

Gesetzesrevision des Revisionsrechtes: Interne Kontrollsysteme gewinnen an Bedeutung

Durch die Revision des Obligationenrechts wird die unternehmensinterne Kontrolle in der Schweiz eine wichtige Rolle erhalten. Unternehmen stehen vor der Herausforderung, die neuen Gesetzesanforderungen auf effiziente und effektive Art und Weise umzusetzen. Wie sollen Unternehmen dabei konkret vorgehen?

Lic. iur. Karin Koç

Mit dem In-Kraft-Treten der revidierten Art. 728a OR und Art. 728b OR wird die Errichtung eines unternehmensinternen Kontrollsystems eine grosse Bedeutung für schweizerische Unternehmen erlangen. Die Notwendigkeit des Vorhandenseins eines internen Kontrollsystems wird im revidierten OR erstmals ausdrücklich erwähnt. Es ist wichtiger Bestandteil der Unternehmenssteuerung, -prüfung und -überwachung. Unter interner Kontrolle werden dabei alle Vorgänge, Methoden und Massnahmen verstanden, die dazu dienen, einen ordnungsgemässen Ablauf der betrieblichen Tätigkeiten sicherzustellen.

Das interne Kontrollsystem soll

- Gewährleistung bieten, dass geschäftliche Ziele durch eine effiziente und wirksame Unternehmensführung erreicht werden;
- den Nachweis liefern, dass die Compliance (Gesetze, Reglemente, Verordnungen und Weisungen) umgesetzt wird;
- Unregelmässigkeiten verhindern, vermindern oder aufdecken;
- eine vollständige und zuverlässige Buchführung sicherstellen.

Das Gesetz beschreibt nicht, wie ein internes Kontrollsystem ausgestaltet werden soll, es schreibt nur dessen Bestehen vor. Bei einer ordentlichen Revision (laut Artikel 728a OR vorgeschrieben, wenn zwei von folgenden drei Messgrössen erreicht werden: Bilanzsumme > CHF 10 Mio., Vollzeitstellen > 50, Umsatz > CHF 20 Mio.) muss der Revisor die Existenz eines internen Kontrollsystems prüfen.

Risikobeurteilung: Wichtige Komponente des internen Kontrollsystems

Voraussetzung für die erfolgreiche Erstellung eines internen Kontrollsystems ist ein den spezifischen Umständen des Unternehmens angepasstes Risikomanagement. Die frühzeitige Erkennung von Risiken und Chancen ist ein wichtiger Erfolgsfaktor für Unternehmen. Das Risikomanagement betrachtet des-

halb nach neueren Ansätzen nicht nur Risiken, sondern auch Chancen. Betrachtet man die

Definition des Begriffs Risiko «als potenzielle Gefahr, die auf Eintretenswahrscheinlichkeit und Schadensausmass beurteilt ist», so wird erkennbar, dass der Unterschied zwischen Risiko und Chance im Schadensausmass liegt. Während Risiken einen negativen Einfluss auf den Geschäftsverlauf haben, sind Chancen positiver Natur, es ändert sich nur das Vorzeichen des bewerteten «Schadens».



Gesetzliche Grundlagen für die Ausgestaltung des Risikomanagements gibt es bis anhin nicht: Im Artikel 663b revOR, Ziffer 12 wird lediglich vorgesehen, dass eine Risikobeurteilung durchgeführt wird. Es ist umstritten, ob die Revision eine inhaltliche Überprüfung der vom Gesetz verlangten Risikobeurteilung vornehmen muss. Fest steht hingegen, dass der Verwaltungsrat die Verantwortung für die Vornahme der Risikobeurteilung trägt.

Die Risikobeurteilung muss sämtliche Geschäftsbereiche einbeziehen: Management, Markt, Leistungserbringung, Personal und v. a. Finanzen. In sämtlichen Bereichen nimmt die Informatik als Enabler von Prozessen eine ausserordentlich wichtige Rolle ein. Ohne Informatik ist weder die Buchführung, noch die Produktion, Planung und Kontrolle durchführbar. Damit wird auch klar, dass alle Informatiksysteme, die in irgendeiner Art und Weise die finanzielle Berichterstattung beeinflussen können, in die Risikobeurteilung einbezogen werden müssen.

Welche Bereiche des internen Kontrollsystems, die die Informationssicherheit betreffen, können in der Praxis von Revisoren geprüft werden?

Aus Erfahrungen mit Unternehmungen, die in den USA an der Börse kotiert sind und deshalb der Sarbanes Oxley Act (SOX) unterliegen, sind die Anforderungen des internen Kontrollsystems (Section 404 von SOX) an die IT gut bekannt. Eine Umfrage bei unterschiedlichen SOX-pflichtigen Unternehmen ergab, dass vor allem folgende Bereiche durch die Revisoren überprüft werden:

- **Change Management:** Werden Anpassungen an IT-Systemen durch das Business (d. h. durch die unternehmenssteuernden Linien) vorgegeben, geplant und überprüft?
- **Storage und Wiederherstellung:** Werden finanzrelevante Daten regelmässig gesichert? Kann das System nach einem «Absturz» wieder hergestellt werden?
- **Problemmangement:** Werden Störungen an Systemen systematisch erfasst und ausgewertet, wird sichergestellt, dass potenzielle Probleme behoben werden?
- **Sicherheit:** Sind die Informationssysteme physisch und logisch geschützt?
- **Berechtigungswesen:** Wird überprüft, wer, weshalb und warum welche Rechte für welche Informationssysteme erhält?

Grundsätzlich sollen die Sicherheitsanforderungen des Unternehmens (und damit diejenigen des internen Kontrollsystems) Vorgaben bezüglich Vertraulichkeit, Datenintegrität und Verfügbarkeit der Informationen erstellen.

Anhand von Sicherheitsaspekten für ein ERP-System (Enterprise Resource Planning) lassen sich die minimalen Anforderungen an ein internes Kontrollsystem gut darstellen. Das interne Kontrollsystem soll im Bereich der Sicherheit unter anderem folgende Fragestellungen schlüssig beantworten können:

- Gibt es organisatorische Sicherheitsvorgaben (beispielsweise für die Regelung von Notfallpasswörtern)?
- Existiert ein Konfigurationsmanagement?
- Sind Test- und Produktionsumgebung definiert?
- Entspricht die Qualität der Handbücher den Anforderungen?
- Gibt es eine Schwachstellenbewertung (Risikoanalyse) mit entsprechenden Massnahmen (beispielsweise für die Authentifizierung, Passwortsicherheit)?
- Ist die Datenübertragung (zum Beispiel zwischen Niederlassungen) den Vorgaben entsprechend gesichert?
- Ist geregelt wie, von wem, wann Sicherheitspatches der Applikation, der Datenbank und des Betriebssystems eingespielt werden?

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de) stellt in einer sehr guten Übersicht Quellen für weitere Informationen dar. In einem schnellen und kompakten Web-Kurs wird zudem die Vorgehensweise nach IT-Grundschutz erklärt und die Anwendung an einem Beispiel demonstriert (www.bsi.de/gshb/webkurs/index.htm). Das BSI stellt zusätzlich eine Software für die Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten zur Verfügung.

Fazit

Die neuen Revisionsvorschriften des Obligationenrechts schreiben die Erstellung eines internen Kontrollsystems für Unternehmen vor, die eine ordentliche Revision vornehmen lassen müssen. Um ein internes Kontrollsystem erfolgreich umzusetzen, muss dabei eine Risikobeurtei-

lung vorgenommen werden, die neu auch durch das Gesetz vorgesehen wird. Wie die Anforderungen in der Praxis im Einzelnen umgesetzt werden, wird die Zukunft weisen. ■

