CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

Controller-Forum 2010
Internes Kontrollsystem: Schießen wir am Ziel vorbei?
17. März 2010
WP Dr. Aslan Milla

PRICEWATERHOUSECOOPERS

Agenda

Rechtliche Grundlagen
Aus dem Leben eines Wirtschaftsprüfers
Praktische Konsequenzen und Vorgehensweisen

Internes Kontrollsystem - Eine einfache Anforderung?

Die Geschäftsführer haben / Der Vorstand hat

dafür zu sorgen, dass ein Rechnungswesen und **ein internes Kontrollsystem** geführt werden, die den Anforderungen des Unternehmens entsprechen.

§ 22 (1) GmbHG bzw. § 82 AktG: keine Legaldefinition von IKS

⇨ Haben daher nur diese Unternehmen ein internes Kontrollsystem (IKS)?

Noch mehr Anforderungen? Schießen wir am Ziel vorbei?

Sarbanes-Oxley Act 2002: betrifft nicht nur die USA, auch Tochtergesellschaften auf der ganzen Welt

J-SOX, Swiss-SOX

Änderungsrichtlinie und Abschlussprüfungsrichtlinie 2006: EU

URÄG 2008 (Unternehmensrechts-Änderungsgesetz): Österreich

- IKS Beschreibung im Lagebericht (Rechnungslegung):
  > nur kapitalmarktorientierte Unternehmen
- Überwachung der Wirksamkeit des IKS durch Prüfungsausschuss/AR:
  > kapitalmarktorientierte Unternehmen und sehr große AGs/GmbHs bzw SEs

⇨ Ist ein IKS daher nur was für die „Großen“?
Und haben wir nun in Österreich SOX-ähnliche Zustände?

Was bedeutet „Internes Kontrollsystem“?

Das **Interne Kontrollsystem** umfasst alle in der Unternehmensorganisation vorgesehenen prozessbezogenen Maßnahmen und Einrichtungen, die dazu bestimmt sind,

- das vorhandene Vermögen zu sichern,
- die betriebliche Leistungsfähigkeit zu steigern und
- die Einhaltung der Geschäftspolitik, sowie
- der Richtigkeit, Zuverlässigkeit und Vollständigkeit der Aufzeichnungen und Rechnungslegungs- bzw. Berichtssysteme zu gewährleisten, sowie
- Die Einhaltung externen und interner Vorschriften und Regelungen

⇨ IKS ist wesentlicher Faktor bei der Einrichtung und Erhaltung von Systemen und betrieblichen Prozessen.
Die Bedeutung des IKS wächst mit der Größe des Unternehmens.

Sicherheitslücken, Verluste, Klagen, Vorstrafen – Beispiele aus dem Leben eines Wirtschaftsprüfers

Thema Benutzerberechtigungen

- Lehrling beginnt in Logistik-Bereich: erhält die Standard-Logistik-Rolle
- Lehrling wechselt in die Finanz: erhält die Standard-Finanz-Rolle
- Lehrling wechselt in die Personalabteilung: erhält die Standard-Personal-Rolle

⇨ Ein Lehrling als Superuser nach zwei Jahren

- Mitarbeiter, die heiraten, haben plötzlich zwei User
- User von temporären Mitarbeitern werden nicht deaktiviert
- CFO: je höher die Hierarchie, desto mehr Berechtigungen – unabhängig von den Jobanforderungen

⇨ Potentiell gefährliche Sicherheitslücken

Sicherheitslücken, Verluste, Klagen, Vorstrafen – Beispiele aus dem Leben eines Wirtschaftsprüfers (Fortsetzung)

Fraud-Fall

- CFO kann in SAP buchen (Berechtigung!)
- Nie analysiert, was er gebucht hat

⇨ Selbst genehmigte Dienstleistungsrechnungen

Facility Management

- Stundenabrechnungen der Schneeräumung nicht überprüft

⇨ Zahlungen für dieselben Stunden in der gleichen Straße

- Lange bestehende Verträge nicht überprüft

⇨ Überhöhte Preise bezahlt

- Vergessene Wartung einer Brandschutztür, die eine Person verletzt

⇨ Arbeitnehmerschutz verletzt – Vorstrafe für Verantwortlichen

Sicherheitslücken, Verluste, Klagen, Vorstrafen – Beispiele aus dem Leben eines Wirtschaftsprüfers (Fortsetzung)

Thema Passwörter

- Richtlinie, Passwörter einzurichten
- Passwortlänge 0 im System

⇨ Etliche Mitarbeiter ohne Passwort

- Login ID und Passwort auf Post-it am Bildschirm der Vorstandssekretärin

Thema physische Sicherheit

- Verwaltungsgebäude ist komplett abgesichert
- Lager ist offen, Workstation ohne Bildschirmschoner mit Passwort

⇨ Manipulation im Warenwirtschaftssystem

Sicherheitslücken, Verluste, Klagen, Vorstrafen – Beispiele aus dem Leben eines Wirtschaftsprüfers (Fortsetzung)

Forderungsmanagement

- Verkaufsleiter beliefert langjährigen guten Kunden, den er persönlich kennt
- Kunde hat wirtschaftliche Schwierigkeiten und meldet Insolvenz an

⇨ Unternehmen erleidet wirtschaftlichen Schaden

Kassa/Bank

- Einzelzeichnungsberechtigungen vergeben
- Ausgeschiedene Mitarbeiter mit Zeichnungsberechtigung nicht gelöscht

⇨ nicht autorisierte Zahlungen

Folgen für die Unternehmen

… Betrügerische Handlungen (Fraud) - KMU sind besonders betroffen
- Veruntreuung wie Entwendung von Vermögen
- Ausgaben für unternehmensfremde Zwecke
- wirtschaftlich für das Unternehmen nicht vorteilhafte Transaktionen

… Fehler in der Berichterstattung und Steuerung (intern wie extern)

… Ineffiziente und ineffektive Abläufe
- Kundenbeschwerden
- Vertrauensverlust
- Nicht/mangelhaft erreichte Unternehmensziele

Die einfache Lösung ist ein angemessenes Internes Kontrollsystem

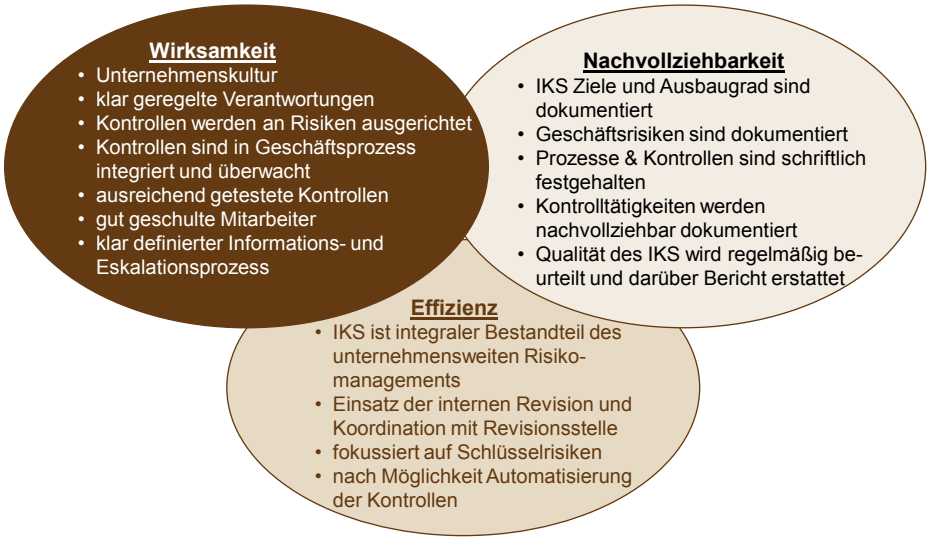
Alle Unternehmen haben irgendeine Form eines IKS.

Die Beispiele zeigen jedoch:
… es ist nicht immer wirksam
… es ist nur ansatzweise oder nur in Teilbereichen eingerichtet

⇨ Alle Unternehmen sollten ein für sie passendes und wirksames IKS haben

⇨ Die gesetzlichen Vorgaben schießen nicht am Ziel vorbei!

Die Anforderungen an ein IKS



Die richtige Balance von Risiko – Kosten – Nutzen ist anzustreben!

… nicht alles ist bis ins letzte Detail zu dokumentieren.
… nicht jeder Mitarbeiter ist zu überwachen.
… nicht jede Tätigkeit muss von einem andere Mitarbeiter ausgeführt werden.

Wichtige Fragen sind:

- Kennen Sie Ihre wesentlichen Risiken?
- Konzentrieren Sie sich auf diese wesentlichen Risiken?
- Sind die Kontrollen darauf ausgerichtet?
- Sind diese wenigen Schlüsselkontrollen ausreichend dokumentiert?
- Wird die Wirksamkeit dieser wenigen Schlüsselkontrollen regelmäßig überprüft?
- Haben Sie Ihr einheitliches Vorgehen nachvollziehbar dokumentiert?
- Haben Sie Ihr Verständnis von IKS allen im Unternehmen kommuniziert?

Das IKS ist immer individuell!

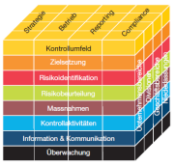
- Jedes Unternehmen muss sich einen Überblick über seine wesentlichen Geschäftsprozesse und Abläufe verschaffen.
- Das IKS ist auf spezifische Geschäftsrisiken und Umfang der Geschäftstätigkeiten abzustimmen
  - Risikoprofil des Unternehmens
  - Größe
  - Komplexität der Geschäftstätigkeit
  - Art der Finanzierung
- Organisatorische Vorgaben und Einrichtungen sind regelmäßig zu überprüfen.

⇨ Die Ausgestaltung eines IKS hat immer unter betriebswirtschaftlichen Aspekten zu erfolgen !

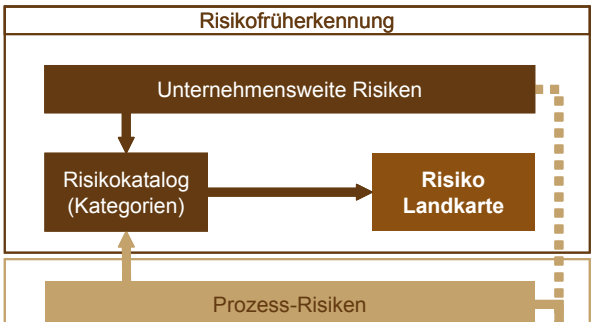
Das sind die Anforderungen an ein wirksames IKS

- Die Kontrollen sind auf mögliche Risiken und Schwachstellen im Prozess ausgerichtet.
- Die Kontrollen sind aufeinander abgestimmt.
- Die Ziele, Risikoüberlegungen, (Betriebs)Prozesse und Kontrollen sind ausreichend dokumentiert.
- Das IKS ist kommuniziert.
- Die vorgesehenen Kontrollen werden durchgeführt und überwacht und sind für einen Dritten nachvollziehbar.

⇨ Ohne Systematik (COSO!) keine Effizienz und keine Effektivität



Integration von IKS im unternehmensweiten Risikomanagement



Strategie
Mission
Unternehmens-ziele

… und so schaut ein funktionierendes Internes Kontrollsystem aus

- Mitarbeiter/innen erhalten ein Zugriffsprofil je nach Abteilung/Geschäftsbereich auf Grundlage der schriftlichen Vorgaben des jeweilig verantwortlichen Vorgesetzten (zB Standardformular)
- Personaldaten (Namensänderungen, Zu-/Abgänge etc.) werden sofort von der Personalabteilung an die EDV weitergemeldet
- Zugriffs- und Transaktionsberechtigungen werden abgestimmt auf die jeweilige Aufgabe in einem betrieblichen Prozess vergeben (SachbearbeiterIn versus kontrollierender Vorgesetzter)
  … Best Practices: Elektronischer Workflow, regelmässiger Soll-Ist Review
- Bezogene Leistungen auf Grund von Verträgen werden regelmäßig von der zuständigen Abteilung angesehen und dem Vorgesetzten berichtet

… und so schaut ein funktionierendes Internes Kontrollsystem aus

- Die Verwendung von nicht-trivialen Passwörter ist systemseitig vorgegeben
- Wesentliche betriebliche Prozesse sind nach dem 4-Augen-Prinzip (bzw. Trennung von Verantwortungen) eingerichtet
  - Produktion versus Einkauf
  - Vertrieb versus Verwaltung/Rechnungswesen
- Der Chef lässt seine Abrechnungen durch eine andere Person kontrollieren und abzeichnen
- Rechnungskontrollen und generell Genehmigungsprozesse mit Wertgrenzen
- Zahlungstransaktionen sind durch zumindest zwei Zeichnungsberechtigte freizugeben

… und so schaut ein funktionierendes Internes Kontrollsystem aus

- Preise sind im System hinterlegt, Abgleich (genehmigter) Bestellung zu Lieferantenrechnung elektronisch
- In regelmäßigen Abständen werden Teams im Unternehmen gebildet, die die betrieblichen Anforderungen und die eingerichteten Kontrollen und Prozesse analysieren und weiter entwickeln
- Eingerichtete Kontrollen werden durch (interne oder externe) prozessunabhängige Personen regelmäßig auf Einhaltung überprüft.
- Laufende Überprüfung von Zahlungsterminen und Bankkonditionen (Ausnutzung von Skonti)
- Stammdatenpflege nur auf Basis schriftlicher Anfragen

Ein wirksames IKS ist eine Chance für alle und bringt Nutzen!

Kontrollen werden auf wesentliche Risiken ausgerichtet

Weniger Fehler in Prozessen – mehr Sicherheit

Prozesse, Ziele, Risiken und Kontrollen sind für die Führungskräfte und Mitarbeiter nachvollziehbar - verständlicher

Arbeitsabläufe und Organisationshilfsmittel werden verbessert

Prozesse lassen sich zielgerichteter und systematischer steuern

Unternehmensüberwachung wird effizienter

⇨ Unterstützt damit die Zielerreichung und den Erfolg des Unternehmens – IKS ist Führungsaufgabe !

„Jeder Fehler tritt erst dann auf, wenn er die letzte Kontrolle durchlaufen hat.“

Folgerung aus Murphys Gesetzen

PRICEWATERHOUSECOOPERS