Sektion 10

Informationssysteme zur Corporate Governance in Unternehmen

Christoph Lattemann

Gliederung

Literatur

- Gleich, R./Oehler, K. (2006): *Corporate Governance umsetzen; Erfolgsfaktoren Controlling und Informationssysteme,* Stuttgart.
- IDW PS 260: "Das interne Kontrollsystem im Rahmen der Abschlußprüfung
- IDW PS 261: "Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken
- Wefer S, M. (2004): Unterstützung von SOA und anderen IKS Projekten durch SAP's „Management of internal Controls“, in: Sarbanes Oxley Act Professionelles Management interner Kontrollen, Menzies, C. (Hrsg.), Frankfurt, S.335-356

Lernziele

- Wofür ist ein Internes Kontrollsystem zuständig
- Was muss ein Internes Kontrollsystem leisten können in der CG
- Welche Rahmenmodelle gibt es an Internen Kontrollsystemen
- Wie sehen diese Kontrollsysteme aus.

Informationssysteme zur Corporate Governance

Informationssysteme

- unterstützen die Unternehmensführung und -kontrolle

  Bsp.: Risikomanagementsystem zur Aufdeckung von bestandsgefährdenden Risiken für das Unternehmen

- dienen den Corporate Governance Prinzipien wie Publizität, Transparenz, Vertrauensbildung oder Kontrolle

  Bsp.: Internes Kontrollsystem zur Überprüfung der Einhaltung von unternehmensinternen Regelungen sowie Prozessen zur Finanzberichterstattung

Informationssysteme zur Corporate Governance

- wahren die Interessen der internen und externen Stakeholder (Mitarbeiter, Kreditgeber, Lieferanten, Anteilseigner etc.)

- Nutzung moderner Informationstechnologien

  Steuerung und Kontrolle der IT durch IT-Governance als Teil der Corporate Governance (z.B. CobiT- Framework)

systembildende Informationssysteme

Systembildende Informationssysteme

- Ansätze, die eine Veränderung und neue Möglichkeiten der Unternehmensführung ermöglichen
- wesentlich ist die Anwendung von IT

1. unternehmensübergreifende Lieferketten (Supply Chains)
2. elektronische Beschaffung (E-Procurement)

systemunterstützende Informationssysteme

Systemunterstützende Informationssysteme

- keine Veränderung von Prozessabläufen der Unternehmensführung
- *Anwendungen:* Buchungsdurchführung, Berichterstellung, Berichtverteilung, automatische Dokumentation

- Schwachstellen in der Vergangenheit (Bilanzskandale)
  - Falschbuchungen, Verschleierungen
  - falsche Jahresabschlüsse (Enron, Worldcom, Flow-Tex, Parmalat, u.A.)
- Folge: Vorgaben zur Einrichtung eines internen Kontrollsystems durch den SOX
- Risikomanagementsystem nach BilReG (Bilanzrechtsreformgesetz), KonTraG in Deutschland

internes Kontrollsystem zur Corporate Governance

Definition:

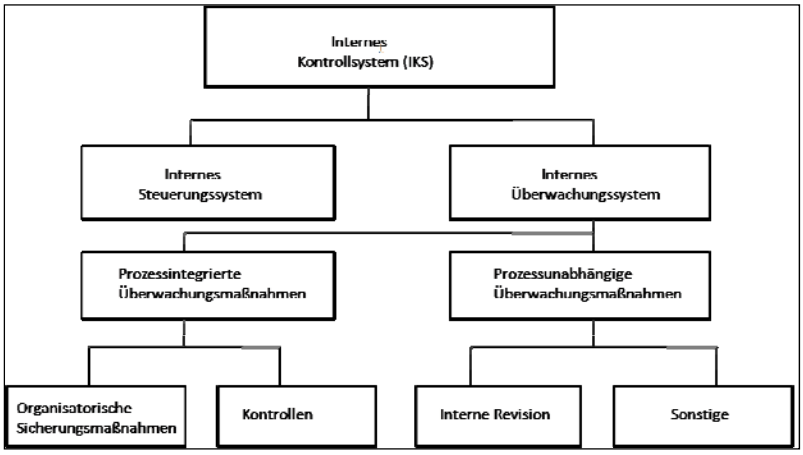
- Unter einem internen Kontrollsystem versteht man ein System aus Regelungen zur Steuerung von Unternehmensaktivitäten (internes Steuerungssystem) und Regelungen zur Überwachung der Einhaltung dieser Regelungen (internes Überwachungssystem)

(vgl. IDW PS 260, WPg (2001), S.322)

Bestandteile:

- prozessunabhängige Überwachungsmaßnahmen (z.B. interne Revision)
- prozessabhängige Überwachungsmaßahmen (z.B. Kontrollen, organisatorische Sicherungsmaßnahmen)

Aufbau des internen Kontrollsystems



In Anlehnung an IDW PS 260, WPg (2001), S. 323

Orientierungsrahmen für ein IKS (COSO)

COSO = „**C**ommittee **o**f **S**ponsoring **O**rganisations at the Treadway Commission“ als Initiative von privatwirtschaftlichen, amerikanischen Wirtschaftsinstituten.

COSO I – Rahmenwerk aus dem Jahre 1992 zur Verbesserung der internen Kontrollsysteme.

- **IKS Definition nach COSO**:

  Das IKS ist ein von der Unternehmensführung, Aufsichtsgremien, Mitarbeitern gesteuerter Prozess, der die Einhaltung der Unternehmensziele mit angemessener Sicherheit gewährleistet.

(vgl. Westhausen (2005), S.98)

COSO-Komponenten

3 Dimensionen (COSO-Würfel):

a) Basisziele
b) Organisationseinheiten
c) Kontrollelemente

a) Elemente der Basisziele
   - Ergebnisorientierung und Wirtschaftlichkeit operativer Prozesse (Operations)
   - Zuverlässigkeit der Finanzberichterstattung (Financial Reporting)
   - Einhalten externer und interner Vorschriften (Compliance)

b) Abstimmen der Basisziele mit den jeweiligen Zielen der einzelnen Organisationseinheiten (Business Units, Konzerntöchter etc.)

COSO-Komponenten

c.) COSO definiert 5 Kontrollelemente zur effizienten Implementierung eines IKS:

1. **Kontrollumfeld** (control environment) → • Vorhandene Corporate Governance Regelungen, Führungsstil („tone at the top"), Kontrollbewusstsein der Mitarbeiter.

2. **Risikoeinschätzung** (risk assessment) → • identifizieren aller wesentlichen Gefährdungen die den Unternehmenszielen entgegenstehen
   • ergreifen von Abwehrmaßnahmen

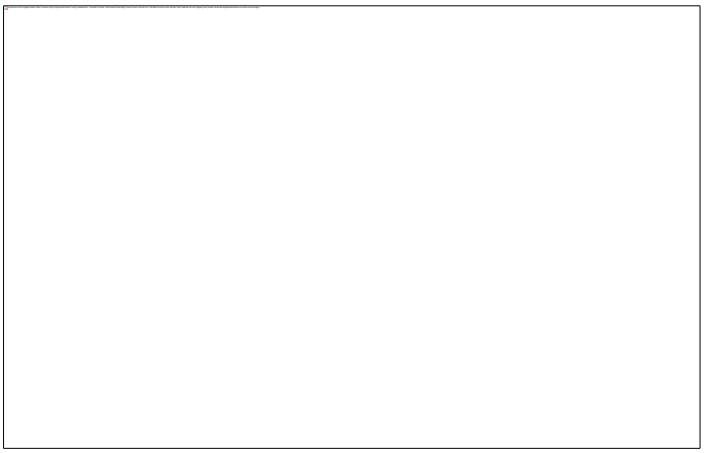
3. **Kontrollaktivitäten** (control activities) → • Grundsätze und Verfahren die sicherstellen sollen, dass die Entscheidungen der Unternehmensführung umgesetzt werden und die Erreichung der Basisziele nicht gefährdet ist.

COSO-Komponenten

4. **Information & Kommunikation** →
   - Kontrollaktivitäten werden durch Systeme der Information & Kommunikation unterstützt.
   - Die für Entscheidungen relevanten Informationen werden rechtzeitig eingeholt, aufbereitet und verlässlich an den Adressaten weitergeleitet.

5. **Überwachung** (monitoring) →
   - Beurteilung der Wirksamkeit der Prozesse und Kontrollaktivitäten durch Mitarbeiter des Unternehmens. Rückkopplung und evtl. Anpassung des Systems.

COSO-Würfel



(In Anlehnung an: Rüter/Schröder/Göldner (2006), S.121.)

interne Kontrollprozesse nach SOX 404

- COSO-Modell ist ein umfassendes System zur Steuerung und Kontrolle in Unternehmen
- Relevant für SOX Sec. 404 (Management Assessment of Internal Control) ist der COSO-Teil Financial Reporting (vgl. Rüter/Schröder/Göldner (2006), S. 121.)
- SOX 404 fokussiert interne Überwachungsmaßnahmen zur externen Finanzberichterstattung
- eingerichtete Kontrollen und Maßnahmen sind auf Prozesse zur Erstellung der Jahresabschlüsse auszurichten
- Dazu zählen Richtlinien und Verfahren die gewährleisten , dass z.B.:
    - Geschäftsvorfälle richtig abgebildet sind,
    - alle Geschäftsvorfälle erfasst sind,
    - Zugriffe auf Vermögenswerte des Unternehmens nicht ohne Erlaubnis des Managements möglich sind

(vgl.: Menzies (2004), S.45-46.)

Übergang zur IT-Governance

- Grund ist die wachsende Bedeutung des IT-Einsatzes in Unternehmen
- IT kann in die COSO-Zielkategorien „Operations“ und „Financial Reporting“ integriert werden,
  - da durch automatisierte Geschäftsprozesse viele Aktivitäten (Operations) von der IT abhängen und
  - die Finanzberichterstattung (financial Reporting) mittlerweile ausschließlich auf Daten der IT-Systeme basiert
- IT verursacht spezielle Risiken, die durch ein spezifisches IT-Kontrollsystem gemanagt werden müssen
- interne IT-Kontrollen beschreibt das CobiT-Framework

IT-Governance

Definition:

„IT-Governance ist die Verantwortung von Führungskräften und Aufsichtsräten und besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die Unternehmens-IT dazu beiträgt, die Organisationsstrategie und -Ziele zu erreichen und zu erweitern.“

(CobiT 4.0 (2005), S.6)

IT-Governance

Ziele („IT-Goals“):

- IT fortwährend auf die Unternehmensziele und –Prozesse auszurichten
- IT-Ressourcen (Mitarbeitende, Systeme und finanzielle Mittel) verantwortungsvoll und nachhaltig einsetzen
- IT-Risiken zu minimieren und optimal zu meistern

(Wyser/Kyburz (2002), S.24)

- Rahmenwerke: ITIL, ISO 17799, CobiT-Framework, u.A.
- Vorgabe eines Bezugsrahmens und klarer Strukturen für das IT-Management (Referenzmodelle)
- „Best Practices“ zum Management von IT in Unternehmen

CobiT-Rahmenwerk

- **CobiT** = *„Control Objectives for Information and Related Technology“* (veröffentlicht vom IT-Governance Institute)
- CobiT ist ein Rahmenwerk zur Einführung eines internen Kontrollsystems, das spezifisch auf die IT und die IT-Risiken ausgerichtet ist (Vgl. Fröhlich/Glasner (2007), S.73.)
- IT-Risiken durch z.B. menschliche Bedienungsfehler, Ausfall von Datenbankservern und kundenspezifischer Daten
- Um IT-Risiken zu begegnen, können spezielle IT-Prozess-Kontrollen eingesetzt werden.
- Hilfsmittel für IT-Revisoren, Unternehmensleitung und für die verantwortlichen IT-Angestellten zur Verständigung in einer einheitlichen Sprache.
- Verknüpft „IT-Goals“ und „Business Goals“

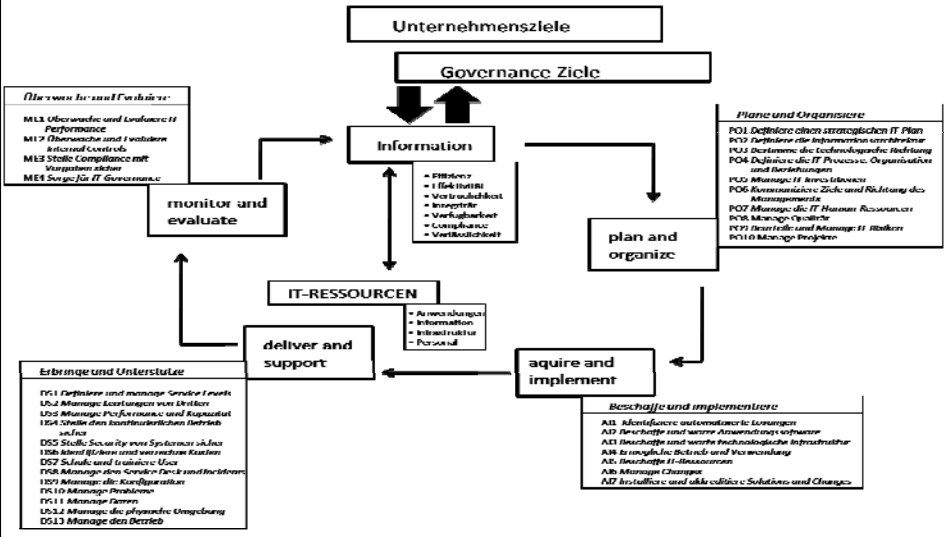
Struktur des CobiT-Rahmenwerks

- Zur Erreichung der Geschäftsziele müssen IT-Ressourcen (Anwendungen, Infrastruktur, Personal etc.) gesteuert und kontrolliert werden.
- Dies erfolgt durch aufeinander abgestimmte IT-Prozesse.
- CobiT enthält 34 IT-Prozesse mit Prozessaktivitäten zur Ermöglichung zielgerichteter IT-Steuerung.
- IT-Prozesse sind in 4 Bereiche (Domains) aufgeteilt.
  - Planen und Organisieren (plan and organize)
  - Beschaffen und Implementieren (aquire and implement)
  - Erbringen und Unterstützen (deliver and support)
  - Überwachen und Evaluieren (monitor and evaluate)
- Zusätzlich beschreibt CobiT in einem erweiterten Band für jeden der 34 IT-Prozesse sogenannte „IT-Control Objectives“ (insgesamt 318 Objectives)

Struktur des CobiT- Rahmenwerks

- Ein IT-Control Objective ist eine Aussage über das gewünschte Ereignis oder den zu erreichenden Zweck, der mit der Umsetzung von bestimmten in Aktivitäten integrierten Kontrollen erreicht werden soll (CobiT (2005) S. 17).
- Jeder IT-Prozess in CobiT enthält ein übergeordenetes Control Objective sowie mehrere detaillierte Control Objectives.
- In der Praxis sind die “controls” vom operativen Management innerhalb der IT-Prozesse zu implementieren .
- Ziel ist die Gewährleistung einer wirksamen Steuerung der IT hinsichtlich der Unternehmensziele (“Business Goals”)

IT-Prozesse von CobiT



In Anlehnung an: CobiT 4.0 (2005), S. 27

Kontrollsystem für IT-Prozesse

1. Einteilung der IT-Prozesse in Haupt- und Subprozesse
2. Aufstellen von Kontrollbereichen für jeden Subprozess
3. In den Kontrollbereichen werden Bestandteile zur technischen Infrastruktur und IT-Infrastruktur genannt.

   a) **technische Infrastruktur:** Zugangssicherungssysteme, Brandmelder, Löschsysteme etc.

   b) **IT-Infrastruktur:** Server, PCs, Netze, Datenbanken, Betriebssysteme, Anwendungen wie Firewalls, Virenschutz und Verfahren wie Backup, Recovery, Archivierung und Auslagerung

vgl. Rüter/Schröder/Göldner (2006), S.127

Kontrollarten für IT-Prozesse

- Interne IT-Kontrollen lassen sich nach folgenden Kriterien ordnen:
  - Zeitlicher Wirkungsrahmen
  - Automatisierungsgrad
  - weitere IT-Kontrollen
- Dabei werden finanzrelevante IT-Prozesse zur Rechnungslegung fokussiert.

Kontrollarten für IT-Prozesse

a) Zeitlicher Wirkungsrahmen:
   1. **vorgelagerte Kontrollen** (vorbeugend): z.B. Pass-Wort Verfahren
   2. **nachgelagerte Kontrollen** (aufdeckend): z.B. Plausibilitätsprüfung

b) Automatisierungsgrad:
   1. **(voll) automatische** Kontrollen meist als permanente Überwachung:
      z.B. Feuermelder, Diebstahlalarm
   2. **halb-automatische** Kontrollen zusätzlich mit manueller Nachbetrachtung durch einen Angestellten
   3. **manuelle Kontrollen** in zeitlichen Intervallen: z.B. Wartungsaktivitäten am Server

Kontrollarten für IT-Prozesse

c) weitere IT-Kontrollen

1. **Anwendungskontrollen** sind direkt in den Geschäftsprozessen integriert: z.B. Toleranzprüfung beim Rechnungseingang, Prüfung der Übereinstimmung von Bestellung, Wareneingang und Rechnung

2. **allgemeine Kontrollen** für alle Bereiche die mit der Einrichtung des IT-Systems im Unternehmen verbunden sind: z.B. Softwareauswahl, Programmentwicklungen oder -Änderungen

Risikomanagementsystem (RMS)

- Überwachungssystem zur frühzeitigen Erkennung und Kommunikation bestandsgefährdender Entwicklungen (Risiken)

- bestandsgefährdende Risiken bspw. durch:

  - risikobehaftete Geschäfte,
  - Unrichtigkeiten der Rechnungslegung und
  - sonstige Verstöße gegen gesetzliche Vorschriften, welche sich auf die Vermögens-, Finanz- und Ertragslage der Gesellschaft auswirken.

Risikomanagementsystem (RMS)

- Die mit der Unternehmensstrategie und -Zielen einhergehenden Risiken sind zu beachten.
- separate Risikostrategie, neben der allgemeinen Geschäfts-, Firmenpolitik
- gesetzliche Grundlagen:
  - § 91 Abs.2 AktG, eingefügt durch KonTraG 1998
  - §§ 76 Abs.1, 93 Abs.1 Satz 1 AktG
  - § 289 HGB, Neufassung durch BilReG
  - Abschnitte 4.1.1, 5.2, 5.3 DCGK (Steigerung des Unternehmenswertes,Arbeit VS/AR, Audit Committee)

RMS-Bestandteile

Das RMS setzt sich zusammen aus

a) internen Überwachungssystem
b) Risikocontrolling
c) Risikofrühwarnsystem

a) internes Überwachungssystem:
- enthält Maßnahmen zur Überwachung des RMS
- Aufgabenträger ist die interne Revision
- Prüfungsgrundlage ist das Risikohandbuch

RMS-Bestandteile

b) Risikocontrolling:

- Integration von Risikoaspekten in die üblichen Controllingprozesse
- Risikoidentifikation, Risikoplanung, Risikoreporting als wichtigste Aufgaben
- Zuständigkeit der Risikosteuerung liegt beim Management, jedoch verwendet es die bei der Risikoplanung des Controllings gewonnenen Informationen (Gleich/Oehler (2006), S. 72, S. 74)
- Instrumente: SWOT-Analyse, Szenario-Technik, Risiko-Balanced Scorecard

RMS-Bestandteile

c) Risikofrühwarnsystem

- Prognosen über zukünftige Entwicklungen die das Erfolgspotential der Gesellschaft beeinflussen (Diskontinuitäten)
- Diskontinuitäten kündigen sich durch schwache Signale (Indikatoren) an
- Indikatoren aus bestimmten Beobachtungsfeldern werden festgelegt
- Beobachtungsfelder (Gesamtwirtschaft, Marktstruktur, unternehmensinterne Daten, etc.)
- Indikatoren (Sozialprodukt, Wettbewerber, Rentabilität, Kosten, etc.)
- große Änderungen der Indikatoren zeigen größere Entwicklungen an
- reaktionsgerechte Erkennung von Risiken/Chancen (Frühwarnung)

Vgl. Gleich/Oehler (2006), S.64-66

Fazit Informationssysteme

- Einhaltung der Corporate Governance Prinzipien: Publizität, Transparenz und Kontrolle

Internes Kontrollsystem

- Regelungen des internen Überwachungssystems dienen im wesentlichen der Vermeidung wesentlicher Fehler in der Finanzberichterstattung.

Fazit Informationssysteme

Risikomanagementsystem

- Beachtung von Entwicklungen und der Chancen und Risiken seitens der Unternehmensleitung zur stakeholdergerechten Unternehmensführung.
- Unternehmensfortbestand als Hauptinteresse der Stakeholder zur Wahrung weiterer Ansprüche

IT-Kontrollsystem

- veränderte Risiken aufgrund Durchdringung von IT in den Unternehmen
- Beachtung durch spezifische IT-Kontrollmaßnahmen

Fragen und Thesen zur Sektion

- Sollte der DCGK auch für größere nicht börsennotierte deutsche Unternehmen verbindlich werden?
- Sollten Corporate Governance Regelungen in Zukunft gesetzlich verankert werden?
- In wie weit steht es dem Gesetzgeber zu, in die internen Organisationsstrukturen eines Unternehmens einzugreifen?
- Ohne Informationssysteme wären die Ansprüche der Stakeholder nicht zu wahren!
- Interne Kontrollsysteme sind im besonderen Maße für die Einhaltung der Rechnungslegungsnormen verantwortlich!