# IKS – Internes Kontrollsystem

**Über ein Jahr ist es her, seit per 1. Januar 2008 die Gesetzgebung geändert wurde. IKS erhielt eine gewichtigere Bedeutung. Was bedeutet das für kleinere und mittlere Unternehmungen? Gibt es einen Einfluss auf die IT aus dem IKS oder beeinflusst die IT gar das IKS? Dieser Beitrag zeigt, was ein IKS ist und warum es hilft, die IT-Sicherheit zu erhöhen.**

Obwohl die revidierten Artikel 728a und b des Obligationenrechts bereits vor über einem Jahr in Kraft getreten sind, verfügen nur wenige Unternehmen über ein IKS. Dies ist sehr schade, bringt ein IKS doch nicht nur Aufwand, sondern hilft, die eigene Organisation im «Griff» zu behalten. Gerade in der turbulenten, unvorhersehbarer Zeit, in der wir uns momentan befinden, ist es wichtig, jederzeit über den eigenen Zustand zu wissen. Was verlangt das Obligationenrecht? (Quelle: www.admin.ch)

**Artikel 728a (OR)**
- Die Revisionsstelle prüft, ob ein internes Kontrollsystem existiert.
- Die Revisionsstelle berücksichtigt bei der Durchführung und bei der Festlegung des Umfanges der Prüfung das interne Kontrollsystem.

**Artikel 728b**
- Die Revisionsstelle erstattet dem Verwaltungsrat einen umfassenden Bericht mit Feststellungen über die Rechnungslegung, das interne Kontrollsystem sowie die Durchführung und das Ergebnis der Revision.

**ZUM AUTOR**

Dipl.-Ing. FH Sandro Müller
Geschäftsführer/Sicherheitsspezialist GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 320 91 20
www.goout.ch
info@goout.ch

Anzeige

## Wer ist davon betroffen?

Betroffen von den im vorhergehenden Abschnitt zitierten Gesetzestexten und damit von der Pflicht ein IKS zu betreiben, sind zwei Arten von Unternehmungen. Einerseits sind dies Publikumsgesellschaften, welche der ordentlichen Revision unterstehen. Dazu gehören Aktiengesellschaften, aber auch die in der Schweiz häufig angewandte Gesellschaftsform der GmbH. Weiter gilt die Regelung auch für sogenannte «wirtschaftlich bedeutende Unternehmen». Der Begriff ist klar definiert.

Damit eine Firma zu einem «wirtschaftlich bedeutenden Unternehmen» zählt, müssen zwei der drei folgenden Kriterien in zwei aufeinanderfolgenden Jahren erfüllt werden:
- Bilanz ≥ CHF 10 Millionen
- Umsatz ≥ CHF 20 Millionen
- Mitarbeiter ≥ 50 Vollzeitstellen im Durchschnitt

## Was ist ein IKS?

Wikipedia definiert dies wie folgt: «Ein internes Kontrollsystem (IKS) besteht aus systematisch gestalteten, organisatorischen Massnahmen und Kontrollen im Unternehmen zur Einhaltung von Richtlinien und zur Abwehr von Schäden, die durch das eigene Personal oder böswillige Dritte verursacht werden können.» In dieser kurzen Beschreibung steckt alles drin, was notwendig ist, ein IKS im eigenen Unternehmen aufzubauen:
- Systematisch gestaltet: selbstverständlich kann dies selbstständig definiert werden. Einfacher ist es, wenn ein bestehender Standard verwendet wird. Im Bereich der IT-Sicherheit kann dies beispielsweise ISO 27001 sein.
- Organisatorische Massnahmen und Kontrollen: bevor überhaupt Massnahmen definiert werden können, muss das Ziel klar sein. Dieses gilt es zuerst zu definieren. Sobald dies klar ist, können Massnahmen zur Erreichung dieses Zieles (oder mehreren Zielen) beschrieben werden. Damit auch festgestellt werden kann, ob man sich noch auf dem richtigen Weg befindet, müssen regelmässig Kontrollen durchgeführt werden. Die Massnahmen zeigen, was kontrolliert wird.
- Abwehr von Schäden: Gefahren und Risiken lauern an vielen Stellen. Diese beeinflussen

Bild: Archiv

die definierten Massnahmen negativ. Damit diese Risiken nicht den Betrieb nachträglich stören, gilt es die Risiken zu bewerten und entsprechende (Gegen-)Massnahmen zu definieren (Siehe dazu auch Blick-Punkt KMU 4.2006).

– Eigenes Personal oder böswillige Dritte: diverse Studien gehen davon aus, dass der Grossteil der Störungen vom eigenen Personal verursacht werden. Aber auch die «bösen» Dritten dürfen nicht vernachlässigt werden, was die neueste Virenepidemie zeigt. Die Massnahmen müssen daher externe, wie auch interne Personen berücksichtigen.

## Umfang eines IKS?

Der Gesetzgeber lässt bewusst offen, wie das IKS aufgebaut werden muss. Damit soll den Firmen der nötige Handlungsspielraum gegeben werden, das IKS auf die Unternehmung anzupassen. Die individuellen Gegebenheiten können und sollen berücksichtigt werden. Folgende Kriterien helfen bei der Wahl der Instrumente:

– Grösse
– Komplexität der Geschäftstätigkeit
– Art der Finanzierung

Sehr wichtig ist, dass ein IKS überprüfbar ist. Eine Dokumentation desselben wird damit unumgänglich. Wird das IKS nicht dokumentiert, kann es von der Revisionsstelle auch nicht im gewünschten Umfang kontrolliert werden. Dies hat zur Folge, dass im Bericht der Revision das IKS als ungenügend deklariert werden muss. Die interne Kontrolle ist Chefsache. Es gilt aber die Mitarbeiter über dieses, in einer sinnvollen Form, zu informieren (zumindest über einzelne Punkte). Die Information ist zwar nicht vorgeschrieben, untermauert aber eine offene Kommunikationspolitik und hilft, die Loyalität zu bewahren.

Welche Konsequenzen drohen bei fehlendem oder mangelhaftem IKS? Das Obligationenrecht schreibt vor, dass die Revisoren verpflichtet sind, die Ausführungen über das interne Kontrollsystem in einem Revisionsbericht zuhanden der Generalversammlung festzuhalten. Im Revisionsbericht wird beschrieben, wenn ein IKS zum Beispiel mangelhaft (zum Beispiel nicht dokumentiert) ist oder komplett fehlt. Die Revisoren müssen weitere Ausführungen über die Feststellungen im Erläuterungsbericht an den Verwaltungsrat vornehmen.

Damit hat der Verwaltungsrat die Möglichkeit festzustellen, wenn die Geschäftsleitung ihre Verantwortung für die Umsetzung des IKS nicht oder mangelhaft wahrnimmt. Im Falle von ungenügendem IKS wird bei den Konsequenzen unterschieden, ob fahrlässig oder nicht fahrlässig gehandelt wurde. Verletzt ein Organ der Gesellschaft seine Pflichten fahrlässig oder absichtlich, haftet dieses für allfälligen Schadenersatz. Bei weitreichenden Folgen machen sich die Fehlbaren strafbar und können gemäss Strafgesetzbuch Artikel 102 (Organisationsverschulden) belangt werden.

Ein IKS ist für viele Firmen in der Schweiz obligatorisch. Es bedeutet jedoch nicht nur Aufwand, sondern kann der Firma einen grossen Nutzen bringen. In regelmässigen Abständen kann sichergestellt werden, dass der definierte Kurs und die Ziele erreicht wurden. Sind Abweichungen ersichtlich, können Gegenmassnahmen ergriffen und eingeschlagen werden. Somit können Fehler erkannt werden, bevor sich diese negativ auf das Unternehmen auswirken können.

Anzeige