Risikomanagement und Internes Kontrollsystem: Gemeinsamkeiten und Abgrenzung

Mit der Verankerung von zwei tief greifenden regulatorischen Vorschriften bezüglich Internem Kontrollsystem (IKS) und Risikomanagement (Art. 728a, Abs. 1, Ziff. 3 OR sowie Art. 663b, Ziffer 12 OR) sind zwei wesentliche Komponenten der Corporate Governance als verbindlich erklärt worden. Als Folge davon wird in der Literatur und in Fachartikeln Internes Kontrollsystem und Risikomanagement in engen Zusammenhang miteinander gebracht oder die beiden Führungs- und Managementsysteme werden teilweise in Diskussionen um gute Corporate Governance sogar weitgehend synonym verwendet.

Einigkeit besteht heute darin, dass Risikomanagement und Internes Kontrollsystem mindestens Schnittstellen und wesentliche Gemeinsamkeiten und Wechselwirkungen zueinander aufweisen; der Versuch jedoch, eine genaue konzeptionelle Einordnung und Abgrenzung der beiden Konzepte vorzunehmen, fehlt aber bislang weitgehend. Wertet man die bestehende Literatur aus, findet man unterschiedliche Ansätze, Risikomanagement und Internes Kontrollsystem in Relation zu stellen. Tendenziell sind sich die meisten Akteure in diesem Umfeld (zumindest in aktuelleren Beiträgen und Präsentationen) einig, dass IKS ein Subsystem des Risikomanagement mit starken gegenseitigen Abhängigkeiten darstellt. Aus Sicht der Autoren bleibt aber nach wie vor hoher Klärungsbedarf, inwiefern sich diese beiden Konzepte decken oder eben in ihrer Art und Ausprägung unterscheiden. Ohne Zweifel beschäftigen sich sowohl IKS als auch das Risikomanagement mit Risiken, Massnahmen und Kontrollen. Dennoch wäre es falsch, von gleichen oder ähnlichen Führungs- und Managementsystemen zu sprechen. Dieser Beitrag unternimmt den Versuch, hinsichtlich der Problematik der Ein- und Abgrenzung beider Systeme etwas Klarheit zu verschaffen.

Risiko ist nicht gleich Risiko

Zweifelsohne kann man sagen, dass sowohl ein Internes Kontrollsystem als auch ein Risikomanagement dieselben grundsätzlichen Ziele verfolgen: Anhand von adäquaten Massnahmen und Kontrollen sollen die Risiken betrieblichen Handelns auf ein für das Unternehmen akzeptables Niveau verringert werden. Voraussetzung dafür ist das frühzeitige, proaktive Identifizieren von Risken und Chancen und die damit verbundene Kompetenz, diese aktiv und in einer adäquaten Weise zu steuern. Jedoch wird der Risikobegriff im Rahmen der beiden Führungssysteme unterschiedlich interpretiert. Beim Risikomanagement versteht man unter Risiko das Erkennen und aktive Steuern von sowohl möglichen negativen als auch von möglichen positiven Abweichungen von einem Planwert, wobei beim IKS der Risikobegriff enger gefasst wird und lediglich die negativen Abweichungen im Sinne von Schadensbegrenzungen adressiert. Gestützt wird diese Interpretation auch von den beiden Rahmenwerken zu IKS und Risikomanagement vom Committee of Sponsoring Organizations of the Treadway Commission (COSO). Insbesondere das COSO IC (Internal Control), welches sich mittlerweile zum Quasi-Standard für IKS-Projekte entwickelt hat, macht deutlich, dass sich ein Internes Kontrollsystem im Wesentlichen auf eine reine Risikobetrachtung im engeren Sinn stützt. Anders interpretiert das COSO ERM (Enterprise Risk Management) den Risikobegriff, wobei explizit Risiken als auch Chancen angesprochen werden.

Risikoidentifikation und -beurteilung als Basis beider Systeme

An dieser Stelle muss zuerst vorweg genommen werden, dass in diesem Beitrag unter einem IKS ein ganzheitlicher Ansatz verstanden wird, der zusätzlich zum gesetzlichen Minimum der Sicherstellung einer verlässlichen finanziellen Berichterstattung auch die Bereiche Leistungsziele (Operations) als auch die Compliance-Anforderungen miteinbezieht.

Aus Überlegungen bezüglich der Effizienz und Nutzung von Synergien zwischen beiden Konzepten wird hier ein integrativer Ansatz aufgezeigt; das heisst, IKS-Elemente sollen sukzessive in das Risikomanagement-System eingearbeitet werden. Als Ausgangspunkt und Basis zur Implementierung eines Risikomanagement-Systems als auch eines IKS kann die unternehmensweite Risikoidentifikation und -beurteilung gesehen werden. Im Rahmen des klassischen Risikomanagement-Prozesses werden in einem ersten Schritt die Geschäftsrisiken hinsichtlich der Jahresrechnung, den Unternehmens- und Leistungszielen sowie den Compliance-Anforderungen identifiziert und analysiert (der Leser sei zum Vorgehen der Risikoidentifikation auf den früheren Beitrag «Entwicklung und Integration interner Prozesskontrollen» im Praxisforum verwiesen). Besteht das Risikoinventar, müssen die einzelnen Risiken nach ihrer Eintrittswahrscheinlichkeit und dem Schadenausmass beurteilt werden. Diese beiden grundlegenden Prozesse stellen die Basis beider Konzepte dar und sollten keinesfalls voneinander isoliert durchgeführt werden, da dadurch Ineffizienzen oder schlimmstenfalls Kontrolllücken auftreten können.

Abgrenzungen und Schnittstellen zum Risikomanagement

Als wesentliche Aufgaben des Risikomanagements kann die Identifizierung, Bewertung und Ableitung von Massnahmen zur Reduzierung von bedeutenden strategischen wie auch operationellen Risiken gesehen werden. Im Allgemeinen werden vom Risikomanagement solche Risiken adressiert, welche auf sehr hohem Niveau mit unmittelbarem Bezug zu den Unternehmenszielen stehen. Eine zentrale Aufgabe des Risikomanagements sind die im Rahmen der definierten Risikostrategie bestimmten Risiken, die auf Grund ihrer hohen Komplexität nicht alleine durch Kontrollen zu bewältigen sind, sondern ausgewählter Massnahmen bedürfen. An dieser Stelle kann eine erste wesentliche Abgrenzung zum IKS hergestellt werden – die allgemein bekannten Massnahmen der Risikobewältigung (Instrumente zur Risikosteuerung: Vermeiden, Verringern, Teilen oder Akzeptieren von Risiken mit dem Ziel, ein Bündel von Massnahmen zum Anpassen der Risiken an den Risikoappetit der Organisation festzulegen) sind klar dem Risikomanagement zuzuordnen. Da solche Massnahmen im Allgemeinen strategische Risiken mit hoher Komplexität adressieren, kann grundsätzlich gesagt werden, dass ein Internes Kontrollsystem sich nicht mit strategischen Risiken beschäftigt, sondern vorwiegend im operationellen Risikobereich anzusiedeln ist.

Diese Feststellung hat durchaus Implikationen auf den Risikobeurteilungsprozess. Da sich im schnell ändernden Marktumfeld Risiken verändern oder neue Risiken dazukommen und sich dadurch die Rahmenbedingungen zur Erreichung der Unternehmensziele immer neu gestalten, muss die Risikobeurteilung im klassischen Risikomanagement periodisch oder zumindest einmal jährlich neu erfolgen. Im operationellen, vorwiegend prozessorientierten Bereich reicht meist eine ereignisgesteuerte Risikobeurteilung, d.h. einmal zu Beginn im Rahmen der erstmaligen Implementierung eines IKS und anschliessend bei sich verändernden Prozessen oder nach einem Business Process Reengineering. Da operationelle Risiken in der Regel durch Kontrollaktivitäten gemanagt werden können, besteht in diesem Bereich eine erhebliche Schnittstelle zum IKS. Die Definition und Dokumentation von Kontrollaktivitäten in Prozessen oder auch auf Unternehmensebene ist ganz klar dem IKS zuzuordnen und vom Risikomanagement abzugrenzen. Auch auf strategischer Ebene bestehen aber durchaus Schnittstellen zum klassischen Risikomanagement. Obwohl die Massnahmen zur Reduzierung dieser Risiken auf ein tragbares Risiko vom Risikomanagement definiert und überwacht werden, trägt hier das Interne Kontrollsystem dazu bei, mittels Kontrollaktivitäten sicher zu stellen, ob diese Massnahmen auch tatsächlich umgesetzt werden.

Fasst man diese Überlegungen zusammen, kann folgende Abgrenzung zwischen den beiden Systemen festgehalten werden. Risikomanagement befasst sich in erster Linie mit der Steuerung von strategischen Risiken mittels Massnahmen, wobei sich das Interne Kontrollsystem vorwiegend auf Kontrollaktivitäten der operationellen Risiken in den Bereichen operative Effizienz, finanzielle Berichterstattung und Compliance-Anforderungen beschränkt. Beiden Systemen liegt die Risikoidentifikation und – beurteilung zu Grunde, welche aus Effizienzgründen nicht unabhängig voneinander durchgeführt werden sollten oder zumindest aufeinander abgestimmt werden müssen.

Folgt man dem klassischen Risikomanagement-Prozess als Regelkreis weiter, bleibt nach der Identifikation, Beurteilung und Bewältigung der Risiken das Monitoring und das Reporting derselben. Die eingeleiteten Massnahmen aus dem Risikomanagement sowie die definierten und dokumentierten Kontrollaktivitäten aus dem IKS werden durch die Verantwortlichen laufend überwacht und auf deren Effektivität im Hinblick auf die Erreichung der Verbesserungsziele überprüft.

Bezieht man sich bei der Gegenüberstellung von IKS und Risikomanagement auf das Rahmenwerk COSO ERM und berücksichtigt dessen Komponenten, ergibt sich folgende mögliche Analyse der Abhängigkeiten und Abgrenzungen der beiden Systeme:

	Abgrenzung / Synergien zwischen RM und IKS
Internes Kontrollumfeld	**IKS** und **RM:** Das Kontrollumfeld schafft die Kontrollkultur und das Kontrollbewusstsein im Unternehmen und ist zentrale Voraussetzung beider darauf aufbauender Systeme
Risikoidentifikation	**IKS und RM:** Schnittstellen beider Systeme. Die Risikoidentifikation sollte nicht isoliert durchgeführt werden. Falls so geschehen, ist zwingend eine Abstimmung der im IKS und Risikomanagement identifizierten Risiken notwendig.
Zielsetzung	**IKS und RM:** Im Rahmen der für eine Organisation festgelegten Mission oder Vision setzt das Management strategische Ziele fest, bestimmt die Strategie und bricht Ziele auf die Ebenen der Organisation herunter, die in folgende Teilkategorien unterteilt werden können: Strategische Ziele – übergeordnete Ziele, die mit der Mission abgestimmt sind und diese unterstützen → RM definiert Massnahmen zur Risikosteuerung (Vermeiden, Verringern, Teilen oder Akzeptieren von Risiken), IKS überprüft Massnahmen mit Kontrollen Operations – wirksamer und wirtschaftlicher Ressourceneinsatz → IKS definiert Kontrollen Reporting – Zuverlässigkeit der Berichterstattung → IKS definiert Kontrollen Compliance – Einhalten anwendbarer Gesetze und Vorschriften → IKS definiert Kontrollen
Risikobeurteilung	**IKS und RM:** Hohe Synergien beider Systeme. Die Risikobeurteilung stellt einen zentralen Schnittstellenbereich zwischen IKS und Risikomanagement dar und bedarf gegenseitiger Abstimmung.
Ereignisreaktion	**RM:** Eindeutige Aufgaben des Risikomanagements. Bestimmung der Ereignisse (Risikobegriff im weiteren Sinn), welche durch geeignete Steuerungsmassnahmen transferiert oder minimiert werden.

Kontrollaktivitäten	**IKS:** Eindeutige Aufgaben des IKS. Durch Bestimmung und Dokumentation geeigneter Kontrollen in den Bereichen Operations, Reporting und Compliance
Information und Kommunikation	**IKS und RM:** Stufengerechtes Reporting über die Qualität des IKS und RM an die Geschäftsleitung, den Verwaltungsrat bzw. an die interne und externe Revisionsstelle.
Überwachung	**IKS und RM:** Die Gesamtheit des RM und IKS wird überwacht und erforderliche Anpassungen werden vorgenommen. Überwachung wird durch periodische Führungstätigkeiten und separate Beurteilungen erreicht

Schlussfolgerungen

Ein zentrales Element beim IKS ist sicherlich die sorgfältige Dokumentation der Kontrollaktivitäten. Im Rahmen der Existenzprüfung des IKS durch die externe Revisionsstelle sind Unternehmen gezwungen, Kontrollaktivitäten schriftlich nachzuweisen. Diese Kontrollaktivitäten beziehen sich in erster Linie auf operationelle Risiken, da diese im Allgemeinen auf Grund ihres eher niedrigen Komplexitätsgrades durch Kontrollen zu bewältigen sind. Auf strategischer Ebene stellt das IKS Kontrollaktivitäten bereit, um die im Risikomanagement definierten Massnahmen zur Steuerung der Risiken zu überprüfen. IKS und Risikomanagement sind zweifelsohne keine isolierten Systeme, sondern weisen starke gegenseitige Wechselbeziehungen zueinander auf. Internes Kontrollsystem bezieht sich schwerpunktmässig auf negative Abweichungen hinsichtlich Schadensbegrenzung, wobei das Risikomanagement den Risikobegriff im weiter gefassten Sinne interpretiert und sich auch auf Chancen konzentriert. Wechselbeziehungen zwischen beiden Systemen und daraus resultierendem Abbau von Redundanzen sind aus Kosten/Nutzen-Überlegungen wünschenswert und werden durch die aufeinander abgestimmten Risiko-Assessments, Definitionen von Risiko- und Kontrollprozessen, sowie Reportingprozessen erreicht.

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. Weiterhin ist er Gesellschafter und Geschäftsführer des Beratungsunternehmens Editus Consulting in Cham und zugleich Autor zahlreicher Publikationen in den Bereichen Controlling, Risikomanagement und Unternehmensnetzwerke.
Stefan Hunziker, MScBA, Studium der Wirtschaftswissenschaften und Soziologie an der Uni Bern. 2004 - 2007 wissenschaftlicher Mitarbeiter am Institut für Wirtschaftsinformatik der Universität Bern. Ab 2007 Wissenschaftlicher Mitarbeiter im Competence Center Controlling/Accounting am Institut für Finanzdienstleistungen Zug IFZ. Externer Doktorand an der Technischen Universität Darmstadt (D). In Ausbildung zum Fachhochschuldozenten an der Hochschule Luzern. Ab 2008 Lehrtätigkeit an der Hochschule Luzern im Bereich Rechnungswesen, Controlling und Risikomanagement. Dozent und Prüfungsexperte im Modul Management Accounting/Controlling der Schweizerischen Akademie für Wirtschaftsprüfung, sowie Prüfungsexperte an der Schweizerischen Treuhänder Schule STS. Stefan Hunziker ist Verfasser zahlreicher Publikationen zu den Themenfeldern Controlling und Finanzmanagement.