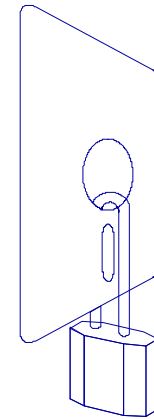


IKS – Internes Kontrollsystem und Kennzahlen

IT-Revision Forum 2007

Wolf Sommer, Senior Consultant, CISM

F.-J. Lang IT-Security Consulting GmbH, München



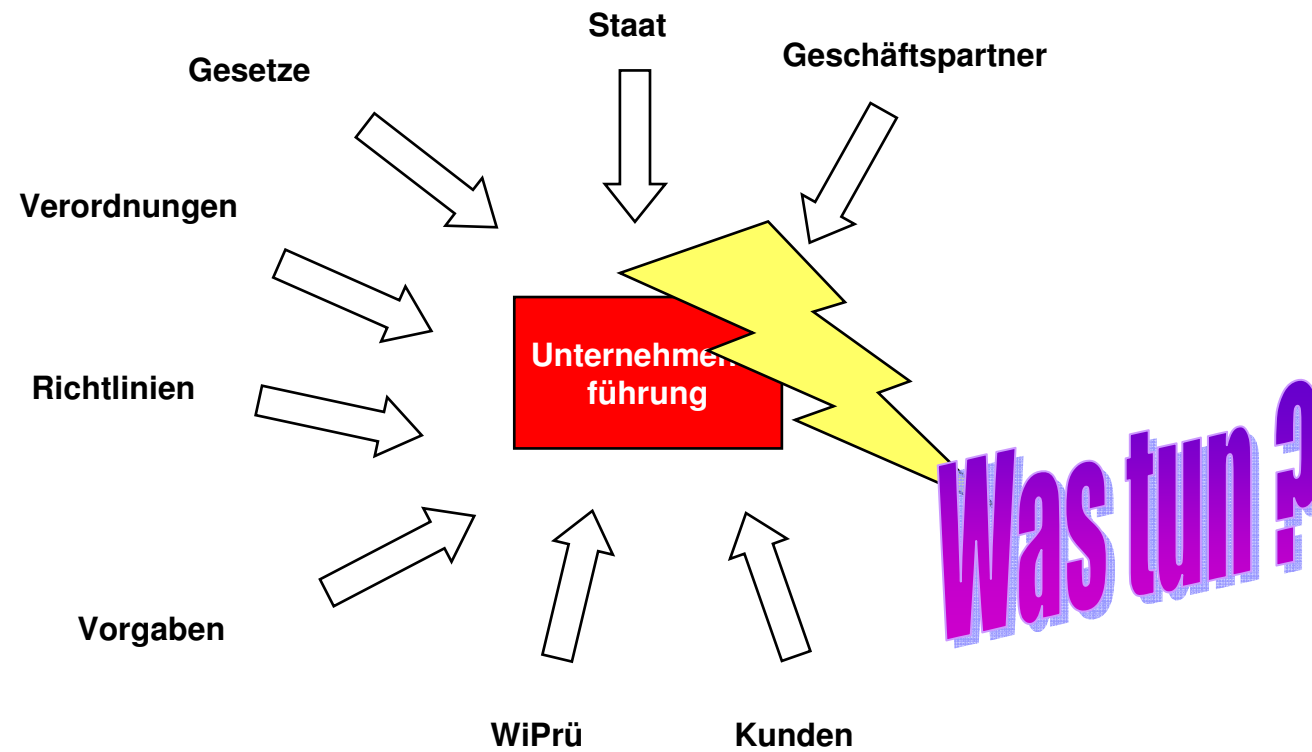
Agenda

1. IKS - Internes Kontrollsystem
2. Rahmenbedingungen
3. Umsetzungsbeispiel
4. Kennzahlen entwickeln
5. Zusammenfassung

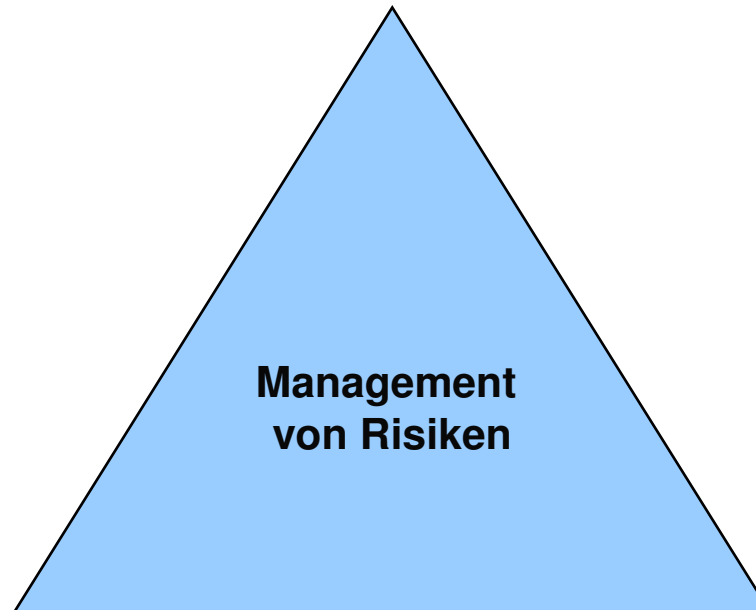
Agenda

1. IKS - Internes Kontrollsystem
2. Rahmenbedingungen
3. Umsetzungsbeispiel
4. Kennzahlen entwickeln
5. Zusammenfassung

Regulatorische Anforderungen



IKS – warum, weshalb, wieso?



Definition des IKS: Steuer- und Überwachungssystem als Gesamtheit aller aufeinander abgestimmter Kontrollen innerhalb eines Systems.

IKS - Internes Kontrollsystem

Ziele

- Systematisch gestaltete organisatorischen Massnahmen und Kontrollen im Unternehmen zur Einhaltung von Gesetzen, Richtlinien, Regeln und zur Abwehr von Schäden, die durch das eigene Personal oder Dritte verursacht werden können
- Technische und organisatorische Massnahmen
- Sie umfassen Aktivitäten und Einrichtungen zur unternehmensinternen Kontrolle sowie ihre Beziehungen zueinander
- Funktionalität und Qualität (z.B. SOX 404)

IKS - Internes Kontrollsystem

Treiber

- Eigentümer
- Management
- Externe Stellen (z.B. Gesetzgeber, EU, Rechnungshöfe, Wirtschaftsprüfer, Versicherungen und Banken)
- Interne Stellen (z.B. QM, Security Management, Risikomanagement, Revision)
- Allgemein: Anforderung Compliance

IKS - Internes Kontrollsystem

Kontrollen

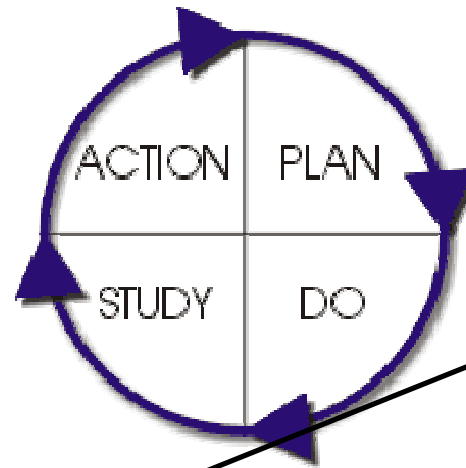
- Verfahren, die in den Arbeitsabläufen integriert sind
- Reduzierung der Wahrscheinlichkeit des Eintritts eines Fehlers
- Erhöhung der Wahrscheinlichkeit, Fehler zu entdecken

IKS - Internes Kontrollsystem

Anforderung

- Dokumentation
- Existenz von definierten Arbeitsabläufen
- Beschreibung der Kontrollmassnahmen
- Angemessenheit
- Vier-Augen-Prinzip
- Funktionstrennung

Die 30er und 40er Jahre ...



Deming-Kreis - Gedankenmodell PDSA

Agenda

1. IKS - Internes Kontrollsystem
2. Rahmenbedingungen
3. Umsetzungsbeispiel
4. Kennzahlen entwickeln
5. Zusammenfassung

Motivation

Regulatorische Anforderungen

- IDW PS 260
- IDW PS 330 (Einsatz von Informationstechnologie)
- IDW PS 331 (bei Outsourcing)
- IDW PS 951 (seit 19.09.07, ausgelagerte Funktionen)
- HGB §314 Abs. 4
- §91 Abs. 2 AktG
- GoB und GoBS
- MaRisk (Finanzdienstleister und indirekt auch für Outsourcingnehmer)
- SOX, Section 404

Motivation

Implementierung eines Standards zur Reduzierung von Risiken

- z.B. Sicherheitsstandards ISO27001, ISO17799, BSI-Grundschutz, CobIT usw.

Nachhaltigkeit der Massnahmen sicherstellen

- Steuerung der Prozesse
- Identifizierung der Risiken für die Geschäftsprozesse
- Transparenz

Primäre Treiber

- Anforderungen der Wirtschaftsprüfer

Agenda

1. IKS - Internes Kontrollsystem
2. Rahmenbedingungen
3. **Umsetzungsbeispiel**
4. Kennzahlen entwickeln
5. Zusammenfassung

Regulatorische Anforderungen

Wesentliche Vorgaben für die IT

Kategorien

- Art der Vorgaben: Gesetze, Verlautbarungen, Rundschreiben, Standards
- Anwendungen für: Branche (Banken, Automobilindustrie etc.), Gesellschaftsform („AG“), Art des Objektes („personenbezogene Daten“), spezielle Unterscheidungen („gelistete Unternehmen“)



- Weitere Vorgaben: Signaturgesetz, Telemediengesetz etc.

Wirtschaftsprüfer – Worauf kommt es an?

PS 260	<p>Das internes Kontrollsystem im Rahmen der Abschlussprüfung</p> <ul style="list-style-type: none">➤ Ausgestaltung des IKS➤ Risikoorientierte Abschlussprüfung➤ Prüfung des Aufbaus und der Funktion eines IKS➤ Grenzen der Prüfung	<p>verwandte Themen:</p> <ul style="list-style-type: none">➤ Organisatorische Konzepte➤ Kontrollen im Prozess IT-Sicherheitsmanagement
PS 331	<p>Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen</p> <p>Themen (z.B.):</p> <ul style="list-style-type: none">➤ Arten der Auslagerung➤ Prüfung beim Dienstleister	<p>verwandte Themen:</p> <ul style="list-style-type: none">➤ Vertragsbeziehungen➤ Outsourcing
PS 951	<p>Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen</p> <ul style="list-style-type: none">➤ Arten der Auslagerung	<p>verwandte Themen:</p> <ul style="list-style-type: none">➤ Bescheinigung Typ A➤ Bescheinigung Typ B (entspr. SAS70)

Wirtschaftsprüfer – Worauf kommt es an?

Anforderung des IDW PS 331

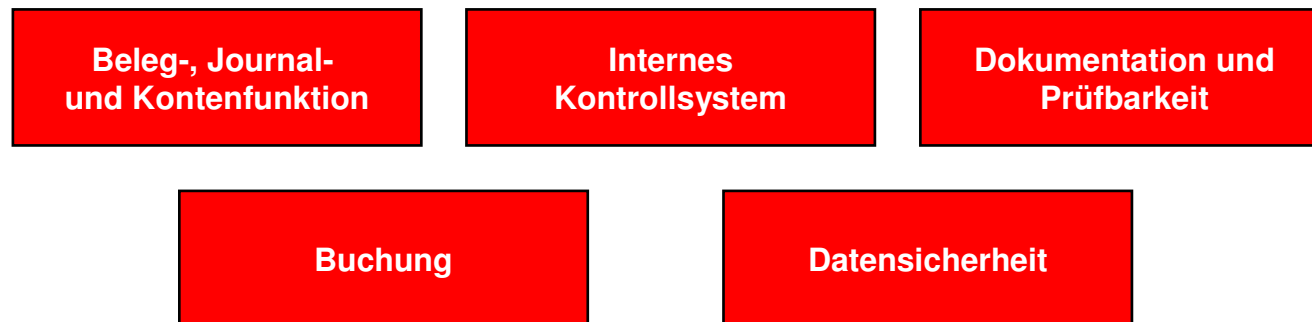
- Die Anforderungen für das IKS im IT-Betrieb leiten sich im Wesentlichen aus den Anforderungen des FAIT 1 ab
- Zusätzlich bestimmt KWG § 25a bei Banken die Anforderungen
- Dokumentation und klare Formulierung der Kontrollziele in den Dokumenten (Prozesse-, Verfahrensbeschreibungen, Arbeitsanweisungen, Handbücher)
- Nachvollziehbarkeit der Ableitung der Kontrollziele aus den gesetzlichen und aufsichtsrechtlichen Vorgaben
- Inhaltliche Ausgestaltung und Berücksichtigung von Anforderungen aus der IT-Sicherheit (z.B. FAIT 1)
- Definierte Kontrollen müssen auch nachweisbar durchgeführt werden
- Nicht die Menge der Kontrollen ist entscheidend, sondern die „Qualität“

Überwachung eines Kontrollsystems nach FAIT1

GoBS

Grundsätze ordnungsgemässer DV-gestützter Buchführungssysteme

→ Die GoBS stellt Anforderungen an:



Überwachung eines Kontrollsystems nach FAIT1

GoBS

Kapitel	Inhalt
1	Vorbemerkungen
2	Das IT-System und der Einsatz von IT im Unternehmen
3	Der Einsatz von IT in der Rechnungslegung
3.1	Sicherheitsanforderungen an rechnungslegungsrelevante Daten
3.2	Grundsätze ordnungsgemäßer Buchführung
4.	Die Errichtung eines IT-Systems mit Rechnungslegungsbezug
4.1	IT-Umfeld und IT-Organisation
4.2	IT-Infrastruktur
4.3	IT-Anwendungen
4.4	IT-gestützte Geschäftsprozesse
4.5	Überwachung des IT-Kontrollsystems
4.6	IT-Outsourcing

Überwachung eines Kontrollsystems nach FAIT1

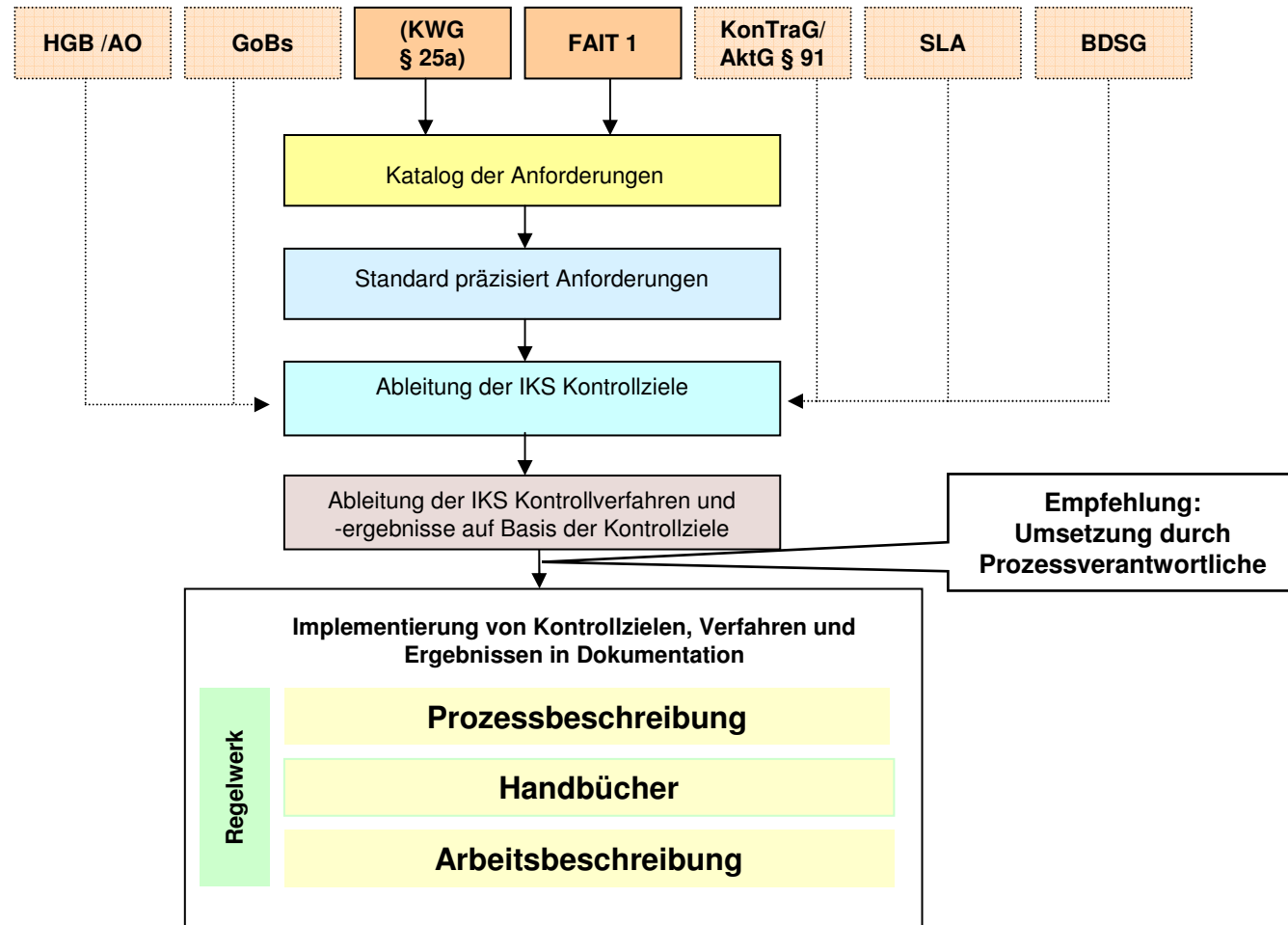
Ziffer	Inhalt	Umsetzung durch Standards (z.B: ISO27001)
110	Unter Überwachung des IT-Kontrollsystems ist die Beurteilung der Wirksamkeit des IT-Kontrollsystems im Zeitablauf durch Mitarbeiter des Unternehmens zu verstehen. Dabei ist zu beurteilen, ob das IT-Kontrollsystem sowohl angemessen ist als auch kontinuierlich funktioniert. Darüber hinaus haben die gesetzlichen Vertreter dafür Sorge zu tragen, dass festgestellte Mängel im IT-Kontrollsystem abgestellt werden.	Verantwortlichkeiten Durchführung von Audits Risikomanagementprozess
111	Ein wesentliches Element des internen Überwachungssystems stellt die Überwachungstätigkeit im besonderen Auftrag der gesetzlichen Vertreter dar ("High-Level-Controls"). Sie beinhaltet im Einzelfall Aktivitäten, die durch die gesetzlichen Vertreter selbst ergriffen bzw. beauftragt werden und eine Beurteilung erlauben, ob die Strategien (Unternehmensstrategie und IT-Strategie), die daraus abgeleiteten Grundsätze, Verfahren und Massnahmen (Regelungen) in Übereinstimmung mit den Unternehmenszielen umgesetzt wurden, ob das eingerichtete Kontrollsystem angemessen und wirksam ist und ob die umgesetzten Massnahmen die Erreichung der Unternehmensziele sicherstellen. Typische Beispiele für diese Kontrollen sind die Durchsicht von Fehler- und Ausnahmeberichten im Hinblick auf die Beeinträchtigung kritischer Erfolgsfaktoren, die Durchführung von Benchmarks oder die regelmäßige Analyse der internen Dienstleistungsqualität.	Verantwortlichkeiten Planerische Aufgaben IT-Strategie IT-Steuerung Risikomanagementorganisation
112	In zahlreichen Unternehmen wird neben prozessintegrierten ÜberwachungsMassnahmen das IT-Kontrollsystem von der Internen Revision überwacht. Zu den Aufgaben der Internen Revision zählt die Beurteilung der Wirksamkeit des eingerichteten IT-Kontrollsystems sowie die Überwachung der Einhaltung der Regelungen und Anforderungen der gesetzlichen Vertreter und der Ordnungsmäßigkeit z. B. durch eine regelmäßige Überwachung sensibler IT-gestützter Geschäftsprozesse.	Definition von Rahmenbedingungen Kontrolle der Innenrevisionstätigkeit

Umsetzung der Anforderungen

Vorgehensmodell

- Identifikation der relevanten regulatorischen Anforderungen
- Auswahl eines Standards und Erstellung eigener Vorgaben
- Mapping der Vorgaben auf regulatorische Anforderungen
- Definition des SOLL-Standes
- Analyse des IST-Standes
- Vereinbarung von Massnahmen

Umsetzung der Anforderungen



Umsetzung

IKS-Basis entwickeln

- IKS-Ziele ableiten/ erarbeiten
- Kontrollen definieren
- Dokumentationsgrad festlegen
- Kontrollen durch Massnahmen, die in den Arbeitsablauf integriert sind
- Abstimmung mit Geschäftsleitung/ Vorstand
- Abstimmung mit Wirtschaftsprüfer
- Abstimmung mit Prozessverantwortlichen und Führungskräfte
- Abstimmung mit Revision

Inhalte

Kontrollziel	Kontrollverfahren	Kontrollergebnis	Anmerkung
Was ist das gültige Kontrollziel, das es zu erreichen gibt?	Wie läuft das Kontrollverfahren ab?	Wie und wo werden die Kontrollziele abgelegt? Wer ist der Verantwortliche?	Detaillierung der Informationen
Ziele aus Vorgaben von Normen (z.B. ISO 27001, BSI)	Ausfüllen von Excel-Listen, webbasierte Eingabe von Kontrollwerten, Abarbeitung eines Workflowtools usw.	Wie wird auf Abweichungen reagiert?	dto.

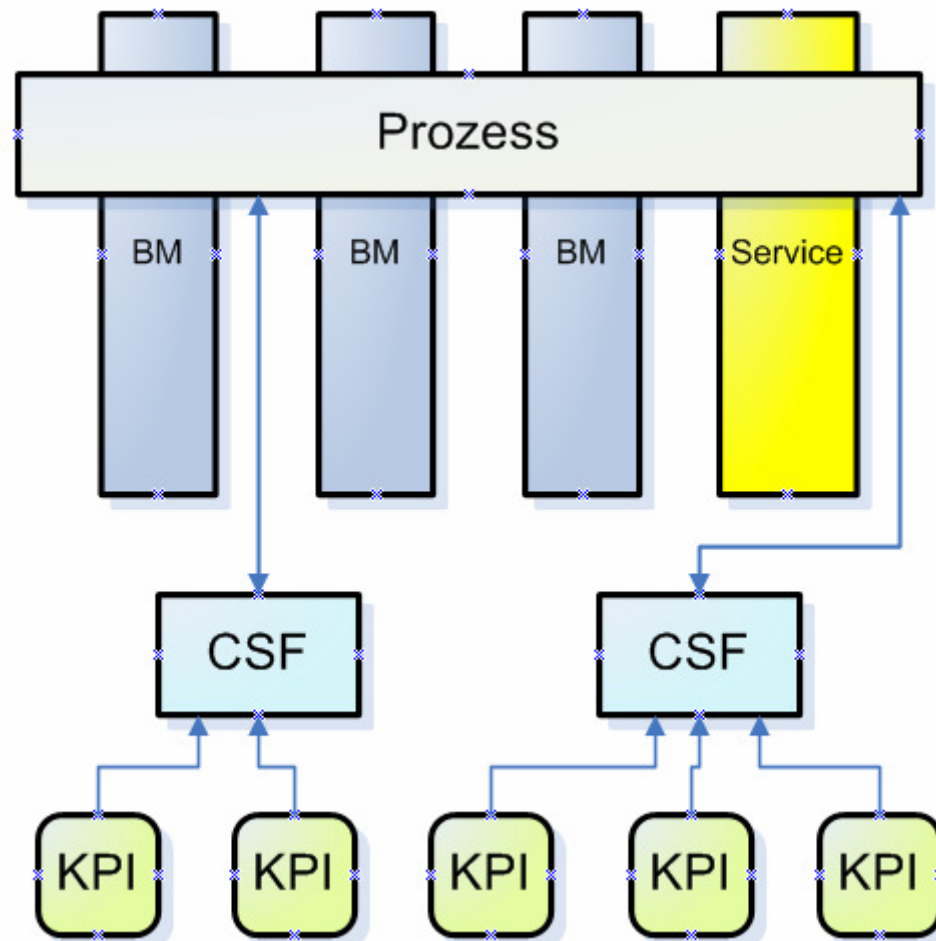
Agenda

1. IKS - Internes Kontrollsystem
2. Rahmenbedingungen
3. Umsetzungsbeispiel
4. Kennzahlen entwickeln
5. Zusammenfassung

Kennzahlen entwickeln

- Prozessverständnis
(vorne kommt etwas „rein“, hinten kommt etwas „raus“)
- Prozesse definieren (Empfehlung: Von hinten beginnen)
- Reifegrad der Prozesse berücksichtigen
- Prozesswelt von Organisationswelt trennen
- Risiken erkennen (und adressieren)
- Nicht versuchen alle Eventualitäten abzufangen (Lösung über Reaktion auf Sonderfälle suchen)
- „Kritische Erfolgsfaktoren“ (KEF) der Prozesse erkennen

Kennzahlen entwickeln



Kritische Erfolgsfaktoren

- Messung über „Kritische Erfolgsfaktoren“ KEF (Critical Success Factors CSF)
- Beachten der KEF bringt in der Regel eine 80%ige Erreichung der Ziele
- „Key Performance Indicators“ KPI für KEF definieren
- Jeder KEF sollte mit mindestens einem oder mehreren KPI's bewertet werden
- Formulierung von Massnahmen

Key Performance Indicators

- Problem: KPI's lassen sich in der Regel nicht ableiten
- Konstruktion der KPI's durch geeignete Fragestellungen und daraus abgeleiteten spezifischen Eigenschaften

Anforderung an ein KPI

- Aktualität
- Zweckeignung
- Genauigkeit
- Einfachheit und Nachvollziehbarkeit
- Kosten-Nutzen Beziehung

Inhalte eines KPI

Beschreibung <ul style="list-style-type: none">➤ Bezeichnung➤ Beschreibung➤ Adressat	<ul style="list-style-type: none">➤ Zielwert➤ Sollwert➤ Toleranzwert	<ul style="list-style-type: none">➤ Eskalationsregel➤ Gültigkeit➤ Verantwortlicher
Datenermittlung <ul style="list-style-type: none">➤ Datenquellen➤ Messverfahren➤ Messpunkte➤ Verantwortlicher	Datenaufbearbeitung <ul style="list-style-type: none">➤ Berechnungsweg➤ Verantwortlicher	Präsentation <ul style="list-style-type: none">➤ Darstellung➤ Aggregationsstufen➤ Archivierung➤ Verantwortlicher
Verschiedenes		

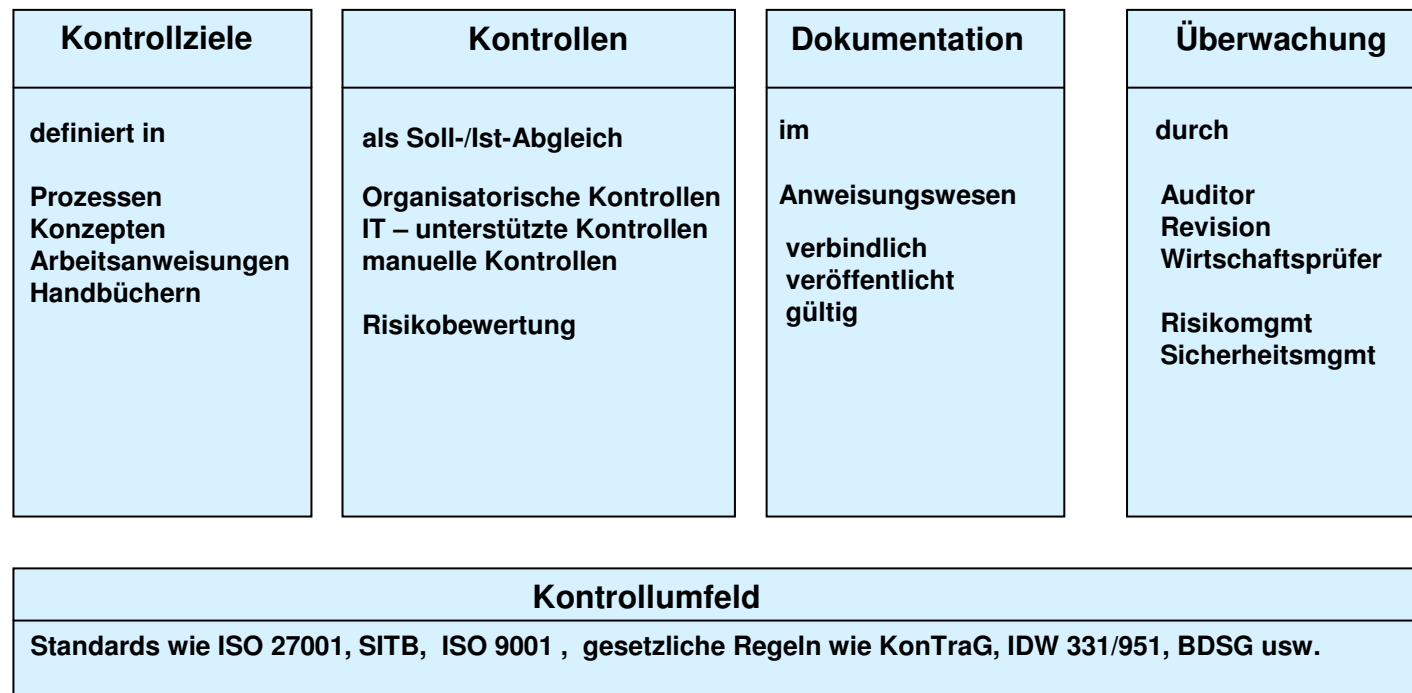
(Quelle: Künz, Kennzahlen in der IT)

Agenda

1. IKS - Internes Kontrollsystem
2. Rahmenbedingungen
3. Umsetzungsbeispiel
4. Kennzahlen entwickeln
5. **Zusammenfassung**

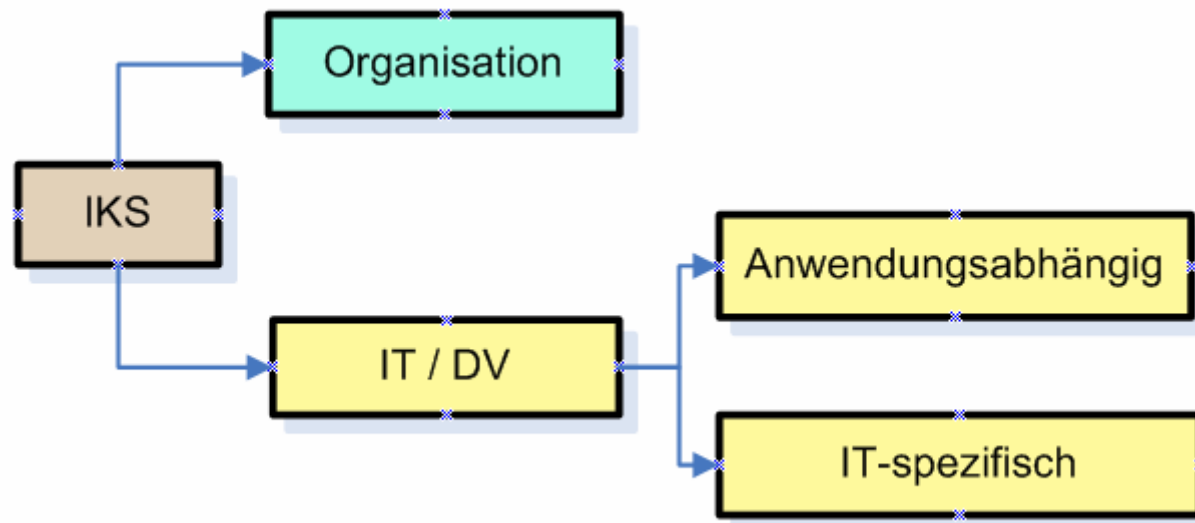
Internes Kontrollsystem

IKS

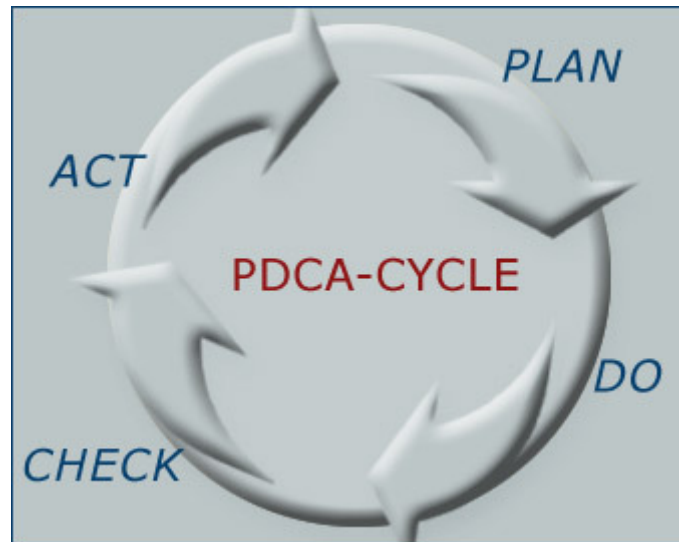


Kontrollen im IKS

Prozessabhängige und –unabhängige Kontrollen



Nachhaltigkeit



- ➔ Sicherstellung der Nachhaltigkeit und Weiterentwicklung
- ➔ Integration der Prozesse in den Geltungsbereich des IKS
- ➔ Berücksichtigung der kritischen Erfolgsfaktoren KEF

- ➔ „EISA – Enterprise IT-Security Analysis“ ist ein effizientes und effektives Verfahren um diesen Regelkreis zu schliessen und Transparenz zu schaffen

IKS - Internes Kontrollsystem und Kennzahlen

Vielen Dank für Ihre Aufmerksamkeit

Noch Fragen ???

F.-J. Lang IT-Security Consulting GmbH

Landsbergerstr. 302 , 80687 München

Fon: +49 (0)89 / 9040-5916

Fax: +49 (0)89 / 9040-5917

eMail: info@fjlang.de

www.fjlang.de