

<b>Forum für Controlling AG, Burgdorf</b> © by Forum für Controlling AG, Burgdorf	Checkliste
<b>=&gt; Internes Kontrollsysteme (IKS)</b>	<b>Version 08.2011</b>

Punkt	Inhalt
	<p><b>Sind formelle Voraussetzungen erfüllt, damit IKS eingeführt werden muss?</b> (OR 727 in Kombination mit OR 663,12 =&gt; Angaben über Durchführung einer Risikobeurteilung)</p> <ul style="list-style-type: none"> <li>- <b>Bilanzsumme</b> über 10 Mio. CHF</li> <li>- <b>Umsatz</b> über 20 Mio. CHF</li> <li>- <b>Anzahl Vollzeitstellen</b> p.a. im Durchschnitt über 50?</li> </ul> <p>2 der drei Kriterien müssen während zwei aufeinanderfolgenden Jahren erreicht sein</p> <p>⇒ IKS für Buchführung und Rechnungslegung</p>
	<p><b>Verantwortlichkeiten (intern)</b></p> <ul style="list-style-type: none"> <li>• Verwaltungsrat: _____</li> <li>• Evtl. Audit Committee oder interne Kontrollstelle: _____</li> <li>• Geschäftsleitung: _____</li> </ul>
	<p><b>Fitness-Fragen zum Stand:</b></p> <ul style="list-style-type: none"> <li>• Verfügt die Unternehmung über eine <b>definierte Politik</b> bezüglich interner Kontrollen über die Finanzberichterstattung?</li> <li>• Sind die <b>Verantwortungsbereiche</b> zwischen <b>VR</b> und <b>GL</b> klar zugewiesen?</li> <li>• Ist das IKS auf der <b>Traktandenliste des VR</b>?</li> <li>• Ist das IKS auf der <b>Traktandenliste der GL</b>?</li> <li>• Besteht eine aktuelle Dokumentation der <b>relevanten Prozesse</b> und Schlüsselkontrollen?</li> <li>• Bestehen definierte <b>Vorgehensweisen für den Umgang</b> mit identifizierten <b>Schwachstellen</b> im IKS?</li> <li>• Ist definiert, <b>wer prüft wie, wann und von wem</b> die definierten Schlüsselkontrollen tatsächlich durchgeführt werden?</li> <li>• Ist sichergestellt, dass die Risiken im Zusammenhang mit der Finanzberichterstattung <b>systematisch erhoben und behandelt</b> werden?</li> <li>• Ist die <b>IT</b> in das IKS miteinbezogen?</li> </ul>

	<p><b>Revisionsstelle (extern)</b></p> <ul style="list-style-type: none"><li>• Wer ist Revisionsstelle: _____</li><li>• Ansprechpartner / Telefon-Nr. / E-Mail _____ _____</li><li>• Was muss die Revisionsstelle prüfen (bei ordentlicher Revision / OR 727):<ul style="list-style-type: none"><li>- Existenz eines IKS (OR 728a)</li><li>- umfassender Bericht über das IKS (OR 728b)</li></ul></li></ul>
	<p><b>Andere Zertifizierungen</b></p> <ul style="list-style-type: none"><li>• Welche hat die Unternehmung bereits? (z.B. ISO<sup>1</sup>, Branchenzertifikate usw.) _____ _____</li><li>• Andere Risikomanagement- und Rechnungslegungssysteme: IAS (Anwendung IFRS 7): _____ US-GAAP: _____ SWISS GAAP FER: _____ SOX: _____</li></ul>

<sup>1</sup> 9001; 14000 (Umwelt); 20000 (IT-Service); 27000 (IT-Security)

**Kernprozesse** der Unternehmung (Input, Transformation, Output)

= > Hauptrisiken daraus

= > Schwerpunkte bilden

**Unterstützungsprozesse** in der Unternehmung

- Geschäftsführung
- Finanzen
- Personal
- Informatik
- Forschung und Entwicklung
- Qualitätssicherung
- Investitionen / Projekte
- Weitere (z.B. Pflege von Minderheitsaktionären)

**Kontrollumfeld**

- Leitungsorgane
- Organisationsstruktur
- Kontrollsysteme (interne Revision, Personalpolitik, Personalwesen, Funktionen-Trennung usw.)
- Funktionenteilung (Anweisend / Ausführung / Kontrollierend)

**Heutiger Stand:**

- Wie werden die **Geschäftsrisiken** identifiziert, definiert und eingebunden?
- Gibt es einen **systematisierten Zielsetzungsprozess** (Strategie usw.)?
- Gibt es eine **sWeisungs-Sammlung**?
- Gibt es weitere **Sammlungen**? Z.B.
  - Vertragsmanagement
  - Handbücher => Prozesssammlungen
  - Finanzierungsgrundsätze
  - Informatik: Richtlinien für den Umgang mit Informatik
  - Datensicherungs- und Datensicherheitskonzept
  - Zugriffsberechtigungskonzept / -liste (Vertraulichkeitsstufen)
  - usw.
- Welche **Kontrollaktivitäten** haben Sie generell (im Finanzbereich)?
  - **manuelle Kontrollen** wie
    - Einhaltung definierte Kompetenzordnung
    - Einhaltung Unterschriftenregelungen (gibt es überhaupt eine?)
      - intern (Visa-Regelung)
      - extern (Handelsregister, Banken usw.)
    - Rechnerische Kontrollen (von zwei Seiten)
    - Abstimmkontrolle (Belegabgleich, Listenvergleich)
    - physische Kontrollen (Wareneingang, Warenausgang, Inventur)
  - **Automatisierte Kontrollen** wie
    - Zugriffsschutz (Datenschutz, Datensicherheit)
    - Prüzziffern
    - Fehlerprotokolle (z.B. über Nacht aufbereitet)
  - **Unabhängige Kontrolle** durch das Management (VR, Geschäftsleitung) wie
    - Reports, Budgetvergleiche usw.
    - Einsatz einer internen Revision (Prüfplan, Berichterstattung)
    - Einsatz externer Kräfte
- Wie sieht **der Budget-Prozess** aus?
- Wie sieht **der Controlling-Prozess** aus?
- Wie sieht **der Kalkulations-Prozess** aus?
- Welche **Kontrollen** werden **IT-unterstützt** durchgeführt?  
=> Vernetzung der Software; Wie sieht die IT-Landschaft aus (HW / SW / NW)
- **Wann geschehen welche Kontrollen**?
  - regelmässig, und zwar \_\_\_\_\_
  - unregelmässig
- Wie werden **die Mitarbeitenden stufengerecht informiert**?  
Welche Mittel dazu werden verwendet (z.B. auch Management Letters)?
  - Persönlich durch \_\_\_\_\_
  - Sitzungen / standardisierte Veranstaltungen (z.B. Kaderinfo, Mitarbeiterinfo o )
  - Via schriftliche Mitteilungen, und zwar \_\_\_\_\_
  - Elektronisch via Mail
  - Intranet
  - Weitere \_\_\_\_\_
- Wie und wann ist **der Informationsfluss** bezüglich Risikoeinschätzungen zwischen **GL** und **VR**?
- Werden die bestehenden Prozesse und Kontrollen **regelmässig neu beurteilt** und ggf. angepasst?
- Sind die Anforderungen (Methode, Umfang, Detaillierungsgrad) an die Dokumentation der Prozesse und Kontrollen **klar definiert**?
- Werden die **gleichen Anforderungen** an ein IKS der operativen Prozesse gestellt, wie bei der Erstellung der Jahresrechnung?
- Wie sieht das **Kosten- / Nutzenverhältnis** für die Unternehmung bezüglich: Zusatzkosten Einführung oder Erweiterung IKS gegenüber Nutz?

**Wo würden Sie sich bezüglich IKS einordnen?**

- **Stufe 1: Wenig verlässlich** (interne Kontrollen sind kaum oder nicht vorhanden)
- **Stufe 2: Informell** (Interne Kontrollen sind vorhanden, aber nicht standardisiert)
- **Stufe 3: Standardisiert:** Einfache Grundsätze für ein IKS, Prozesse sind definiert
- **Stufe 4: Überwacht:** Detaillierte Beschreibung und Überwachung IKS-Prozesse
- **Stufe 5: Optimiert:** IKS-Aktivitäten sind auch auf alle anderen Prüffunktionen abgestimmt

⇒ Auf Grund Selbstbeurteilung: **Jedes Jahr von einer Stufe auf die nächste!**

⇒ **Anschliessend: KVP auf Stufe 5**

**Überblick über die Risiken (Vermögensrisiken) => Schwerpunkte bilden!!**

- **Strategische Risiken**
- **Geschäftsführungsrisiken**
- **Risiken der Nichteinhaltung von Gesetzen und Vorschriften (Compliance)**
- **Risiken der Vernichtung von Geschäftsvermögen**
  - **Kreditrisiko**
    - Debitoren
    - Darlehen (Aktiv)
  - **Liquiditätsrisiko**
    - Flüssige Mittel (inkl. Zugriffsregelung)
    - Warenlager (Warenpreis, Demodierung)
    - Zahlung (Kreditoren)
  - **Marktpreisrisiko**
    - Fremdwährungen
    - Finanzanlagen
    - Sachanlagen
    - immateriellen Anlagen (z.B. verfallende Lizenzen, Patente usw.)
    - Fremdkapital => Zinsen
  - **Verpflichtungsrisiken (Obligo)**
    - Offerten
    - Bestellungen
- **Risiken durch Fehler und Unregelmässigkeiten**
- **Risiken durch Unvollständigkeit oder Unzuverlässigkeit der Buchführung zB**
  - Abgrenzungen
  - Transitorien
  - Rückstellungen
  - Bewertungen
  - Archivierung => Siehe auch Checkliste sArchivierungsgrundsätze%
- **Risiken, dass nicht zeitgerecht und nicht verlässlich finanziell Bericht erstattet wird**
- **Versicherungen**
- **Kalkulationsrisiken**

**Zusammenfassung der Risiken (Vorseite)**

- **Hauptrisiken definieren (max. 5)** => Eintretenswahrscheinlichkeit / max. Schaden
- **Hauptrisiken in Quadranten einteilen:**
  - Risikopotenzial tief, Eintretenswahrscheinlichkeit tief: Kein Handlungsbedarf
  - Risikopotenzial hoch, Eintretenswahrscheinlichkeit tief: klassisches Riskmanagement
  - Risikopotenzial tief, Eintretenswahrscheinlichkeit hoch: Qualitätssicherung / qualitativ messen
  - Risikopotenzial hoch, Eintretenswahrscheinlichkeit hoch: Sollte eigentlich nicht sein (sonst: gezielte Einzelmassnahmen und Hauptgewicht zuerst hier)



- **pro Hauptrisiko RISK OWNER benennen** (wer schaut zu diesen Risiken?)
- **Schwerpunkte bilden (1 ÷ 5)**
- **IKS-Ziele pro Schwerpunkt (max. 3 pro Hauptrisiko)**
- **Zeitmass-Stäbe pro Risiko (wann ist Bericht zu erstatten durch Risk Owner?)**

**Kurzrepetition (kann ausgelassen werden): Was gibt es?**

**Weisungen   Prozesse   Organigramm   Check- Anweisungen  
listen**

**Kreditrisiken**

**Marktrisiken**

**Asset / Liability-R.**

**Operationelle Risiken**

<p><b>Nächste Schritte (allfälliges Projekt):</b></p> <p><b>Ziel des Projektes, Phase 1:</b></p> <p><b>Dauer / Zeitraum des Projektes, Phase 1:</b></p> <p><b>Beteiligte und ungefähre Kosten des Projektes Phase 1:</b></p> <p><b>Intern:</b></p> <ul style="list-style-type: none"><li>- VR / GL</li><li>- CFO</li><li>- QM</li><li>- Mitarbeitende Rechnungswesen</li><li>- ö ö ö</li></ul> <p><b>Extern:</b></p> <ul style="list-style-type: none"><li>- Forum für Controlling AG</li><li>-</li><li>- Kontrollstelle (evtl. Synergien)</li><li>- ö ö .</li></ul>
--

<p><b>Umsetzung / Unterstützung durch Forum für Controlling AG:</b></p> <ul style="list-style-type: none"><li>- 2 . 3 Mal jährlich unangekündigte Prüfung eines Teilprozesses</li><li>- 1 . 2 Mal jährlich: Dokumentenprüfung (ist das Ding noch aktuell?)</li></ul>
--

<p><b>Tätigkeit der Revisionsstelle:</b></p> <ul style="list-style-type: none"><li>- Rahmenbedingungen der Treuhandkammer (Prüfungsstandard 890)</li><li>- Bearbeitungsfelder:<ul style="list-style-type: none"><li>- Strategische Risiken</li><li>- Beurteilung der Risiken</li><li>- Kommunikation der Risiken: Finanzielle Berichterstattung</li><li>- Kontrollumfeld</li><li>- Kontrollaktivitäten</li><li>- Operative Umsetzung und Implementierung</li><li>- Überwachung (laufend)</li></ul></li></ul>
--