



Michael Annen

lic. oec. HSG, dipl. Wirtschaftsprüfer
Partner der SRG Schweizerische
Revisionsgesellschaft AG und der
Buchhaltungs- und Revisions-AG, Zug
Mitglied Kommission Fachfragen
STVIUSF
www.srgch.ch/www.brag.ch

Internes Kontrollsystem und Risikobeurteilung

Mit Inkrafttreten des neuen Revisionsrechts wurden neue Prüfungsgegenstände eingeführt, die der Revisor anlässlich der jährlichen Prüfung bestätigen muss: Die Existenz des internen Kontrollsystems sowie die Anhangsangaben über die Durchführung einer Risikobeurteilung. Die Umsetzung und die Dokumentation des internen Kontrollsystems sowie die Durchführung der Risikobeurteilung müssen bis zum Jahresende implementiert sein. Im folgenden Artikel werden schwergewichtig die Aspekte eines Internen Kontrollsystems (IKS) und der neue Prüfungsstandard «Prüfung der Existenz des internen Kontrollsystems (PS 890)» vorgestellt. Im Weiteren werden Ansätze aufgezeigt, wie den gesetzlichen Anforderungen in klassischen KMU-Verhältnissen nachgekommen werden kann.

Einleitung: Zwei neue Prüfungsgegenstände

Die Selbstregulierung weicht einer umfassenden Gesetzesregelung und ab 2008 werden Kapitalgesellschaften unabhängig von ihrer Rechtsform¹ prüfungspflichtig. Prüfungsumfang und -intensität hängen von Grössenkriterien der Gesellschaft ab. Kapitalgesellschaften, welche zwei der folgenden Kriterien in zwei aufeinander folgenden Jahren überschreiten (Art. 727 Abs. 2 OR) oder als Publikumsgesellschaften qualifizieren (Art. 727 Abs. 1 OR), unterliegen der ordentlichen Revision:

- Bilanzsumme 10 Mio.
- Umsatz 20 Mio.
- Arbeitnehmer 50 (Vollzeitstellen)

Gesellschaften, welche einer ordentlichen

Revision unterliegen, werden als wirtschaftlich bedeutende Unternehmen eingestuft.

Alle übrigen Gesellschaften, die diese Kriterien nicht erfüllen, sind neu eingeschränkt prüfungspflichtig und unterliegen der eingeschränkten Revision (Art. 727a Abs. 1 OR).

Die ordentliche Revision bedeutet nicht nur Mehraufwand für die Revisionsstelle, sondern auch zusätzliche Anforderungen an das zu prüfende Unternehmen. Das ordentlich geprüfte Unternehmen muss neu das interne Kontrollsystem (IKS) dokumentieren und eine Risikobeurteilung vornehmen, welche im Anhang der Jahresrechnung unter dem Punkt «Durchführung einer Risikobeurteilung» (Art. 663b Ziff. 12 OR) offen gelegt werden muss. Die Dokumentation des internen Kontrollsystems ist an die Grösse und Komplexität der Unternehmung anzupassen und es soll pri-

mär auf die wesentlichen Prozesse und Schlüsselkontrollen der Fokus gelegt werden, welche für die Jahresrechnungserstellung von Bedeutung sind. Die Offenlegungen im Anhang zur Risikobeurteilung setzt grundsätzlich im Ansatz ein Risikomanagement oder zumindest eine jährliche Risikobeurteilung voraus. Der Verwaltungsrat sollte im Rahmen der Durchführung einer Risikobeurteilung die wesentlichen Geschäftsrisiken, die gegenwärtig bestehen oder in Zukunft entstehen können, inventarisieren, bewerten und Massnahmen zur Steuerung bzw. Überwachung der Risiken beschliessen und umsetzen.² Der Verwaltungsrat steht in der Pflicht und hat die Risikobeurteilung für jede Gesellschaft vorzunehmen, welche einen Anhang nach Gesetz erstellen muss. Da der Anhang Bestandteil der Jahresrechnung ist, wird die Bestimmung über die Risiko-

beurteilung auch Prüfungsgegenstand sowohl für die ordentliche als auch die eingeschränkte Revision. Die Revisionsstelle hat allerdings keine Prüfung des Risikomanagements oder der «richtigen» Identifizierung und Bemessung der Risiken vorzunehmen; vielmehr beschränkt sich die Revisionsstelle auf die rein formale Überprüfung der Angaben über die Durchführung einer Risikobeurteilung im Anhang der Jahresrechnung.

In der Praxis machen die Mehrheit der Gewerbetreibenden und KMU sowie die Grossunternehmer ihre Risikoüberlegungen bereits heute – neu ist, dass diese jetzt auch zu Papier gebracht werden müssen. Denn im Rahmen der ordentlichen Revision hat der Revisor von Gesetzes wegen zu prüfen, ob eine Risikobeurteilung durchgeführt wurde und ob ein internes Kontrollsystem existiert. Logischerweise kann der Prüfer nur prüfen, was auch vorhanden, sprich dokumentiert, ist. So schreiben es die Prüfungsstandards vor. Dabei hat sich der Prüfer nicht auf die materiellen Aspekte der Risikobeurteilung ein Urteil zu bilden; er beschränkt sich auf eine formelle Prüfung. In der Praxis ist stark umstritten, was überhaupt in den Anhang bzgl. Risikobeurteilung gehört; das Gesetz und die Botschaft äussert sich dazu unklar und teilw. sind die gemachten Aussagen widersprüchlich. Die KWP der Treuhänderkammer³ hat drei Varianten als mögliche Lösungen für die Offenlegung im Anhang vorgeschlagen: Die erste Variante wäre, dass die Gesellschaft nur den Risikobeurteilungsprozess im Anhang offenlegt. Als erweiterte Offenlegung (Variante zwei) würden zusätzlich die wesentlichen Risiken, welche einen Einfluss auf die Jahresrechnung haben, beschrieben werden. Bei Variante drei als weitestgehende Offenlegung werden zusätzlich zu Variante zwei die operativen und strategischen Risiken im Anhang offengelegt. Die letzte Variante geht sehr weit und wird wahrscheinlich in der Praxis der KMU weniger zum Zug kommen.

Bei der Prüfung des internen Kontrollsystems ist neben der Formalisierung (sprich: Dokumentation) der wesentlichen Prozesse mit ihren Schlüsselkontrollen auch die Umsetzung im Rahmen der Revision zu prüfen.

Bereits in der geplanten zweiten Aktienrechtsreform⁴ wird die Offenlegung bzgl. Durchführung einer Risikobeurteilung vom Anhang in den neu geschaffenen Lagebericht verschoben. Dies hat den Vorteil, dass die eingeschränkt zu prüfenden Unternehmen ab Inkrafttreten der nächsten Aktienrechtsreform (kaum vor 2011) keine Risikobeurteilung mehr offenlegen müssen und damit für diese Gesellschaften dieser Prüfungsgegenstand wieder wegfällt.

Das Interne Kontrollsystem (IKS)⁵

a) Ein systematischer Ansatz

Ein IKS soll nicht Selbstzweck oder Schikane für den Unternehmer sein. Die Chance, dass das IKS nun auch gesetzlich vorgeschrieben ist, soll von den Unternehmen und Kunden genutzt werden. Wichtig ist, dass der Treuhänder und Revisor dies entsprechend auch kommuniziert. Mit dem IKS wird sichergestellt, dass

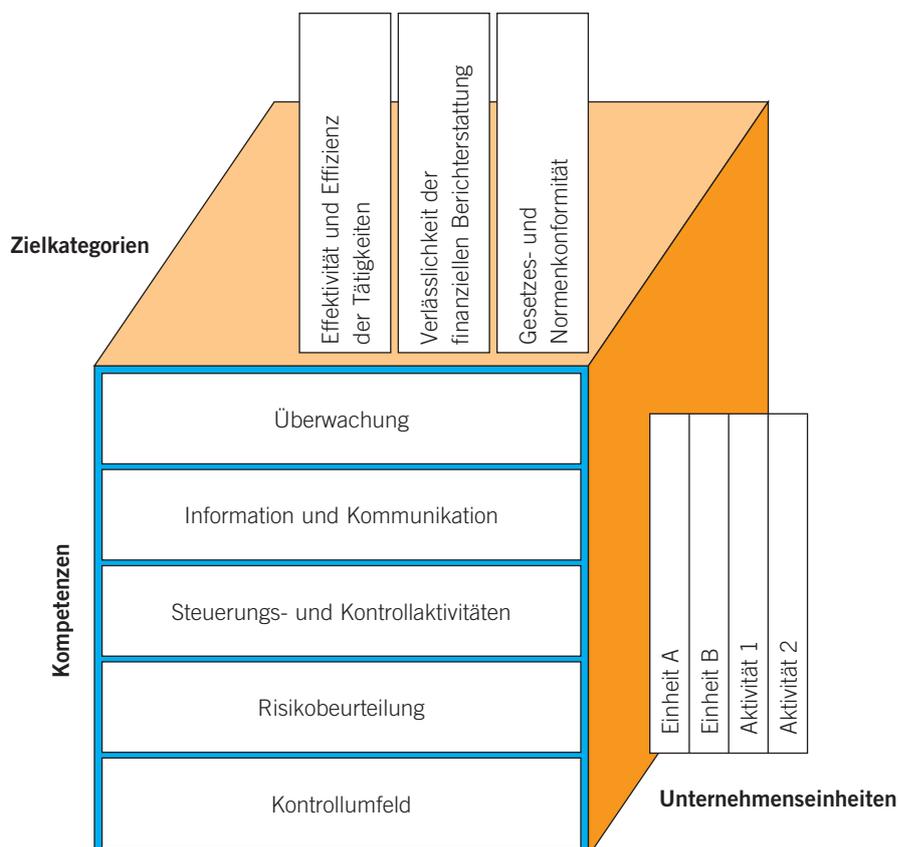
- die geschäftspolitischen Ziele erreicht werden,
- die Gesetze und Vorschriften eingehalten werden (compliance),
- das Vermögen der Unternehmung geschützt wird,
- Fehler und Unregelmässigkeiten aufgedeckt und korrigiert werden,
- die Buchführung ordnungsgemäss und die Rechnungslegung verlässlich und zeitgerecht ist.

Richtig, was Sie jetzt denken: Das ist ja nichts Neues. Und wenn man genau überlegt, macht dies jeder Unternehmer bzw. hat die oben genannten Ziele im Hinterkopf: Ein erfolgreicher Unternehmer kennt seine Risiken und hat Massnahmen ergriffen, um das Geschäftvermögen zu schützen, Gesetze und Vorschriften einzuhalten, damit keine Fehler und Unregelmässigkeiten entstehen oder diese zumindest vermindert werden, und die Buchführung und

finanzielle Berichterstattung sind soweit ausgebaut, dass der Unternehmer sich auf die Zahlen verlassen kann.

Man könnte meinen, dass für viele KMU sich wenig mit der neuen Gesetzgebung ändert. Wer bisher erfolgreich als Unternehmer tätig war, hat die Ziele des IKS bewusst oder unbewusst befolgt. Damit müssen auch keine neuen Ziele definiert oder gar die Buchhaltung und Prozesse auf den Kopf gestellt werden. Nur: Der Gesetzgeber verlangt mit der Existenzbestätigung des IKS, dass dieses nun formalisiert und dokumentiert wird. Und da gibt es Nachholbedarf, vor allem bei KMU. Je grösser die Unternehmung, desto eher ist ein formalisiertes IKS implementiert, denn bei steigender Komplexität und Grösse der Unternehmung ist eine Führung der Unternehmung nur noch mit formalisierten und dokumentierten Regeln und Abläufen möglich. Es ist festzustellen, dass die neue Gesetzgebung gerade die KMU trifft, weil bei diesen der Formalisierungs- und Dokumentationsbedarf am grössten ist.

Sie bietet im Bereich IKS aber vor allem Chancen, sich strukturiert und vertieft mit der Thematik auseinanderzusetzen, Prozesse und Abläufe intern zu überdenken und Mängel bei den Kontrollen zu beheben. Das fundierte Verständnis der Prozessabläufe, Kontrollen und Risiken bietet Chancen, welche zu Vorteilen gegenüber den Mitbewerbern führen können.



Die Existenzbestätigung des IKS nach Art. 728a OR fokussiert im Wesentlichen auf das Ziel der Verlässlichkeit der Berichterstattung. Der Gesetzgeber sagt nicht, wie ein IKS auszugestaltet ist. Es gibt bereits verschiedene gesetzliche Grundlagen,⁶ aber es hat sich international im Wesentlichen ein Referenzmodell durchgesetzt, wie ein IKS strukturiert werden kann: das COSO-Modell,⁷ welches sich anhand eines Würfels darstellen lässt (siehe Abbildung Seite 271).

Das COSO-Modell ist ein Framework, welches ein einfaches, systematisches und umfassendes Verständnis für das IKS erreichen soll. Dies hilft, um die IKS-Systematik einfacher zu kommunizieren, da COSO bei den IKS-Anwendern bestens bekannt ist. Es ist aber nicht so, dass nun jeder IKS-Verantwortliche bei KMU sich durch die COSO-Literatur durchwälzen muss. Denn das COSO-Modell geht viel weiter, als für die IKS Existenzbestätigung im Sinne des Schweizer Gesetzes erforderlich ist.

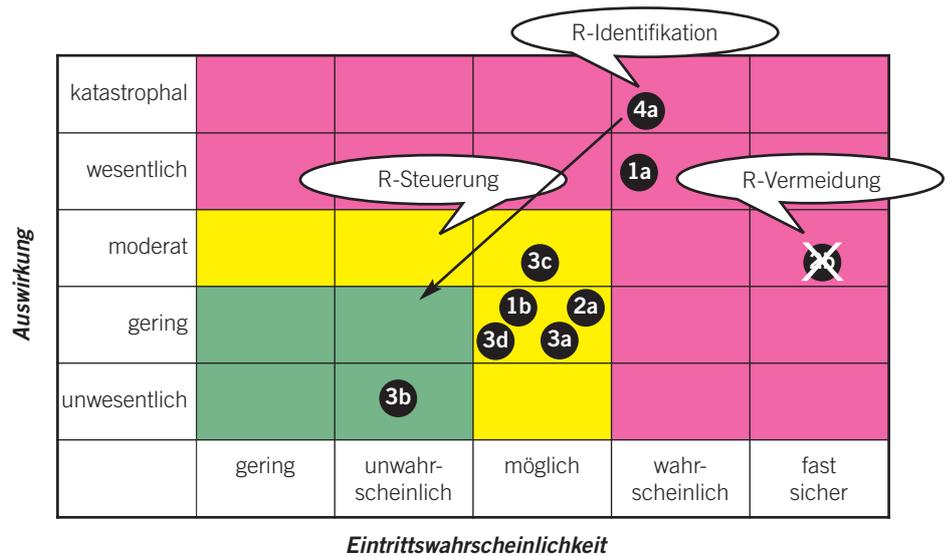
Das COSO-Framework dringt durch die verschiedenen Unternehmenseinheiten hindurch, d. h. es ist universell für alle Geschäftstätigkeiten, Branchen und Einheiten in der gleichen Systematik anwendbar. Für die Ausgestaltung eines IKS sind folgende Aspekte abzudecken, im COSO-Modell auch Komponenten genannt:

- Kontrollumfeld
- Risikobeurteilung
- Steuerungs- und Kontrollaktivitäten
- Information und Kommunikation
- Überwachung

Beschränkt man sich auf die Zielsetzung der Schweizerischen Gesetzgebung, d. h. die Verlässlichkeit der finanziellen Berichterstattung sicherzustellen, sind diese Komponenten nur in Bezug auf dieses Ziel abzuarbeiten und auszugestalten. Entscheidet sich das Unternehmen, ein umfassendes IKS nach dem COSO-Framework einzuführen, sind die Zielsetzungen der effektiven und effizienten operationellen Tätigkeit sowie die Gesetzes- und Normenkonformität (Compliance) ebenfalls mit den oben genannten Komponenten abzudecken. Dies bedeutet eine umfassendere und zeitintensivere Ausgestaltung des IKS.

b) Das Kontrollumfeld

Das Kontrollumfeld umfasst vor allem die Softfaktoren wie Einstellung zu Kontrollen, Bewusstsein, Verhalten der Mitarbeiter, Führungsstil, Organisationsstruktur, Kompetenzen der Mitarbeiter und Kommunikation, aber auch ethisches Verhalten, Managementphilosophie, Integrität, Sorgfalt des Personals und beeinflusst die anderen Komponenten wie Risikobeurteilung, Kommunikation oder Überwachung. Ein «positives» Kontrollumfeld im Sinne



eines existierenden IKS ist schliesslich die grundlegende Basis. Wenn es im Kontrollumfeld schon nicht stimmt, dann helfen die besten Risikobeurteilungsprozesse und Kontrollaktivitäten wenig, um ein IKS funktionsfähig zu halten. Eine konsistente und kontinuierliche Personalpolitik und vor allem -auswahl ist der Schlüssel für ein gutes Kontrollumfeld⁸. Ob die Werte in der Unternehmung effektiv auch gelebt werden, hängt zentral vom Verhalten sowie der Arbeitsweise des Verwaltungsrates und der oberen Führungsebene ab.

c) Risikobeurteilung

Das Kennen der unternehmensrelevanten Risiken und die Gewichtung und Beurteilung dieser Risiken ist eine Grundvoraussetzung für ein funktionierendes IKS. Von Bedeutung sind vor allem Risiken, welche die unternehmerische Zielsetzung gefährden könnten. Dabei ist die Auswirkung und Eintretenswahrscheinlichkeit pro Risiko zu beurteilen. Diese Risikobeurteilung kann in Form einer Risikomatrix grafisch dargestellt werden (siehe Abbildung oben).

Die Ausformulierung sowie Massnahmen und Zuständigkeiten können in einfacheren Verhältnissen in Form einer Tabelle zusammengefasst werden (siehe Tabelle 1).⁹

Es ist wiederum zu beachten, dass sich die Zielsetzung auf die Verlässlichkeit der finanziellen Berichterstattung beschränkt und die beiden anderen COSO-Zielsetzungen vernachlässigt werden können, wenn als Minimalziel nur die gesetzgeberischen Anforderungen erfüllt werden sollen. Damit die Finanzverantwortlichen die Risiken auch korrekt identifizieren und beurteilen und daraus entsprechende

Massnahmen ableiten, ist die zeitnahe Kommunikation mit dem Verwaltungsrat oder Geschäftsführer unerlässlich. Schliesslich soll die Risikobeurteilung der gesamten Geschäftsleitung und des Verwaltungsrates ein transparenteres Bild und besseres Verständnis der Unternehmensrisiken abgeben, damit auch ein unternehmerischer Nutzen aus diesem Prozess gezogen werden kann.

Die Erstellung des IKS nach COSO erfolgt mittels eines Top-down-Ansatzes: Der Startpunkt ist die Risikoanalyse auf Ebene der Gesamtunternehmung und bricht diese auf die einzelnen Positionen der Jahresrechnung bis auf Kontoebene hinunter. Die Analyse der Geschäftsprozesse, welche die Jahresrechnung beeinflussen, ist dabei die Vorarbeit für eine Risikoanalyse. Alternativ lässt sich ein IKS auch mittels eines bottom-up-Ansatzes realisieren: Ausgangspunkt sind die Jahresrechnungspositionen und die damit zusammenhängenden Hauptprozesse. Je nach Risiko- und IKS-Verständnis in der Unternehmung sind beide Ansätze gangbare Wege, damit eine Risikobeurteilung resultiert, welche als Schlüsselinput bei der Bestimmung von notwendigen Kontrollaktivitäten Verwendung findet.

d) Steuerungs- und Kontrollaktivitäten

Die Steuerungs- und Kontrollaktivitäten sind das Herzstück eines IKS und sollen sicherstellen, dass man die Risiken «im Griff» hat und die entsprechenden Massnahmen auch umgesetzt werden. Mittels Richtlinien und Sollvorgaben werden die Steuerungs- und Kontrollaktivitäten in die Geschäftsprozesse integriert. Diese sind nach Komplexität und Grösse der

Tabelle 1

Aussage in der JR	Risikoanalyse	H / M / T	Massnahmen	Zuständig	Beurteilung

Tabelle 2

Teilprozesse / Teilprozessziele	Risikoanalyse		Steuerungs- und Kontrollmassnahmen			Beurteilung und Schlussfolgerung (ok / nein, Kommentar)
	Risikofaktoren / Risikobeschreibung	Rating	Massnahmen / Kommentare	Verantwortliche(r)	Typ (manuell / automatisch, präventiv / detektiv)	
...

Unternehmung unterschiedlich ausgestaltet. Ein Patentrezept gibt es dazu nicht. Kontrollaktivitäten können sein:

- Genehmigungen
- Autorisierungen
- Nachprüfungen
- Kontenabstimmungen
- Leistungsprüfungen
- Funktionentrennungen

Bei KMU sind Genehmigungen durch die Geschäftsleitung und/oder Verwaltungsrat sowie das Vier-Augen-Prinzip wohl eine der gängigsten Kontrollen. Dazu gehört auch die Kollektivunterschrift anstelle der Einzelunterschrift.

Wichtig ist, dass die eingeführten Massnahmen ausgewogen sind und sowohl das gewünschte Verhalten unterstützen (steuernde Massnahmen) und unerwünschtes Verhalten verhindern (präventive Massnahmen). Die Regelung der Arbeitsabläufe, Ablauf- und Aufbauorganisation, aber auch eine saubere Instanzgliederung sind Beispiele von Massnahmen. Dabei hilft der Einsatz von IT und Standardsoftware oft, um auf einfache und kostengünstige Weise angemessene Kontrollen einzuführen. Die Funktionentrennung ist eine gute und effiziente Kontrolle, aber bei kleinen Unternehmen sind mangels begrenzter personeller Ressourcen Grenzen gesetzt.

Damit die richtigen Kontrollen auch am richtigen Platz sind, ist es notwendig, die Geschäftsprozesse zu analysieren (Soll-Ist-Vergleich) und allfällige Kontrolldefizite zu identifizieren. Für die Dokumentation der Risiken und Kontrollen ist eine Risiko-Kontrollmatrix¹⁰ zu empfehlen, welche auf einem einfachen Excel basieren könnte (siehe Tabelle 2).

Neben dem Verhältnis von Kosten zu Nutzen stellt sich für die Unternehmung immer auch die Frage, wie detailliert ein IKS ausgestaltet werden soll. Der Vorteil einer Excel-Tabellen-Lösung ist, dass diese beliebig ausgebaut werden kann. Im Markt gibt es ausgereifere Modelle und Dokumentationstools für ein umfassendes IKS. Diese Modelle basieren oft

auf gängiger Softwarebasis wie Excel und sind durchaus für grössere KMU interessant oder für welche, die mehr als nur das gesetzliche Minimum bzgl. IKS und Risikobeurteilung umsetzen wollen.¹¹ Eine Risiko-Kontrollmatrix sollte zumindest folgende Informationen abdecken:

- (Teil-)prozess
- Risikoanalyse mit Risikobeschreibung und -gewichtung
- Steuerungs- und Kontrollmassnahmen
 - Massnahme/Kommentar
 - Verantwortlicher
 - Massnahmentyp
- Beurteilung mit Schwächen und Handlungsbedarf

Eine Risiko-Kontrollmatrix mit dem oben vorgeschlagenen Detaillierungsgrad erfüllt die Vorgaben der Dokumentation eines IKS, der Transparenz und die Möglichkeit des Unternehmens, eigenständig eine Risiko-Kontrollanalyse durchzuführen. Zusammenfassend wird mit Hilfe dieser Risiko-Kontrollmatrix der Risikoumfang qualitativ umschrieben und gewichtet sowie die dazugehörigen Kontrollen und Massnahmen festgehalten. Dies ermöglicht der Unternehmung periodisch eine Beurteilung der Kosten/Nutzen und zeigt potenzielle Schwächen und Verbesserungsmöglichkeiten auf. Die Darstellung der Geschäftsprozesse in Flowcharts unterstützt eine Risiko-Kontrollmatrix visuell und kann bei der IKS-Implementierung hilfreich sein.

e) Information und Kommunikation

Ein wichtiger Bestandteil im COSO-Modell und in einem IKS ist die Information und Kommunikation. Es ist wichtig, dass die Mitarbeiter über das IKS Bescheid wissen und über die Massnahmen und Schwachpunkte informiert sind sowie die Verbesserungspotenziale eruieren können. Bezüglich der Informationen zur Finanzberichterstattung können auch externe Quellen von Bedeutung sein wie Publikationen von Verbänden, Lieferanten, Wettbewerbern oder Informationen zum ökonomischen Um-

feld. In grösseren Unternehmen ist beispielsweise klar zu kommunizieren, wer für welche Konten verantwortlich ist, wer Konten eröffnen und schliessen kann und wer für die Verbuchung autorisiert ist. Im Idealfall werden diese Vorgaben über IT-Kontrollen, d.h. mittels Autorisierungen, festgehalten. Die Anwendung eines COSO-Modells unterstützt die Kommunikation und Information.

Nur wer informiert ist, kann auch entsprechend handeln: Daher sind die Mitarbeiter vollumfänglich über das bestehende IKS zu informieren. Die Kommunikation erfolgt auch über Richtlinien, welche durch den Verwaltungsrat zu entwickeln resp. vorzugeben sind.

f) Überwachung

Schlussendlich ist das IKS auch zu überwachen. Gerade im Bereich der finanziellen Berichterstattung ist es essenziell, die Abweichungen vom Soll-Zustand zeitgerecht zu erfassen und die nötigen Massnahmen abzuleiten. Die Überwachung erfolgt einerseits über die laufenden Überwachungsmassnahmen sowie über die Berichterstattung von Mängeln, wobei diese gerade bei kleineren Unternehmen eher informeller ablaufen wird.

Umsetzung des IKS in KMU

Ein umfangreiches IKS im Sinne des COSO-Modells lässt sich für KMU nicht immer verwirklichen, da gerade in Bezug auf das IKS restriktive Rahmenbedingungen vorherrschen. So sind die verfügbaren Ressourcen für die Einführung eines umfassenden IKS meistens sehr begrenzt und der Umsetzung aller Kontrollmassnahmen sind Grenzen gesetzt. Gerade im Bereich der finanziellen Berichterstattung sind die Ressourcen oft ungenügend und die technischen Kontrollmassnahmen im Bereich der IT lassen sich nicht vollumfänglich umsetzen.

Die internen Kontrollen bei KMU lassen sich mit der Stärkung des Verwaltungsrates in Bezug auf Finanz-Knowhow merklich verbessern. Dabei ist auf die wesentlichsten Risiken zu fokussieren und das «Vier-Augen-Prinzip» zu stärken. Vorgaben von Abläufen mittels einfachen Richtlinien verbessern die Kontrollmassnahmen und das Gesamtverständnis für das IKS. Die Geschäftsleitung resp. Verwaltungsrat sind in die Überwachung des IKS stärker einzubeziehen. Zusätzlich nimmt die Revisionsstelle eine wichtige Kontrollfunktion bei KMU, gerade in Bezug auf die Verlässlichkeit der finanziellen Berichterstattung, ein. Mit Hilfe einer auf Excel basierenden Risiko-Kontrollmatrix, eventuell mit Unterstützung einer Risikomatrix, lässt sich ein den gesetz-

lichen Anforderungen und KMU-taugliches IKS umsetzen, um ein vernünftiges Kosten/Nutzen-Verhältnis zu wahren. Auf dieser Basis kann jedes Unternehmen sein IKS weiter ausbauen; technische Hilfsmittel gibt es dabei genügend, wie z. B. die Verwendung einer Software für die Erstellung von Flowcharts. Nicht zu vergessen sind die bestehenden Organigramme, Kompetenzregelungen, Reglemente und Dienstabweisungen usw., welche als Bestandteil der IKS-Dokumentation dienen. In der Risiko-Kontrollmatrix soll auf diese (bestehenden) Dokumente verwiesen werden. Das Rad ist nicht neu zu erfinden!

Ein IKS soll auch in einem KMU nicht Selbstzweck, sondern als integrierter Prozess verstanden werden. Es ist in die bestehende Struktur und Prozesse des Unternehmens einzubetten.

PS 890 – Prüfung der Existenz des internen Kontrollsystems

Die Grundlage für die Prüfung der Existenz des internen Kontrollsystems ist der Schweizer Prüfungsstandards PS 890,¹² welcher von der Treuhandkammer im Frühjahr 2008 herausgegeben wurde und für Jahresrechnungen ab 1.1.2008 anzuwenden ist. Für den Prüfer stellt sich primär die Frage, welche Prüfungshandlungen er durchführen muss, damit er die Existenz des internen Kontrollsystems einwandfrei und ohne Einschränkung bestätigen kann. In diesem Zusammenhang ist wichtig, dass für die Ausgestaltung, Implementierung und Aufrechterhaltung eines geeigneten und angemessenen IKS der Verwaltungsrat verantwortlich ist und nicht die Revisionsstelle. Nach Art. 728a Abs. 1 Ziff. 3 OR bestätigt die Revisionsstelle einmal jährlich die Existenz dieses vom Verwaltungsrat definierten IKS. Der Verwaltungsrat hat dafür zu sorgen, dass das definierte IKS

- schriftlich dokumentiert ist und
- zur Anwendung

kommt. Die dauerhafte und mängelfreie Funktion des IKS ist nicht Prüfungsgegenstand, d.h. die Existenz kann vom Revisor bejaht werden, wenn eine schriftliche Dokumentation des IKS vorhanden ist und der Nachweis erbracht werden kann, dass es auch «gelebt» wird im alltäglichen Betrieb.

Eine weitere Einschränkung für die Prüfung: Im Idealfall verfügt das Unternehmen in allen Bereichen des Unternehmens über ein funktionierendes IKS, welches dokumentiert ist und tagtäglich umgesetzt wird. Der Revisor kann sich aber auf die Elemente des IKS beschränken, die im Hinblick auf die ordnungsmässige

Buchführung und finanzielle Berichterstattung notwendig sind. Es ist demnach ausreichend, wenn die Dokumentation sich auf die Prozesse, Risiken und Schlüsselkontrollen beschränkt, welche eine Verbindung zur finanziellen Berichterstattung resp. darauf Einfluss haben. Die Ausgestaltung des IKS wird weder im Gesetz noch in der Botschaft definiert und daher gibt es einen grossen Spielraum bei der Umsetzung des IKS. Ein IKS nimmt für den Prüfer seit jeher eine wichtige Funktion ein, die Abschlussprüfung zu planen; dort wo ein funktionierendes IKS vorhanden war, konnte sich der Prüfer auch in der Vergangenheit auf die Prüfung der Kontrollen beschränken und die ergebnisorientierten Prüfungen entsprechend minimieren.¹³ In einfachsten Verhältnissen hat man die Prüfung der Kontrollen weggelassen und ist direkt zu ergebnisorientierten Prüfungshandlungen geschritten.

PS 890 orientiert sich bei den Kontrollkomponenten am COSO-Modell und spezifiziert diese bezüglich des Prüfungsziels: Kontrollumfeld, Risikobeurteilungsprozess des Unternehmens, rechnungslegungsrelevante Informationssysteme und damit verbundene Geschäftsprozesse/Kommunikation, Kontrollaktivitäten sowie die Überwachung der Kontrollen.

Von Bedeutung ist als Basis das Kontrollumfeld. Der Risikobeurteilungsprozess des Unternehmens ist Basis für die Identifizierung der Risiken. Die Risikoidentifikation ist wiederum Grundlage, damit die Schlüsselkontrollen am richtigen Ort platziert werden. Der Revisor arbeitet schon seit längerem mit einem risikoorientierten Ansatz; Ende der 90er-Jahre haben die grossen Revisionsgesellschaften die risikoorientierten Prüfungsansätze lanciert. Dabei legt der Revisor dort seine Prüfungsschwerpunkte, wo die Risiken auf wesentliche Falschangaben in der Jahresrechnung am grössten sind. Eine risikoorientierte Prüfung ist für den Berufsstand nichts Neues, so ist dieser im HWP 1998 bereits detailliert beschrieben.

Die rechnungslegungsrelevanten Systeme und Prozesse sind die Abläufe und Aufzeichnungen, welche in der Unternehmung eingerichtet wurden, um die entsprechenden Nachweise und Jahresabschlüsse produzieren zu können. PS 890 nennt die Voraussetzungen für die Existenz eines IKS:

- Das IKS muss vorhanden und überprüfbar sein, d.h. es ist zu dokumentieren.
- Das IKS muss den Geschäftsrisiken und der -tätigkeit angepasst sein.
- Das IKS muss den Mitarbeitenden bekannt sein und durch sie angewendet werden.
- Das IKS muss auf einem vorhandenen Kontrollbewusstsein basieren, welches in der Unternehmung vorherrscht.

Die Prüfung der Existenz des IKS kann mit folgenden Prüfungsverfahren erfolgen:

- Durchsicht der Dokumentation der Ausgestaltung
- Befragung, Beobachtung und Überprüfung
- Walk-through-Test

Eine reine Dokumentationsprüfung wird im Normalfall nicht ausreichen, um die Existenz zu testen. Dabei ist der Walk-through-Test ein effizientes Prüfungsverfahren zum Nachweis der Existenz des IKS. Bei diesem Verfahren wird ein einzelner Geschäftsvorfall von Anfang bis zum Ende nachvollzogen und die entsprechende Dokumentation der Durchführung der definierten Schlüsselkontrollen geprüft.

Wichtig ist bei zu prüfenden KMU-Unternehmen auch, einen gewissen Pragmatismus walten zu lassen und nicht zu formalistisch zu werden. In einfachen KMU-Verhältnissen kann es durchaus ausreichen, dass der Revisor die Dokumentation des IKS durchgeht und aufgrund seiner tieferen Kenntnisse des Unternehmens auf weitere Prüfungsverfahren wie Befragung und/oder Walk-through-Test verzichten kann. Der Revisor muss sich evtl. vermehrt auf Diskussionen mit der Unternehmensleitung stützen und sich ein Bild machen, wie Risiken identifiziert und beurteilt werden und welche Kontrollen implementiert wurden. Dabei ist es vertretbar, wenn in einfachen Verhältnissen generell eine weniger starke Formalisierung des Risikobeurteilungsprozesses und des IKS stattfindet. Es darf nicht vergessen werden, dass es eine Vielzahl von klassischen KMU geben wird, die unter die ordentliche Revision fallen, aber bei denen nach wie vor relativ einfache Verhältnisse vorherrschen. In solchen einfacheren Verhältnissen kann z. B. ein dokumentiertes IKS auf ein paar wenigen A4-Seiten (z. B. Risiko-Kontrollmatrix als Excel-Tabelle!) durchaus ausreichen, um die gesetzlichen Bestimmungen sowie den PS 890 zu erfüllen. Der Revisor wird sich in diesen Fällen für die Existenzprüfung des IKS sowie der Risikobeurteilung verstärkt auf Befragung und Beobachtung abstützen, die für den Prüfungsnachweis ausreichend sind.

Damit der Prüfungsumfang auf ein vernünftiges Mass reduziert werden kann, sind nicht jedes Jahr alle Schlüsselkontrollen durchzuführen; eine Rotation ist erlaubt. Der Revisor hat sich zu vergewissern, dass gegenüber dem Vorjahr keine Änderungen eingetreten sind. Er hat angemessene Prüfungshandlungen vorzunehmen, damit er die Existenz des IKS jährlich bestätigen kann. Dies bedeutet, dass jährlich Prüfungshandlungen in diesem Bereich durchgeführt werden müssen, wenn auch jedes Jahr Schwerpunkte oder Rotation erlaubt sind.

Neben der Berichterstattung an die Generalversammlung, in welcher der Revisor die Existenz des IKS bestätigt (Art. 728a Ziff. 3 OR), erstattet der Revisor dem Verwaltungsrat einen umfassenden Bericht, in welchem er Feststellungen über die Rechnungslegung und insbesondere über das IKS darlegt. Dabei sind aus Sicht der Revisionsstelle Verbesserungsmöglichkeiten darzulegen und auf Mängel im IKS hinzuweisen, welche im Rahmen der Revision der Existenzprüfung festgestellt wurden.

Im Rahmen der Prüfungsarbeiten muss der Revisor zum Schluss kommen, dass die definierten und dokumentierten Schlüsselkontrollen umgesetzt sind. Liegen einzelne Schwächen oder Verbesserungspotenzial vor oder sind nicht alle wesentlichen Prozesse und Schlüsselkontrollen dokumentiert, dann kann die Existenz des IKS bejaht werden. Allerdings hat der Revisor zu beurteilen, ob eine fehlende Dokumentation von Schlüsselkontrollen und wichtiger Prozesse eine Einschränkung im Revisionsbericht erfordert. Die Existenz des IKS kann im Revisionsbericht nicht bestätigt werden, wenn das IKS den Risiken des Unternehmens in keiner Weise Rechnung trägt oder das vom Verwaltungsrat definierte IKS nicht umgesetzt wurde.

IKS für KMU – Herausforderung für den Revisor

Die Herausforderung für den Revisor ist sicherlich die Dokumentation, die vorhanden sein muss, damit überhaupt geprüft werden kann. Ohne eine eingehende Dokumentation ist die Prüfung und Nachweis eines IKS nur sehr eingeschränkt möglich. Interessanterweise wird diese Möglichkeit in den internationalen Standards aufgegriffen und z. B. empfiehlt ISA 315, in diesen Fällen vermehrt Befragungen und Beobachten als Prüfungshandlungen einzusetzen.

Ein weiteres Problem sind die sehr flachen Hierarchien in KMU und damit die begrenzte Möglichkeit der Überwachung des IKS; ressourcenbedingt sind viele Funktionen bei einer Person angesiedelt und damit ist das Risiko grösser, dass Kontrollen unterlaufen werden. Gerade die Einstellung von Eigentümer-Unternehmern zu Kontrollaktivitäten kann den Prüfungsansatz beeinflussen. Für ein erhöhtes Risiko sprechen:

- Vermischung von privaten und geschäftlichen Transaktionen
- Einkommensniveau und Lebensstil sind nicht im Verhältnis
- Häufiger Berater- und Revisionsstellenwechsel
- Zeitdruck bei der Revision ohne nachvollziehbare Gründe
- Ungewöhnliche Transaktionen vor und nach dem Bilanzstichtag
- Ungewöhnliche Transaktionen mit nahe stehenden Personen

Schliesslich braucht es auch vom Revisor eine gute Portion gesunden Menschenverstand, um die Gesamtsituation beim Unternehmen in Bezug auf das IKS beurteilen zu können. Dabei sind die Minimalanforderungen gemäss PS 890 nicht aus den Augen zu verlieren.

Fazit

In der ganzen Diskussion um das interne Kontrollsystem darf nicht vergessen werden, dass auch dem besten IKS Grenzen gesetzt sind. Man könnte auch von IKS-immanenten Grenzen sprechen, wie z. B. den menschlichen Einflussfaktor durch Irrtum oder fehlerhafte Ermessenentscheide, aber auch bewusste Verletzung der IKS-Regeln. Gerade in KMU ist es oft nicht möglich, ein umfassendes IKS einzurichten und gewisse Lücken bleiben bestehen. Andererseits hat der Unternehmer von KMU weitreichende Kenntnisse der Tätigkeit

und einen tieferen Einblick in die operative Tätigkeit des Unternehmens, was ihm erlaubt, die Kontrolldefizite zu kompensieren. Das interne Kontrollsystem ist immer der Grösse und Komplexität sowie dem Risikoprofil des Unternehmens anzupassen. ■

¹ Vom neuen Revisionsrecht sind auch Genossenschaften, Vereine und Stiftungen erfasst. Personengesellschaften sind nach wie vor von der Revision befreit.

² Aus dem Positionspapier «Neues Revisionsrecht – Ausgewählte Fragen und Antworten» der Treuhandkammer, Juni 2008

³ KWP ist die Kommission der Wirtschaftsprüfung, welche ihre Meinung zum Thema im Positionspapier «Neues Revisionsrecht – Ausgewählte Fragen und Antworten» der Treuhandkammer, Juni 2008, kundgetan hat.

⁴ Der Entwurf wird voraussichtlich im Herbst 2008 im Parlament beraten.

⁵ Die folgenden Ausführungen basieren u. a. auf dem Standardwerk von Dieter Pfaff/Flemming Ruud, Schweizer Leitfaden zum internen Kontrollsystem (IKS).

⁶ Gesellschaftsrecht betr. ordnungsmässiger Rechnungslegung, Art. 662ff. OR, Verwaltungsrat und Oberleitung, Art. 716a Ziff. 1–3 OR/ Corporate-Governance-Richtlinie der SWX/Swiss Code of Best Practice for Corporate Governance der Economie-suisse.

⁷ COSO steht für die Abkürzung «Committee of Sponsoring Organizations of the Treadway Commission», welche dieses Framework für IKS entwickelt hat. Das COSO-Framework ist der international anerkannte Bezugsrahmen. Auch der berühmte Sarbanes-Oxley Act (SOX) bezieht sich auf das COSO-Framework als anerkannte Grundlage für die periodische Beurteilung des IKS und der finanziellen Berichterstattung. In diesem Fachartikel wird vor allem auf das COSO-Modell Bezug genommen.

⁸ Die Ausformulierung eines Verhaltenskodexes, wobei die Mitarbeiter schriftlich bestätigen, dass sie ihn gelesen und verstanden haben, unterstützt die Förderung ethischer Werte und Integrität i. S. der Unternehmung.

⁹ Aus: Schulungsunterlagen von Karl Renggli, dipl. Wirtschaftsprüfer.

¹⁰ Abgeleitet aus Dieter Pfaff/Flemming Ruud, Schweizer Leitfaden zum internen Kontrollsystem (IKS).

¹¹ Dabei sei als Beispiel auf das IKS der BDO verwiesen «IKS für KMU», welches einen bottom-up-Ansatz verfolgt oder das Riskmanagement- und IKS-Tool von Hermann Grab, Mattig, Suter und Partner, welches auf dem COSO-Ansatz basiert.

¹² Nachfolgende Ausführungen basieren auf dem Schweizer Prüfungsstandard: Prüfung der Existenz des internen Kontrollsystems (PS 890), herausgegeben von der Treuhand-Kammer. Der Standard ist ab 1.1.2008 verbindlich.

¹³ Sog. Mittel-zum-Zweck-Funktion. Dabei sei auch auf PS 400 verwiesen.