

Audit Update

Internes Kontrollsystem und Risk Management
Stand der Diskussion und Umsetzungsempfehlungen

ADVISORY

Februar/März 2007

Inhalt

1. IKS Projekt Navigator	2
2. Berücksichtigung des IKS bei der Revision	5
3. Risikobeurteilung: Gesetzliche Anforderungen	6
4. Risikomanagement: Mehr als eine Risikobeurteilung	7

Die Neuordnung des Schweizerischen Revisionsrechts (OR) wird voraussichtlich per 1. Januar 2008 in Kraft treten. 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.

Der generische Ansatz zur Implementierung und kontinuierlichen Weiterentwicklung eines IKS über die Buchführung und Rechnungslegung ist für alle Unternehmen gleich. Der Umfang und die Ausgestaltung des IKS sind jedoch auf die individuellen Bedürfnisse und Risiken der jeweiligen Unternehmung auszurichten. Wir stellen hierzu ein generisches Modell vor – den IKS Projekt Navigator.

Die Prüfung der Existenz eines IKS wird neu in Art. 728a Abs. 1 Ziff. 3 rev. OR für die ordentliche Revision ausdrücklich als eigenständiger Prüfungsgegenstand erwähnt. Dies stellt eine Ausweitung des gesetzlichen Prüfungsauftrags dar. Wir gehen auf die Veränderungen bezüglich IKS in der Revision gegenüber der bisherigen Handhabung ein.

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. Von dieser Gesetzesänderung sind alle Aktiengesellschaften betroffen, sowie andere Rechtsformen, für welche die aktienrechtlichen Rechnungslegungsvorschriften gelten. Was genau im Anhang offengelegt werden muss, ist vom Gesetzgeber nicht klar geregelt.

Ein ganzheitliches Risikomanagement geht über die Risikobeurteilung hinaus. Es schliesst ein systematisches Überwachen und Steuern der Risiken ein und bietet über die gesetzlichen Anforderungen hinaus Chancen und Vorteile für das Unternehmen. Wir stellen die wesentlichen Elemente eines Risikomanagements vor, welche je nach Grösse und Komplexität unterschiedlich auszugestaltet sind.

1. IKS Projekt Navigator

Das Vorgehen in einem IKS-Projekt über die Buchführung und Rechnungslegung besteht in der Regel aus acht Schritten, die in eine kontinuierliche Projektleitung, -überwachung und -steuerung eingebettet sind. In diesem Vorgehen sind die Kontrollen auf drei unterschiedlichen Ebenen und deren Zusammenspiel zu berücksichtigen (vgl. nebenstehende Abbildung):

- **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 Initiierung, Registrierung, Verarbeitung, Verbuchung bis zum Ausweis von Geschäftsvorfällen innerhalb einzelner Prozesse ab. Es handelt sich entweder um so genannte manuelle Kontrollen oder automatische Applikationskontrollen. Manuelle Kontrollen sind beispielsweise die Überprüfung der Korrektheit von Bewertungen oder Bank- und Postcheckkonto-Bestätigungen. Automatische Applikationskontrollen werden durch IT-Applikationen, beziehungsweise End-User Computing-Applikationen (zum Beispiel Tabellenkalkulationen), durchgeführt. Es handelt sich beispielsweise um die Plausibilisierung von Dateneingaben oder automatische Abstimmungen von Hauptbuch und Nebenbüchern.
- **Generelle IT-Kontrollen** gewährleisten, dass die automatischen Applikationskontrollen ordnungsmässig funktionieren. Gibt es beispielsweise im Einkaufsprozess eine automatische Abstimmung zwischen Bestellung, Wareneingang und Rechnung (automatische Applikationskontrolle), funktioniert diese Abstimmung nur verlässlich, wenn die entsprechende IT-Applikation den systematischen Änderungsverfahren der IT-Abteilung unterliegt (generelle IT-Kontrolle).

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



1. Ist-Analyse

Jedes Unternehmen 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, ein Risikomanagement, Organisations- oder Managementhandbücher, Qualitätsmanagement, ein Berechtigungskonzept, Prozess- oder Kontrollbeschreibungen handeln.

2. 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. Die Erfahrung hat gezeigt, dass der Umfang bei der Einführung nicht zu weit gesteckt werden soll, da das IKS-Projekt komplexer und zeitintensiver wird und man sich im Detail verlieren kann. Es empfiehlt sich daraus eine phasenweise Erfassung der einzelnen Zielbereiche.

Ein weiterer Aspekt ist die Konsistenz und Qualität der Dokumentation. In der Regel ist es sinnvoll, wenn jede Einheit eines Konzerns oder jede Abteilung einer Unternehmung dieselben Vorlagen, die gleiche Terminologie, beziehungsweise ein einheitliches Dokumentationssystem benutzt. Es ist auch zweckmässig, die Rollen und Verantwortlichkeiten der einzelnen Funktionen bezogen auf das IKS zu definieren

Risiko-/Kontrollmatrix (illustratives und unverbindliches Beispiel)

Jahresrechnung								Prozess	Risiko	Kontroll-Nummer	Schlüsselkontrolle		Kontrolle	Kontrollhäufigkeit	Kontrollverantwortlicher
Position	Konto	Aussagen									Ja	Nein			
		Vollständigkeit	Vorhandensein	Genauigkeit	Bewertung	Rechte und Verpflichtungen	Darstellung und Offenlegung								
Forderungen aus Lieferungen und Leistungen	1100				X			Verkauf	Die Mutation (Eingabe bzw. Veränderung) der Kreditlimite im System erfolgt ohne Autorisierung des CFOs.	KO_3	X		Eine Mutation der Kreditlimite wird im System nur vorgenommen, wenn der Mutationsantrag durch den CFO autorisiert ist.	Ereignis	Debitorenbuchhalter
Verkauf Handelsware	3000														
...

und zu kommunizieren. Es handelt sich beispielsweise um Funktionen wie Konzernleitung/Geschäftsleitung, Enterprise Risk Management, Controlling oder Interne Revision.

3. Auswahlverfahren (auch Scoping genannt)

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. Die Erfahrung zeigt, dass Non-Routine Prozesse und Schätzungen tendenziell höhere Risiken enthalten. Top-down heisst, dass in Bezug auf die wesentlichen Prozesse zuerst identifiziert wird, welche übergreifenden Kontrollen bestehen, um das Risiko einer Fehlaussage zu vermindern. Falls keine übergreifenden Kontrollen vorhanden sind oder sie nicht alle Risiken abdecken, werden die ergänzenden Kontrollen auf Prozessebene identifiziert. Wenn es sich bei den Kontrollen auf Prozessebene um automatische Applikationskontrollen handelt, sind ausserdem die generellen IT-Kontrollen für die betreffenden IT-Applikationen zu erfassen.

Im Auswahlverfahren ist weiter zwischen der Ebene Konzernrechnung und der Ebene statutarische Jahresrechnung für jene Tochtergesellschaften in der Schweiz zu unterscheiden, die einer ordentlichen Revision unterliegen. Auf der Ebene Konzernrechnung bildet der Konzernabschluss die Ausgangslage. Deshalb können sowohl wesentliche Prozesse in schweizerischen als auch in ausländischen Tochtergesellschaften in den Projektumfang fallen. Auf der Ebene statutarische Jahresrechnung bildet der Einzelabschluss die Ausgangslage. Da die Wesentlichkeitsgrenze auf der Ebene Konzernrechnung in der Regel höher ist als auf der Ebene statutarische Jahresrechnung, können auf der Ebene statutarische Jahresrechnung zusätzliche Prozesse in den Projektumfang fallen, die auf der Ebene Konzernrechnung nicht wesentlich sind. Deshalb ist es wichtig, das Auswahlverfahren sowohl auf der Ebene Konzernrechnung

als auch auf der Ebene statutarische Jahresrechnung durchzuführen. In diesem Schritt werden auch die Pilot-Einheiten und/oder Pilot-Prozesse identifiziert, um die in Schritt 2 festgelegte Methodik für die Schritte 4 bis 7 zu testen und allenfalls anzupassen, damit ein optimaler Ansatz ausgerollt werden kann.

4. 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 (vgl. obige Abbildung). Diese systematische und umfassende Gegenüberstellung zeigt beispielsweise auf, wenn für ein Risiko keine Kontrolle besteht (=Kontrolllücke). Es kann aber auch festgestellt werden, dass für ein Risiko mehrere Kontrollen bestehen und allenfalls eine Kontrolle andere Kontrollen ersetzen, beziehungsweise ein bestimmtes Risiko allein abdecken kann (=Kontrolloptimierung).

Die Risiko-/Kontrollmatrix enthält in der Regel auch Kontrollen ohne wesentlichen Einfluss auf die Buchführung und Rechnungslegung. Deshalb sind diejenigen Kontrollen mit wesentlichem Einfluss, die so genannten Schlüsselkontrollen, entsprechend zu identifizieren, da in den nächsten Schritten des Vorgehens nur noch diese Kontrollen berücksichtigt werden.

5. Kontrollbeschreibung

Für die in den Risiko-/Kontrollmatrizen identifizierten Schlüsselkontrollen wird eine detaillierte Kontrollbeschreibung erstellt, welche für einen sachverständigen Dritten nachvollziehbar sein muss. Deshalb ist es wichtig, dass die Kontrollbeschreibung die W-Fragen (wer, was, wie, wie oft, wann, wo, warum) beantwortet. Für automatische Applikationskontrollen sind konkrete Funktionsbeschreibungen erforderlich.

6. Beurteilung der Existenz

Mit der Dokumentation ist noch nicht sichergestellt, dass die Kontrollen richtig ausgestaltet sind und die Schlüsselkontrollen wirklich gelebt werden. Deshalb ist die Beurteilung der Existenz vorzunehmen. Dies kann auf verschiedene Arten erfolgen, zum Beispiel durch Selbstevaluationen (so genannte Control Self Assessments), durch das Management, durch Prüfungen der internen Revision oder durch Dritte. Dabei können allfällige Schwachstellen identifiziert werden.

7. Behebung der Schwachstellen

Für die identifizierten Schwachstellen ist der Handlungsbedarf festzulegen. Die Korrekturmassnahmen sind entsprechend zu implementieren und deren Umsetzung ist zu überwachen.

Der Massnahmenplan inklusive Überwachung kann beispielsweise in einer ähnlichen Struktur wie ein Management Letter der Revisionsstelle aufgebaut werden.

8. Externe Revisionsstelle

Das Management der Unternehmung stellt die relevanten Unterlagen bereit, welche die Revisionsstelle als Ausgangslage zur Beurteilung der Existenz des IKS heranzieht.

Wir empfehlen eine frühzeitige Abstimmung mit der Revisionsstelle in den einzelnen Schritten des Vorgehens, um Erwartungslücken zu vermeiden.

Ausblick

Die Erfahrung hat gezeigt, dass es sich lohnt, mit der Umsetzung des IKS-Projekts rechtzeitig zu beginnen, damit nicht nur die gesetzlichen Rahmenbedingungen erfüllt werden können, sondern vor allem auch ein wirkungsvolles Führungs- und Steuerungsinstrument entwickelt und implementiert werden kann.

Wir würden uns freuen, Sie bei der Einführung und Weiterentwicklung eines effektiven und effizienten internen Kontrollsystems unterstützen zu dürfen. Mögliche Einstiegsdienstleistungen von KPMG sind:

- Durchführung von Workshops zur Sensibilisierung der Thematik «internes Kontrollsystem»
- Erstellung eines Konzeptpapiers (Projekt-Planung; Auswahlverfahren von Einheiten, Konten und/oder Prozessen; Aufwandschätzung; etc.)
- Beurteilung des Entwicklungsgrades des bestehenden internen Kontrollsystems
- Erhebung und Dokumentation eines Pilot-Prozesses oder einer Pilot-Einheit

Beispielhafte Fragestellungen zur Beurteilung des Entwicklungsgrades des 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 (Einzelgesellschaft/Konzern) hinweg sichergestellt (wie Vorlagen, Terminologie, Sprache oder Dokumentationssystem)?
- Wie werden die Rollen und Verantwortungen der einzelnen Funktionen (wie Konzern/Geschäftsleitung, Enterprise Risk Management, Controlling oder Interne Revision) 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?
- Deckt das Projekt die Ebene Konzernrechnung wie auch die Ebene statutarische Jahresrechnung für jene Tochtergesellschaften in der Schweiz ab, die einer ordentlichen Revision unterliegen?
- 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?

2. Berücksichtigung des IKS bei der Revision

Neue Bestimmungen zum IKS

Im revidierten Revisionsrecht wird das interne Kontrollsystem (IKS) nun erstmals explizit in verschiedenen Bestimmungen erwähnt. Art. 728a rev. OR verlangt für die ordentliche Revision, dass die Revisionsstelle prüft, ob ein IKS existiert (Abs. 1 Ziffer 3). Die Revisionsstelle ist verpflichtet, bei der Durchführung und bei der Festlegung des Umfangs der Prüfung das IKS zu berücksichtigen (Abs. 2). Art. 728b Abs. 1 rev. OR bestimmt, dass die Revisionsstelle im umfassenden Bericht an den Verwaltungsrat Feststellungen über das IKS vorzunehmen habe.

Die neuen Bestimmungen betreffen nur Unternehmen, die einer *ordentlichen Revision* unterliegen. Aufgrund der rechtsformunabhängigen Regelung der Revision betrifft dies die AG, die GmbH, die Genossenschaft, den Verein und die Stiftung.

Das Vorhandensein des IKS wird im OR nicht als ausdrückliche Pflicht der geprüften Gesellschaft formuliert, sondern nur bei den Aufgaben der Revisionsstelle geregelt. Es kann jedoch gefolgert werden, dass der Gesetzgeber erwartet, dass bei Unternehmen, die einer ordentlichen Revision unterliegen, ein IKS vorhanden ist.

Berücksichtigung des IKS bei der Revision

Schon bisher sahen die massgeblichen Regelwerke der Revisionsbranche vor, dass sich die Revisionsstellen bei ihren Arbeiten auf bestehende Kontrollen innerhalb des Unternehmens abstützen habe. Die Revision sollte den Ausbaugrad und die Qualität des IKS bei der Planung der Jahresabschlussprüfung berücksichtigen.

Der Grundsatz, wonach die Revisionsstelle bei der Festlegung des Umfangs der Revision das IKS berücksichtigen muss, wird nun in Art. 728a Abs. 2 rev. OR gesetzlich verankert. Stellt die Revisionsstelle strukturelle Mängel beim IKS fest, kompensiert sie dies durch eigene Prüfungshandlungen.

Nach Auffassung der Revisionsbranche ist die Prüfung der Existenz eines IKS wegen der ausdrücklichen Erwähnung in Art. 728a Abs. 1 Ziffer 3 rev. OR für die ordentliche Revision ein eigenständiger Prüfungsgegenstand und stellt eine Ausweitung des gesetzlichen Prüfungsauftrags dar. Die Revisionsstelle muss deshalb angemessene Prüfungshandlungen vornehmen, die es ihr erlauben, die Existenz eines IKS bezüglich Verlässlichkeit der finanziellen Berichterstattung zu bestätigen.

Gemäss Art. 728b Abs. 1 rev. OR erstattet die Revisionsstelle dem Verwaltungsrat einen *umfassenden Bericht*. Es ist unbestritten, dass in diesem Bericht Feststellungen über das IKS enthalten sein müssen. Hier kann die Revisionsstelle Ausführungen darüber machen, wo sie auf Grund ihrer verfahrensorientierten Prüfungshandlungen Schwächen im IKS aufgedeckt hat, die sie kompensieren musste.

Fraglich ist demgegenüber, ob sich die Revisionsstelle im *zusammenfassenden Bericht an die Generalversammlung* in jedem Fall zum IKS äussern muss. Manche Stimmen vertreten die Auffassung, dass die Feststellung, es existiere kein (genügendes) IKS oder dieses sei nicht funktionsfähig, nicht in den zusammenfassenden Revisionsbericht zuhanden der Generalversammlung gehöre, wenn die Jahresrechnung regelkonform ist. In der Revisionsbranche neigt man demgegenüber eher zur Auffassung, im zusammenfassenden Revisionsbericht oder einem allfälligen besonderen Bericht an die Generalversammlung müsse in jedem Fall ein Hinweis angebracht werden, wenn kein IKS besteht.

Literaturhinweis: Weitere Details zum neuen Revisionsrecht finden sich in der Publikation «Neuerungen im Gesellschafts- und Revisionsrecht» (Schulthess Verlag, ISBN 978-3-7255-5329-7).

Auszug aus dem Schweizerischen Obligationenrecht (OR)

Art. 728a

- 1 Die Revisionsstelle prüft, ob:
 1. die Jahresrechnung und gegebenenfalls die Konzernrechnung den gesetzlichen Vorschriften, den Statuten und dem gewählten Regelwerk entsprechen;
 2. der Antrag des Verwaltungsrats an die Generalversammlung über die Verwendung des Bilanzgewinnes den gesetzlichen Vorschriften und den Statuten entspricht;
 3. ein internes Kontrollsystem existiert.
- 2 Die Revisionsstelle berücksichtigt bei der Durchführung und bei der Festlegung des Umfangs der Prüfung das interne Kontrollsystem.
- 3 Die Geschäftsführung des Verwaltungsrats ist nicht Gegenstand der Prüfung durch die Revisionsstelle.

3. Risikobeurteilung

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. Die Interpretation des Artikels 663b ist schwierig und es ist zur Zeit noch nicht abschliessend ersichtlich, was von den betroffenen Unternehmungen effektiv im Anhang unter Angaben zur Durchführung einer Risikobeurteilung aufgeführt werden muss. KPMG hat sich intensiv mit den Diskussionen im Parlament, der Botschaft des Bundesrates sowie verschiedenen Stellungnahmen von renommierten Juristen auseinandergesetzt. In der Publikation «Neuerungen im Gesellschafts- und Revisionsrecht», welche KPMG im Februar 2007 in Zusammenarbeit mit dem Schulthess Verlag herausgibt, beschreiben wir den heute erkennbaren Stand der Diskussion. Nachstehend zeigen wir Auszüge aus der erwähnten Publikation.

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 («Risiko-Landkarte»), einen laufenden Überwachungs- und Rapportierungsprozess sowie die Kontrolle und Steuerung der Risiken mittels operativer Massnahmen.

Risikobeurteilung nach bisherigem Recht

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. Ziff. 19 Swiss Code verlangt vom Verwaltungsrat von Publikumsgesellschaften, für ein dem Unternehmen angepasstes Risikomanagement besorgt zu sein. Gesellschaften, deren Aktien an der SWX kotiert sind, müssen im Corporate Governance-Bericht Angaben zur Ausgestaltung der Informations- und Kontrollinstrumente des Verwaltungsrats machen (Ziff. 3.7 Anhang RLCG). Als Beispiel solcher Angaben werden in Ziff. 3.7 Anhang RLCG Angaben zum Risikomanagement-System genannt.

Angaben über die Durchführung einer Risikobeurteilung im Anhang: Anwendungsbereich

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. Von dieser Gesetzesänderung sind alle Aktiengesellschaften betroffen, unabhängig davon, ob diese einer ordentlichen oder einer eingeschränkten Revision unterliegen. Art. 663b Ziff. 12 rev. OR ist auch auf alle Unternehmen anwendbar, die einen Anhang nach den Vorschriften des Aktienrechts erstellen müssen.

Ausgestaltung der Risikobeurteilung

Das Gesetz äussert sich nicht zur Ausgestaltung der Risikobeurteilung. Aus den Unterlagen ergibt sich lediglich, dass der Gesetzgeber vom Verwaltungsrat eine inhaltliche Auseinandersetzung mit den Unternehmensrisiken erwartet. Hinsichtlich der Ausgestaltung der Risikobeurteilung ist der Verwaltungsrat somit frei. Er muss insbesondere die Grösse, die Komplexität und das Risikoprofil des Unternehmens berücksichtigen.

Risiken mit wesentlichem Einfluss auf die Beurteilung der Jahresrechnung

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. In den Materialien wird als Beispiel der Mangel eines Produkts genannt, welcher zu einem Bewertungsrisiko bei Lagervorräten und zu Erlösminderungen führt.

Berichterstattung im Anhang

Das Gesetz regelt nicht detailliert, welche Informationen zur Risikobeurteilung im Anhang der Jahresrechnung gemacht werden müssen. Von Bundesrat Blocher wurde in den parlamentarischen Beratungen im Sinne einer Negativabgrenzung klargestellt, dass lediglich die Angabe eines Sitzungsdatums und die Aussage, man habe über die Risiken gesprochen, nicht ausreiche. Weitergehende Schlüsse lassen sich aus den Materialien nicht ziehen. Die Unternehmen dürften deshalb einen gewissen Ermessensspielraum haben.

4. Risikomanagement: Mehr als eine Risikobeurteilung

Das Risikomanagement geht über die Risikobeurteilung hinaus, da dieses zusätzlich ein systematisches Überwachen und Steuern der Risiken beinhaltet. Im Rahmen der nächsten Strategieentwicklung wäre es sinnvoll, die Risikobeurteilung einfließen zu lassen. Denn erstens gehören Risiken genau gleich wie Chancen in den Prozess der Strategieerarbeitung, und zweitens wird damit der gesetzlichen Neuerung frühzeitig Rechnung getragen. Einen zusätzlichen Nutzen bietet das Risikomanagement, indem es als Basis für den Aufbau eines internen Kontrollsystems dient, für die Banken eine zusätzliche Information innerhalb dem Rating nach Basel II ergibt und nicht zuletzt ein Bestandteil von Corporate Governance darstellt, was im Swiss Code of Best Practice for Corporate Governance deutlich unterstrichen wird.

Ein Risikomanagement besteht aus folgenden Elementen, welche je nach Grösse und Komplexität unterschiedlich ausgereift sind:

1. Die **Risikopolitik und ein Risikohandbuch bilden** den Rahmen für ein umfassendes Risikomanagement. Diese bilden die Basis für eine gemeinsame Sprache, und wir empfehlen, diese in die gesamte Unternehmensüberwachung («Corporate Governance») zu integrieren.
2. Die **Risikoidentifikation** kann mittels Interviews, Fragebogen oder Workshops durchgeführt werden. Wir empfehlen, diese Top-Down (also mit den Führungsorganen) sowie gleichzeitig Bottom-Up (mit ausgewählten mittleren Kadern oder Mitarbeitenden) zu erarbeiten. Der Weg ist das Ziel, und oftmals sind die Diskussionen genau so interessant wie die Resultate an sich, vor allem, wenn diese zusätzlich über die Divisions- und Funktionsgrenzen hinweg geführt werden.
3. Die **Quantifizierung der Risiken** kann in einem ersten Schritt pragmatisch sein, und vielleicht sollte es sogar eher eine qualitative Bewertung sein. Die Quantifizierung kann perfektioniert werden, indem Sensitivitätsanalysen und Ursachen-Wirkungs-Analysen durchgeführt werden. Damit werden diejenigen Parameter und Treiber definiert, die in der Folge für die Risikoüberwachung und Steuerung durch Massnahmen entscheidend sind.
4. Risikoüberwachung und -Reporting bedingt die Definition von Risiko-Verantwortlichen, die Zuteilung der Risiken und deren Treiber inklusive geeigneter Messgrössen als Indikatoren. Wir empfehlen, das «Controlling» möglichst eng an die bereits existierenden Controlling-Abläufe anzulehnen und das Risikoreporting in das bestehende MIS (Management Informationssystem) zu integrieren.
5. Die Risikokontrolle und -steuerung, beziehungsweise die laufende Steuerung der Risiken, ist eine wiederkehrende Aufgabe der Führungskräfte, genau so wie die laufende Optimierung der übrigen Geschäftsprozesse. Durch ein Involvieren der Verantwortlichen und die Festlegung der zu überwachenden Indikatoren trägt das Risikomanagement massgeblich zu einer Performance-Verbesserung und zur Erreichung der gesetzten Ziele bei.

«Swiss Code of Best Practice for Corporate Governance» als Leitlinie und Empfehlung

Der «Swiss Code» wendet sich an die schweizerischen Publikumsgesellschaften. Einzelne Punkte betreffen institutionelle Anleger und Intermediäre. Er soll Leitlinien setzen und Empfehlungen abgeben, nicht den Schweizer Unternehmen eine Zwangsjacke anziehen. Jede Gesellschaft soll die Möglichkeit behalten, eigene Gestaltungsideen zu verwirklichen.

Internes Kontrollsystem, Umgang mit Risiken und Compliance (Kapitel II, Teil f)

19 Der Verwaltungsrat sorgt für ein dem Unternehmen angepasstes internes Kontrollsystem und Risikomanagement.

- Das interne Kontrollsystem ist der Grösse, der Komplexität und dem Risikoprofil der Gesellschaft anzupassen.
- Das interne Kontrollsystem deckt, je nach den Besonderheiten der Gesellschaft, auch das Risikomanagement ab; dieses bezieht sich sowohl auf finanzielle wie auf operationelle Risiken.
- Die Gesellschaft richtet eine interne Revision ein. Diese erstattet dem Prüfungsausschuss («Audit Committee») oder gegebenenfalls dem Präsidenten des Verwaltungsrats Bericht.

24 Der Prüfungsausschuss bildet sich ein eigenständiges Urteil über die externe Revision, das interne Kontrollsystem und den Jahresabschluss.

- Der Prüfungsausschuss macht sich ein Bild von der Wirksamkeit der externen Revision (Revisionsstelle und gegebenenfalls Konzernrechnungsprüfer) und der internen Revision sowie über deren Zusammenwirken.
- Der Prüfungsausschuss beurteilt im Weiteren die Funktionsfähigkeit des internen Kontrollsystems mit Einbezug des Risikomanagements und macht sich ein Bild vom Stand der Einhaltung der Normen (Compliance) in der Gesellschaft.

Contact us

Hauptsitz

Günter Haag

Partner, Leiter Audit
KPMG Schweiz
Tel. +41 44 249 2046
Fax +41 44 249 2029
ghaag@kpmg.com

IKS / Risikobeurteilung

Hans-Ulrich Pfyffer

Partner, Leiter Internal Audit
Services
KPMG Schweiz
Tel. +41 44 249 2777
Fax +41 44 249 4963
hpfyffer@kpmg.com

Simon Marti

Leiter Kompetenzcenter
Interne Kontrolle Schweiz
KPMG Schweiz
Tel. +41 44 249 4519
Fax +41 44 249 4963
smarti@kpmg.com

Stefan Buser

Leiter Kompetenzcenter
Enterprise Risk
Management
KPMG Schweiz
Tel. +41 44 249 2191
Fax +41 44 249 4963
sbuser@kpmg.com

Deutschschweiz

Reto Stalder

Leiter Audit
KPMG Aarau
Tel. +41 62 834 4860
Fax +41 62 834 4880
rstalder@kpmg.com

Stefan Inderbinen

Leiter Audit
KPMG Basel
Tel. +41 61 286 9318
Fax +41 61 286 9401
stefaninderbinen@kpmg.com

Christoph Andenmatten

Partner, Leiter Audit
KPMG Bern
Tel. +41 31 384 7723
Fax +41 31 384 7647
candenmatten@kpmg.com

Markus Forrer

Partner, Leiter Audit
KPMG Luzern
Tel. +41 41 368 3759
Fax +41 41 368 3888
mforrer@kpmg.com

Kurt Stocker

Partner, Leiter Audit
KPMG St. Gallen
Tel. +41 71 272 0056
Fax +41 71 272 0051
kstocker1@kpmg.com

Martin Schaad

Partner, Leiter Audit
KPMG Zürich
Tel. +41 44 249 2026
Fax +41 44 249 3311
martinschaad@kpmg.com

Ingrid Marbacher

Partner, Leiterin Audit
KPMG Zug
Tel. +41 41 727 7439
Fax +41 41 727 7400
imarbacher@kpmg.com

Liechtenstein

Hans Vils

Partner, Leiter Audit
KPMG Liechtenstein
Tel. +423 237 7055
Fax +423 237 7050
hvils@kpmg.com

Suisse Romande

Adrian Duerig

Leiter Audit
KPMG Fribourg
Tel. +41 26 347 4931
Fax +41 26 347 4901
aduerig@kpmg.com

William Laneville

Partner, Leiter Audit
KPMG Genf
Tel. +41 22 704 1624
Fax +41 22 347 7313
williamlaneville@kpmg.com

Stéphane Gard

Partner, Leiter Audit
KPMG Lausanne
Tel. +41 21 345 0335
Fax +41 21 345 3888
sgard@kpmg.com

Stefano Ponta

Leiter Audit
KPMG Neuenburg
Tel. +41 32 727 6137
Fax +41 32 727 6158
sponta@kpmg.com

Joel Etique

Partner, Leiter Audit
KPMG Délemont
Tel. +41 32 423 4515
Fax +41 32 423 4511
jetique@kpmg.com

Ticino

Lorenzo Job

Partner, Leiter Audit
KPMG Lugano
Tel. +41 91 912 1220
Fax +41 91 912 1213