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet?

Überwachung

- Kann die IT-Performance gemessen werden?
- Können IT-Probleme rechtzeitig erkannt werden?

Risikokommunikation und -berichterstattung

Ständige Kommunikation innerhalb und außerhalb eines IT-Projektes

- vielleicht wichtigster Punkt für erfolgreiches Risikomanagement

Evaluierung und Modifizierung während eines Projektes nicht ausgeschlossen werden

- Meetings abhalten
- Effektivität der Risikoevaluierung und des Risikomanagements einordnen
- Feedback verwenden, um den Prozess zu verbessern

Die wichtigsten Aspekte

- Kommunikation der Risikoinformationen an alle Stakeholder
- Motivation zum freien Informationsfluss über alle Risiken
- Regelmäßige Updates für alle Teammitglieder
- Einfache Kommunikationsformen untereinander
- Allen Teammitgliedern muss ständiger Zugriff zu den Risikoinformationen zur Verfügung stehen

Standardberichtsformat hat sich Zeit bewährt

- Inhalt dieses Berichts ist der aktuelle Stand des gesamten Risikomanagementplans

Bericht umfasst folgende Punkte

- Wann wurde die letzte Risikoinventur durchgeführt?
- Ist die Risikoanalyse aktuell?
- Welche Risiken sind hinzugekommen, welche evtl. aufgelöst worden?
- Ist ein Trend abzusehen?
- Bewertung der getroffenen Maßnahmen zur Risikobewältigung

Erfolg wird durch Beeinflussung der ergriffenen Maßnahmen messbar

Überwachung von Maßnahmen

Fragen

Wer Überwacht die Maßnahmen?

Wer setzt diese eigentlich um?

RASCI Methode

Überwachung befasst sich zum größten Teil mit folgenden Fragen

- Responsible (R)
  - Wer ist verantwortlich?
- Approved/Accountable (A)
  - Wer hat es abgesegnet?
- Supports (S)
  - Wer setzt es um?
- Consults (C)
  - Wer hilft bei der Umsetzung („Experte“)?
- Informed (I)
  - Wer muss benachrichtigt werden?

Typical RACI / RASCI chart

	Program Manager	PM Assistant	Board of Directors	Service Manager	Legal Adviser
Activity 1	R		A		
Activity 2	A	R		S	C
Activity 3	RA		I		I
Activity 4	RA				C
Activity 5	A	R		S	

Bewertung

Risikomanagement sollte nicht als lästige Pflicht angesehen werden

- sondern als eine Chance
  - IT-Prozesse optimieren
  - Risikoverständnis und Sicherheitsniveau im Unternehmen verbessern

Wirtschaftlicher Nutzen des Risikomanagement

- Je nach der Größe und Bedeutung eines Projektes
  - kann das Risikomanagement in seinem Umfang unterschiedlich ausgelegt werden.
- Bei kleineren Projekten
  - erscheint es unter Umständen weniger sinnvoll, aufwendige Analysen wie z.B. die FMEA durchzuführen
  - Hier kann mit einfachen Mitteln bereits ein adäquates Risikomanagement betreiben werden
    - Brainstorming
    - guter Dokumentation
    - Kommunikation der Risiken

Risiken können nicht immer vollständig eliminiert werden

- aber durch das Risikomanagement beherrschbar bleiben

Bedrohungsanalyse

Risikoanalyse (risk assessment)

Risikobewertung anhand Wahrscheinlichkeiten

- Eintreten verschiedener Bedrohungen
- potentieller Schadenshöhe

Bewertung der Eintrittswahrscheinlichkeit

- Geschätzter Aufwand zur Angriffsdurchführung
  - Anzahl der Angriffsschritte
  - Komplexität Angriffsschritte
- Nutzen für den Angreifer
  - finanziell
  - politisch
  - Reputation
- Motive des Angreifers, Angreifertyp
  - Script Kiddie
  - Hacker
  - Mitarbeiter
  - Wirtschaftsspion
  - politische Aktivisten
- Ressourcen / Kenntnisse des Angreifers
  - Know How
  - Werkzeuge
  - Zugänge

Bedrohungsanalyse
Angriffsbäume

Systematische Ermittlung potentieller Ursachen für Bedrohungen

- organisatorisch
- technisch
- benutzerbedingt

Vorteile von Angriffsbäume

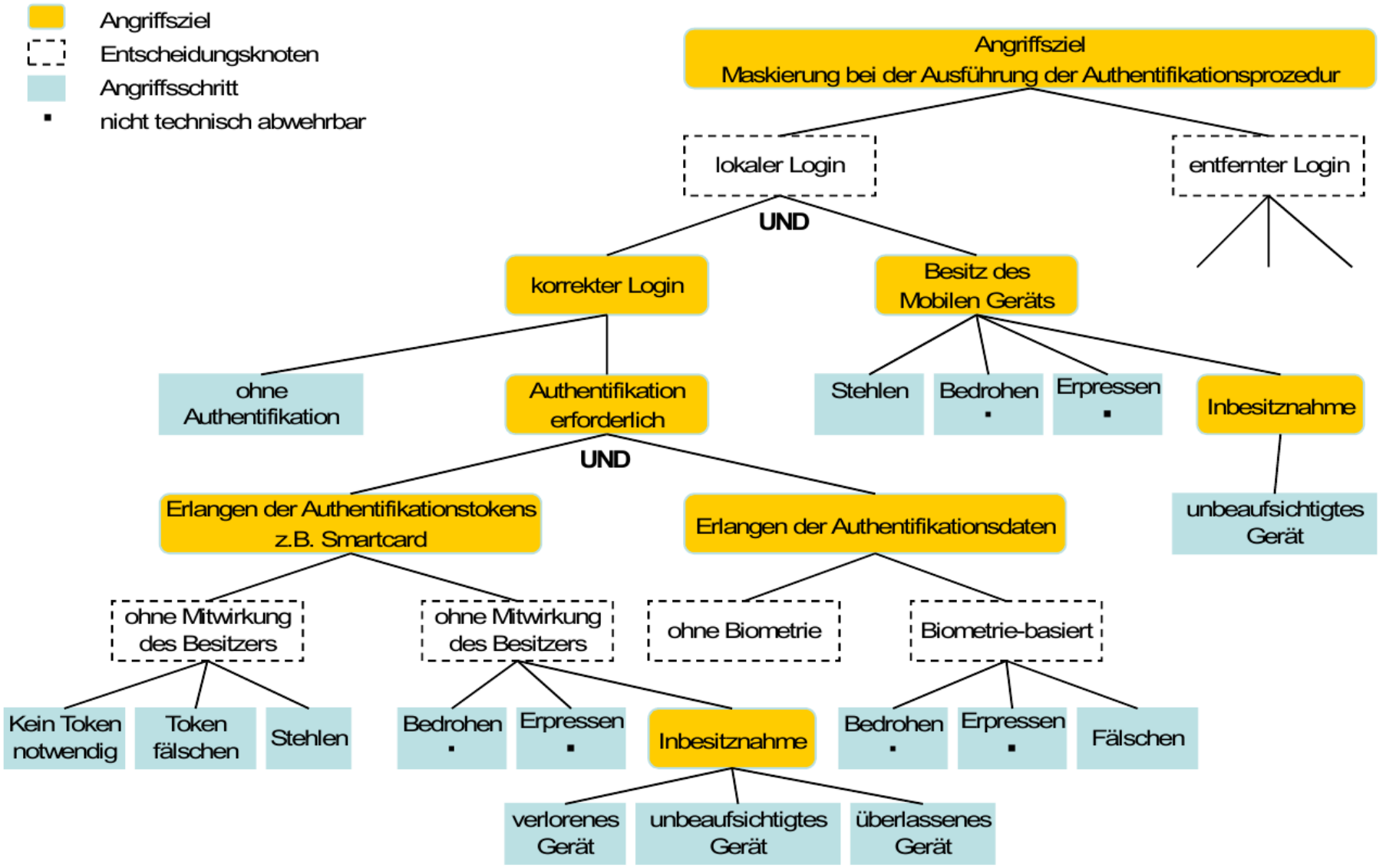
- Bedrohungsmodelle werden besser verstanden
- Bedrohungen besser erkennbar
- Schutzmaßnahmen besser erkennbar
- Berechnungen der Sicherheit
- Sicherheit verschiedener Systeme vergleichbar

Visualisierung über Bedrohungs-/Angriffsbäume (attack tree)

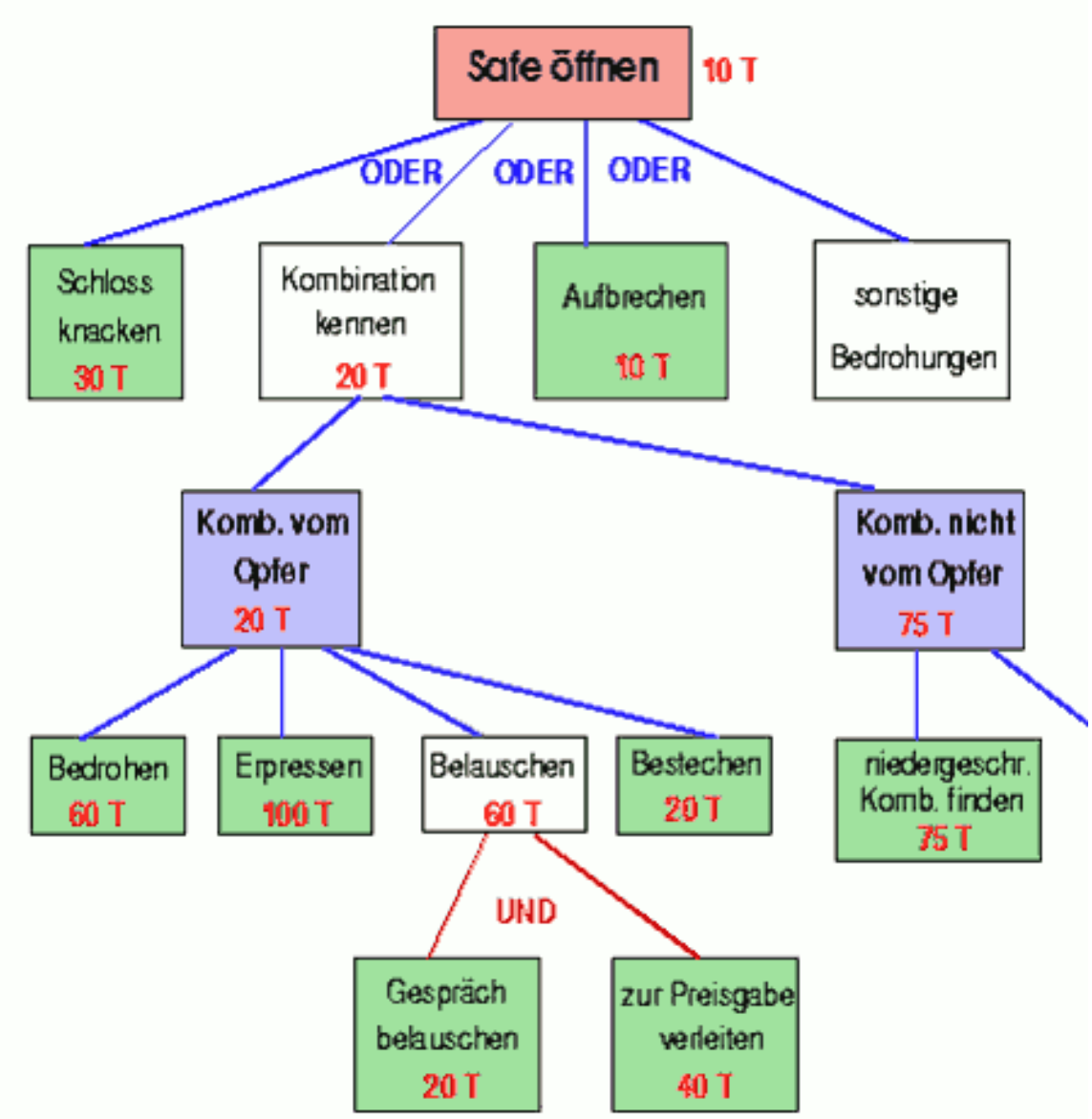
- Wurzel definiert mögliches Angriffsziel
- Zeichenziele zur Erreichung des Gesamtziels ergeben die nächste Ebene
- Verwendung von UND- und ODER-Knoten, um Bedingungen zu formulieren
  - Bedeutung des Erreichens von Zeichenzielen
- Äste verknüpfen Zwischenziele mit höheren Zielen
- Blätter des Baumes beschreiben einzelne Angriffsschritte

Bedrohungsbaum

Maskierungsangriff



Bedrohungsanalyse



Bedrohungsmatix

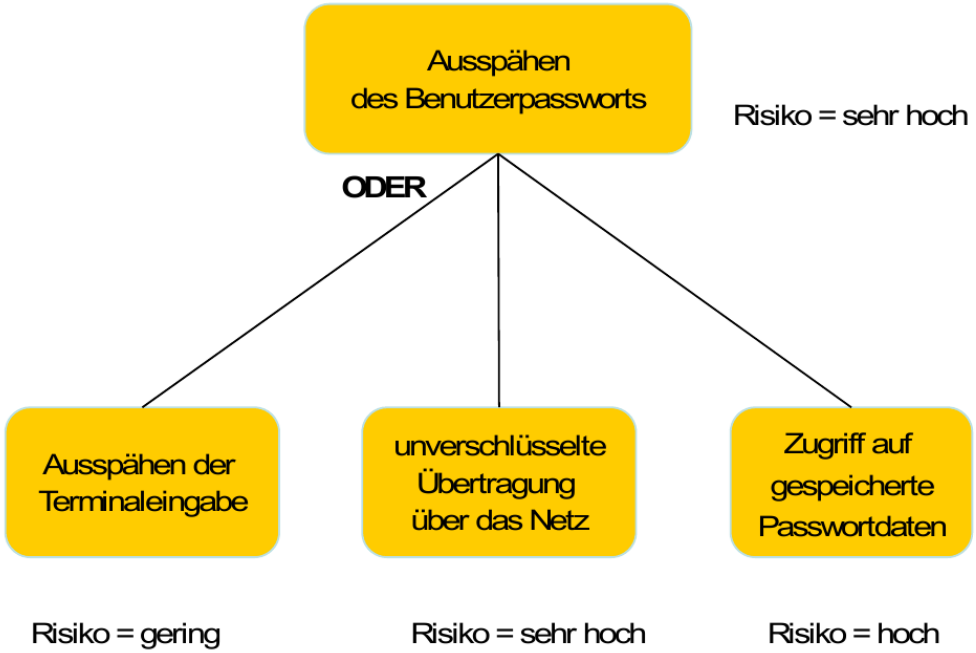
- Zeilen: Gefährdungsbereiche
- Spalten: potentieller Auslöser

	Program-mierer	interner Benutzer	externer Benutzer	mobiler Code
Externe Angriffe	Vandalismus	Beobachtung der Passwort-eingabe		
Interne Angriffe	Direkter Speicherzugriff	Logische Bomben	Passwort cracken	Viren Trojaner
Verfügbarkeit	Speicher belegen	Prozesse erzeugen	Netzlast generieren	Monopolisierung der CPU
Abstreiten		Transaktionen	Accounting	
Rechtemiss-brauch	Manuipulation von Daten			

Bedrohungsanalyse

Schritt	Bedrohung	A	B	C	D
1	Schaden durch erfolgreichen Angriff	500.000 €	10.000 €	100.000 €	10.000 €
2	Auftretenswahrscheinichkeit	80%	20%	5%	70%
3	Schwere der Bedrohung	400.000 €	2.000 €	5.000 €	7.000 €
4	Kosten für Gegenmaßnahmen	100.000 €	3.000 €	2.000 €	20.000 €
5	Wert des Schutzes	300.000 €	- 1.000 €	3.000 €	- 13.000 €
6	Gegenmaßnahmen anwenden?	Ja	Nein	Ja	Nein
7	Priorität	1	NA	2	NA

Risikoberechnung



Schlussfolgerung

- Auch bei einfachem Angreifermodell sehr hohes Risiko
- Passworte sollten nur verschlüsselt übertragen werden!

Zeitliche Entwicklung beachten

MCA:	1 Tag		2 Tage		1 Woche		2 Wochen		1 Monat	
	Bemerkungen	Bew.	Bemerkungen	Bew.	Bemerkungen	Bew.	Bemerkungen	Bew.	Bemerkungen	Bew.
Finanzielle Auswirkung										
Verlust von Reputation										
Rechtliche Konsequenzen										
Sicherheit von Personen										
Summe										

Konstruktion sicherer Systeme

Entwicklungsprozess

Dezidierte Methoden bislang kaum entwickelt

- allgemeine methodische in der Regel

top-down Vorgehensweise aus Software-Engineering

- Schwierig, da Angreifer viele Möglichkeiten hat

allgemeine Prinzipien

- 1975 Saltzer und Schröder
- Heute noch gültig

Allgemeine Konstruktionsprinzipien

- Erlaubnis-Prinzip
- Vollständigkeits-Prinzip
- Need-To-Know-Prinzip
- Prinzip der Benutzerakzeptanz

Erlaubnis (fail-safe defaults)

Grundsätzlich jeder Zugriff verboten (default deny)

- nur durch explizite Erlaubnis wird Zugriffsrecht gewährt.

Configfiles

- Apache
- SMB

Vollständigkeit (complete mediation)

Jeder Zugriff ist auf Zulässigkeit zu prüfen!

- System, das nur beim Öffnen Erlaubnis prüft, nicht bei jedem Schreiben, verletzt das Prinzip

Rechte können sich zwischendurch verändert haben.

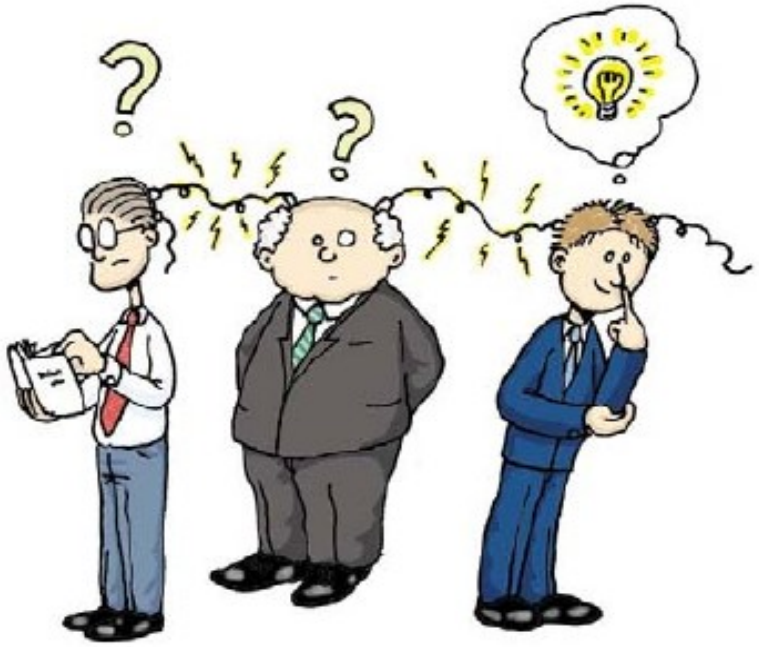
Need-to-Know

Prinzip der minimalen Rechte

- Jedes Subjekt bekommt nur genau die Zugriffsrechte, die es zur Erfüllung seiner Aufgaben benötigt.

System, in dem ein Admnistratoren unbeschränkte Rechte hat, verstößt gegen dieses Prinzip.

- AppAmor
- SELinux
- Rollenbasierte Rechte



Akzeptanz (economy of mechanism)

Benutzerakzeptanz

Sicherheitsmechanismen müssen einfach zu nutzen sein

routinemäßig und automatisch angewendet werden

Offener Entwurf (open design)

Sicherheit eines Systems darf nicht von der Geheimhaltung spezieller Verfahren abhängig sein

- Verwendete Verfahren und Mechanismen, die beim Entwurf des Systems verwendet werden, müssen offen gelegt werden

No security through obscurity

- Sicherheit kryptografischer Verfahren sollte nicht darauf basieren, dass Verschlüsselungsverfahren nicht bekannt ist.
- „Schlüssel unter der Fußmatte“

KISS - Prinzip

Keep it simple, stupid.

- „Halte es einfach, Dummkopf!“; sinngemäß: Mach's so einfach wie möglich

Keep it simple [and] stupid

- „Halte es einfach und [dumm=] beschränkt“
  - sinngemäß: „Mit einfachsten Mitteln verständlich und bewältigbar.“

Keep it short and simple

- „Gestalte es kurz und einfach“
  - aus dem Bereich des Marketing

Keep it simple and smart

- „Mach es einfach und schlau“

Keep it simple and straightforward

- „Gestalte es einfach und überschaubar“

Keep it safe and sound

- „Halte es sicher und stimmig“

Keep it sweet and simple

- „Gestalte es gefällig und einfach“

Keep it small and simple

- „Gestalte es klein und einfach“

Keep it simple and safe

- „Mach es einfach und sicher“

Keep it safe and simple

- „Mach es sicher und einfach“

Keep it strictly simple

- „Mach es konsequent einfach“

Keep it speckless and sane

- „Mach es sauber und gesund“

Keep it sober and significant

- „Mach es schlicht und wesentlich“

Grundaussage: Wähle die einfache Lösung

Wissenschaftlich

- Bevorzuge die Theorie, die weniger Annahmen machen muss, um gemachte Beobachtungen zu erklären
- Vergleichbar dem Prinzip der Einfachheit

Angeblich von Clarence "Kelly" Johnson geprägt

- Ingenieur bei Lockheed Skunk Works (Hersteller von Militärflugzeugen)

Lange als "Keep it simple, stupid" interpretiert

- Johnson: 'Keep it simple [&] stupid'
- so von vielen Autoren verwendet

Aufgabe zur Verdeutlichung des Prinzips

- entwerfe Düsentriebwerk, dass
  - mit wenigen einfachen Werkzeugen
  - von einem durchschnittlichen Ingenieur
  - im Felde unter Kampfbedingungen
  - mit nur diesen Werkzeugen reparierbar ist

„stupid"

- zielt auf die Beziehung zwischen der Art und Weise, wie Dinge zu Bruch gehen, und deren Ausgereiftheit bezüglich der Reparatur
- Es soll ein möglichst einfacher und „beschränkter“ Ansatz sein

KISS-Prinzip
Hintergründe

Verbreitet ist das KISS-Prinzip in

- den United States Air Force
- der Softwareentwicklung

Designprinzip

- beschreibt es im Gegensatz zu einer Problemlösung in der Form einer Fehlerumgehung ("workaround")
- die möglichst einfache, minimalistische und leicht verständliche Lösung eines Problems

Beispiel ist die TCP/IP-Protokollfamilie

- einfacher Aufbau der Protokolle führt zu enormer Skalierbarkeit
- obwohl sie für ein kleines Netzwerksystem entwickelt wurden
  - Forschungszentren der DARPA

KISS-Prinzip immer häufiger im allgemeinen Zusammenhang mit komplexen Planungsaufgaben

„Keep It Short and Simple“-Version an englischen Schulen und Universitäten

- Schreiben von Essays, Inhaltsangaben und Interpretationen

Modellierung

Modellierung, Entwurf und Betrieb (I)

Vergleich

- Soll-Zustand
  - beschreibt Schutzbedarf
- Ist-Zustand
  - beschreibt Bedrohungs- und Risikoanalyse

Ergebnis

- Maßnahmen zur Abwehr der Bedrohungen

Klassifizierung der Maßnahmen

- Wichtigkeit
- Kosten
- Aufwand

Modellierung, Entwurf und Betrieb (II)

Erfassung der erforderlichen Maßnahmen

- zur Erfüllung des Schutzbedarfs in Sicherheitsstrategie (security policy)
  - informell oder präzise formalisiert

Klassen von Anwendungen haben ähnliche Schutzbedürfnisse

- deshalb können allgemeine Sicherheitsgrundfunktionen eingesetzt werden.

Kriterienkataloge definieren Funktionsklassen für Anwendungsszenarien

- europäische ITSEC
- internationale Common Criteria

Anwender sollte klären

- ob seine Sicherheitsanforderungen bereits von einer dieser Klassen abgedeckt wird
- welche Kombination von Grundfunktionen er braucht

Modellierung, Entwurf und Betrieb (III)

Systemarchitektur

- Architekturgrobentwurf
- Identifikation der zu schützenden Komponenten

Definition der Sicherheitskomponenten

Feinentwurf

- Verfeinerung und detaillierte Spezifikation der Komponenten
- präziser Rahmen für Implementierung
- Wahl der nötigen Datenstrukturen, Algorithmen
- Nutzung von Standardmechanismen
  kryptografische Protokolle, Passwortschutz, ACLs, Protokolle zur Schlüsselverteilung,…

Validierung / Evaluierung

Testen

- Methodisches Testen des implementierten Systems
- Wenn möglich: Verifizierung der sicherheitsrelevanten Funktionen
- Testziele, -pläne, -verfahren festlegen, dokumentieren.
- Vollständigkeit der Tests
- Code Review

Evaluierung durch Dritte

Sicherheitsgrundfunktionen (I)

Baukasten

- Identifikation und Authentifikation
- Rechteverwaltung
- Rechteprüfung
- Vollständigkeitsprinzip
- Ausnahmen
- Beweissicherung
- Wiederaufbereitung
- Gewährleistung der Funktionalität

Sicherheitsgrundfunktionen (II)

Baukasten

Identifikation und Authentifikation

- Objekte / Subjekte müssen eindeutig identifizierbar sein
  - Identität nachweisen können
- Abwehr von Maskierungsangriffen, unautorisierten Zugriffen

Sicherheitsanforderungen legen fest

- ob und wenn ja, welche Subjekte zwar zu identifizieren, aber nicht zu authentifizieren sind.
  - Betriebssystem
    - Authentifikation nur bei Login
    - Gültigkeit späterer Aktionen beruhen auf Gültigkeit dieser Kontrolle
  - Internet-Banking
    - Authentifikation bei jeder relevanten Aktion (TAN)
- Angabe, welche Aktionen zur Abwehr systematischer Angriffsversuche ergriffen werden
- Protokollieren, Sperrung der Kennung

Sicherheitsgrundfunktionen (III)

Baukasten

Rechteverwaltung

- Basis zur Abwehr von Bedrohung der Integrität und Vertraulichkeit
- Sicherheitsanforderungen legen Rechte für zu schützende Objekte fest
- Vergabe (UNIX: owner-Prinzip)
- Wahrnehmung

Rechteprüfung

- Zugriffskontrolle
- Bei welchen Aktionen muss Rechteprüfung stattfinden?

Vollständigkeitsprinzip

- Jeder Zugriff sollte kontrolliert werden
  - Oft prüfen nur beim öffnen einer Datei
  - Danach Konformitätsprüfung: Wenn lesen, dann weiterlesen.
  - File Handles

Ausnahmen

- Welche Aktionen bei unautorisierten Zugriffen
  - permission denied

Sicherheitsgrundfunktionen (IV)

Baukasten

Beweissicherung

- Nichtabstreitbarkeit
- Protokollierung
- Computer-Forensik

Wiederaufbereitung

- Maßnahmen zur Wiederaufbereitung von gemeinsam aber exklusiv nutzbaren Betriebsmitteln
  - Prozessor, Register, Cache

Gewährleistung der Funktionalität

- Maßnahmen zur Gewährleistung der Verfügbarkeit
- Abwehr von DoS
- Priorisierung von Funktionalitäten

Einfaches Modell der Datenübertragung

Passiver Angreifer: nur abhören, nicht manipulieren

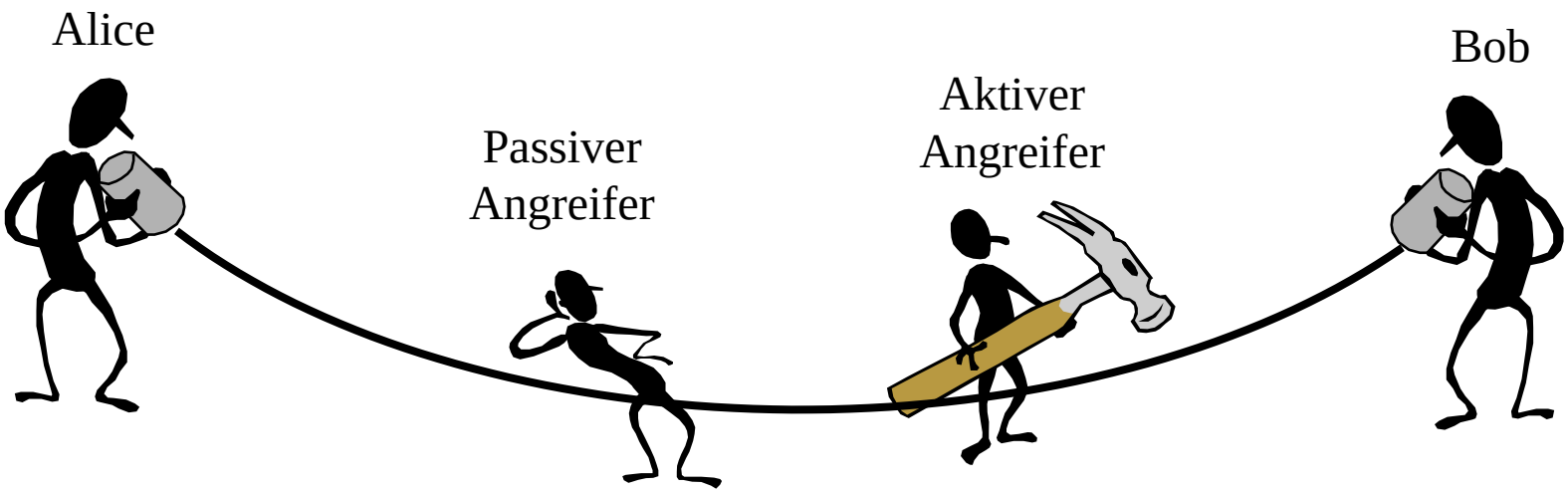
- Bedrohung für Vertraulichkeit

Aktiver Angreifer: abhören, ändern, löschen, duplizieren

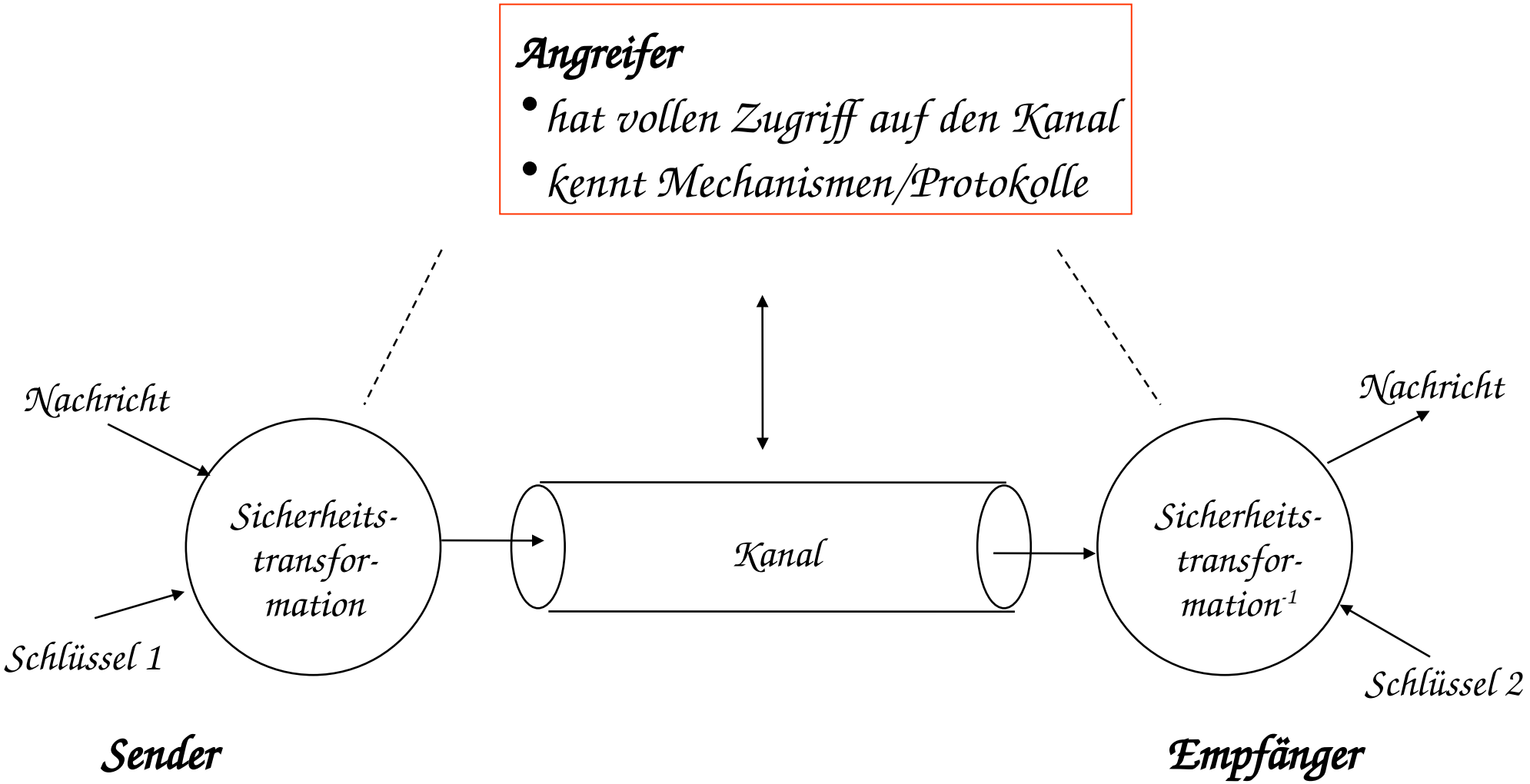
- Bedrohung für Vertraulichkeit, Integrität, Authentizität

Unterschied Authentizität/Verbindlichkeit

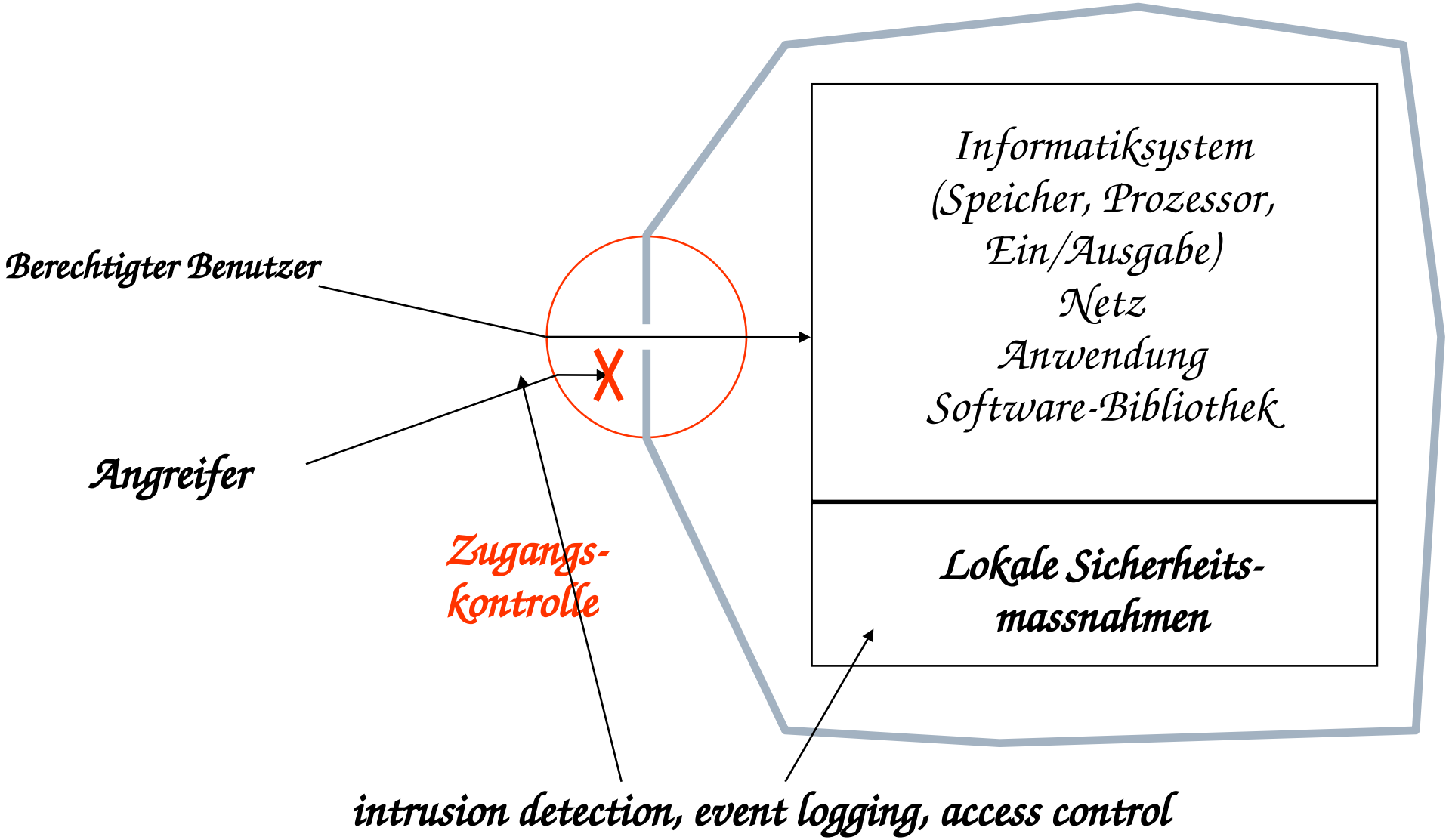
- Authentizität: Bob ist sicher, dass Daten von Alice kommen
- Verbindlichkeit: Bob kann dies gegenüber Dritten beweisen



Modell I: Sichere Kommunikation über einen unsicheren Kanal



Modell II: Schutz durch Zugangskontrolle



Bewertungskriterien

Kriterienkataloge stellen Bewertungsschema zur Verfügung

Zertifikate

Nationale internationale Kataloge

- Orange Book (US)
- Grünbuch (DE)
- ITSEC (Europa)
- Common Criteria (international)