



Kleiner & Kleiner GmbH
Wirtschaftsprüfer & Steuerberater
A-8010 Graz, Burgring 22
www.kleiner.co.at

Stadt **GRAZ** Stadtrechnungshof

Workshop

Internes Kontroll-System

Dipl.-Dolm. Dr. iur. Fritz Kleiner
WP/StB

Dr. Günter Riegler
Stadtrechnungshof – WP/StB

Magistrat Graz
Vermögens- und Finanzdirektion

6. 6. 2006

Definition IKS

- Das **Interne Kontroll-System** umfasst alle in der Unternehmensorganisation vorgesehenen Maßnahmen, die dazu bestimmt sind, das vorhandene Vermögen zu sichern, die betriebliche Leistungsfähigkeit zu steigern und die Einhaltung der Geschäftspolitik, sowie der Richtlinien und Vollständigkeit der Aufzeichnungen zu gewährleisten. Die Bedeutung des IKS wächst mit der Größe des Unternehmens.

(Definition laut Studie der Unterlage zur WP-Fachprüfung.)

Definition IKS

- Unter dem Begriff des „Internen Kontroll-Systems“ (IKS) versteht man das individuelle System von aufeinander abgestimmten und sich ergänzenden (schriftlich festgelegten oder auch nur tatsächlich angewandten) Methoden und Maßnahmen in der Aufbau- und Ablauforganisation eines Unternehmens, die dazu dienen, Fehler zu verhindern und die Einhaltung vorgegebener Normen zu gewährleisten, und insbesondere auch
 - die Vollständigkeit und Richtigkeit der geschäftlichen Aufzeichnungen zu sichern,
 - die vorhandenen Vermögenswerte zu sichern,
 - die betriebliche Leistungsfähigkeit zu steigern,
 - die Geschäftsführung bei ihrer Überwachungsaufgabe zu unterstützen.

(Zitat aus einer Prüferinformation zur Prüfung des IKS für Wirtschaftsprüfer)

Definition IKS

- Das interne Kontrollsystem (IKS) umfasst alle Formen von prozess- und organisationsimmanenten Überwachungsmaßnahmen, die in die zu überwachenden Geschäftsvorfälle integriert sind. Dies hat den Zweck, das Unternehmensvermögen vor Verlusten zu sichern und zu schützen. Daneben soll mit einem IKS zum einen die Genauigkeit und Zuverlässigkeit der Zahlen gewährleistet und zum anderen die Einhaltung des unternehmensinternen Regelwerks unterstützt werden.

(Fachartikel IKS Belser/Berchthold, Ernst & Young AG)



Internes Kontrollsystem

COSO-Systematik

- Das interne Kontrollsystem ist ein Managementinstrument.
- Es soll Unternehmensziele sicherstellen. Es wird in den Bereichen Prozesse, Informationen, Vermögensschutz und Compliance eingesetzt.
- Das IKS umfasst alle dafür von der Geschäftsleitung angeordneten organisatorischen Methoden und Maßnahmen.

COSO Modell: „ The Committee of Sponsoring Organizations of the Treadway Commission“ (www.coso.org)

Die Elemente des IKS

- 1. Risikobeurteilung:**
Sind sich Geschäftsleitung und Aufsichtsrat aller wesentlicher Risiken (Geschäftsrisiken, Vermögensrisiken) bewusst?
- 2. Kontrollumfeld:**
Welches Klima herrscht im Unternehmen in Bezug auf Risikobewusstsein?
- 3. Kontrolltätigkeiten:**
Welche Kontrollen sind im Unternehmen installiert?
- 4. Information und Kommunikation:**
Welche Berichtsstrukturen gibt es und sind diese ausreichend? (Erhalten alle „Manager“ die für ihre Kontrolltätigkeit notwendigen Informationen?)

Fazit: IKS ist mehr als bloß ein Kontrollinstrument – es vermittelt Steuerungsmöglichkeiten und die dafür benötigten Informationen und es zieht sich durch alle Prozesse



Interne Revision

- Die Prüfungstätigkeit der Internen Revision hat sich unter Berücksichtigung des Umfangs und des Risikogehaltes der Betriebs- und Geschäftstätigkeit auf alle Betriebs- und Geschäftsabläufe zu erstrecken.
- Die interne Revision hat dabei insbesondere (und unter anderem) die **Funktionsfähigkeit**, Wirksamkeit, Wirtschaftlichkeit und Angemessenheit **des Internen Kontroll-Systems** zu prüfen und zu beurteilen.
- Die Interne Revision hat ihre Aufgaben selbstständig und unabhängig wahrzunehmen und darf bei der Berichterstattung und Wertung der Prüfungsergebnis keiner Weisung unterworfen sein.

IKS – Interne Revision

- Die Prüfungsorgane der internen Revision überprüfen die Wirksamkeit des IKS

Verpflichtung

- Es gehört zu den Pflichten der Geschäftsleitung von Kapitalgesellschaften aller Größenordnungen, nach § 82 Aktiengesetz, § 22 GmbHG im Rahmen des Rechnungs-wesens die Führung eines Internen Kontrollsystems (IKS) einzurichten, wobei dieses System den Anforderungen des Unternehmens zu entsprechen hat.

IKS - Abschlussprüfer

- Der Abschlussprüfer (Wirtschaftsprüfer) hat im Rahmen seiner pflichtgemäßen Abschlussprüfung ein Urteil abzugeben über die Einrichtung, **Eignung und Einhaltung des IKS**. Sollte der Abschlussprüfer kein bzw. ein nur schlecht ausgebildetes IKS vorfinden und ist darin ein schwerwiegender Verstoß im Sinne des § 273 (2) HGB zu sehen, löst dies seine Redepflicht gegenüber dem gesetzlichen Vertreter und dem Aufsichtsrat aus.

Strafrechtliche Überprüfung

- Im Rahmen der strafgerichtlichen Beweiswürdigung werden im Regelfall Sachverständigengutachten eingeholt. Diese beziehen sich auf die strafrechtlich relevante Vorgangsweise von Unternehmen und Organen. Das Vorliegen eines IKS, die Tätigkeit der internen Revision und die Prüfungstätigkeit des Abschlussprüfers fließen in diese Begutachtung ein. Wesentliche Verdachtsmomente werden unter dem Blickwinkel des § 146 StGB (Betrug) § 153 StGB (Untreue), § 156 StGB (betrügerische Krida), § 159 StGB (Fahrlässige Beeinträchtigung von Gläubiger-interessen) aber auch nach dem Kapitalmarktgesetz, dem Bankwesengesetz, dem GmbH-Gesetz (§ 122) und dem Aktiengesetz § 255 (Bilanzfälschung) beurteilt.



Rechnungshof

- Der Rechnungshof prüft die Wirtschaftlichkeit, Zweckmäßigkeit und Sparsamkeit der Gebarung der Stadt sowie ihrer Unternehmen.
- Dazu gehört auch die Zuverlässigkeit der Kontrollsysteme der geprüften Stellen, um unkontrollierte Vermögensabflüsse hintan zu halten.
- Fazit: in diesem Punkt besteht eine "Überlappung" zwischen den Prüfungszielen des Abschlussprüfers und des RH.

Funktionstrennung im Unternehmen

1. Unternehmensführung
2. Finanz-/Rechnungswesen, Controlling
3. Beschaffung
4. Produktion und Technik
5. Handel, Absatz, Marketing
6. Personalverwaltung
7. Forschung und Entwicklung

Selbstkritische Frage:

Kommt es im Unternehmen zu Besetzungen dieser Funktionen durch ein- und dieselbe Person?

Risikobeurteilung 1

Sind sich **Management und Aufsichtsrat** der wesentlichen Risiken bewusst?

Beispiele:

- **Marktrisiken:**
 - Bedrohung durch Mitbewerber?
 - Abhängigkeit von einzelnen Kunden?
 - Abhängigkeit von einzelnen Lieferanten?
 - Produktrisiken?
 - Politische/Wirtschaftliche Risiken?
- **Vermögensrisiken:**
 - Sicherheit des gelagerten Vermögens? (zB Warenlager, Geldbestände, Anlagen ...)
 - Risiken bei Vermögenstransaktionen? (zB Geldflüsse, Warenbewegungen ...)
- **Sonstige Risiken (beispielhaft):**
 - IT-Risiken? (zB Datenverlust, Datenmissbrauch, IT-Beschädigungen ...)
 - Abhängigkeit von Schlüsselpersonal? (Know-How-Sicherung, Marktbeziehungen der Mitarbeiter ...)
 - Abhängigkeit von externen Lieferanten? (IT-Lieferant, Berater ...)
 - Vertragsrisiken? („Schlummernde Zeitbomben in Verträgen“)
 - Steuerliche Risiken?



Risikomanagement

- Um Kontrollen wirksam werden zu lassen, ist das Prozessrisiko einer Vorgangsweise abzuschätzen. Diese Risikoeinschätzung besteht darin, das Risiko zu definieren und zu analysieren und zu klären wie mit dem Risiko umzugehen ist. Risiken können verhindert werden, umgangen werden, abgesichert werden oder in Kauf genommen werden.
- Die Risikoeinschätzung ist Aufgabe der zuständigen Abteilung.

Risikobeurteilung 2

Welche **Strategien zur Risikobewältigung** gibt es?

Mögliche Antworten:

- **Funktionstrennung, 4-Augen-Prinzip, IKS schlechthin**
- **Marktrisiken:** Marktbeobachtung, Streuung von Kunden-/Lieferantenbeziehungen oder Absatz-/Beschaffungsmärkten, Beobachtung des technischen Fortschrittes
- **Vermögensrisiken:**
 - Zugangsbeschränkungen, regelmäßige Kontrollen und Berichte über den Vermögensbestand
 - Jede Vermögenstransaktion ist eine potenzielle Fehlerquelle – wird vertieft!
- **Versicherung von Risiken**
- **Abwälzung von Risiken** (zB Wechselkursrisiken, Zinsrisiken etc)
- **Einbindung des gesamten Managements in die Risikoanalyse** (Risk-Assessments)
- **Diskussion der Risikobeurteilung auch mit dem Aufsichtsrat**

Kontrollumfeld 1

Welches **Klima herrscht im Unternehmen in Bezug auf Risikobewusstsein?**

Beispielhafte Aspekte:

- **Geschäftspolitik – Unternehmenskultur**
 - Risikofreudigkeit oder -aversion?
 - Will man der Beste oder der Billigste am Markt sein?
 - Sind die Produkte und Leistungen am „Stand der Technik“
- **Qualität der Mitarbeiter:**
 - Sind die Mitarbeiter gut ausgebildet, gut bezahlt, motiviert?
 - Gibt es eine Personalpolitik? (oder wird aktionistisch gehandelt?)
 - Wie werden disziplinaire Vergehen behandelt?
- **Unternehmensführung und Aufsichtsrat:**
 - Gibt es genügend Informationsaustausch zwischen den Geschäftsführern bzw zwischen GF und Aufsichtsrat
 - Hat die Geschäftsführung genügend Zeit, um sich mit sachlichen Einzelfragen des Geschäftes zu befassen?
 - Werden Fragen, die fachlich dem jeweils anderen Geschäftsführer zugeordnet sind, ausreichend diskutiert und kommuniziert?

II. Die Elemente des IKS

Risikobeurteilung – Kontrollumfeld –
Kontrolltätigkeiten – Information und
Kommunikation

Kontrollumfeld 2

Welches **Klima herrscht im Unternehmen in Bezug auf Risikobewusstsein?**

Beispielhafte Aspekte:

- **Hält das Top-Management ausreichend Kontakt mit dislozierten Bereichen, mit Mitarbeitern von Tochtergesellschaften uä?**
- Fördert die **Organisationsstruktur** den Informationsfluss oder ist sie hinderlich?
- Wird die **Organisationsstruktur** regelmäßig hinterfragt und nötigenfalls angepasst?
- Werden wesentliche **Entscheidungsspielräume für Abteilungen, Tochtergesellschaften, ausgelagerte Betriebsteile** festgelegt, ausgeweitet oder begrenzt, nach oben kommuniziert und von der Unternehmensführung hinterfragt?
- Gibt es **dominierende Persönlichkeiten** („informelle Führer“) im Betrieb und sind diese dem Management bekannt?
- Gibt es **Regelungen für außergewöhnliche Geschäfte/Sachverhalte? („Notfallspläne“)**
- Werden für **schwierige Entscheidungen/Fragestellungen** adäquate Fachauskünfte eingeholt/zugekauft?
- Gibt es eine freiwillige/verpflichtende Jahresabschlussprüfung?

Kontrollumfeld 3

Welches **Klima herrscht im Unternehmen in Bezug auf Risikobewusstsein?**

... und der vielleicht wichtigste Aspekt:

- Gibt es **Arbeitsanweisungen** für wesentliche Prozesse, insbesondere für jegliche Arten von **Vermögenstransaktionen**?
 - Gibt es für alle **wichtigen Funktionen** (siehe „Funktionstrennung“) eine/n **zuständige/n und auch verantwortliche/n MitarbeiterIn**?
 - Ist **schriftlich festgelegt, wer welche Tätigkeiten nach außen durchführen** kann (Bestellungen, Zahlungen, Ausstellung von Rechnungen, Mahnungen, Klagen, Kredite, Bankkonten, Stundungen, Rabatte, uä)?
 - Gibt es **Regelungen für urlaubsweise/krankheitsbedingte Vertretungen** und wird verhindert, dass es zu solchen Zeiten zur Funktionsvereinigung „in einer Person“ kommt?
 - Gibt es **betragsmäßige/inhaltliche Limits**, ab denen eine zusätzliche Stelle/eine zusätzliche Person eingeschaltet werden muss?
 - Gilt für **wesentliche Schritte** (nicht unbedingt für alle Schritte!) in den Abläufen das **4-Augen-Prinzip**?



Vertragsrisiko/Beispiel/1

- Vertragspartner – Existenz, Geschichte
- Vertragsinhalt
 - wer leistet
 - worin besteht die Leistung
 - wer bezahlt
 - welche Gewährleistung oder Leistungskontrolle ist vereinbart?
 - Leistungsversicherung (completion bond)
 - etc.
- Von welchen Parametern hängt die
 - Leistung
 - Zahlung, ab.

Vertragsrisiko/Beispiel/2

- Wer ist abschlussberechtigt?
- Bestehen Berechtigungsbeschränkungen?
- Wer ist über Vertragsverhandlungen und/oder Vertragsabschluss zu informieren?
- Welche nachfolgenden Schritte (Konsequenzen) ergeben sich aus der Leistungserbringung?
- Rolle des Abschlussprüfers (Vollständigkeitserklärung)?

IKS Beschaffungsbereich

- Wesentlichste Unvereinbarkeit zwischen Bestellung und Warenentnahme
- Übernehmen der Ware und Freigeben der Rechnung zur Zahlung
- Gibt es ein Einkaufssystem?
- Bedarfsmeldung mit/ohne Wertgrenzen, Mindestbestände
- Angebotseinholung
- Bestellung
- Bestellüberwachung
- Wareneingang



IKS Einkauf und Rechnungsprüfung

- Zusammenspiel Lieferant und Einkäufer
- Freigabe zur Zahlung mittels Rechnungskopie
- Anerkennung einer fingierten Rechnung
- Anerkennung einer privaten Rechnung des Rechnungsprüfers
- Eine gerechtfertigte Belastung an den Lieferanten wird nicht erstellt

IKS Finanzmittel

- Inkasso ohne Ausstellung eines Belegs
- Kassaeingangsbelege verschwinden
- Unerklärbare Stornierungen
- Verbuchung fingierter Kassaausgangsbelege
- Manipulation von Kassaausgangsbelegen
- Entnahme von Bargeld
- Überweisungen an ein falsches (eigenes) Konto
- Nichterfassen von eingehenden Wechsel und Schecks
- Aufnahme von Darlehen zu marktunüblichen ungünstigen Konditionen
- Darlehensgewährung ohne Sicherheiten

IKS Absatzbereich

- Unvollständige Fakturierung von erbrachten Leistungen
- Verrechnung niedrigerer Preise bei bestimmten Kunden
- Verrechnung ungerechtfertigter Rabatte bei bestimmten Fakturen (Stammkundenvereinbarung)
- Ausstellung von ungerechtfertigten Gutschriften an Kunden
- Fingierte Gutschriften an Lieferanten



IKS Personalverwaltung

- Verwendung von untergeordneten Mitarbeitern für private Zwecke
- Unvollständiges Führen von Leistungsaufzeichnungen durch Mitarbeiter
- Abrechnung von fiktiven Mitarbeitern (doppelt verrechnete Reisekosten einmal bei Tochtergesellschaft, einmal bei Muttergesellschaft im Ausland)



IKS im IT Bereich

- Der Grad der Sicherheit von IT Systemen wird in großen internationalen Unternehmen heute durch Einführung nationaler Sicherheitsstandards definiert.
 - Folgende Standards sind dabei in Anwendung:
 - Cobit, Control Objectives for Information and related Technology, eine Trademark der ISACA
 - British Standard 7799 (www.bspsl.com/secure/17799/cvm.cfm)
 - ISO 17799 bzw. A7799 (dies ist der BS7799 der von der ISO bzw. der ÖNORM übernommen wurde).
 - IT Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnologie in Deutschland
 - KFS/DV1 und KFS/DV2 der Kammer der Wirtschaftstreuhänder Österreich. Die Positionen 1 bis 5 zielen vorrangig auf die Sicherheit von Informationen und Informationssystemen ab.
 - Das Fachgutachten unserer Kammer definiert die Vorraussetzung eines IT-Systems, um als Buchführungssystem anerkannt zu werden.

II. Die Elemente des IKS

Risikobeurteilung – Kontrollumfeld –
Kontrolltätigkeiten – Information und
Kommunikation

Kontrolltätigkeiten

Welche **Kontrollen sind im Unternehmen installiert**? Werden die vorstehend aufgezählten Kontrollelemente auch tatsächlich „gelebt“ und wird dies vom Management auch überwacht?

Beispiele:

- Achtet der Geschäftsführer bei der Zahlungsfreigabe darauf, dass alle vorgelagerten Schritte eingehalten wurden?
- Werden vor Zahlungsfreigabe durch die Geschäftsführung stichprobenartig die Eingangsrechnung, der Kostenvoranschlag und die Bestellung durchgesehen?
- Wird stichprobenartig kontrolliert, ob tatsächlich alle nötigen Unterschriften/Paraphen auf einer Eingangsrechnung vorhanden sind?
- Wird dies auch **wechselseitig durch die Geschäftsführer kontrolliert**?
- Wird der **Abschlussprüfer** dazu motiviert, entsprechende Systemprüfungen durchzuführen und über die Ergebnisse zu berichten?
- Werden **Soll-Ist-Vergleiche** angestellt, eingeholt, analysiert und wird Abweichungen nachgegangen?
- Erfolgt eine **Abstimmung von Finanz-/Ergebnisberichten mit Berichten aus der Produktion/Technik/Einkauf/Verkauf**?
- Gibt es eine interne Revision und einen Revisionsplan?

Information und Kommunikation

II. Die Elemente des IKS

Risikobeurteilung – Kontrollumfeld –
Kontrolltätigkeiten – Information und
Dokumentation

Welche **Berichtsstrukturen** gibt es und sind diese ausreichend?
(Erhalten alle „Manager“ die für ihre Kontrolltätigkeit notwendigen Informationen?)

Beispiele:

- Gibt es eine **definierte Anzahl und Beschaffenheit interner Berichte**?
- Werden diese **regelmäßig eingefordert**, erhalten, analysiert, hinterfragt, diskutiert?
- Wird das Berichtswesen **regelmäßig hinterfragt und verbessert**?
- Werden die berichteten **Daten mit Daten anderer Stellen (Quellen) abgestimmt** und plausibilisiert?
- Werden auf Grund der vorliegenden Berichte neue Maßnahmen gesetzt, Weisungen erteilt, **bisherige Vorgehensweisen geändert**?
- Werden empfangene Berichtsergebnisse an zuständige MitarbeiterInnen anderer Stellen zur Kenntnis gebracht?
- Werden **Berichtsdaten mit Daten Externer (zB Mitbewerber) verglichen**?
- Werden wesentliche Positionen/Aussagen des Jahresabschlusses hinterfragt?
- Wie wird mit Berichten der internen Revision umgegangen?



Und nach der Einführung eines IKS?

- Die Einführung eines IKS muß in seiner Bedeutung, Handhabung und Wirksamkeit kontrolliert werden. Dazu dient die Interne Revision, die sowohl unternehmensintern als auch unternehmensextern durchgeführt werden kann.
- Bei einer externen Auftragsvergabe ist jedenfalls der Wirtschaftsprüfer des Unternehmens der die pflichtgemäße Abschlussprüfung durchführt, von der Durchführung der internen Revision ausgeschlossen.

Corporate Governance Kodex

- Der österreichische Corporate Governance Kodex ist eine freiwillige Selbstregulierungsmaßnahme börsennotierter Aktiengesellschaften. Das heißt nicht, dass ein derartiger Kodex nicht auch in kleineren Aktiengesellschaften oder GesmbH's anwendbar und durchsetzbar ist.
- Die Maßnahmen umfassen folgende Kategorien:
 - Eine Regel des Kodex beruht auf zwingenden Rechtsvorschriften
 - Eine Regel des Kodex soll eingehalten werden, eine Abweichung muß erklärt und begründet werden (comply or explain)
 - Eine Regel hat Empfehlungscharakter; Nichteinhaltung ist weder offenzulegen noch zu begründen.
 - **Anzuregen** ist die erste Fassung eines **Corporate Governance Codex für gemeindenahe Unternehmen** welche auch ein Audit Committee beinhalten sollte.



6 Fragen an die Geschäftsleitung

1. Erfolgt eine regelmässige und systematische Neubeurteilung der wesentlichen Geschäftsrisiken, verbunden mit einer stufengerechten Information über die eingeleiteten Massnahmen?
2. Wird die Wirksamkeit der internen Kontrolle von der Geschäftsleitung periodisch mit dem Verwaltungsrat bzw. dem Audit Committee erörtert?
3. Werden die bestehenden Prozesse und Kontrollen regelmässig neu beurteilt und, falls notwendig, entsprechend angepasst?
4. Sind die Anforderungen (Methode, Umfang, Detaillierungsgrad) and die Dokumentation der Prozesse und Kontrollen klar definiert?
5. Stellt das IKS an die Erstellung der Jahresrechnung die gleichen Anforderungen wie an die operativen Prozesse?
6. Werden die Kosten der Kontrollmassnahmen – unter Berücksichtigung eines nachhaltigen Nutzens – im Verhältnis zum Risiko beurteilt?



Danke für Ihre Aufmerksamkeit!

Dipl.-Dolm. Dr. iur. Fritz Kleiner
WP/StB

Dr. Günter Riegler
Stadtrechnungshof – WP/StB