



Herzlich Willkommen
zum 52. UVD User Kreis
in Datteln, Westfalen



07. Dezember 2006

IT Risikomanagement



■ Risiken im IT-Bereich

- ◆ Beispiele von Risiken im IT-Bereich
- ◆ Ursachen und Folgen solcher Risiken
- ◆ FME-Analyse als Steuerungsinstrument

■ Klassifizierung der IT-Risiken

- ◆ Risiken im Softwarebereich

■ Aufbau einer IT-Scorecard

■ Risikosteuerung und -kontrolle



■ Risiken im IT-Bereich

- ◆ Beispiele von Risiken im IT-Bereich
- ◆ Ursachen und Folgen solcher Risiken
- ◆ FME-Analyse als Steuerungsinstrument

■ Klassifizierung der IT-Risiken

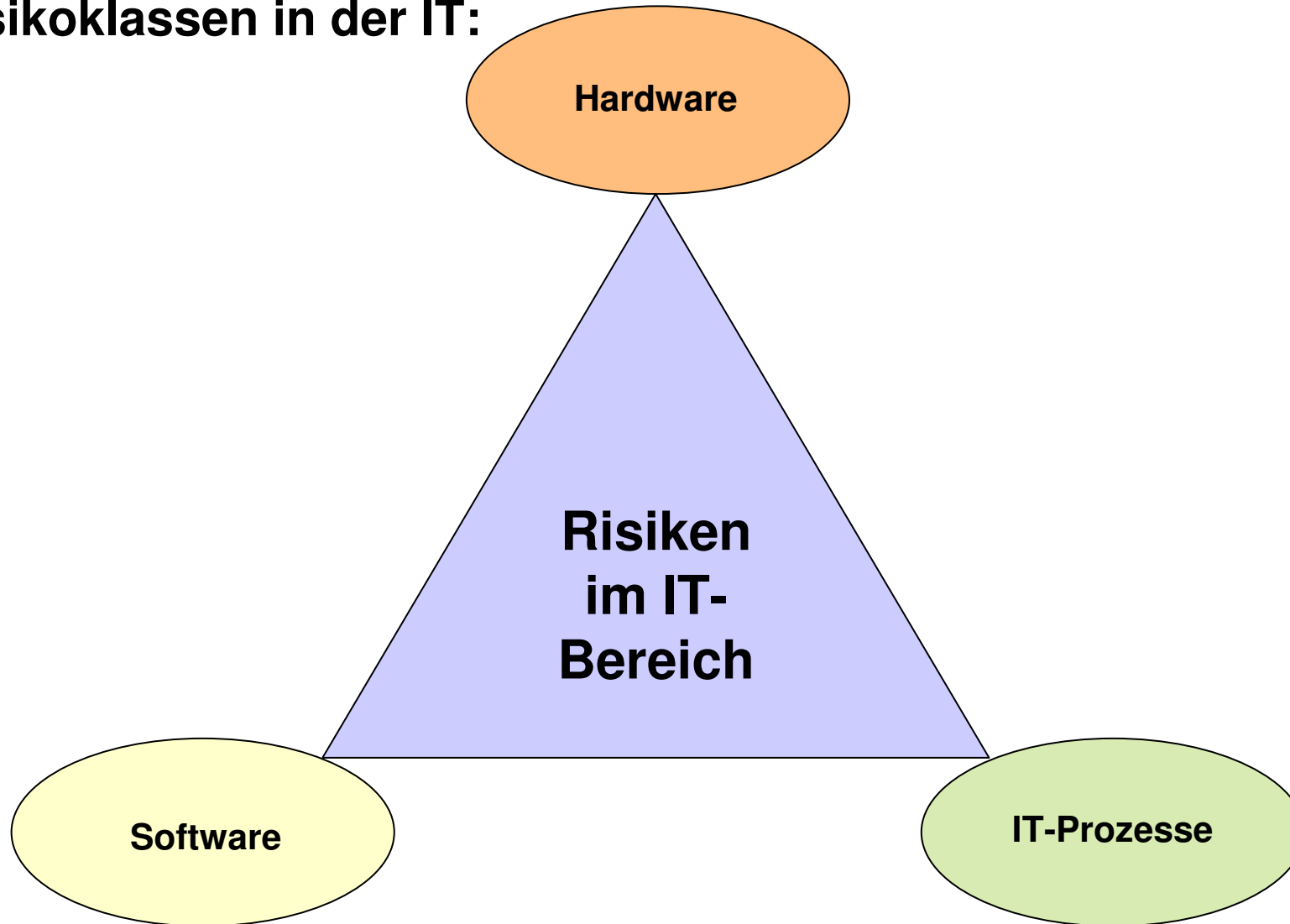
- ◆ Risiken im Softwarebereich

■ Aufbau einer IT-Scorecard

■ Risikosteuerung und -kontrolle



■ Risikoklassen in der IT:



■ Risiken im Softwarebereich

Als Risiken in diesem Bereich gehören u.a. folgende:

- ◆ Fehlende Orientierung der Software an dem Arbeitsablauf neuer SW- Systeme
- ◆ Mangelnde Softwareeinführung (z. Bsp. Schulung, Dokumentationen)
- ◆ Probleme im laufenden Betrieb bei Releasewechseln (Systemüberlastung, fehlende Informationen über Releasevoraussetzungen, etc.)
- ◆ Verlässlichkeit der Programme und deren Performance
- ◆ Rollen- und Benutzerkonzepte für die Softwarenutzung
- ◆ Datensicherheit und Replikationsmöglichkeiten im Falle von Programmabstürzen
- ◆ Softwarediebstahl und Kopiermöglichkeiten

■ Risiken im Hardwarebereich

Folgende Risiken lassen sich in diesem Bereich lokalisieren:

- ◆ Hardwaredefekte (z. Bsp. Festplattenausfall, Sicherungstape beschädigt)
- ◆ Performance der Hardware im Hinblick auf die jeweilige Verwendung (z. Bsp. fehlende Kapazität bei den Servern)
- ◆ Diebstahl von Datenträgern (z. Bsp. Disketten, Festplatten, sonstige Speichermedien)
- ◆ Ersatzteilversorgung (Festplatten sollten mindestens 5 Jahre verfügbar sein)
- ◆ Ordnungsgemäße Aufbewahrung und Lagerung der Datenträger
- ◆ Sicherheitsvorkehrungen (z. Bsp. Einsatz von Dongle)
- ◆ Sicherstellung der Lesbarkeit der Daten auf Dauer
- ◆ Archivierung von Daten

■ Risiken im Umfeld der IT-Steuerung

Mögliche Risiken sind beispielsweise:

- ◆ Zugriffskontrollen zum Rechenzentrum und den Arbeitsstationen
- ◆ Definierte und organisierte Sicherheitsroutinen (z. Bsp. Sicherung nach Generationsprinzip, Sicherung auf andere Datenträger, Biometrische Sicherheitskontrollen (Fingerprint, Iris-Scan))
- ◆ Zugriffskontrollen auf Daten und Einhaltung der datenschutzrechtlichen Bestimmungen (Sicherheitsprozeduren)
- ◆ Notfallplanung / Ausfallzeiten (Kompletter Systemausfall, USV für Server und wichtige Clients)
- ◆ Dokumentationen zu IT-Prozessen und IT-Komponenten (z. Bsp. fehlende Prozessdokumentationen und Ausfallszenarien)
- ◆ Internet- und Intranetnutzung
- ◆ Risiken im Umfeld des Outsourcing von IT

■ Risiken im IT-Bereich

- ◆ Beispiele von Risiken im IT-Bereich
- ◆ Ursachen und Folgen solcher Risiken
- ◆ FME-Analyse als Steuerungsinstrument

■ Klassifizierung der IT-Risiken

- ◆ Risiken im Softwarebereich

■ Aufbau einer IT-Scorecard

■ Risikosteuerung und -kontrolle



■ Ursachen für die Risiken im IT-Umfeld:

Die Ursachen für die Vorhandensein möglicher Gefahren in diesem Bereich sind häufig:

- ◆ mangelnde Integration der IT-spezifischen Überlegungen in die Unternehmensprozesse (z. Bsp. Einbindung der IT in strategische Überlegungen)
- ◆ fehlende Transparenz der IT-spezifischen Erfordernissen und Notwendigkeiten für das Unternehmen im Hinblick auf die Leistungserbringung und Steuerung (z. Bsp. keine bedarfsadäquate Softwareausstattung, unzureichende Sicherheitsvorkehrungen, Mehrfache und ggf. inkonsistente Datenhaltung, mangelnde Ausfall- und Notfallkonzepte)
- ◆ Ausrichtung des Personals und anderer Ressourcen in Bezug auf die IT (z. Bsp. fehlende bedarfskonforme Einweisungs- und Schulungskonzepte für neue Software bzw. Versionen, fehlender internem IT-Support)

■ Klassifizierung der Risiken

Grundsätzlich lassen sich im Hinblick auf den Betriebsprozess folgende 4 Klassen von IT-Risiken definieren:

- ◆ Ausfallrisiken
 - ➔ Risiken durch den Ausfall von Programmen und Systeme
- ◆ Sicherheitsrisiken
 - ➔ Risiken durch fehlende Sicherheitsmassnahmen im Bereich IT
- ◆ Effizienzrisiken
 - ➔ Risiken durch nicht adäquate Nutzung von Programmen und Systemen
- ◆ Qualitätsrisiken
 - ➔ Risiken durch Programm- und Systemmängel

■ Folgen der Risiken im IT-Bereich:

Die möglichen Risiken und deren Folgen im IT-Bereich lassen sich wie folgt klassifizieren:

- ◆ **Ausfallrisiken** können zu Behinderungen im betrieblichen Ablauf führen, die i.d.R. Kosten verursachen und sogar Zielvorgaben gefährden können (z. Bsp. längere Wartezeiten wegen Netzüberlastung, Programmabstürze wegen fehlender Performance oder Programmschwächen, Systemausfälle).
- ◆ **Sicherheitsrisiken** können zum Verlust interner und externer Vertraulichkeit führen, die Gewährung datenschutzrechtlicher Normen gefährden und sogar zu Betriebsspionage führen (z. Bsp. fehlende Sicherheitsvorkehrungen hinsichtlich Softwarenutzung, fehlende Zugangs- und Zugriffskontrollen, fehlende Sicherheitsroutinen bez. der Datenhaltung und -sicherung).

■ Folgen der Risiken im IT-Bereich:

- ◆ **Effizienzrisiken** führen i.a. zu zusätzlichen Kosten im betrieblichen Ablauf und wirken somit direkt auf die Wirtschaftlichkeit der betrieblichen Leistungen (z. Bsp. ineffiziente und fehlerhafte Bedienung von Soft- und Hardware aufgrund mangelnder Einweisung und Dokumentation, fehlende Integrität der Software (Schnittstellenprobleme), mangelnde Ausrichtung der Software an den betrieblichen Abläufen (Organisationsproblem), fehlende Reife der eingesetzten Software)
- ◆ **Qualitätsrisiken** können zu Fehlern bez. der betrieblichen Leistungen führen (beispielsweise falsche Bewertung von Positionen aufgrund von Bewertungs- und Bedienungsfehlern), die Qualität der betrieblichen Leistungen gefährden (z. Bsp. nur unvollkommene Marktanalysen wegen fehlenden Auswertungs- und Erhebungsmöglichkeiten) und die Qualität der Abstimmung und Koordination interner Prozesse (TQM) erheblich beeinträchtigen (z. Bsp. unvollkommene Daten und Auswertungen aus Programmen, fehlende Abstimmung und Erfahrung bei Softwareeinführung und Releasewechsel)

■ Risiken im IT-Bereich

- ◆ Beispiele von Risiken im IT-Bereich
- ◆ Ursachen und Folgen solcher Risiken
- ◆ FME-Analyse als Steuerungsinstrument

■ Klassifizierung der IT-Risiken

- ◆ Risiken im Softwarebereich

■ Aufbau einer IT-Scorecard

■ Risikosteuerung und -kontrolle



■ FME-Analyse als Steuerungsinstrument

Die sogenannte „**F**ehler-**M**öglichkeiten-**E**influss-Analyse“ zielt darauf festgestellte Fehler und potentielle Risiken anhand der 3 Kriterien:

- ◆ Bedeutung (I)
- ◆ Schwierigkeit der Fehlerentdeckung (D)
- ◆ Fehlerhäufigkeit (P)

zu bewerten. Hierzu werden die im Rahmen einer Prozessanalyse festgestellten Fehler anhand einer ordinalen n-stufigen Bewertungsskala (z. Bsp. $n = 3, 5$ oder 10) bzgl. der 3 Kriterien jeweils einzeln bewertet. Um die Bewertung der 3 Kriterien zu erleichtern werden im Rahmen der Fehleraufzählung die möglichen Ursachen und Folgen zu den jeweiligen Fehlern mit aufgelistet. Nach vollzogener Bewertung erfolgt durch Produktbildung die Ermittlung der sogenannten Prioritätenzahl (PZ) wie folgt:

■ FME-Analyse als Steuerungsinstrument

Beispiel für $n = 3$:

$n = 1 \rightarrow$ geringe Bedeutung, geringe Fehlerhäufigkeit, geringe Schwierigkeit der Fehlerentdeckung (1 %)

$n = 2 \rightarrow$ mittlere Bedeutung, mittlere Fehlerhäufigkeit, mittlere Fehlerauffälligkeit (50 %)

$n = 3 \rightarrow$ hohe Bedeutung, hohe Fehlerhäufigkeit, hohe Fehlertransparenz (100 %)

Definition der Prioritätenzahl (PZ):

$$PZ = I * D * P$$

Nach Ermittlung dieser Kennzahl pro Fehler werden diese hinsichtlich ihrer Wertigkeit absteigend sortiert und als Ergebnis erhält man eine quantifizierte Fehlerliste mit absteigender Priorität, die nun zu beheben ist.

■ Risiken im IT-Bereich

- ◆ Beispiele von Risiken im IT-Bereich
- ◆ Ursachen und Folgen solcher Risiken
- ◆ FME-Analyse als Steuerungsinstrument

■ Klassifizierung der IT-Risiken

- ◆ Risiken im Softwarebereich

■ Aufbau einer IT-Scorecard

■ Risikosteuerung und -kontrolle



■ Risiken im Softwarebereich

Beim Einsatz von Software in Unternehmen besteht in den folgenden Bereichen erhöhtes Gefahrenpotential:

- ◆ Einführung neuer Softwaresysteme bzw. weiterer SW-Module

Die Einführung neuer Systeme bzw. Erweiterung von Produktivsysteme durch neue Module birgt nicht nur in der Implementierungsphase Gefahren (versteckte Fehler in den SW-Funktionalitäten, mangelnde Prozessorientierung der Software, mangelnde SW-Einweisung und – Dokumentation, etc.) in sich, die zu einer permanenten Mehrbelastung der Anwender und Ineffizienz der Prozesse führen kann.

- ◆ Releasewechsel bei den Softwaresystemen

Der Releasewechsel bei Softwaresystemen kann ggfs. durch fehlende Informationen und mangelnde Erfahrungen hinsichtlich Einspielung und Systemvoraussetzungen zu erheblichen Störungen des Produktivsystems führen.

■ Risiken im Softwarebereich

◆ Softwarenutzung

Folgende Risikoquellen existieren:

- ◆ Autorisierte Softwarenutzung
- ◆ Berechtigungs- und Rollenkonzepte der einzelnen SW-Systeme
- ◆ Korrektheit der Funktionalitäten
- ◆ Softwareverlässlichkeit und -performance
- ◆ Datensicherheit und Replikationsmöglichkeiten

Diese Quellen möglicher Risiken werden in einem ersten Schritt bei der Softwarebeschaffung durch die Formulierung entsprechender Anforderungen in den jeweiligen Pflichtenheften berücksichtigt, müssen jedoch auch im laufenden Betrieb nicht nur aufgrund stetiger Änderungen in der Software und Vorgaben (gesetzliche Anforderungen, etc.) kontrolliert und überwacht werden.

■ Einführung neuer Softwaresysteme bzw. weiterer SW-Module

- ◆ Bewertung der Risiken durch Betrachtung empirisch messbarer Effekte im Rahmen der Einführung und späteren Nutzung (Wirkung):
 - ◆ Einführungs-Effizienz-Effekt (EEE)
 - ◆ Prozess-Strukturänderungs-Effekt (PSE)
 - ◆ Software-Reifegrad-Effekt (SRE)
- ◆ Kennzahlen zur Bewertung der beobachtbaren Effekten:
 - ◆ Anspannungskoeffizient für EEE
 - ◆ Zeitbedarf pro Prozess und Tätigkeit für PSE
 - ◆ Reife-Erfüllungsgrad für SRE
- ◆ Bewertung der definierten Kennzahlen durch Prozessbeobachtung und -analyse.
- ◆ Benchmarking mit entsprechenden Vergleichswerten.

■ Risiken im IT-Bereich

- ◆ Beispiele von Risiken im IT-Bereich
- ◆ Ursachen und Folgen solcher Risiken
- ◆ FME-Analyse als Steuerungsinstrument

■ Klassifizierung der IT-Risiken

- ◆ Risiken im Softwarebereich

■ Aufbau einer IT-Scorecard

■ Risikosteuerung und -kontrolle



■ Ziel einer IT-Scorecard

Ziel des IT-Scorecard ist es die speziellen Risiken im IT-Umfeld in Unternehmen transparent und messbar zu machen, um somit die Voraussetzung für die Handhabung von IT-Risiken im Unternehmensalltag und Projekten zu schaffen.

■ Aufgaben

- ◆ Aufzeigen und Klassifizieren von Risiken im IT-Umfeld (Identifikation)
- ◆ Messbarkeit der verschiedenen Risikofaktoren (Messbarkeit)
- ◆ Bewertung von IT-Risiken durch geeignete Indikatoren (Bewertung)
- ◆ Analyse der Veränderung der definierten IT-Scorecard (Analyse)

■ Philosophie einer IT-Scorecard

Ausgehend von den spezifischen Aufgaben der Informationstechnologie im Hinblick auf die Unternehmensziele, sind anhand der Erfolgsfaktoren:

- ◆ Ergebnis (IT-Gesamterlös, Investitionen, Servicekosten, etc.)
- ◆ Marktakzeptanz (Neukunden, Serviceanfragen, etc.)
- ◆ Performance (Terminreue, Einhaltung von Projekt-Budgets, etc.)
- ◆ Potenziale (Mitarbeiterschulungen, Mitarbeiterzufriedenheit, etc.)

ein darauf aufbauendes Kennzahlensystem zu entwickeln, das die Leistungsfähigkeit einzelner Bereiche der IT auf der Basis ausgewählter und aussagekräftiger Performance-Indikatoren darstellt.

■ Modelle der Messbarkeit von IT

Frage: „Was sind geeignete Kontrollen für die IT meines Unternehmens und wie kann ich diese messen?“

◆ Maturity Model

Hier geht es um die Verbesserung von IT-Prozessen in Hinblick auf die Ressourcen Zeit, Personal und Kapital, die zuerst in einer Bewertung (in Form eines Assessment) der Geschäftsprozesse den sogenannten „Reifegrad“ anhand eines Kriterienkataloges (mit 18 Hauptkriterien) ermittelt.

➡ ... für strategische Entscheidungen und Benchmark-Vergleiche

◆ Modell der kritischen Erfolgsfaktoren (Critical Success Factors)

Definition der wesentlichen Umsetzungsvorgaben zur Erreichung der Kontrolle in und über die IT-Prozesse.

➡ ... Fähigkeit, die Prozesse unter Kontrolle zu bringen

■ Modelle der Messbarkeit von IT

◆ Ziel Schlüsselindikatoren (Key Goal Indicators)

Hier erfolgt eine Definition von Kenngrößen zur Messung der Erreichung von Zielvorgaben und Anforderungen an die IT und die IT-Prozesse

➡ ... Für Messen der Erreichung der IT-Prozessziele

◆ Performance Schlüsselindikatoren (Key Performance Indicators)

Es handelt sich um Indikatoren zur Messung des Leistungsgrades des IT-Prozesses im Hinblick auf die Unterstützung der Ziel Spitzenindikatoren.

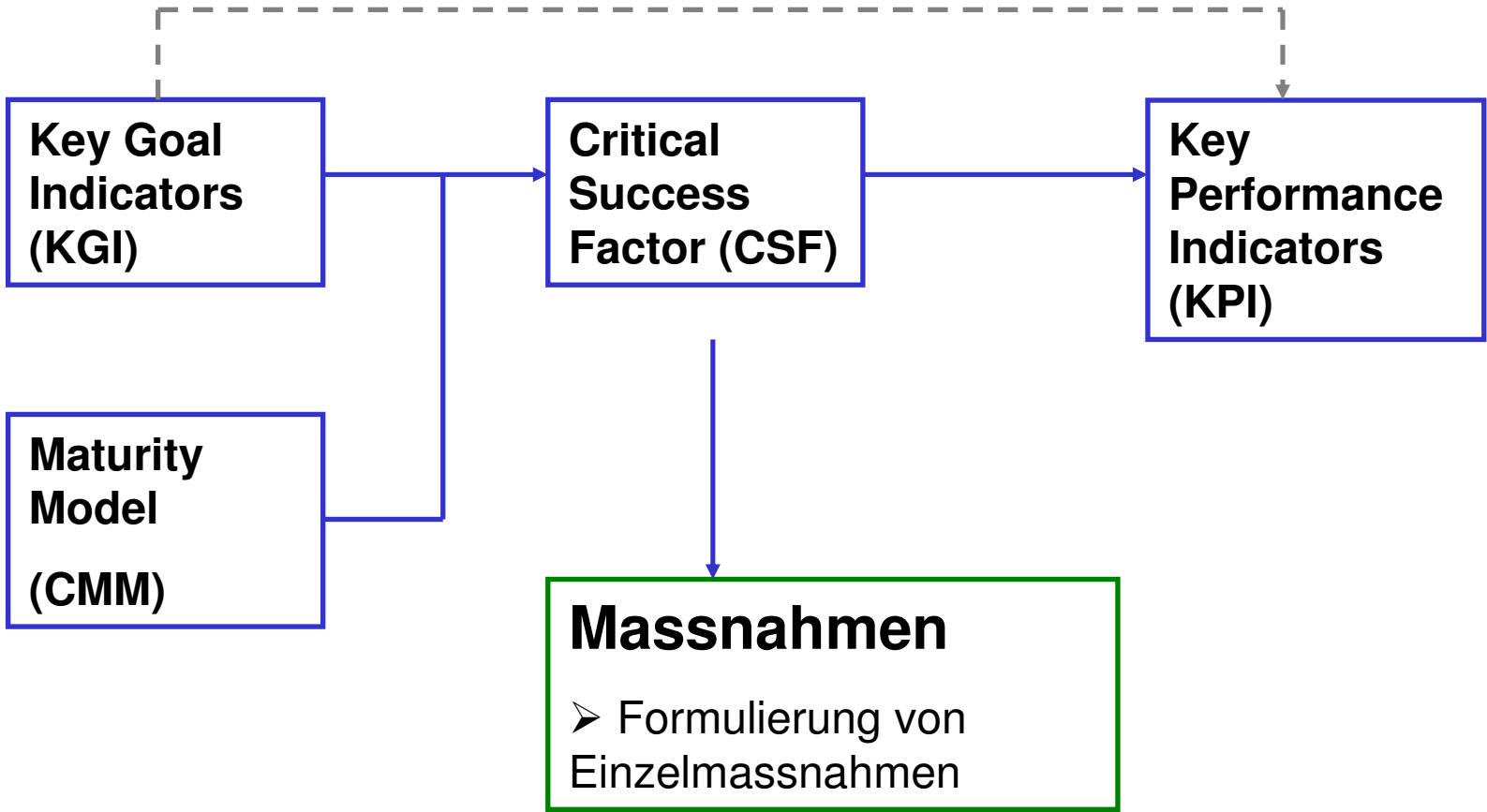
➡ ... Für Messen der Performance in den IT-Prozessen

IT-Kontrollmodell

Planung

Umsetzung

Überwachung



SMART – Anforderung der KPI

■ SMART Anforderung der KPI

Die zu definierenden Performance Schlüsselindikatoren müssen:

Spezifisch

- KPI müssen klar und spezifisch sein
- Aufforderung zu spezifischen Aktionen/Verhalten
 - Vereinbar mit den Unternehmens- und Bereichszielen

Relevant

- KPI müssen die Unternehmenszielsetzungen (Vorgaben, Aufgaben) reflektieren
- Mitarbeiter müssen die KPI als ihre eigenen verinnerlichen

Messbar

- KPI müssen messbar sein
- Fortschritte bei der Erreichung der KPI werden erkennbar
 - Reporting-System notwendig

Ausführbar

- KPI müssen herausfordernd und erreichbar sein
- Herausfordernde KPI motivieren zu höherer Leistung, aber nur wenn sie realistisch erscheinen
 - KPI müssen im Einflussbereich des Mitarbeiters liegen

Terminiert

- KPI müssen einen festgelegten Gültigkeitszeitraum haben
- Die Erfüllung muss in bestimmten Zeiträumen möglich sein

Beispiele von KPI

Perspektivencluster für den IT-Prozess End-User Support

■ Kosten [Finanzperspektive]

- ◆ Anteil der Personalkosten
- ◆ Durchschnittliche Kosten je Anwender

■ Qualität [Kundenperspektive]

- ◆ Erreichbarkeit
- ◆ Kundenzufriedenheit

■ Leistung [Kundenperspektive]

- ◆ Anzahl der Anfragen
- ◆ Umfang des Serviceangebotes

■ Prozess [Prozessperspektive]

- ◆ Durchschnittliche Bearbeitungszeiten
- ◆ Standardisierungsgrad

■ Innovation [Wachstumsperspektive]

- ◆ Reaktionsfähigkeit auf veränderte Serviceanforderungen

Beispiele von KPI

■ Prozessbeispiel: End-User Support

Kosten:

KPI-Name	Anteil der Personalkosten an den IT Gesamtkosten
Definition	Ermittlung der IT-MA, deren Aufgabengebiet ausschließlich in Help Desk, Support liegt
Zielvorgabe (qualitativ)	Bestehender Anteil soll konstant gehalten werden (keine Erhöhung!)
Zielvorgabe (quantitativ)	7 IT-MA; 12 % Kostenanteil
Datenquellen	IT Betriebsergebnis und Kontenauswertung
Ergebnisse	Ist-Personalkosten des End-User-Service an den IT Gesamtkosten
Periodizität	Zweimal im Jahr

Qualität:

KPI-Name	Kundenzufriedenheit
Definition	Durchschnittliche Differenz zwischen der vereinbarten und tatsächlich geleisteten Servicequalität anhand einer 5-Punkte Likert-Skala (stimme voll zu – stimme überhaupt nicht zu)
Zielvorgabe (qualitativ)	Hohe Service Qualität (Umfrage von mindestens 70 Punkten)
Zielvorgabe (quantitativ)	4 Punkte (durchschnittlich bei Auswertung von 100 Anwendern)
Datenquellen	Anwenderbefragung; Service Level Agreements (SLAs)
Ergebnisse	Tatsächlich geleistete Servicequalität; Performance Gap
Periodizität	Einmal im Jahr

IT-Scorecard als Controlling Instrument

Ziel	Kritischer Erfolgsfaktor	Indikator	Kennzahlen-Kandidaten
Herstellung von Kosteneffizienz (im Markt vergleichbar)	Kenntnis der Kosten pro Arbeitsplatz, Vergleichsrechnungen	Kosten pro Arbeitsplatz verfügbar	Kostenabweichung pro Arbeitsplatz gegenüber best practice (in %)
Stetige Sicherstellung der Liquidität	Kenntnisse (zukünftig) Kosten und Erträge, Frühwarn- und Prognosesystem	Liquiditätsplan vorhanden, Frühwarn-/Prognosesystem vorhanden	Working Kapital, Cash Flow, Liquiditätsgrad, Betriebsergebnis
Minimierung von Risiken	Risiken werden erkannt, Gegenmaßnahmen sind definiert	Risiken sind dokumentiert, Gegenmaßnahmen sind vorhanden	Risikofaktoren der Infrastruktur, Applications, Working Capital
Effektiver Ressourceneinsatz	Ressourcen werden zielbezogen eingesetzt, Ressourceninfos sind verfügbar	Zielbezogener Ressourcenplan ist vorhanden	Pro Application umgelegter Ressourceneinsatz in IT-MA

Strategische IT-Durchdringung

Aufgabe:

Sicherstellung, dass sowohl IT-Sachverhalte als auch IT-Möglichkeiten im Unternehmen angemessen bewertet werden und sich in den kurz- und langfristigen Unternehmensplänen widerspiegeln.

Zielindikatoren	Leistungsindikatoren
% Businesspläne, welche in IT Kurz- und Langfristpläne/-ziele münden	Häufigkeit Beurteilung IT-Services (Anzahl Monate seit letztem Update)
% Organisationseinheiten (OE) mit klar definierten IT-Mitteln	Letzter Update IT-Strategieplan (Monate)
Managementbestätigungen zum Link Verantwortung Business → IT-Ziele	% Zufriedenheit Teilnehmer im IT-Planungsprozeß
% OE mit IT-Mitteln gemäss IT-Technologieplan	Periode zwischen Update strategische IT-Planung und operative Pläne
% IT-Budget verantwortet durch Benutzer	Anzahl, Stellung, Aufwand, Verhältnis IT <->Business der Planungspersonen
Anzahl laufender IT-Projekte im Verhältnis zu Ressourcen	Planungsqualität: Zeitgerechtheit, Vollständigkeit, Prozesseinhaltung

IT-Investitions-Controlling

Aufgabe:

Feststellung, ob eine Budgetüberwachung und eine aussagekräftige Kosten-/Leistungsrechnung mit entsprechenden Indikatoren besteht.

Zielindikatoren	Leistungsindikatoren
% Investitionen größer Erwartungen (ROI, Benutzerfeedback)	% Projekte mit Standard IT-Investitionsmodell
Soll/Ist IT-Aufwand in % Unternehmenskosten	% Projekte mit Owner aus Geschäftsbereichen
Soll/Ist IT-Aufwand in % Unternehmensertrag	Anzahl Monate seit letztem Budget-Review
% eingehaltene IT-Budgets von Business Owners	Periode zwischen Abweichung und Abweichungsreporting
Keine Projektverzögerungen durch keine/späte Investitionsentscheidungen	% Projektdokumentationen mit Investitionsberechnungen
	Anzahl Projekte ohne Post-ROI-Review
	Anzahl Projekte mit Investitions-Delta

IT - Projekt - Controlling

Aufgabe:

Stellt fest, ob eine generelle Projektmanagement-Struktur besteht, welche die Inhalte und Grenzen des Projektmanagements und die für jedes laufende Projekt anzuwendende Projektmanagementmethode definiert (Verantwortlichkeiten, Detailaufstellung von Aufgaben, Budgetierung von Zeit und Ressourcen, Meilensteine, Kontrollpunkte und Freigaben).

Zielindikatoren	Leistungsindikatoren
Erhöhung Anzahl Projekte innerhalb Budget und Termin	Zunahme Anzahl Projekte mit Umsetzung Projektmanagementmethode
Verfügbarkeit Termin- und Budget-Info	% Stakeholder in Projekten (Index)
Abnahme Anzahl Projektproblemfälle	Anzahl Trainingstage/Teammitglied
Verkürzung Zeit für Erheben und Beurteilen Projektrisiken	Anzahl Reviews Termine und Budget
Erhöhung Zufriedenheit mit Projektergebnissen	% Projekte mit Post-Projekt-Review
Verbesserung Zeitgerechtheit Projektmanagement-entscheidung	Durchschnittliche Anzahl Jahre Erfahrung der Projektmitglieder

IT - Risiko - Controlling

Aufgabe:

Stellt fest, ob das Vorgehen bei der Risikobeurteilung sicher ist, dass die Analyse von Informationen aus der Risikoidentifikation in einer quantitativen und/oder qualitativen Bemessung des Risikos resultiert, unter Berücksichtigung des Ausmaßes der Risikoakzeptanz des Unternehmens?

Zielindikatoren	Leistungsindikatoren
Zunahme Bedarf Risikobeurteilung	Anzahl Risikomanagement Meetings, WS
Abnahme Problemfälle durch erst bei Eintritt identifizierte Risiken	Anzahl Projekte zur Verbesserung des Risiko-Management
Zunahme erkannte und bei Eintritt reduzierte Risiken	Anzahl Verbesserungen für Prozess der Risikobeurteilung
Zunahme Anzahl IT-Prozesse mit formalisierter Risikobeurteilung	Finanzielle Mittel für Risikomanagementprojekte
% Anzahl kosteneffektiver Maßnahmen zur Risikobeurteilung	Anzahl Updates für kommunizierte Risikolimits und -weisungen
	Anzahl und Frequenz von Risk-Management-Berichten

■ Risiken im IT-Bereich

- ◆ Beispiele von Risiken im IT-Bereich
- ◆ Ursachen und Folgen solcher Risiken
- ◆ FME-Analyse als Steuerungsinstrument

■ Klassifizierung der IT-Risiken

- ◆ Risiken im Softwarebereich

■ Aufbau einer IT-Scorecard

■ Risikosteuerung und -kontrolle



■ Wirkungszusammenhänge

Um die mit Hilfe einer Scorecard definierten Kennzahlen zur Etablierung eines effektiven Risikomanagementsystems zu nutzen, ist es erforderlich, die Kennzahlen unmittelbar mit den Risiken zu koppeln und entsprechende Wirkungszusammenhänge zu definieren. Grundsätzlich lassen sich folgende 2 Effekte definieren:

◆ Effekte von „**Außen**“ nach „**Innen**“

Hierbei handelt es sich um IT-Risiken, die von außen (z. Bsp. neue Softwareversionen, Releasewechsel, neue IT-Techniken, Dokumentationen der SW-Hersteller, neue gesetzliche Bestimmungen) in die Unternehmen wirken und sich in den 4 Risikokategorien wiederfinden.

◆ Effekte von „**Innen**“ nach „**Außen**“

Unternehmensentscheidungen und -vorgänge (z. Bsp. Änderung der Organisationsstruktur, Investitionsentscheidungen) führen hier zu IT-Risiken, die nach außen hin getragen werden (z. Bsp. neues Softwareprodukt verursacht Qualitätsverlust).

■ Funktionsbausteine:

Im Rahmen des weiteren Ausbaus der IT-Scorecard für ein effektives Risikomanagementsystem sind mit Hilfe einer geeigneten Software folgende Funktionsbausteine Zug um Zug zu etablieren:

- ◆ Aufbau von Kennzahlenhierarchien gemäß DUPONT-Schema bei den betriebswirtschaftlichen Kennzahlen (**Rückverfolgung von Abweichungen**)
- ◆ Sensitivitätsanalysen betriebswirtschaftlicher Kennzahlen und Funktionen (**Ermittlung der Parameterempfindlichkeit**)
- ◆ Lösungsverhalten nichtlinearer Systemlandschaften sogenannter Hardfacts durch numerische Iterations- und Simulationsverfahren (**Bestimmung stabiler Szenarien mit den Randbedingungen**)
- ◆ Ermittlung von Kenngrößen für Softfacts (Qualitätsanforderungen, Mitarbeitermotivation, etc.) durch Definition „prozessunterstützender“ Zustandsräume (**ordinale Wertskalen für alle qualitativen Größen**)

Internes Kontrollsystem (IKS)



■ Zielsetzung eines IKS

- ◆ Welche gesetzlichen Anforderungen?
- ◆ Was ist ein IKS?
- ◆ Wie sind interne Kontrollen definiert?
- ◆ Welche Aufgaben hat ein IKS?
- ◆ Welche Anforderungen sind an ein IKS zu stellen?
- ◆ Welche Risiken sind im Unternehmen zu finden?
- ◆ Regelungsbereiche in einem IKS

■ Ausgestaltung eines IKS

■ Vorgehensmodell zur Realisierung IKS



Zielsetzung eines IKS

■ Welche gesetzlichen Anforderungen müssen erfüllt werden?

◆ Gesetzliche Grundlage:

- § 317 Abs. 4 HGB-Gesetz

„Bei einer börsennotierten Aktiengesellschaft ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.“

- § 91 Abs. 2 AktG

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden

- implizit: Datenschutzgesetz

Zielsetzung eines IKS

- **Welche gesetzlichen ähnlichen Anforderungen müssen erfüllt werden?**
 - ◆ IDW PS 260:
 - Prüfungsstandard des IDW (Instituts der Wirtschaftsprüfer in Deutschland e.V.), die dem internationalen Prüfungsstandard ISA 400 „Risk Assessments and Internal Control“ entspricht
 - ◆ GoB und GoBS
 - Grundsätze ordnungsgemäßer Buchführung und Buchführungssysteme sind teils geschriebene, teils ungeschriebene Regeln zur Sicherstellung der Ordnungsmäßigkeit, Sicherheit, Nachvollziehbarkeit und Vollständigkeit der Buchführung und Bilanzierung
 - ◆ SOX 404:
 - Sicherstellung der Etablierung eines funktionierenden, rechnungslegungsbezogenen internen Kontrollsystems für alle Firmen, die an der US-Börse notiert werden.

Zielsetzung eines IKS

■ Was ist ein Internes Kontrollsystem?

◆ Definition IKS = Steuer- und Überwachungssystem

Gesamtheit aller Grundsätze, Verfahren und aufeinander abgestimmten und miteinander verbundenen Kontrollen innerhalb eines Systems, die von der Unternehmensleitung autorisiert wurden.

Der Begriff System umfasst nicht nur das DV-System, sondern auch den gesamten organisatorischen und kaufmännischen Bereich.

Zielsetzung eines IKS

■ Wie sind Kontrollen definiert?

- ◆ Kontrollen erfolgen durch Maßnahmen, die in den Arbeitsablauf integriert sind.
- ◆ Kontrollen sollen die Wahrscheinlichkeit für das Auftreten von Fehlern in den Arbeitsabläufen vermindern bzw. aufgetretene Fehler aufdecken.

Zielsetzung eines IKS

■ Welche Aufgaben hat ein IKS?

- ◆ Sicherstellung der gesetzlich geforderten Ordnungsmäßigkeit der Buchführung und der DV-gestützten Anwendungssysteme
- ◆ Schutz von Vermögenswerten
- ◆ Einhaltung der Geschäftspolitik bzw. der Strategie
- ◆ Wirtschaftlichkeit und Transparenz der Arbeitsabläufe
- ◆ Erhöhung der Informationsqualität durch genaue, aussagefähige, zeitnahe Aufzeichnungen
- ◆ Fehlerprävention und Fehleraufdeckung
- ◆ Verhinderung doloser Handlungen und Rechnungslegungsdelikte

Zielsetzung eines IKS

■ Welche Anforderungen sind an ein IKS zu stellen?

- ◆ Zwangsläufigkeit von Arbeitsabläufen
- ◆ Funktionstrennung
- ◆ Kontrollmaßnahmen
- ◆ Realisierung des Vier-Augen-Prinzips
- ◆ Dokumentation der Prozesse
- ◆ Angemessenheit der vorgesehenen Maßnahmen

Zielsetzung eines IKS

■ Welche Risiken sind im Unternehmen zu finden?

◆ Aufbauorganisation

- unzureichende Kompetenzabstimmung
- unzureichende Funktionstrennung in der IT-Abteilung und im kaufmännischen Bereich
- Abhängigkeit des Unternehmens von einzelnen Mitarbeitern des DV-Bereichs und des kaufmännischen Bereichs

Zielsetzung eines IKS

■ Welche Risiken sind im Unternehmen zu finden?

- ◆ Systementwicklung und -pflege
(insbesondere Anwendungssystem-Programmierung)
 - nicht genehmigte, versehentliche falsche, bewusst manipulierte Programmentwicklungen/-änderungen gelangen in das Produktivsystem und bewirken
 - Instabilität
 - Inkonsistenz oder
 - fehlende Integrität der Daten

Zielsetzung eines IKS

■ Welche Risiken sind im Unternehmen zu finden?

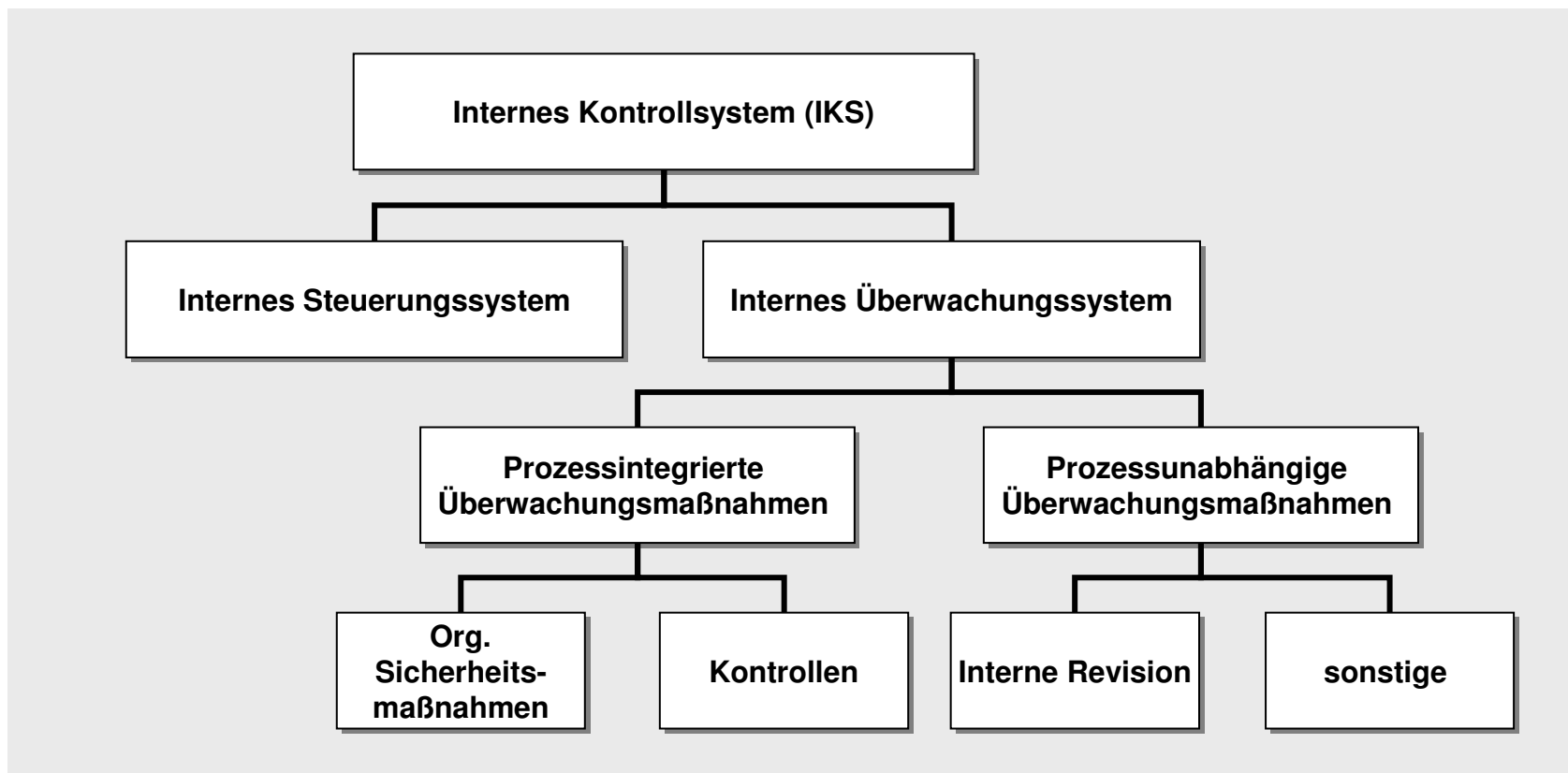
- ◆ Datenfluss und Datenerfassung
 - unvollständige Datenerfassung, -verarbeitung
 - unautorisierte Veränderung von Daten
 - die Datenübertragung an den Schnittstellen erfolgt unbemerkt fehlerhaft oder gar nicht
- ◆ Prüfung der sachlichen Verarbeitungsregeln
 - unrichtige Datenverarbeitung
 - Fehleinstellungen von Tabellen/Parametern
 - Rückgriff auf eine fehlerhafte Stammdatenbasis

Zielsetzung eines IKS

- **Welche Risiken sind im Unternehmen zu finden?**
 - ◆ Verfahrensdokumentation
 - Abhängigkeit von den mit der DV beauftragten Personen
 - keine Nachvollziehbarkeit der Verarbeitungsverfahren und Geschäftsvorfälle

Zielsetzung eines IKS

■ Regelungsbereiche des Internen Kontrollsystems



■ Zielsetzung eines IKS

- ◆ Welche gesetzlichen Anforderungen?
- ◆ Was ist ein IKS?
- ◆ Wie sind interne Kontrollen definiert?
- ◆ Welche Aufgaben hat ein IKS?
- ◆ Welche Anforderungen sind an ein IKS zu stellen?
- ◆ Welche Risiken sind im Unternehmen zu finden?
- ◆ Regelungsbereiche in einem IKS

■ Ausgestaltung eines IKS

■ Vorgehensmodell zur Realisierung IKS



Ausgestaltung eines IKS

- Welche Kontrollen finden bezogen auf die Unternehmensorganisation statt?

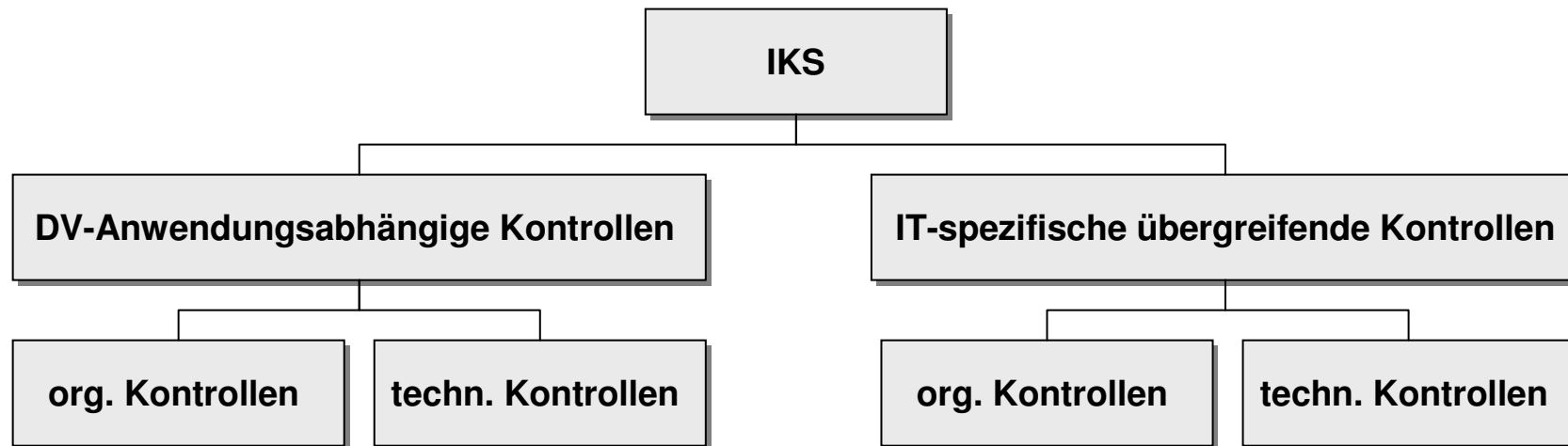


Beispiele:

- Organigramme
- Stellenbeschreibungen
- Kompetenzen und Vollmachten (auch Kontrollinstanzen)
- organisatorische Grundsätze und Prinzipien
- Zugriffsberechtigungskonzept

Ausgestaltung eines IKS

■ Welche Kontrollen gibt es im DV-technischen Bereich?



Beispiele:

- Datenfluss und Verarbeitungsprozeduren, Sicherstellung der Zwangsläufigkeit von Arbeitsabläufen (z. B. Fehlerkontrolle EDI)
- Jobverarbeitung
- Archivierung
- Verfahrensdokumentation und Nachweis der Parametrierung/Customizing

Beispiele:

- Programmentwicklung/-änderung
- Change-Management
- Operating und Systemüberwachung
- Support und Wartung
- Datensicherheit (z. B. Zugriffsberechtigungen, Passwortverfahren)
- Datensicherung und Recovery

■ Zielsetzung eines IKS

- ◆ Welche gesetzlichen Anforderungen?
- ◆ Was ist ein IKS?
- ◆ Wie sind interne Kontrollen definiert?
- ◆ Welche Aufgaben hat ein IKS?
- ◆ Welche Anforderungen sind an ein IKS zu stellen?
- ◆ Welche Risiken sind im Unternehmen zu finden?
- ◆ Regelungsbereiche in einem IKS

■ Ausgestaltung eines IKS

■ Vorgehensmodell zur Realisierung IKS



Vorgehensmodell zur Realisierung IKS

■ Bestandsaufnahme der Prozessorganisation

- ◆ Aufnahme der Prozessorganisation im Geltungsbereich des IKS, einschließlich der Schnittstellen vor- und nachgelagerter Prozesse
 - Abstimmung mit der Geschäftsleitung/Vorstand bez. der definierten Unternehmensstrategie und risiko-relevanter Prozesse
 - Definition der Prozessverantwortlichen (Prozess-Owner)
 - Analyse vorhandener Risiken und Schwachstellen

Vorgehensmodell zur Realisierung IKS

■ Erarbeitung der Zielarchitektur des IKS in folgenden Schritten:

- ◆ Herausarbeitung prozessintegrierter und prozessunabhängiger Überwachungsmaßnahmen und der Beziehungen zwischen ihnen
- ◆ Aufteilung der beiden Komplexe von Überwachungsmaßnahmen in abgrenzbare, überschaubare Kontrollbereiche (ebenfalls prozessorientiert)
- ◆ Abgrenzung der Bestandteile und Inhalte des IKS von anderen Systemen und deren Inhalte (wie beispielsweise Management-Info-Systeme)
- ◆ Bestimmung von Kontrollgremien und Verantwortlichkeiten je Kontrollbereich, differenziert nach Planung, Steuerung und Kontrolle

Vorgehensmodell zur Realisierung IKS

■ Aufnahme und Wertung der:

- ◆ vorhandenen methodisch-organisatorischen Planungs-, Steuerungs- und Überwachungselemente je Kontrollbereich IKS
- ◆ durch die genutzten DV-Systeme unterstützten Abstimm- und Kontrollverfahren (z. Bsp. Verprobung, Konsistenzprüfung, Prüfung Datenübernahme, etc.)
- ◆ durch die genutzten DV-Systeme unterstützten Fehlerkontrollen und Plausibilitätsprüfungen (d.h. der maschinellen Kontrollen)
- ◆ vorgefundenen Geschäftsverteilung, Funktionszuordnung und Verantwortungsabgrenzung (einschließlich Zugriffsberechtigungskonzept für die wichtigsten DV-Anwendungssysteme) im Kernbereich des IKS
- ◆ zur Absicherung einer gleichermaßen sicheren (kontrollierten) und effizienten Funktionstrennung und Verantwortungsabgrenzung
- ◆ der Form der im Bereich der Planung, Steuerung und Überwachung verwendeten Arbeitsmittel

Vorgehensmodell zur Realisierung IKS

■ Zusammenfassung der Ergebnisse zur Zielarchitektur

- ◆ Hier sind die Ergebnisse zur Zielarchitektur des IKS sowie zum Ausgangsstand und Festlegung der Hauptzielrichtung der weiteren Arbeit, wichtig zu abzusichernder Einzelergebnisse, einer geeigneten Vorgehensweise, sinnvollen Arbeitsteilung, Kalkulation des erforderlichen externen und internen Aufwandes etc. zusammenzufassen, und zwar in einer solchen Form, dass sie als Entscheidungsvorlage für Geschäftsführung/Vorstand dienen kann.

Vorgehensmodell zur Realisierung IKS

■ Konzept-Abstimmung

- ◆ In diesem Schritt erfolgt die Abstimmung des Konzeptes (Ziele, Zielarchitektur, Vorgehensweise, etc.) mit weiteren zum Thema her Beteiligten bzw. Zuständigen, darunter
 - die Geschäftsleitung bzw. der Vorstand,
 - dem Wirtschaftsprüfer,
 - den zuständigen Führungskräften der Bereiche Rechnungswesen, Controlling und Revision

Vorgehensmodell zur Realisierung IKS

- **Ausgestaltung bzw. Neuentwicklung der Arbeitsmittel zur Planung, Steuerung und Überwachung mit dem Ziel, einheitlicher, in Form und Inhalt der Funktion angemessener Ausgestaltung:**
 - ◆ Vorgaben von Geschäftsführung/Vorstand und deren Kontrollgremien
 - ◆ Richtlinien für einzelne Bereiche der Prozessorganisation
 - ◆ Regelwerke mit Querschnittcharakter
 - ◆ Organisations-, Arbeits- und Verfahrensanweisungen
 - ◆ Abstimm- und Kontrollanweisungen

Vorgehensmodell zur Realisierung IKS

- **Konsolidierung, Weiterentwicklung und – wo erforderlich – Neuentwicklung der Methoden, Verfahren und Instrumentarien für die Kernprozesse innerhalb des IKS und zwar zur Sicherung ihrer**
 - ◆ Einheitlichkeit in Diktion und Form
 - ◆ Verbindlichkeit und Zwangsläufigkeit ihrer Anwendung/Durchführung
 - ◆ Durchgängigkeit im Gesamtprozess von Planung, Steuerung und Überwachung (im Sinne eines Regelkreises)
 - ◆ Praktikabilität, Effizienz und Wirtschaftlichkeit

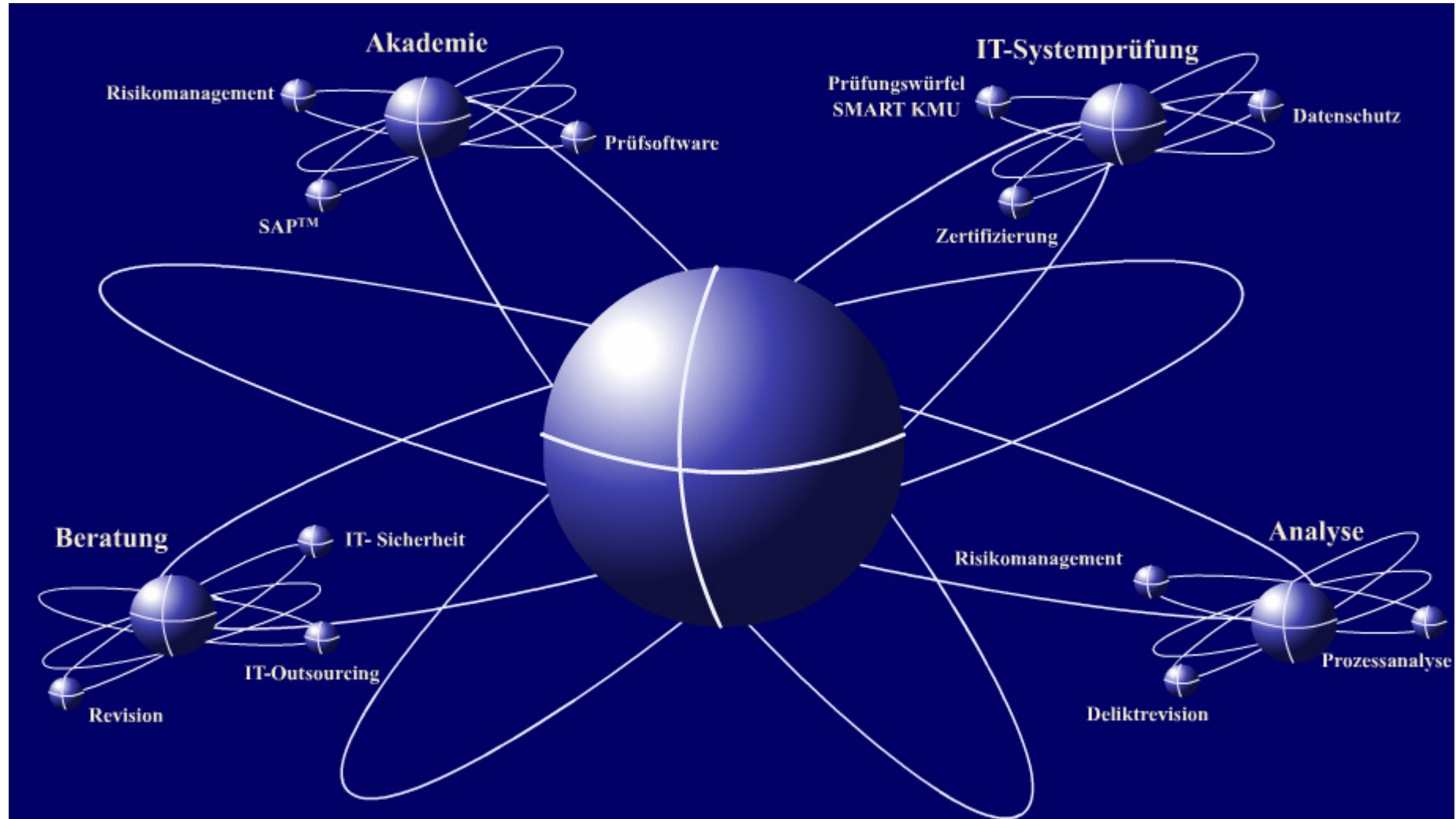
Vorgehensmodell zur Realisierung IKS

■ Gestaltungs- und Parametrisierungsphase

- ◆ Ausgestaltung des Anwendungsumfeldes bzw. Parametrisierung (Customizing) jener Komponenten der genutzten DV-Anwendungssysteme, die in besonders starkem Maße Ordnungsmäßigkeit, Sicherheit und Funktionsfähigkeit des IKS beeinflussen und damit gleichermaßen Gewährleistung der gesetzlichen Minimalanforderungen (HGB, AO, GoBS u.a.) und entsprechender Bereichsstandards (IT-Mindestanforderungen, IDW PS 260, IDW PS 880, ID PS 330 u.a.).

Vorgehensmodell zur Realisierung IKS

- **Sicherung der Grundlagen für Geschäftstätigkeit und IKS, insbesondere der erforderlichen**
 - ◆ Datenbasis (nicht codierte und codierte Daten)
 - ◆ Funktionalität der DV-Anwendungssysteme (Verfügbarkeit, Zuverlässigkeit, Service-Levels, etc.)
 - ◆ Dokumentation (primär Verfahrensdokumentation im Sinne GoBS)
- **Konzipierung des weiteren Aus- und Aufbaus des IKS im mittelfristigen Zeitraum in Form einer Entscheidungsvorlage (Phasenkonzept mit Meilensteine)**



Wir freuen uns auf Ihren geschätzten Besuch!

Danke für Ihr Interesse