

## EURO-IKS

### Neue Prozess- und System- anforderungen im Kontroll- und Risikomanagement

Mag. Werner Kolarik  
act Management Consulting

Loipersdorf, 8. Mai 2008



- 1. Aktuelle EURO-IKS Rahmenbedingungen**
- 2. IKS Umsetzung in Österreich - Ergebnisse einer aktuellen act MC Studie**
- 3. Fachliche Anforderungen an eine wirksame IKS-Umsetzung**
- 4. Diskussion**

# Die Notwendigkeit eines funktionierenden Internen Kontroll- und Risikomanagementsystems

- Das **Risiko- und Kontrollbewusstsein** der Unternehmen und Organisationen hat sich seit den großen internationalen Bilanzskandalen wie etwa Enron, MCI-Worldcom oder Parmalat zu Beginn des 21. Jahrhunderts stark geändert.
- Die Aussagekraft der Jahresabschlüsse sowie veröffentlichter Unternehmenszahlen geriet international in ein schiefes Licht. Auch im deutschsprachigen Raum wurden ähnliche Fälle bekannt, die das **Vertrauen der Aktionäre und Investoren** in die veröffentlichten Unternehmensdaten stark beeinträchtigten.
- Den inhaltlichen und organisatorischen Rahmen für die Erstellung verlässlicher Unternehmenszahlen bildet das **Interne Kontrollsystem (IKS)**, gewissermaßen das „Rückgrat“ für die Ermittlung der Jahresabschlusszahlen. Ohne ein funktionierendes und zeitgemäßes IKS im Bereich der Rechnungslegung (Jahresabschlusserstellung) können weder aus rechtlicher noch aus betriebswirtschaftlicher Sicht **verlässliche Daten des Jahresabschlusses** sichergestellt werden.
- Änderungen hinsichtlich der **gesetzlichen Anforderungen** und Rahmenbedingungen erhöhen den Handlungsbedarf im Bereich IKS (SOX, URÄG 2008)

# Das URÄG 2008/EURO-IKS erhöht die Anforderungen an das IKS für große und börsennotierte Unternehmen (1/2)

---

- **Corporate Governance Erklärung** für börsennotierte Gesellschaften
- Verpflichtende Bestellung eines **Prüfungsausschusses** für börsennotierte Aktiengesellschaften sowie Gesellschaften, deren Aufsichtsrat aus mehr als 5 Mitgliedern besteht
- **Beschreibung der wichtigsten Merkmale des internen Kontrollsystems (IKS)** im Hinblick auf die Rechnungslegung im Lagebericht durch börsennotierte Gesellschaften
  - Fokus: Rechnungslegungsprozess (end to end Betrachtung, von der Entstehung des Geschäftsfalls bis zur Verbuchung und Berichterstattung über alle betroffenen Unternehmensbereiche hinweg)
  - Detailgestaltung bleibt Unternehmen vorbehalten, kein expliziter Formalismus wie bei Sarbanes-Oxley
  - 8. EU-RL/URÄG 2008 ist kein EURO-SOX!

# Das URÄG 2008/EURO-IKS erhöht die Anforderungen an das IKS für große und börsennotierte Unternehmen (2/2)

- Prüfung der **Wirksamkeit des Internen Kontrollsystems**, gegebenenfalls **des internen Revisionssystems**, und **des Risikomanagementsystems der Gesellschaft** durch den Prüfungsausschuss
  - Prüfung der Wirksamkeit bezieht sich auf die Validierung eines gelebten IKS!
  - EIN IKS dass nicht gelebt wird, ist KEIN IKS
  - Notwendige integrierte Betrachtung von IKS, IR und RMS
- **Bestätigung durch den Abschlussprüfer**, dass die **Beschreibung der wichtigsten Merkmale des Internen Kontrollsystems** im Hinblick auf die Rechnungslegung im Lagebericht in Einklang mit dem Jahresabschluss steht und den gesetzlichen Vorschriften entspricht
- **Verstärkte Redepflicht des Abschlussprüfers bei IKS-Schwächen**
- **Umsetzungszeitplan**
  - Inkrafttreten des Gesetzes mit 1. Juni 2008
  - Anzuwenden auf Geschäftsjahre, die nach dem 31. Dezember 2008 beginnen

1. Aktuelle EURO-IKS Rahmenbedingungen
2. IKS Umsetzung in Österreich - Ergebnisse einer aktuellen act MC Studie
3. Fachliche Anforderungen an eine wirksame IKS-Umsetzung
4. Diskussion

## Ziele der Studie

---

- Erhebung der Ist-Situation von Risiko- und Kontrollsystemen in Österreichs Top-Unternehmen und -Organisationen
  - Darstellung der IKS-Soll-Anforderungen
  - Darstellung der Ist-Ergebnisse
  - Aufzeigen eines möglichen Handlungsbedarfs
  
- Ausblick auf zukünftige Entwicklungen und Trends
  
- Vergleich mit anderen österreichischen Unternehmen bzw. Organisationen

# Grundlagen der Studie

Die Studie beinhaltete Fragen

- zur allgemeinen Darstellung des Unternehmens bzw. der Organisation (Größe und Charakteristika)
- zu den IKS-Bereichen (Kontrollumfeld, Information und Kommunikation, Risikobeurteilung, Kontrollaktivitäten und Überwachung)
- zur IT-Sicherheit

Insgesamt wurden rund 50 Fragebögen ausgewertet. An der Studie haben Unternehmen unterschiedlicher Sektoren und Branchen teilgenommen:

- 43% sind öffentliche bzw. öffentlichkeitsnahe Organisationen
- 57% sind private Unternehmen
- ¼ der StudienteilnehmerInnen sind börsennotierte Unternehmen

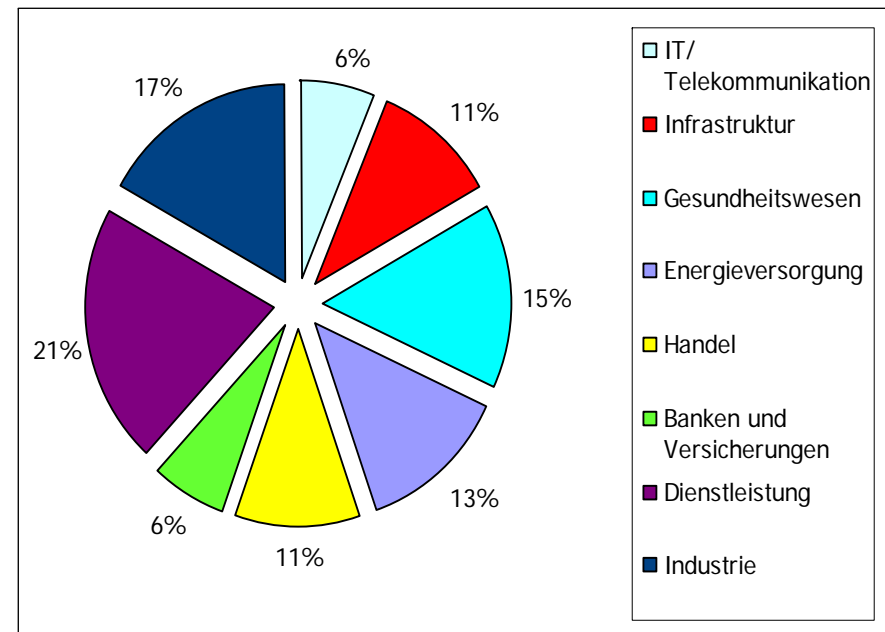


Abb.: Gliederung der befragten Unternehmen bzw. Organisationen nach Branchen

# Definition Risikomanagement bzw. Internes Kontrollsystem (IKS)

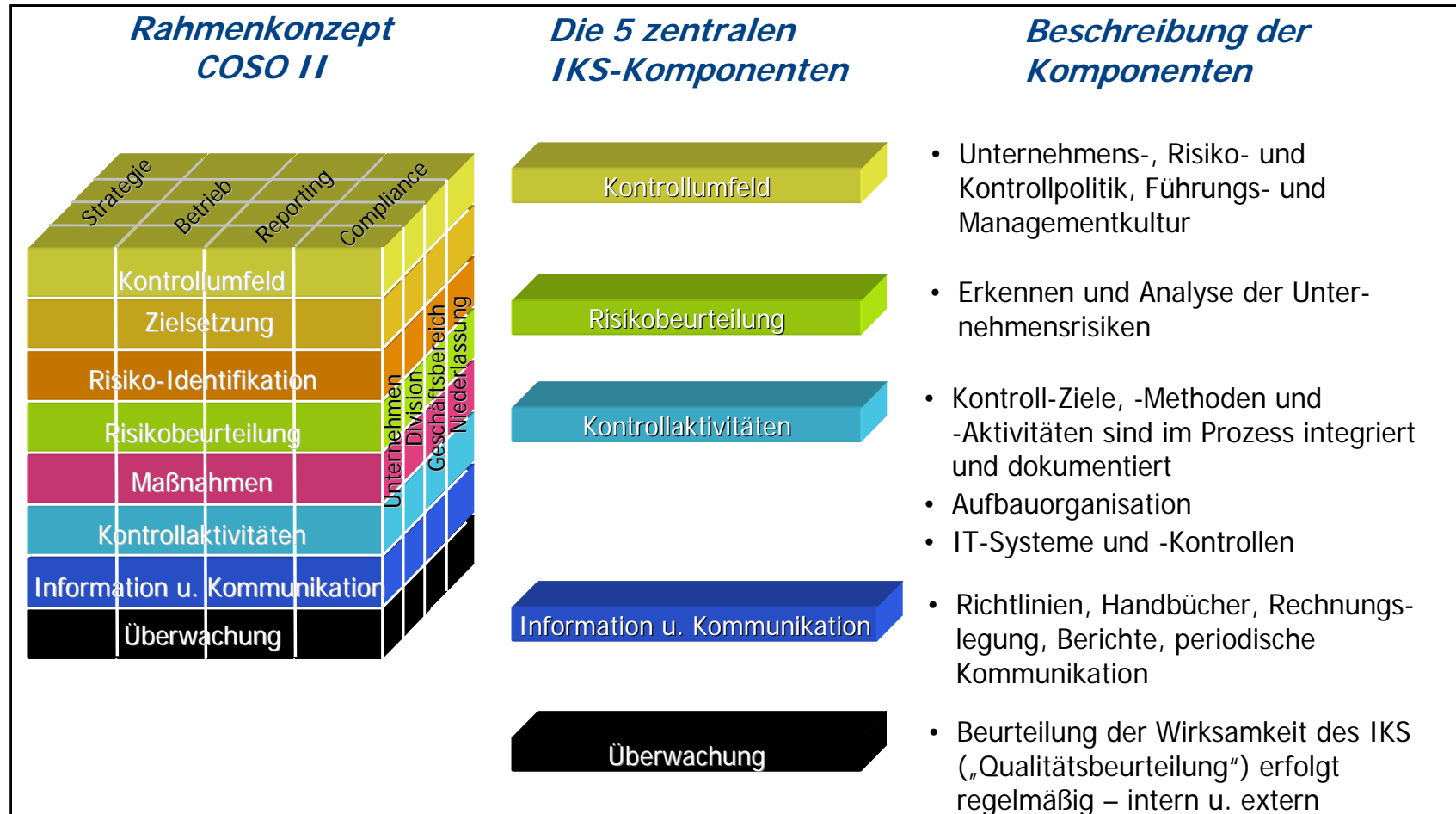
## Risikomanagement

- Das Rahmenkonzept COSO (Committee of Sponsoring Organizations of the Treadway Commission) ist ein weltweit anerkanntes Regelwerk für die Implementierung von Risikomanagement- und Kontrollsystemen und bietet eine ganzheitliche Sichtweise auf Corporate Governance und interne Kontrollsysteme.
- Es handelt sich hierbei um einen umfassenden, unternehmensweiten Risikomanagementansatz, der auf Basis einer definierten Risikostrategie ein systematisches und permanentes Vorgehen mit den Elementen *Identifikation, Bewertung, Steuerung von Risiken* sowie *Überwachung der Aktivitäten* umfasst. Risikomanagement wird hierbei als integraler Bestandteil der operativen Geschäfts-, Planungs- und Kontrollprozesse gesehen.

## Internes Kontrollsystem

- Ausgehend vom Rahmenkonzept COSO umfasst das IKS sämtliche Maßnahmen und Vorkehrungen mit dem Ziel zur
  - Bewahrung des Vermögens des Unternehmens
  - Sicherung der Einhaltung der Geschäftspolitik
  - Gewährleistung der Zuverlässigkeit des Rechnungswesens
  - Verbesserung der Effizienz betrieblicher Abläufe

# COSO<sup>1</sup> als Rahmen für das Interne Kontrollsystem (IKS)



1 ... The Committee of Sponsoring Organizations of the Treadway Commission ([www.coso.org](http://www.coso.org))

# Unternehmensethik und Grundsätze der Integrität spielen eine wesentliche Rolle

---

- Zur Schaffung eines entsprechenden IKS-Kontrollumfeldes werden die Grundsätze der Integrität und Unternehmensethik von der Mehrheit der befragten Unternehmen und Organisationen in Regelwerken unterschiedlichster Form festgehalten.
- Der Dokumentationsgrad von Verantwortungen, Aufgaben und Kompetenzen ist hoch zu bewerten, dabei wird vor allem auf Transparenz, Nachvollziehbarkeit und Eindeutigkeit geachtet.

Dieses Ergebnis darf als positiv eingeschätzt werden und stellt damit Basis für ein/das Risikomanagementsystem- und Kontrollsystem dar.

Für sich allein ist das IKS-Kontrollumfeld jedoch nicht ausreichend für ein funktionierendes IKS.

# Unternehmen und Organisationen managen vermehrt ihre Risiken

- Ein Risikomanagement-Prozess ist bei einer überwiegenden Mehrheit der Unternehmen und Organisationen in Teilen implementiert.
- Eine systematische Nutzung des Risikomanagementprozesses liegt nicht einmal bei der Hälfte der StudienteilnehmerInnen vor.
- Die größten Risiken werden im politischen und regulatorischen Umfeld, im Markt- und Kundenbereich, in der IT sowie im Finanzbereich gesehen

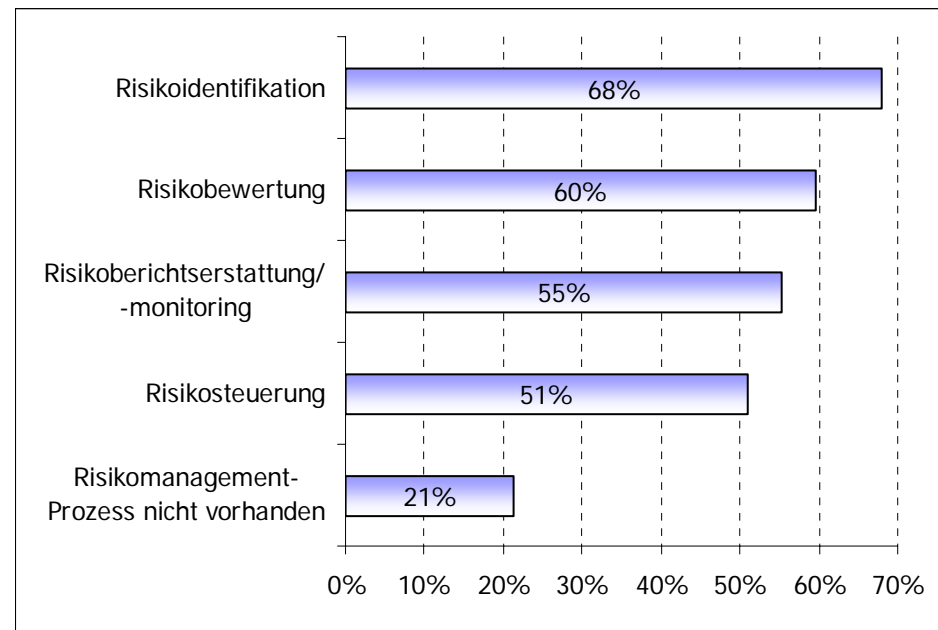


Abb.: Implementierte Elemente im Risikomanagement-Prozess

# Mehrheit der Unternehmen dokumentiert IKS Risiken und Kontrollen

- 60% der StudienteilnehmerInnen dokumentieren IKS-Risiken und -Kontrollen, weitere 30% dokumentieren zumindest Risiken oder Kontrollen.
- Lediglich 10% der befragten Unternehmen und Organisationen geben an, keine Risiken oder Kontrollen zu dokumentieren. Dies sind vor allem kleinere bis mittlere Unternehmen mit weniger als 1000 MitarbeiterInnen.

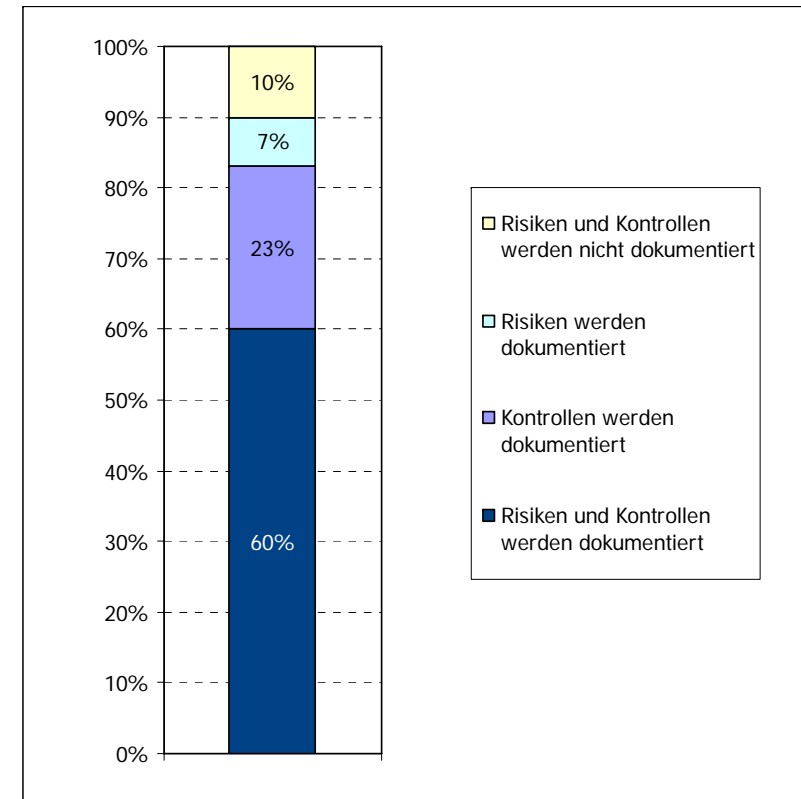


Abb. Dokumentation von IKS-Risiken und -Kontrollen

# Kontrollaktivitäten werden kaum auf Effektivität überprüft

- Die Kontrollaktivitäten werden von den Unternehmen und Organisationen überwiegend dokumentiert.
- Ein regelmäßiger Abgleich zwischen Risiken und Kontrollaktivitäten findet nicht einmal bei der Hälfte der StudienteilnehmerInnen statt.
- Eine Anpassung von Maßnahmen erfolgt bei einem Drittel gar nicht oder nur in mehrjährigen Abständen.
- Von rund 70% der StudienteilnehmerInnen werden die Kontrollmaßnahmen nicht zur Gänze eingehalten.

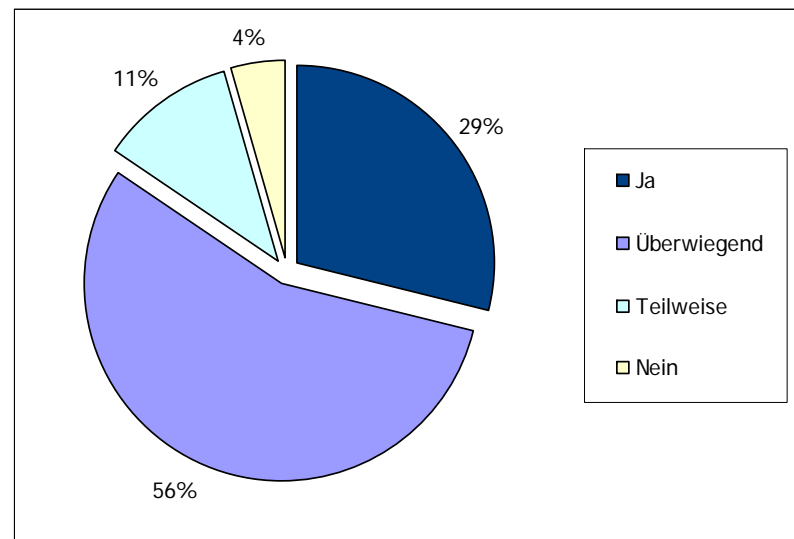


Abb.: Einhaltung angeordneter Kontrollmaßnahmen

# Die Interne Revision erhält einen positiveren Stellenwert

- Die Interne Revision nimmt neben der eigentlichen internen Prüftätigkeit verstärkt die Rolle des „internen Beraters“ wahr.
- Die innerhalb des IKS wichtige Aufgabe und Rolle der Internen Revision ist den MitarbeiterInnen im Unternehmen bzw. in der Organisation überwiegend bekannt.

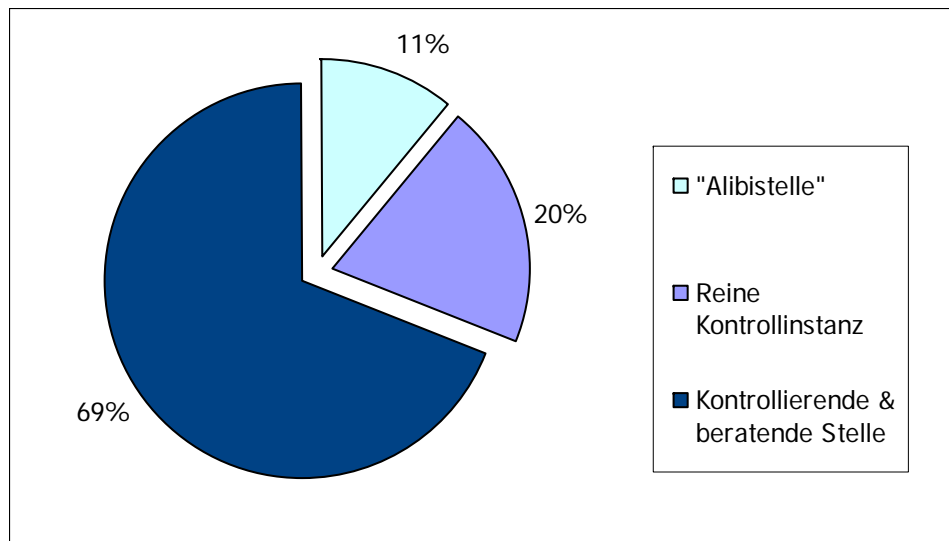


Abb.: Wahrnehmung der Internen Revision durch MitarbeiterInnen

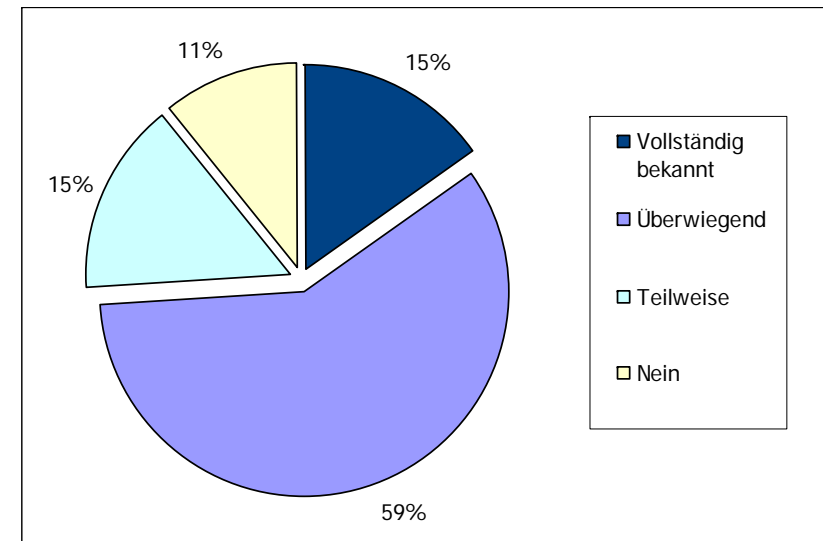


Abb.: Bekanntheit der Aufgaben der Internen Revision bei den MitarbeiterInnen

# IT-Sicherheit spielt eine wesentliche Rolle im internen Kontrollsystem

- Die Problematik der Datensicherheit (z.B. Vertraulichkeit, Verfügbarkeit, Integrität) wird von den meisten Unternehmen und Organisationen im IKS berücksichtigt.
- Bei fast allen StudienteilnehmerInnen zeigt sich ein Verbesserungspotenzial im Incident Management Prozess („Störfallmanagement“).

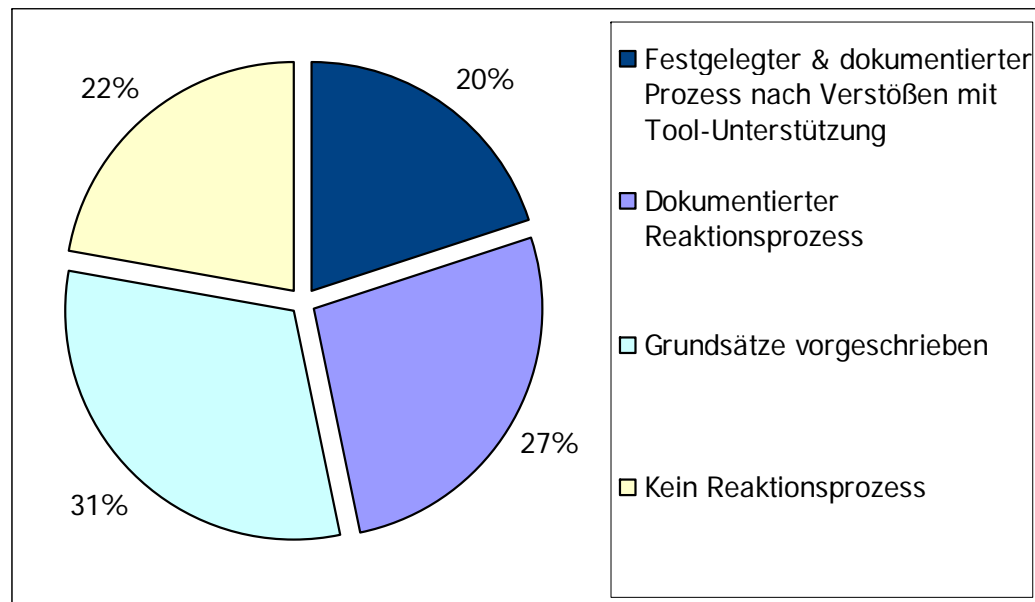


Abb. Reaktionsprozess auf Verstöße gegen die IT-Sicherheit

# Methodik zur Überwachung des IKS

- In rund 50% der befragten Unternehmen und Organisationen gibt es unternehmensweite Vorschriften zur Überwachung von bedeutenden Kontrollmaßnahmen
- Rund 36% der Unternehmen und Organisationen verfügen über einen festgelegten, dokumentierten Prozess.
- 15% der befragten Unternehmen und Organisationen haben keine definierte Methodik zur Überwachung der IKS-Effizienz.
- Die Überwachung des IKS liegt bei jedem/r zweiten StudienteilnehmerIn in der Verantwortung der Projekt- bzw. Abteilungsleitung

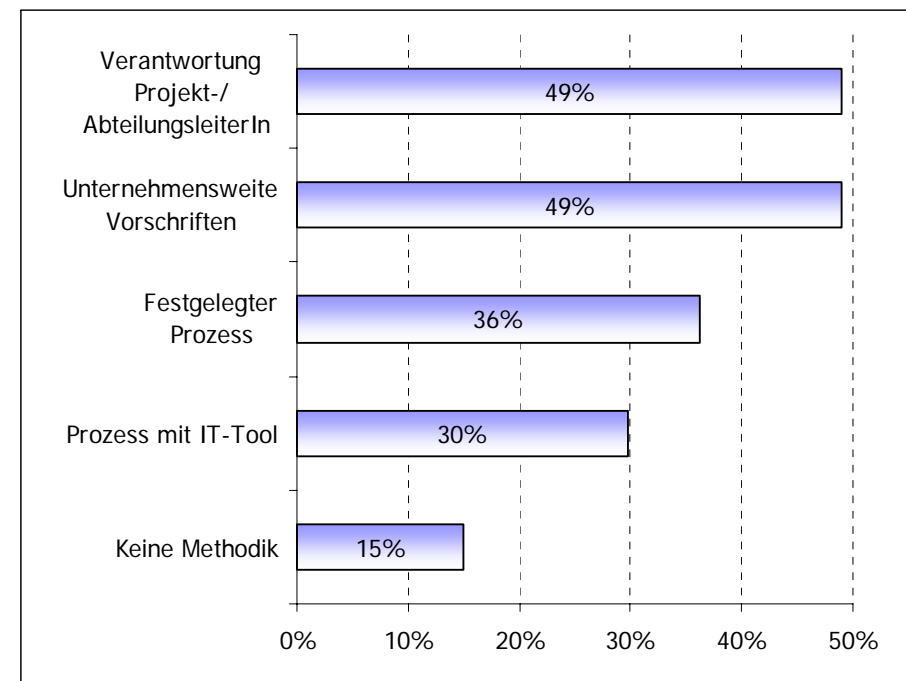


Abb. Methodik zur Überwachung des IKS

# Der IKS Reifegrad in Selbsteinschätzung der StudienteilnehmerInnen

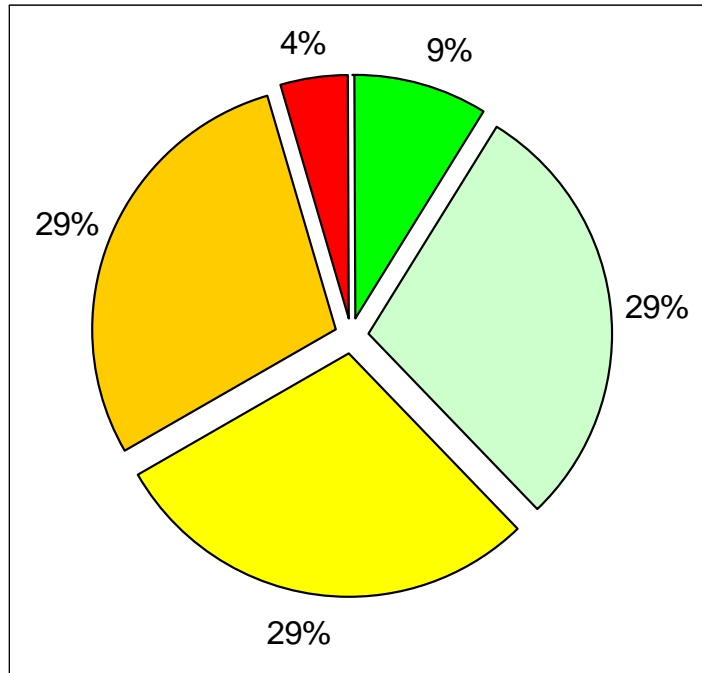


Abb. IKS-Reifegrad der Studienteilnehmer

- Nur 9% der befragten Unternehmen und Organisationen stufen den IKS-Reifegrad ihres Unternehmens bzw. ihrer Organisation als optimiert ein.
- Rund 1/3 der befragten Unternehmen und Organisationen sieht seinen IKS-Reifegrad als maximal informell an.

#### Stufe 5: IKS ist optimiert

Integrierter Ansatz von IKS und Risikomanagement. Weitgehende Automatisierung der Kontrollaktivitäten. Hohe Reaktionsfähigkeit auf Veränderungen durch entsprechenden Einsatz von Tools

#### Stufe 4: IKS ist überwacht

IKS-Grundsätze sind detailliert dokumentiert. Regelmäßige Überwachung der Kontrollen. Laufende Aktualisierung der Kontrollen. Regelmäßige IKS-Berichterstattung. IKS-Gesamtverantwortlicher ist definiert

#### Stufe 3: IKS ist standardisiert

IKS-Grundsätze sind dokumentiert. Kontrollen sind in Prozesse dokumentiert u. integriert. Nachvollziehbarkeit der Kontrollen ist gegeben. Information/Kommunikation und Schulung findet statt.

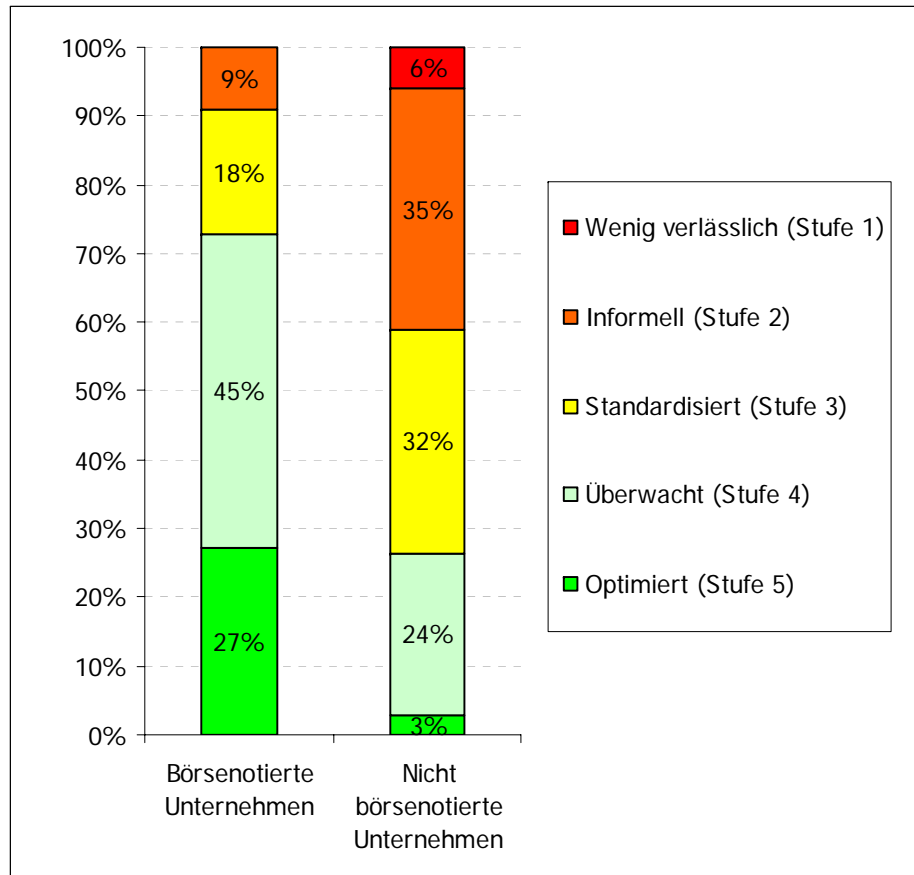
#### Stufe 2: IKS ist informell

Interne Kontrollen sind vorhanden, nicht standardisiert. Fehlende Nachvollziehbarkeit der Kontrollen. Kontrollen sind personenabhängig. Fehlende Schulung und Kommunikation.

#### Stufe 1: IKS ist wenig verlässlich

Interne Kontrollen sind kaum oder nicht vorhanden. Vorhandene Kontrollen sind nicht verlässlich.

# Reifegrad des IKS in börsennotierten und nicht börsennotierten Unternehmen



- Börsennotierte Unternehmen weisen erwartungsgemäß einen deutlich höheren und damit besseren IKS-Reifegrad vor (über 70% Stufe 4 bzw. Stufe 5).
- Unter den nicht börsennotierten Unternehmen verfügen rund 40% ein nicht den Anforderungen entsprechendes IKS-System.

Abb.: Einschätzung des IKS-Reifegrads – Unterscheidung börsennotierte und nicht börsennotierte Unternehmen

# Inhalt

---

1. Aktuelle EURO-IKS Rahmenbedingungen
2. IKS Umsetzung in Österreich - Ergebnisse einer aktuellen act MC Studie
3. Fachliche Anforderungen an eine wirksame IKS-Umsetzung
4. Diskussion

## Wann ist ein IKS wirksam?

---

- Ein IKS ist wirksam, wenn es
  - a) **Vollständig** ist
  - b) **Nachvollzogen** werden kann
  - c) **Effizient eingerichtet** ist und
  - d) **Gelebt** wird

# Fachliche Anforderungen an eine wirksame IKS Umsetzung

## a) Vollständigkeit

- Ein IKS ist wirksam, wenn es

a) **Vollständig** ist

b) **Nachvollzogen** werden kann

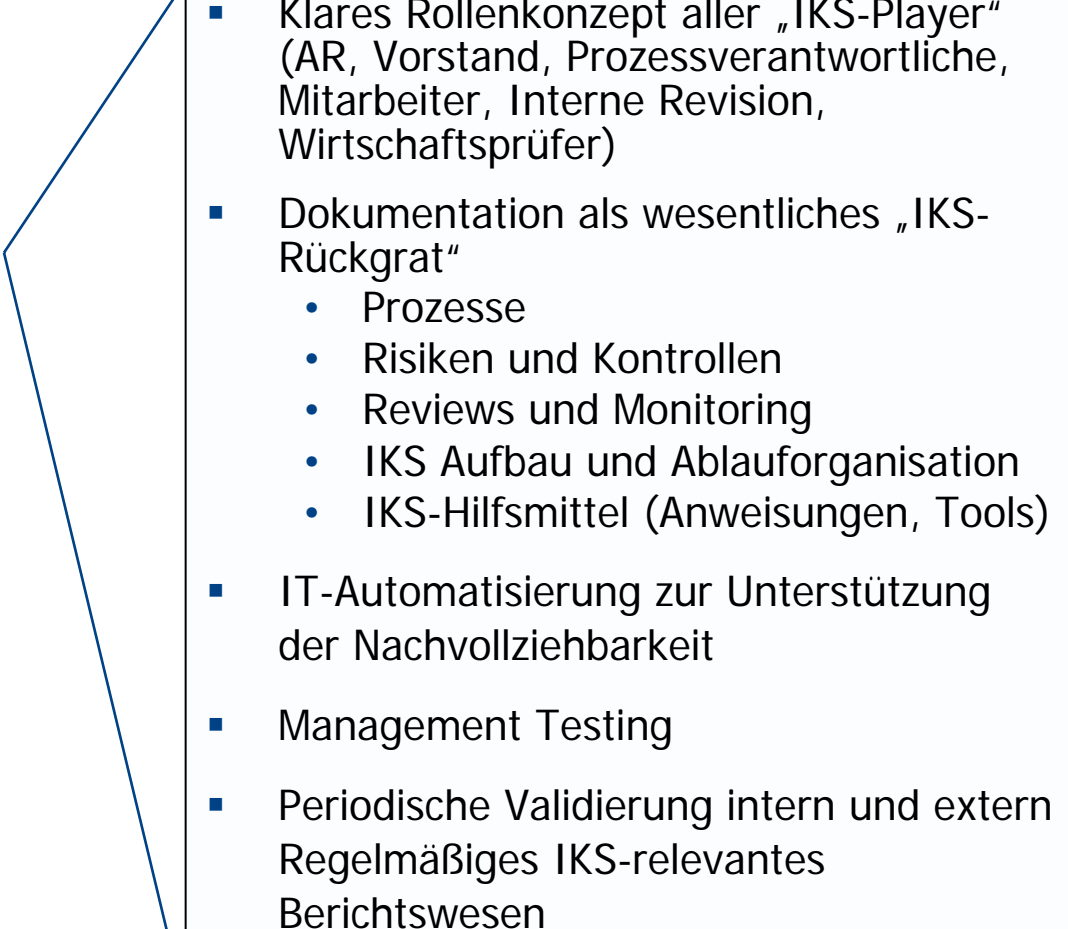
c) **Effizient eingerichtet** ist und

d) **Gelebt** wird

- Klare inhaltliche Ausrichtung
  - Compliance
  - Finanzberichtswesen
  - Integration in (betriebliches) Risikomanagement
  - Effizienz und Effektivität
- Gesamthafte Struktur
  - Kontroll-Umfeld
  - Risikobeurteilung
  - Kontrollaktivitäten (Prozess, IT)
  - Information & Kommunikation
  - Überwachung
- Risikoorientierte Konkretisierung und Detaillierung
- Relevanz für Jahresabschluss
- Kriterium der Wesentlichkeit

# Fachliche Anforderungen an eine wirksame IKS Umsetzung

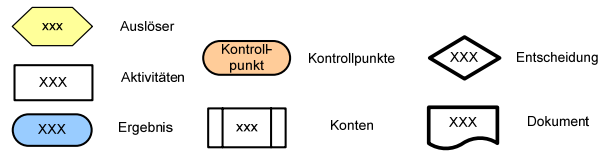
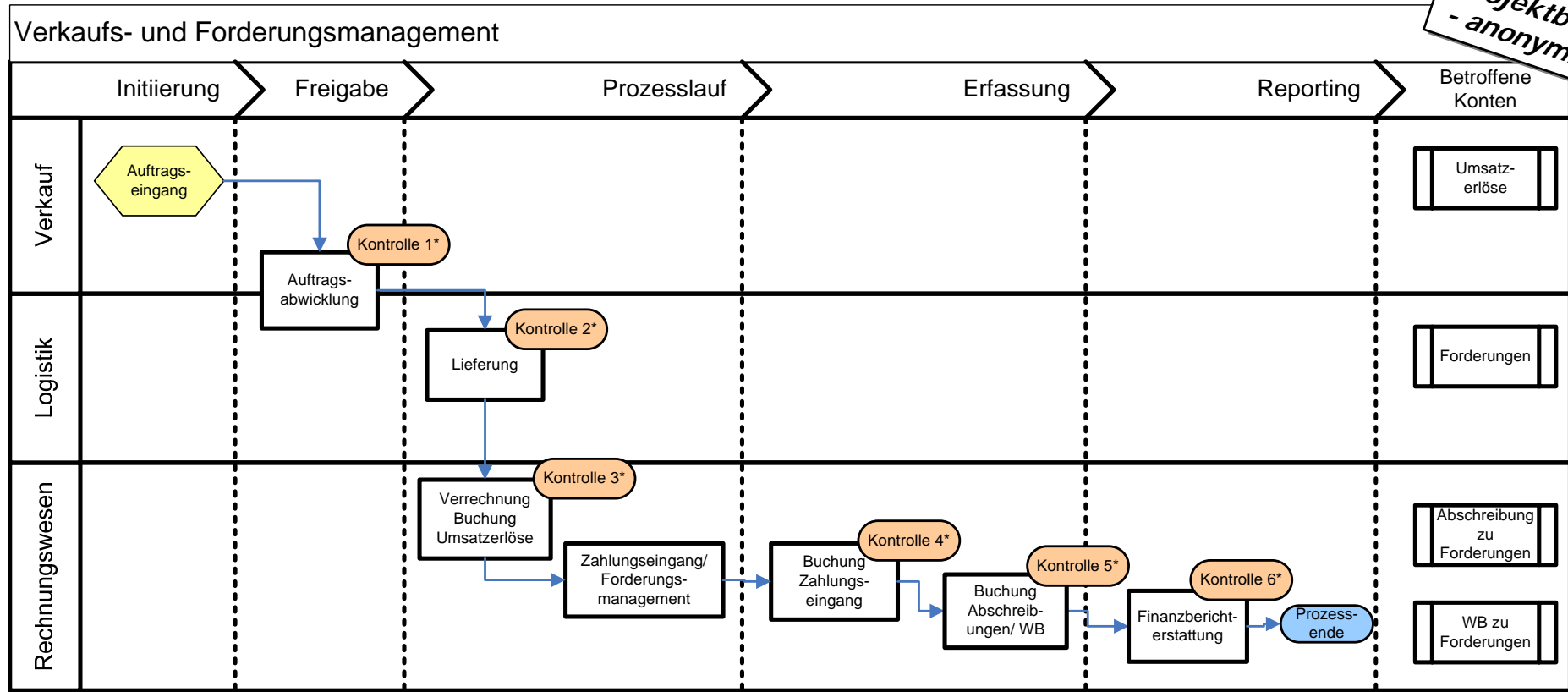
## b) Nachvollziehbarkeit

- Ein IKS ist wirksam, wenn es
    - a) **Vollständig** ist
    - b) **Nachvollzogen** werden kann
    - c) **Effizient eingerichtet** ist und
    - d) **Gelebt** wird
- 
- Klares Rollenkonzept aller „IKS-Player“ (AR, Vorstand, Prozessverantwortliche, Mitarbeiter, Interne Revision, Wirtschaftsprüfer)
  - Dokumentation als wesentliches „IKS-Rückgrat“
    - Prozesse
    - Risiken und Kontrollen
    - Reviews und Monitoring
    - IKS Aufbau und Ablauforganisation
    - IKS-Hilfsmittel (Anweisungen, Tools)
  - IT-Automatisierung zur Unterstützung der Nachvollziehbarkeit
  - Management Testing
  - Periodische Validierung intern und extern
    - Regelmäßiges IKS-relevantes Berichtswesen

# Fachliche Anforderungen an eine wirksame IKS Umsetzung

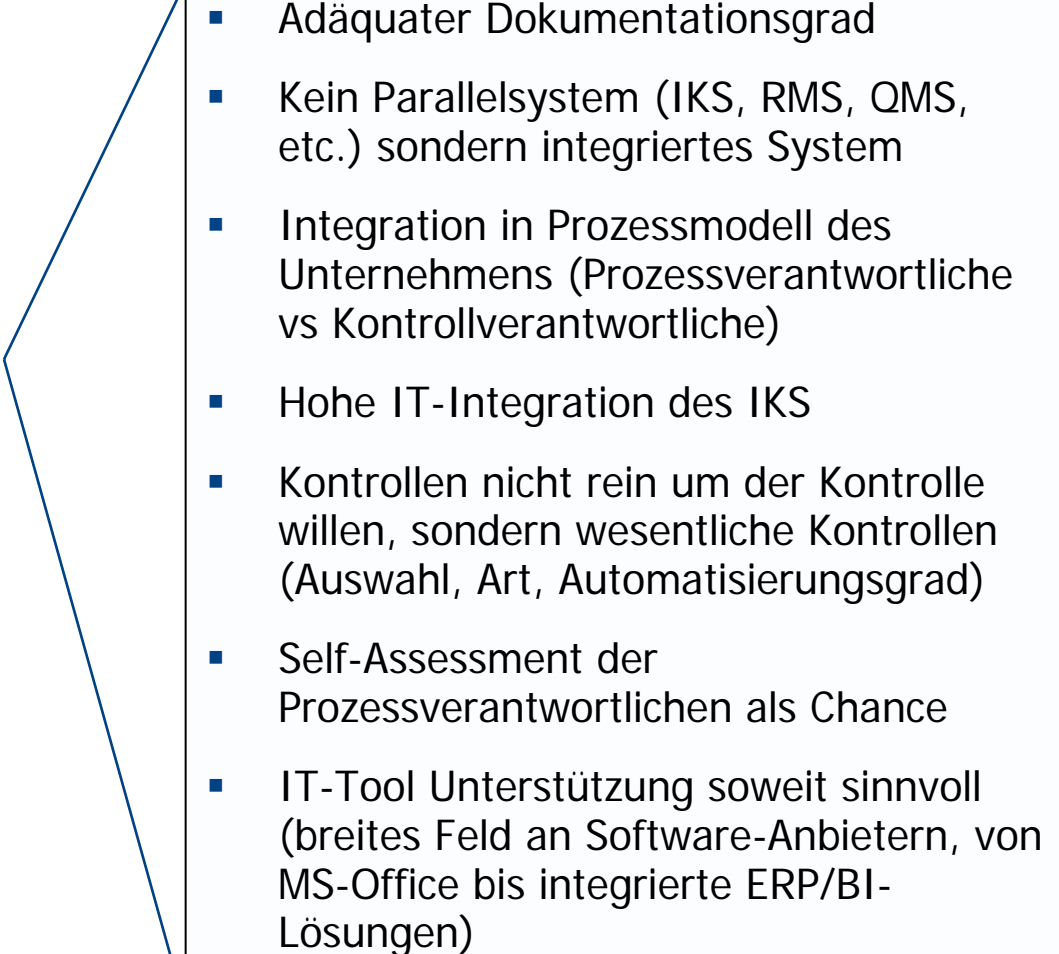
## b) Nachvollziehbarkeit – Beispiel IKS-Prozessdokumentation

*Projektbeispiel  
- anonymisiert*



# Fachliche Anforderungen an eine wirksame IKS Umsetzung

## c) Effiziente Einrichtung

- Ein IKS ist wirksam, wenn es
    - a) **Vollständig** ist
    - b) **Nachvollzogen** werden kann
    - c) **Effizient eingerichtet** ist und
    - d) **Gelebt** wird
- 
- Adäquater Dokumentationsgrad
  - Kein Parallelsystem (IKS, RMS, QMS, etc.) sondern integriertes System
  - Integration in Prozessmodell des Unternehmens (Prozessverantwortliche vs Kontrollverantwortliche)
  - Hohe IT-Integration des IKS
  - Kontrollen nicht rein um der Kontrolle willen, sondern wesentliche Kontrollen (Auswahl, Art, Automatisierungsgrad)
  - Self-Assessment der Prozessverantwortlichen als Chance
  - IT-Tool Unterstützung soweit sinnvoll (breites Feld an Software-Anbietern, von MS-Office bis integrierte ERP/BI-Lösungen)

# Fachliche Anforderungen an eine wirksame IKS Umsetzung

## d) IKS muss gelebt werden

- Ein IKS ist wirksam, wenn es
  - a) **Vollständig** ist
  - b) **Nachvollzogen** werden kann
  - c) **Effizient eingerichtet** ist und
  - d) **Gelebt** wird

- Vorbildwirkung durch Vorstand/GF
- IKS als Teil der Management-Agenda
- Umsetzung der risikoorientierten Vorgehensweise
- IKS nicht als Selbstzweck sondern als Instrument eines risikobewußten und zukunftsorientierten Management
- Anreiz- und nutzenorientierte Umsetzung (begleitendes Projekt- und Kommunikationsmanagement)
- Kontinuierliche Verbesserung durch Self-Assessment und Management Assessment, ergänzend durch externe Revision

# Vorgehensweise von act MC zur Weiterentwicklung und Optimierung des Internen Kontrollsystems (1/2)

- Durchführung einer IKS-Standortbestimmung mittels standardisierter Checklisten:
  - Kontrollumfeld (z.B. Risiko- und Kontrollpolitik)
  - IKS-Prozesse und Prozesskontrollen
  - IT-Sicherheits- und Risikomanagement (z.B. IT-Prozesse, Zugriffsberechtigungen)
  - IKS-Überwachung (z.B. Überwachungsart, -zyklus, Berichtswesen)

## Ermittlung des IKS-Reifegrades (Stufe 1 – 5)



### Checkliste IKS-Allgemein

	Auszug	Ja/Nein/z. T.
1. Gibt es gültige IT-Projektmanagement-Guidelines?		<input type="checkbox"/> <input type="checkbox"/>
2. Existieren dokumentierte IT-Architektur-Guidelines?		<input type="checkbox"/> <input type="checkbox"/>
3. Werden neue Anforderungen an IT-Systeme dokumentiert und von der Fachabteilung abgenommen?		<input type="checkbox"/> <input type="checkbox"/>
4. Existiert ein Testkonzept und ein Testplan für neue oder adaptierte Anwendungssoftware?		<input type="checkbox"/> <input type="checkbox"/>
5. Wie werden Software-Tests dokumentiert?		<input type="checkbox"/> <input type="checkbox"/>
6. Nach welchem Prozess erfolgt die Produktivsetzung von Software-Changes?		<input type="checkbox"/> <input type="checkbox"/>
7. Wie erfolgt das Monitoring des Produktivbetriebs?		<input type="checkbox"/> <input type="checkbox"/>
8. Nach welchen Prinzipien erfolgen Back-up bzw. regelmäßige Restore-Tests?		<input type="checkbox"/> <input type="checkbox"/>
9. Wie erfolgt die Vergabe und das Monitoring von Benutzerrechten (Berechtigungskonzepten)?		<input type="checkbox"/> <input type="checkbox"/>
10. Wie ist der Zugang zur produktiven Infrastruktur abgesichert (physisch, Betriebssystem, Datenbank)?		<input type="checkbox"/> <input type="checkbox"/>
11. ....		<input type="checkbox"/> <input type="checkbox"/>

### Checkliste-IKS IT

	Auszug	Ja/Nein/z. T.
1. Sind die IKS-Grundsätze und IKS-Ziele inkl. Qualitätsanforderungen definiert?		<input type="checkbox"/> <input type="checkbox"/>
2. Sind die IKS-Verantwortlichen bekannt?		<input type="checkbox"/> <input type="checkbox"/>
3. Werden die Risiken erfasst und laufend beurteilt?		<input type="checkbox"/> <input type="checkbox"/>
4. Sind die Geschäftsprozesse dokumentiert?		<input type="checkbox"/> <input type="checkbox"/>
5. Sind die Kontrollen in die Geschäftsprozesse integriert?		<input type="checkbox"/> <input type="checkbox"/>
6. Erfolgt eine laufende Überwachung und Aktualisierung der Risiken und Kontrollen?		<input type="checkbox"/> <input type="checkbox"/>
7. Werden die Mitarbeiter über das IKS regelmäßig informiert?		<input type="checkbox"/> <input type="checkbox"/>
8. Werden die Mitarbeiter über Kontrollaufgaben und IKS-Verantwortung regelmäßig informiert (z. B. Mitarbeitergespräche, interne Mitteilungen...)?		<input type="checkbox"/> <input type="checkbox"/>
9. Werden Hinweise von Mitarbeitern hinsichtlich möglicher Kontrollschwächen aufgenommen und weiterverfolgt?		<input type="checkbox"/> <input type="checkbox"/>
10. Die Aufgaben der Internen Revision sind den Mitarbeitern bekannt.		<input type="checkbox"/> <input type="checkbox"/>
11. Werden Maßnahmen ergriffen, wenn Schwachstellen im IKS aufgetreten sind?		<input type="checkbox"/> <input type="checkbox"/>
12. Das IKS wird intern und extern überprüft.		<input type="checkbox"/> <input type="checkbox"/>
13. ...		<input type="checkbox"/> <input type="checkbox"/>

**Stufe 5: IKS ist optimiert**  
 Integrierter Ansatz von IKS und Risikomanagement. Weitgehende Automatisierung der Kontrollaktivitäten. Hohe Reaktionsfähigkeit auf Veränderungen durch entsprechenden Einsatz von Tools

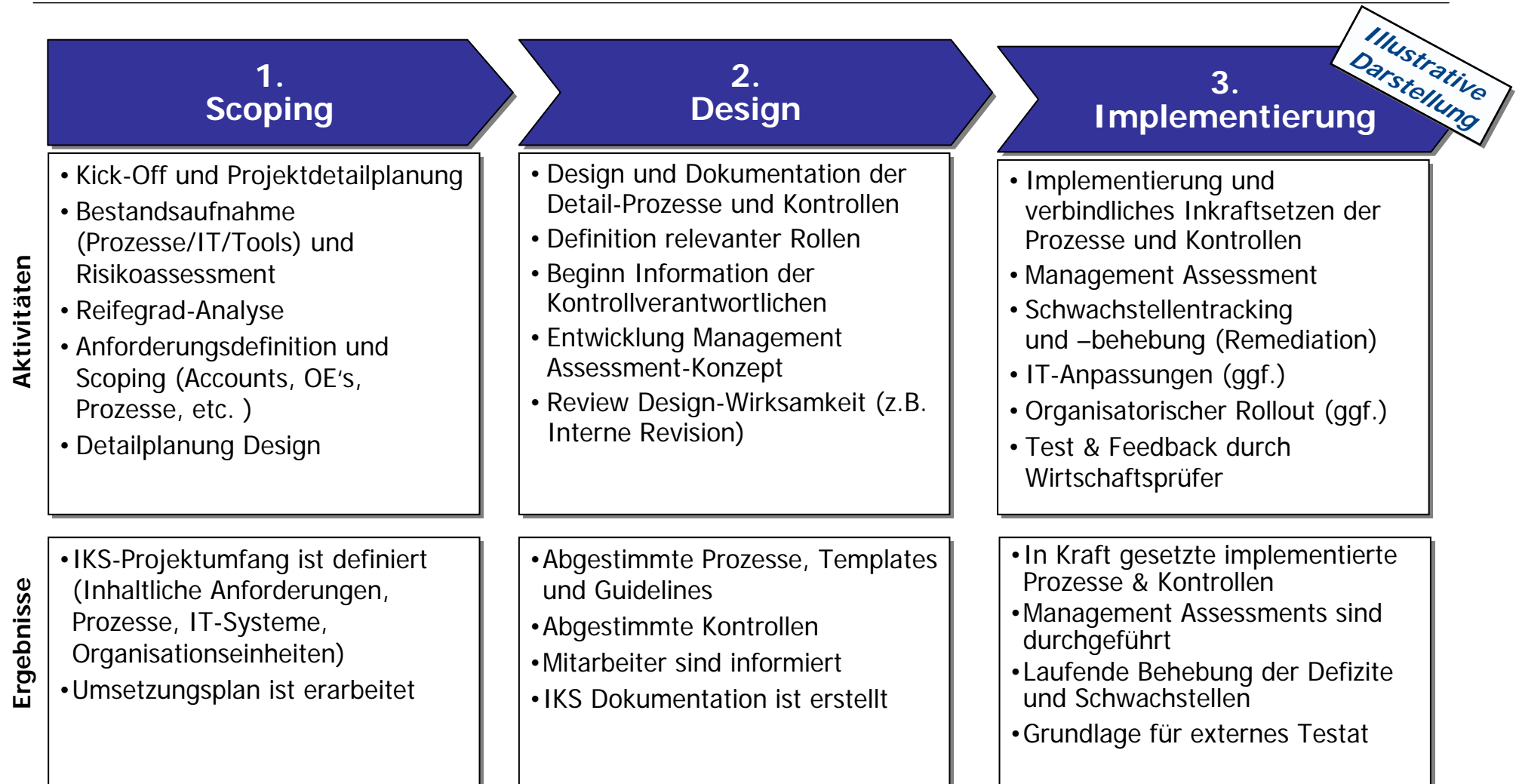
**Stufe 4: IKS ist überwacht**  
 IKS-Grundsätze sind detailliert dokumentiert. Regelmäßige Überwachung der Kontrollen. Laufende Aktualisierung der Kontrollen. Regelmäßige IKS-Berichterstattung. IKS-Gesamtverantwortlicher ist definiert

**Stufe 3: IKS ist standardisiert**  
 IKS-Grundsätze sind dokumentiert. Kontrollen sind in Prozesse dokumentiert u. integriert. Nachvollziehbarkeit der Kontrollen ist gegeben. Information/ Kommunikation und Schulung findet statt.

**Stufe 2: IKS ist informell**  
 Interne Kontrollen sind vorhanden, nicht standardisiert. Fehlende Nachvollziehbarkeit der Kontrollen. Kontrollen sind personenabhängig. Fehlende Schulung und Kommunikation.

**Stufe 1: IKS ist wenig verlässlich**  
 Interne Kontrollen sind kaum oder nicht vorhanden. Vorhandene Kontrollen sind nicht verlässlich.

# Vorgehensweise von act MC zur Weiterentwicklung und Optimierung des Internen Kontrollsystems (2/2)



## Resümee – Bedeutung von EURO-IKS für die Praxis

---

- EURO-IKS ist eine große Chance für die Unternehmen das vorhandene IKS zu optimieren und weiterzuentwickeln.
- Die Umsetzung der gesetzlichen Verpflichtung, ein wirksames und integriertes Internes Kontrollsystem einzurichten, lässt den Unternehmen Freiräume in der Ausgestaltung (kein EURO-SOX) und sollte genutzt werden.
- Wichtige Schwerpunkte für die Weiterentwicklung des IKS
  - Fokussierung auf einen risiko- und kontrollorientierten Steuerungsansatz
  - Erarbeitung eines effizienten, unternehmensspezifischen IKS-Mindeststandards
  - Stärkere Integration des IKS mit IT-Governance und dem IT-Kontrollsystemen
  - Aufbau eines internen Kontroll- und Risiko-Reportings als Grundlage für eine effektive Überwachung
  - Sicherstellung eines durchgängigen Risikomanagementprozesses (Integration von Identifikation, Bewertung, Steuerung und Überwachung)
- Dazu ist es sinnvoll, eine IKS-Standortbestimmung durchzuführen und darauf aufbauend die Handlungsfelder zur Optimierung des internen Kontrollsystems zu identifizieren.

# Inhalt

---

1. Aktuelle EURO-IKS Rahmenbedingungen
2. IKS Umsetzung in Österreich - Ergebnisse einer aktuellen act MC Studie
3. Fachliche Anforderungen an eine wirksame IKS-Umsetzung
4. Diskussion



### **Mag. Werner Kolarik** Partner, Mitglied der Geschäftsleitung

---

**act** Management Consulting GmbH

1010 Wien, Seilerstätte 18 – 20

Telefon +43 (1) 2051920 321

Mobil +43 (0) 664 4125217

Telefax +43 (1) 2051920 500

E-Mail [werner.kolarik@act-mc.at](mailto:werner.kolarik@act-mc.at)

Internet [www.act-mc.at](http://www.act-mc.at)



**act Management Consulting GmbH**

Seilerstätte 18 – 20 | 1010 Wien | Tel. +43 / 1 / 2051920-0 | [www.act-mc.at](http://www.act-mc.at)