

Die Risiko-Kontroll-Matrix als effizientes Risikomanagement-Tool



Nach dem In-Kraft-Treten der neuen bzw. revidierten Vorschriften des Obligationenrechts (siehe Art. 728a / 728b sowie Art. 663b OR) zur Internen Kontrolle und zum Risikomanagement sind revisionspflichtige Unternehmen verpflichtet sowohl Interne Kontrolle als auch Risikomanagement aktiv zu betreiben. Dies ist allerdings nicht alleinige Ursache für die Konjunktur dieser Themen: auch im Markt- und Wettbewerbsumfeld vieler Unternehmen lässt sich eine signifikante Verschärfung der Risikosituation beobachten, die beispielsweise durch den technischen Wandel oder steigenden Preis- und Qualitätsdruck auf globalisierten Märkten ausgelöst wird.

Neben dem Interesse von Gesetzgeber, Regulatoren und Stakeholdern die Corporate Governance und den Umgang mit Unternehmensrisiken eines Unternehmens muss es auch ein Interesse des Unternehmens selbst geben, durch aktives Risikomanagement das eigene Chancen/Risiken-Verhältnis zu optimieren.

Risikomanagement wird in diesem Zusammenhang als kontinuierlicher Prozess im Unternehmen verstanden, der sich in eine strategische Phase, in der die Ziele und die organisatorische Ausgestaltung des Risikomanagements festgelegt werden, und die operativen Phasen der Risikoidentifikation, Risikobewertung und Risikosteuerung einteilen lässt.

Als Grundvoraussetzung der später zu erstellenden Risiko-Kontroll-Matrix gilt es, die Schlüsselrisiken im Hinblick auf die zuvor definierten Kontrollziele zu identifizieren. Eine mögliche Vorgehensweise zur Erfassung der Schlüsselrisiken wird im Folgenden vorgestellt.

Die Risikoidentifikation und -analyse soll sich auf quantitative wie auch qualitative Kriterien stützen die auch Risiken des Betrugs (Fraud) berücksichtigen. Folgende Arbeitsschritte können dabei durchlaufen werden:

- **Prüfung der Positionen von Bilanz- und Erfolgsrechnung anhand quantitativer Größen.** Dabei wird z.B. unterstellt, dass eine einzelne Bilanzposition, die mehr als 5 Prozent ihrer Kategorie (Assets, Erträge, usw.) im Wert ausmacht, mittlerem Risiko ausgesetzt ist. Übersteigt die Position die 10 Prozentlimite, wird hohes Risikopotential unterstellt. Die entsprechenden risikobehafteten Positionen werden ausgewählt.
- **Prüfung der Merkmale von Bilanz- und Erfolgsrechnungspositionen.** Das Management beurteilt qualitative, interne Faktoren wie das Transaktionsvolumen durch eine Position oder die Komplexität der Rechnungslegungsstandards, welche diese Position betreffen. Externe Faktoren, die geprüft werden sollen, sind z.B. regulatorische oder politische Änderungen sowie sich wandelnde politische, ökonomische und wettbewerbsrechtliche Konditionen, welche die Position beeinflussen können. Die entsprechenden Positionen werden ausgewählt.
- **Auswahl der Schlüsselprozesse.** Nach Durchlaufen der beiden oben genannten Arbeitsschritte gilt es nun, alle Unternehmensteile und Geschäftsprozesse, die einen Einfluss auf die

vorher bestimmten risikobehafteten Positionen haben, zu identifizieren. Dabei sollen auch IT-Prozesse, welche die Verarbeitung von Transaktionen unterstützen erfasst werden. Das Management muss weiter alle Prozesse bestimmen, die mit Risiken der Möglichkeit eines vorsätzlichen Betrugs behaftet sind.

- **Identifikation der Schlüsselrisiken.** Schliesslich sollen die ausgewählten Unternehmensteile und Schlüsselprozesse auf ihre inhärenten Risiken geprüft werden. Alle identifizierten Risiken sollen in einem Risikoinventar übersichtlich aufgelistet und beschrieben werden.

Die anschliessende Risikobeurteilung beinhaltet die Analyse der zuvor identifizierten Schlüsselrisiken. Jedem Risiko wird eine Wahrscheinlichkeit des Eintretens wie auch das potentielle Schadensausmass zugeordnet, d.h. möglichst objektiv ermittelt oder realistisch geschätzt. Die daraus resultierende Beurteilung wird als zentraler Input bei der Determination von den notwendigen Kontrollaktivitäten verwendet.

Alle Risiken müssen nun dahingehend geprüft werden, ob eine entsprechende manuelle, halbmanuelle oder automatisierte Kontrolle im Unternehmen schon etabliert ist. Dazu muss zuerst eine Kontrollinventur durchgeführt werden, d.h. alle bestehenden Kontrollen sollen zusammengetragen und übersichtlich aufgeführt werden. Fehlen für einzelne Risiken adäquate Kontrollen, müssen diese neu geschaffen werden. Möglicherweise wird bei der Kontrollinventur festgestellt, dass mehrere Kontrollen bestehen, die alle dasselbe Risiko abdecken. Solche Kontrollredundanzen, d.h. das Vorhandensein mehrerer Kontrolle für ein spezifisches Risiko, sollten aus Effizienz- und Kostenüberlegungen in der Regel eliminiert werden.

Um für identifizierte Risiken in effizienter Weise angemessene und wirksame Kontrollen zu gestalten und zu implementieren bietet sich die Verwendung einer Risiko-Kontroll-Matrix an, die im Folgenden vorgestellt wird. Risiko-Kontroll-Matrizen haben beim Einsatz in der Unternehmung einen doppelten Zweck. Erstens wird den Verantwortlichen ermöglicht, sich ein Gesamtbild über die internen Kontrollaktivitäten zu machen. Dabei sollen Informationen über Teilprozesse und Prozessziele, deren inhärenten Risiken sowie Steuerungs- und Kontrollmassnahmen vorhanden sein. Idealerweise wird auch eine Beurteilung des jeweiligen Restrisikos vorgenommen sowie potentielle Verbesserungsmöglichkeiten aufgezeigt. Zweitens ist die Risiko-Kontroll-Matrix ein wichtiges Instrument für die Dokumentation des IKS und somit ein Hilfsmittel gegenüber dem Abschlussprüfer, das Risikomanagement nachzuweisen.

Die Risiko-Kontroll-Matrix wird als umfassendes Dokument im Sinne eines Risikoinventars bezüglich Kontrollen auf Unternehmensebene, Kontrollen auf der Prozessebene und generelle IT-Kontrollen erstellt. Kontrollfragen auf Unternehmensebene können z.B. sein, ob aktuelle Statuten, ein aufdatiertes Organigramm, Stellenbeschreibungen oder ein Verhaltenskodex vorliegend sind. Auf der Prozessebene sind beispielsweise Kontrollen zur Sicherstellung der vollständigen und richtigen Belastung sämtlicher Warenbezüge, der korrekten Erfassung sämtlicher Umsätze oder der gesetzeskonformen Abrechnung der Mehrwertsteuer auf sämtlichen Umsätzen einzurichten. Generelle IT-Kontrollen beschäftigen sich z.B. mit Fragen des Vorhandenseins von vollständigen Dokumentationen der angewendeten Software und allfälligen Software-Änderungen sowie der Sicherstellung, dass kein unerlaubter Zugriff auf vertrauliche Daten oder Programme erfolgt.

Die Risiko-Kontrollmatrix stellt Risiken und entsprechende Kontrollen in tabellarischer Form gegenüber und zeigt auf, welche Kontrollen welche zuvor identifizierten Schlüsselrisiken in den einzelnen Prozessen abdecken. Je nach Komplexität der Unternehmung, der Quantität sowie der Interdependenzen der einzelnen Risiken muss entschieden werden, wie umfassend eine Risiko-Kontroll-Matrix ausgestaltet werden soll. Beispielsweise ist zu überlegen, welche Attribute einer Schlüsselkontrolle in die Matrix aufgenommen werden sollen. Aus Gründen der Übersichtlichkeit sollte eine Risiko-Kontroll-Matrix jedoch

eher einfach gehalten werden und nur die wesentlichsten Aspekte enthalten; für die detaillierte Dokumentation der Schlüsselkontrollen bieten sich separate Dokumente an.

In ihrer einfachsten Form ist in der folgenden Abbildung ein Beispiel einer Risiko-Kontroll-Matrix aufgeführt. Sie soll lediglich als Grundgerüst für eine dem Unternehmen entsprechend anzupassende Version dienen.

Prozess		Schlüsselrisiko		Kontrollmassnahmen	
Nr.	Beschrieb	Nr.	Beschrieb	Nr.	Beschrieb
1	...	1	...	1	...
2	...	2	...	2	...

Erweitert könnte die abgebildete Risiko-Kontroll-Matrix mit zusätzlichen Spalten wie z.B. der Beurteilung der Kontrolle hinsichtlich Kosten- und Nutzenanalyse, der Kontrollverantwortung (Person bzw. Stellen), etwaigen Schwächen und Verbesserungspotentialen der Kontrolle oder der Typisierung der Kontrolle nach Kriterien wie Automatisierungsgrad und Klassifizierung in detektive sowie präventive Kontrollen.

Fazit

Das im Rahmen der Risikomanagement-Konzeption geplante Kontrollniveau und die mit der Umsetzung von Kontrollmassnahmen anfallenden Kosten sind wichtige Grössen im Rahmen des Risikomanagements, die durch eine Risiko-Kontroll-Matrix systematisch gestaltet und dokumentiert werden können. Durch die Umsetzung von effizienten Kontrollen wird das Kontrollniveau, das von den bestehenden Risiken, vorhandenen Schwachstellen und den Wechselwirkungen mit bereits implementierten Kontrollen abhängt, gesteigert, d.h. die Wahrscheinlichkeit des Eintretens eines Risikos aufgrund einer fehlenden oder nicht wirksamen Kontrolle wird gesenkt.

Literaturquellen

- COSO: Internal Control over Financial Reporting - Guidance for Smaller Public Companies / Committee of Sponsoring Organizations of the Treadway Commission. 2006.
- Münzel, C. ; Jenny, H.: Risikomanagement für kleinere und mittlere Unternehmen. Wegleitung zur Einführung und zum Unterhalt eines Risikomanagement-Systems. Zürich: Schulthess, 2005
- Pfaff, D. ; Ruud, F.: Schweizer Leitfaden zum Internen Kontrollsystem (IKS). Orell Füssli, 2007
- Treuhand-Kammer: Prüfungsstandard zur Prüfung der Existenz des internen Kontrollsystems. Version: 2007.

Prof. Dr. Rautenstrauch und Stefan Hunziker, MScBA

Prof. Dr. Thomas Rautenstrauch ist Dozent und Projektleiter am Institut für Finanzdienstleistungen Zug (IFZ) der Hochschule Luzern Wirtschaft und hat darüber hinaus Lehraufträge an der Universität Fribourg sowie weiteren Universitäten in Deutschland und Finnland. Seine Interessen- und Forschungsschwerpunkte liegen im Bereich IKS / Risikomanagement, International Accounting und Controlling. Stefan Hunziker ist Wissenschaftlicher Mitarbeiter und Doktorand am IFZ und verfügt zudem über Erfahrungen aus mehreren IKS-Projekten. Für weitere Informationen: www.interne-kontrolle.ch