IKS

Wie entsteht ein internes Kontrollsystem?

Über ein Jahr ist es her, seit per 1. Januar 2008 die Gesetzgebung geändert wurde. Das interne Kontrollsystem (IKS) erhielt eine gewichtigere Bedeutung. Was bedeutet das für kleinere und mittlere Unternehmungen? Beeinflusst das IKS die IT – oder gar umgekehrt?

Autoren: Andreas Wisler, Sandro Müller

Dieser Beitrag zeigt, was ein internes Kontrollsystem genau ist und warum es hilft, die IT-Sicherheit zu erhöhen. Gleichzeitig ist dieser Artikel der Start zu einer Reihe von Werkzeugen, mittels derer ein ISMS (Information Security Management System) aufgebaut werden kann. Den Anfang macht in der nächsten Woche die ISO-Reihe 2700x.

Obwohl die revidierten Artikel 728a und b des Obligationenrechts bereits vor über einem Jahr in Kraft getreten sind, verfügen nur wenige Unternehmen über ein internes Kontrollsystem. Dies ist sehr schade, bringt ein IKS doch nicht nur Aufwand, sondern hilft, die eigene Organisation im "Griff" zu behalten. Gerade in der turbulenten, unvorhersehbaren Zeit, in der wir uns befinden, ist es wichtig, jederzeit über den eigenen Zustand Bescheid zu wissen.

Zu den Autoren

Andreas Wisler (Tel.: 052 320 91 20), Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.

Sandro Müller, Dipl. Ing. FH, ist Sicherheitsspezialist bei GO OUT. Als Fachmann für IKS trug er zur Entstehung dieses Artikels bei.

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.

Wer ist davon betroffen?

Betroffen von den im vorhergehenden Abschnitt zitierten Gesetzestexten und damit von der Pflicht, ein IKS zu betreiben, sind Publikumsgesellschaften, welche zwei der drei folgenden Kriterien in zwei aufeinanderfolgenden Jahren erfüllen:

- Bilanzsumme ≥ CHF 10 Mio.
- Umsatz ≥ CHF 20 Mio.
- 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:

- Systematische Gestaltung: Selbstverständlich kann dies selbstständig definiert werden. Einfacher ist es, wenn ein bestehender Standard verwendet wird. Im Bereich der IT-Sicherheit kann dies beispielsweise die Norm ISO 27001 sein.
- Organisatorische Massnahmen und Kontrollen: Bevor überhaupt Massnahmen festgelegt werden können, muss das Ziel klar sein. Dieses gilt es zuerst zu definieren, dann können Massnahmen zur Erreichung dieses Zieles (oder mehrerer Ziele) beschrieben werden. Damit auch festgestellt werden kann, ob man sich noch auf dem richtigen Weg befindet, müssen regelmässig Kontrollen durchgeführt werden.
- Abwehr von Schäden: Gefahren und Risiken lauern an vielen Stellen. Diese beeinflussen 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 Blickpunkt:KMU 4.2006).
- Eigenes Personal oder böswillige Dritte: Diverse Studien gehen davon aus, dass der Grossteil der Störungen vom eigenen Personal verursacht wird. 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 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 an die Generalversammlung festzuhalten. Dort wird festgehalten, wenn ein IKS zum Beispiel mangelhaft (etwa weil 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. ◆

Online-Tipp

Unter www.gosecurity.ch kann kostenlos und unverbindlich ein Newsletter zu aktuellen Sicherheitsthemen abonniert werden (INFONEWS). Die Website archiviert auch ältere Ausgaben des Newsletters – die Nummer 3/2008 befasst sich detailliert mit der Errichtung eines internen Kontrollsystems.