hotelleriesuisse

Monbijoustrasse 130

Postfach

CH-3001 Bern

Telefon +41 (0)31 370 41 11

Fax +41 (0)31 370 44 44

info@hotelleriesuisse.ch

www.hotelleriesuisse.ch

Risikomanagement und Internes Kontrollsystem

Führungselemente in der Hotellerie und im Gastgewerbe

hotellerie suisse
www.hotelleriesuisse.ch

Inhaltsverzeichnis

Impressum

Herausgeber
hotelleriesuisse, Bern

Gestaltung
TYPOMANIA Franziska Liechti, Bern

Druck
Druckerei Läderach AG, Bern

Verfasser

ELTSCHINGER Audit & Consulting AG
Martin Eltschinger

KPMG
Hans Knobel

Bern, November 2007

1. Gesetzliche Grundlagen

Risikobeurteilung und **internes Kontrollsystem** (IKS) sind wichtige Bestandteile einer wirksamen Corporate Governance und stehen deshalb zunehmend im Fokus von Investoren, Kreditgebern und weiteren Stakeholdern. Dies schlägt sich in der regulatorischen Entwicklung sowohl auf internationaler Ebene (z.B. Sarbanes-Oxley Act, 8. EU-Richtlinie) als nun auch in der Schweizer Gesetzgebung nieder.

Mit der **Neuordnung des schweizerischen Revisionsrechts (OR)** und dem neuen **Revisionsaufsichtsgesetz (RAG)** werden nicht nur die Aktiengesellschaften sondern auch andere Rechtsformen von Kapitalgesellschaften erfasst, so vor allem grosse GmbH, Genossenschaften, Stiftungen und Vereine.

Der neue **Art. 663b OR** verlangt, dass der Verwaltungsrat im Anhang der Jahresrechnung Angaben über die **Durchführung einer Risikobeurteilung** macht. Damit wird dies zum Prüfungsgegenstand der Revisionsstelle (für ordentliche und eingeschränkte Revision).

Unverändert gehören Aufbau und Umsetzung eines geeigneten **IKS** zu den Aufgaben des Verwaltungsrates (OR Art. 716a).

Bereits heute sehen die geltenden Prüfungsstandards vor, dass sich die Revisionsstelle bei ihren Arbeiten auf bestehende Kontrollen abstützt und diese somit in die Abschlussprüfung einbezieht. Damit werden aber rein prüfungstechnische Ziele wie die Identifikation risikobehafteter Prüfungsgebiete, die Festlegung der Prüfungshandlungen und eine möglichst hohe Effizienz des Prüfungsansatzes verfolgt. Gemäss Art. 728a Abs. 1 Ziff. 3 rev. OR muss neu sich nun bei der **ordentlichen Revision** der Prüfer ausdrücklich auch zur Existenz eines **IKS** und gegebenenfalls zu festgestellten Mängeln äussern. Eine ordentliche Revision erfolgt bei Unternehmen, die zwei der folgenden drei Grössen in zwei aufeinander folgenden Geschäftsjahren überschreiten: Bilanzsumme 10 Mio. CHF, Umsatzerlös 20 Mio. CHF, 50 Vollzeitstellen im Jahresdurchschnitt.

Risikobeurteilung und IKS können nur dann einer unabhängigen Prüfung unterzogen werden, wenn sie **dokumentiert** sind. Voraussetzung für positive Aussagen der Revisionsstelle zur Existenz eines IKS ist ferner, dass das IKS seitens der Unternehmung **tatsächlich etabliert** ist und **praktiziert** wird.

Die Neuordnung des Schweizerischen Revisionsrechts (OR) tritt per **1. Januar 2008 in Kraft** und gilt somit erstmals für die Jahresabschlüsse per 31. Dezember 2008. Die Auseinandersetzung mit den Themen **internes Kontrollsystem** (IKS) und **Risikobeurteilung** respektive **Risikomanagement,** gewinnt somit immer mehr an Bedeutung, und der Zeitdruck zur Umsetzung nimmt zu. Die leitenden Organe sollten sich darum bereits heute Gedanken zu den Auswirkungen dieser Gesetzesänderungen auf ihr Unternehmen machen und entsprechende Projekte, deren Zeitbedarf nicht zu unterschätzen ist, frühzeitig in die Wege leiten.

2. Risikomanagement und Risikobeurteilung

Risikomanagement

Im Allgemeinen wird die Risikobeurteilung als ein Teilaspekt eines umfassenden Risikomanagements und damit ein Teil der strategischen Führung eines Unternehmens verstanden. Ein umfassendes Risikomanagement überwacht und steuert sämtliche Unternehmensrisiken, wie beispielsweise die strategischen, operativen, finanziellen und rechtlichen Risiken. Der Risikomanagement-Prozess beinhaltet typischerweise eine Identifikation der Risiken, eine Analyse der Risiken hinsichtlich Höhe der Auswirkung eines Risikos und der Eintretenswahrscheinlichkeit inklusive einer Gesamtdarstellung der Risiken, einen laufenden Überwachungs- und Rapportierungsprozess sowie die Kontrolle und Steuerung der Risiken mittels operativer Massnahmen.

Risikobeurteilung

Das Aktienrecht enthielt bisher keine ausdrückliche Regelung zur Risikobeurteilung. Gemäss herrschender Auffassung ist die Einschätzung der Risiken ein zentrales Element der Strategiebildung und gehört daher zur Oberleitung der Gesellschaft im Sinne von Art. 716a Abs. 1 Ziff. 1 OR. Die Verantwortung für die Risikobeurteilung liegt demnach primär beim Verwaltungsrat und den anderen mit der Geschäftsführung betrauten Personen. Der Verwaltungsrat hat für ein Risikomanagement zu sorgen, die Durchführung des Risikomanagements ist eine Aufgabe der mit der Geschäftsführung betrauten Personen.
Art. 663b Ziff. 12 rev. OR verlangt von den Unternehmen, dass sie im Anhang der Jahres- und Konzernrechnung Angaben über die Durchführung einer Risikobeurteilung machen. Dieser Gesetzesartikel ist auf alle Unternehmen anwendbar, die einen Anhang nach den Vorschriften des Aktienrechts erstellen müssen und unabhängig davon, ob das Unternehmen einer ordentlichen oder einer eingeschränkten Revision unterliegt.
Das Gesetz äussert sich nicht zur Ausgestaltung der Risikobeurteilung. Der Gesetzgeber erwartet vom Verwaltungsrat lediglich eine inhaltliche Auseinandersetzung mit den Unternehmensrisiken. Hinsichtlich der Ausgestaltung der Risikobeurteilung ist der Verwaltungsrat somit frei. Er muss insbesondere die Grösse, die Komplexität und das Risikoprofil des Unternehmens berücksichtigen. Die Risikobeurteilung im Sinne von Art. 663b Ziff. 12 rev. OR umfasst nicht sämtliche Geschäftsrisiken. Betroffen sind nur jene Risiken, welche einen wesentlichen Einfluss auf die Beurteilung der Jahresrechnung haben könnten. Das Gesetz regelt nicht detailliert, welche Informationen zur Risikobeurteilung im Anhang der Jahresrechnung gemacht werden müssen. Die Unternehmen haben deshalb einen gewissen Ermessensspielraum.

3. Internes Kontrollsystem

Das Interne Kontrollsystem (IKS) ist ein wichtiges Führungsinstrument und Bestandteil eines funktionierenden Risikomanagements eines Unternehmens. Verwaltungsrat und Geschäftsleitung benötigen darum transparente und verlässliche Informationen über die Zuverlässigkeit und Wirksamkeit des IKS.
Das IKS ist als ergänzendes Kontrollsystem für mögliche bereits bestehende Qualitätsmanagementsysteme zu betrachten. Die Qualitätsmanagementsysteme decken im heutigen Zeitpunkt die Anforderungen, wie sie der Gesetzgeber verlangt, nicht abschliessend ab.
Obwohl die Prüfung der Existenz des IKS durch die Revisionsstelle in Art. 728a Abs. 1 Ziff. 3 rev. OR nur für die ordentliche Revision ausdrücklich als eigenständiger Prüfungsgegenstand zwingend ist, empfiehlt sich auch für kleinere Unternehmen zum Erreichen der nachstehend erwähnten Ziele soweit wie möglich die wesentlichen Kontrollen zu beachten.

Definition Begriff IKS und Ziele des IKS

Das IKS ist ein Managementinstrument zur zweckmässigen Sicherstellung der Erreichung von Unternehmenszielen in den Bereichen «Prozesse», «Informationen», «Vermögensschutz» und «Compliance». Das IKS umfasst alle dafür von der Geschäftsführung planmässig angeordneten organisatorischen Methoden und Massnahmen.
Das IKS umfasst in Bezug auf die finanzielle Berichterstattung diejenigen Vorgänge und Massnahmen, welche eine ordnungsmässige Buchführung und Rechnungslegung sicherstellen und dementsprechend die Grundlage jeder finanziellen Berichterstattung darstellen. In diesem Sinne beschränkt sich das IKS bezüglich der Abschlussprüfung auf die finanzielle Berichterstattung.

Umfang und Ausgestaltung des IKS

Damit bei der Abschlussprüfung beurteilt werden kann, ob ein Internes Kontrollsystem existiert, braucht es entsprechende inhaltliche Anforderungen, was unter einem IKS zu verstehen ist:

- Ein IKS muss vorhanden und überprüfbar sein, das heisst es muss eine aktuelle Dokumentation vorliegen, welche es erlaubt, die Existenz des IKS zu überprüfen.
- Das IKS muss den Mitarbeitern bekannt sein.
- Das IKS muss angewendet werden.
- Das IKS muss den jeweiligen Geschäfts-Risiken und dem Umfang der Geschäfts-Tätigkeit angepasst sein.
- Das Kontrollbewusstsein muss im Unternehmen vorhanden sein.

4. Aufbau und Kontrollen im Internen Kontrollsystem

Neben den angeordneten Vorgängen und Massnahmen spielt die innerhalb jedes Unternehmens gepflegte Kultur eine sehr wichtige Rolle. Alle Mitarbeiter und Führungskräfte prägen das Kontrollumfeld mit ihrer Integrität, ihren ethischen Werten und ihrer Vorbildfunktion.

Das IKS wirkt unterstützend bei:

- der Erreichung der geschäftspolitischen Ziele
- der Einhaltung von Gesetzen und Vorschriften
- dem Schutz des Geschäftsvermögens
- der Verhinderung, Verminderung und Aufdeckung von Fehlern und Unregelmässigkeiten bzw. absichtlich vorgenommenen Falschdarstellungen der Jahresrechnung
- der Sicherstellung der Zuverlässigkeit und Vollständigkeit der Buchführung
- einer zeitgerechten und verlässlichen finanziellen Berichterstattung, sowie
- einer wirksamen und effizienten Geschäftsführung.

Die organisatorischen Massnahmen des IKS sind in die betrieblichen Arbeitsabläufe integriert, d.h. sie erfolgen arbeitsbegleitend oder sind dem Arbeitsvollzug unmittelbar vor- oder nachgelagert. Die organisatorischen Massnahmen sollen das Management von Kontrolltätigkeiten entlasten und den ausführenden Stellen mehr Verantwortung übertragen. Der Einsatz der Informatik kann, je nach Ausbaugrad, eine wichtige Rolle spielen. Gut ausgebaute Verarbeitungsprogramme und Datenbanken ermöglichen einen hohen Grad an Automatisierung und Standardisierung und stellen eine wirksame interne Kontrolle dar.

Kontrollmassnahmen

Kontrollen bzw. Kontrollmassnahmen sind die einzelnen Vorgänge, Methoden und Massnahmen, die im Rahmen eines IKS auf den Ebenen eines Unternehmens umgesetzt werden.

Kontrollen auf Unternehmensebene sind Kontrollen mit durchgreifendem Charakter, die Einfluss auf mehrere Aspekte der Aufbau- und Ablauforganisation und somit auch auf mehrere Prozesse innerhalb der Unternehmung haben können. Es handelt sich beispielsweise um Kompetenzregelungen, Kontrollgremien, eine übergreifende Überwachung von Kontrollen auf Prozessebene oder ein systematisches Weisungswesen mit entsprechender Durchsetzung.

Kontrollen auf Prozessebene decken die Risiken einer wesentlichen Fehlaussage in der Buchführung und Rechnungslegung von der Initialisierung, Registrierung, Verarbeitung, Verbuchung bis zum Ausweis von Geschäftsvorfällen innerhalb einzelner Prozesse ab.

Generelle IT Kontrollen gewährleisten, dass die automatischen Applikationskontrollen ordnungsmässig funktionieren. Gibt es beispielsweise im Einkaufsprozess eine automatische Abstimmung zwischen Bestellung, Wareneingang und Rechnung.

Unterscheidung der Kontrollmassnahmen

Die Kontrollmassnahmen lassen sich in folgende Kategorien einteilen:

- präventive oder detektive Kontrollen
- selbsttätige, programmierte oder manuelle Kontrollen
- Kontrollen durch das Management.

Präventive Kontrollen

Als präventive Kontrollen bezeichnet man die zwangsläufigen Kontrollen, die auftauchende Fehler unmittelbar feststellen. Mit präventiven Kontrollen soll verhindert werden, dass Fehler überhaupt gemacht werden. Präventivkontrollen können in Form von selbsttätigen Kontrollen, manuellen oder automatisierten Kontrollen bestehen.

Detektive Kontrollen

Unter detektiven Kontrollen versteht man die sogenannten Aufdeckungskontrollen, die vorgenommen werden müssen, wenn bei der Überprüfung von präventiven Kontrollen eine zu grosse Fehlerhäufigkeit aufgetreten ist.

Selbsttätige und programmierte Kontrollen

Die selbsttätige Kontrolle ist die wirksamste, effizienteste wie auch wirtschaftlichste Kontrolle, da sie durch organisatorische oder technische Massnahmen direkt in die betrieblichen Abläufe integriert ist.

Organisatorische Massnahmen sind z.B. Funktionentrennung, Errichten von Kompetenzstufen und Regelung von Arbeitsabläufen.

Unter programmierten Kontrollen (Generelle IT- und Applikationskontrollen) versteht man die Zugriffsdifferenzierung, Authentisierung (durch Passwörter), Autorisierung (zum Beispiel elektronische Unterschrift), Plausibilisierungen, Prüfziffern, Kontrollsummen, Datenabgleich usw.

Manuelle Kontrollen

Die manuellen Kontrollen ergänzen die programmierten Kontrollen. Beispiele manueller Kontrollen sind: Genehmigungen, kritische Durchsicht, Abstimmungen, Abklärung von Differenz- oder Fehlermeldungen, physische Kontrollen usw.

Kontrollen durch das Management

Die prozessunabhängige Kontrolle durch das Management (Verwaltungsrat, Geschäftsleitung und übrige Führungsverantwortliche) beruht auf dessen Fachkenntnis und auf der Wahrnehmung der Führungs- und Überwachungsaufgaben. Diese Kontrollen werden nach freiem persönlichen Ermessen oder gestützt auf Geschäftsreglemente und Pflichtenhefte durchgeführt.

Organisatorische Hilfsmittel

Die wichtigsten organisatorischen Hilfsmittel des IKS können wie folgt umschrieben werden:

- Organigramm
- Ablauf- und Funktionendiagramm
- Stellen- und Prozess-Beschreibung
- Kompetenzregelung und Limiten-System
- Reglemente, Anordnungen und Dienstanweisungen
- Kontenplan, Kontierungsrichtlinien und Kontendefinitionen
- Aktivierungs- und Bewertungsrichtlinien
- Handbücher
- Übrige technische Hilfsmittel (z.B. Tresore, verschlossene Lagerräume, Zutrittskontrollen, Scanning-Kassen etc.)
- Identifikation der Schlüsselkontrollen und deren Umsetzung.

5. Projektablauf
Internes Kontrollsystem

In der Folge werden die einzelnen Schritte beschrieben und es wird punktuell auf spezifische Aspekte der Kontrollen auf Unternehmungsebene, der Kontrollen auf Prozessebene und der generellen IT-Kontrollen eingegangen.

Ist-Analyse

Jedes Untenehmen verfügt über interne Kontrollen. Die Frage ist jedoch, wie weit das IKS entwickelt und wie nachhaltig es ist. Deshalb ist eine Ist-Analyse der vorhandenen Informationen, Dokumentationen und Evaluationsinstrumente durchzuführen. Es kann sich beispielsweise um Managementinformations-Systeme, Risikomanagement, Organisations- oder Managementhandbücher, Qualitätsmanagement, ein Berechtigungskonzept, Prozess- oder Kontrollbeschreibungen handeln.

Bestimmung der Methodik

Basierend auf den Erkenntnissen der Ist-Analyse ist die Methodik für die nächsten fünf Schritte festzulegen: Auswahlverfahren, Risiko-/Kontrollmatrix, Kontrollbeschreibung, Beurteilung der Existenz und Behebung der Schwachstellen. Ein Aspekt ist die Definition, welche Risiken und Kontrollen im Projekt abgedeckt werden sollen – nur jene über die Buchführung und Rechnungslegung oder auch operationelle und Compliance-Risiken und -Kontrollen.

Auswahlverfahren

Das Ziel des Auswahlverfahrens ist die Identifikation der wesentlichen Prozesse mittels risikoorientierten top-down Vorgehens. Risikoorientiert heisst, dass grundsätzlich jene Prozesse berücksichtigt werden, in welchen das Risiko einer wesentlichen Fehlaussage in der Buchführung und Rechnungslegung hoch ist.

Risiko-/Kontrollmatrix

Für die im Auswahlverfahren bestimmten wesentlichen Prozesse werden die Risiken einer wesentlichen Fehlaussage in der Buchführung und Rechnungslegung sowie die bestehenden Kontrollen im Unternehmen identifiziert und in einer Risiko-/Kontrollmatrix einander gegenübergestellt.

Beispielhafte Fragestellungen zur Beurteilung des Entwicklungsgrades eines bestehenden Internen Kontrollsystems:

Ist-Analyse

- Wie wird der Ist-Zustand erhoben und analysiert?
- Wie werden die gewonnenen Erkenntnisse dokumentiert?

Bestimmung der Methodik

- Welche Risiken und Kontrollen werden im Projekt abgedeckt – nur jene über die Buchführung und Rechnungslegung oder auch operationelle und Compliance-Risiken und -Kontrollen?
- Wie wird die Konsistenz der Dokumentation über die Organisation hinweg sichergestellt?
- Wie werden die Rollen und Verantwortungen der einzelnen Funktionen bezogen auf das IKS definiert und kommuniziert?

Auswahlverfahren

- Wird das Auswahlverfahren top-down und risikoorientiert vorgenommen?
- Werden Risiken und Kontrollen auf Unternehmensebene, auf Prozessebene und generelle IT-Kontrollen berücksichtigt?
- Ist ein Pilot-Prozess oder eine Pilot-Einheit definiert, damit erste Erfahrungen gewonnen werden können?

Risiko-/Kontrollmatrix

- Wie werden die Risiken und Kontrollen für einen Prozess definiert und wie werden sie dokumentiert?
- Sind alle in der Risiko-/Kontrollmatrix enthaltenen Kontrollen auch Schlüsselkontrollen?

Kontrollbeschreibung

- Wie und durch wen wird die Qualität der erstellten Beschreibungen sichergestellt?

Beurteilung der Existenz

- Wie plant die Unternehmung, die Beurteilung der Existenz des IKS vorzunehmen?
- Wie und durch wen wird die Qualität der Beurteilung der Existenz sichergestellt?

Behebung der Schwachstellen

- Wie ist die Behebung der Schwachstellen im Dokumentationsansatz berücksichtigt?
- Wie wird die Umsetzung der Korrekturmassnahmen überwacht und wer fasst entsprechend nach?

6. Beispiel einer Risiko- und Kontrollmatrix

In einfacheren Verhältnissen kann eine Risiko- und Kontrollmatrix wie folgt aufgebaut werden:

Horizontal werden Spalten mit den folgenden Kriterien gebildet:

- Kontrollfragen zur Organisation
- Antwort zu den Kontrollfragen (mit Spalten für Ja, Nein und n/a bzw. nicht anwendbar)
- Risikobezeichnung für Falschdarstellung in der Jahresrechnung (betreffend Vollständigkeit, Bestand, Bewertung, Vorhandensein, Genauigkeit, Bewertung, Eigentum bzw. Besitz, Darstellung)
- Kontrollverantwortung (Person bzw. Stellen)
- Ablauf- bzw. Prozessbeschreibung
- Schwachstelle (mit Spalten für Ja, Nein und n/a bzw. nicht anwendbar)
- Beschreibung der Schwachstelle und des Risikos

Vertikal in der Spalte Kontrollfragen zur Organisation werden die unternehmungsspezifischen Kontrollfragen für die drei entsprechenden Ebenen (Kontrollen auf der Unternehmungsebene, Kontrollen auf der Prozessebene und Generelle IT Kontrollen) gestellt. Beispiele für solche Kontrollfragen können sein:

1. Kontrollfragen auf der Unternehmungsebene

- Bestehen nur Kollektiv-Zeichnungsberechtigungen?
- Liegen aktuelle Statuten vor?
- Besteht ein aktuelles Organigramm?
- Liegen Pflichtenhefte und Stellenbeschreibungen vor?
- usw.

2. Generelle IT-Kontrollen

- Besteht ein Verzeichnis der angewendeten EDV Hard- und Software?
- Besteht eine vollständige Dokumentation der angewendeten Programme sowie über Programmänderungen?
- Wird der physischen Sicherheit der IT-Mittel genügend Beachtung geschenkt (Wassereinbruch, Feuer, Diebstahl, Zutrittskontrollen, Alarmvorrichtungen usw.)?
- Ist sichergestellt, dass kein unerlaubter Zugriff auf vertrauliche Daten oder Programme erfolgt?
- usw.

3. Kontrollfragen auf der Prozessebene

- Werden sämtliche Umsätze der einzelnen Profitcenter bzw. Restaurant- und Barbetriebe vollständig und richtig erfasst?
- Ist sichergestellt, dass keine ungerechtfertigen Gutschriften und Déductionen erstellt werden?
- Werden sämtliche Warenbezüge vollständig und richtig belastet?
- Wird der Umsatz der Kassensysteme systemkonform, vollständig und richtig im Backofficesystem erfasst?
- Wird die Mehrwertsteuer auf sämtlichen Umsätzen entsprechend den gesetzlichen Vorschriften abgerechnet?
- usw.

In den einzelnen Spalten werden in der Folge diese Fragen entsprechend beantwortet. In kleinen Verhältnissen kann in der Spalte Ablauf- bzw. Prozessbeschreibung direkt eine Beschreibung erfolgen, wie die Organisation des Prozesses das Risiko, wie dies aus der Fragestellung hervorgeht, abdeckt. Bei mittleren Betrieben empfiehlt sich, eine separate Prozessbeschreibung für die einzelnen Kernprozesse mit einem Flow-Chart zu erstellen. Die Risiko- und Kontrollmatrix kann dann kurz gehalten werden, indem in der Spalte Ablauf- bzw. Prozessbeschreibung auf die entsprechende Stelle der separaten Prozessbeschreibung bzw. des Flow-Charts hingewiesen wird.

Die Autoren, die nachstehend aufgeführt sind, haben durch ihre langjährige Berufserfahrung bei der Prüfung von Klein- bis Grossbetrieben und ihrer Spezialisierung im Gastgewerbe einschlägige Erfahrung bezüglich Ausgestaltung des Internen Kontrollsystems.

Für weitere Informationen stehen zur Verfügung:

Hans Knobel
KPMG AG, Zürich
Telefon +41 44 249 20 82
hknobel@kpmg.com

Martin Eltschinger
EAC Eltschinger Audit & Consulting AG, Thalwil
Telefon +41 44 721 42 42
consulting@eac-eltschinger.ch

Für Informationen betreffend IT- und Applikationskontrollen steht folgender Spezialist zur Verfügung:

Paul Petzold
Mirus Software AG, Davos
Telefon +41 81 415 66 88
petzold@mirus.ch

Ausserdem stehen weitere Ansprechspartner von hotelleriesuisse zur Verfügung:

Bei Fragen zum Kontenplan:
Thomas Allemann, 031 370 43 36
thomas.allemann@hotelleriesuisse.ch

Bei allgemeinen Beratungsauskünften sowie Fragen zu weiteren Spezialisten aus dem Beraternetzwerk oder bezüglich Integration in Qualitätsmanagement-System:
Daniel Beerli, 031 370 43 35
daniel.beerli@hotelleriesuisse.ch

www.hotelleriesuisse.ch -> Beratung -> Beraternetzwerk