Kontrolle ist gut – Risikomanagement ist besser

Mehr Effizienz für interne Kontrollsysteme durch Enterprise Risk Management

Autor
Rolf Rauchhaus

ist Senior Consultant bei der Gerling Consulting Gruppe GmbH, Köln.

Unter einem Internen Kontrollsystemen (IKS) werden – in Anlehnung an das Institut der Wirtschaftsprüfer (IDW Prüfungsstandard PS 260) – die von der Unternehmensleitung eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen) verstanden, die darauf abzielen, die Entscheidungen der Unternehmensleitung organisatorisch umzusetzen. Sie dienen der Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit, der Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung sowie der Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften. Dabei stehen der Schutz des Vermögens und/oder vorhandener Informationen im Fokus, einschließlich der Verhinderung und Aufdeckung eventueller Vermögensschädigungen.

Die Einrichtung Interner Kontrollsysteme wurde in der Vergangenheit vor allem durch die rechtlichen Verpflichtungen der Unternehmensleitung stark geprägt (etwa durch die Transparenzanforderungen des KonTraG oder die Prüfung der Ordnungsmäßigkeit der Geschäftsführung öffentlicher Unternehmen).

International hat diese Verpflichtung mit der Verabschiedung des US-amerikanischen Sarbanes-Oxley-Acts (SOX) im Juli 2002 besondere Aktualität gewonnen. Hierbei stehen insbesondere die Regelungen gemäß Section 404 SOX (IKS im Finanzberichtswesen) im Fokus der Diskussion. Sämtliche internen Prozesse müssen dokumentiert werden, sofern sie Einfluss auf die Finanzberichterstattung haben können. Entsprechendes gilt für die Kontrollen dieser Prozesse, die zudem prozessunabhängig zu prüfen sind („Testing"). Über die Wirksamkeit interner Kontrollen und eventuelle Lücken oder Schwachstellen im Kontrollsystem hat der Vorstand (CEO, CFO) einmal jährlich zu berichten. Schließlich muss der Abschlussprüfer die Effektivität des Kontrollsystems sowie die Einschätzung des Managements bewerten und testieren. Pflichtverletzungen werden als Straftat qualifiziert und sind – abhängig vom Verschuldensgrad – mit teilweise drastischen Sanktionen belegt.

Entsprechend stehen IKS-Anstrengungen in Unternehmen meist einseitig unter dem Diktat der Haftungsvermeidung. Dieser Motivlage entsprechend dominieren in der Praxis leider eher formalistisch geprägte Ansätze mit einem eindeutigen Schwerpunkt auf der Dokumentation relevanter Prozesse. Die Frage nach der Effizienz oder Risiko-Relevanz von Prozessen und Kontrollen wird bedauerlicherweise viel zu selten gestellt.

Gegenüberstellung der Konzepte „Internes Kontrollsystem" und „Enterprise Risk Management"

Da sie als lästige Pflichtübung empfunden werden, genießen IKS-Themen im Allgemeinen nur eine geringe Aufmerksamkeit des Managements – im Wesentlichen werden sie als „Arbeit für die Revision" angesehen. Das ist vermutlich auch der Grund, warum sich bislang nur wenige wissenschaftliche Arbeiten mit der Verzahnung von IKS und ERM auseinandersetzen. Dabei könnten beide Systeme deutlich voneinander profitieren.

Autor
Dr. Carina Sieler

ist Mitglied der Geschäftsleitung der Gerling Consulting Gruppe GmbH, Köln.

Autor
Knut Sterrenberg

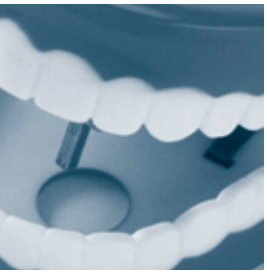
ist Consultant bei der Gerling Consulting Gruppe GmbH, Köln.

Sowohl IKS als auch ERM sind wesentliche Bestandteile einer zukunftsorientierten Unternehmensführung und dienen der nachhaltigen Erreichung und Stabilisierung des Unternehmenserfolges. Gemeinsamkeiten und Unterschiede beider Konzepte und ihr mögliches Zusammenwirken zur Effizienzsteigerung Interner Kontrollen werden daher im Folgenden näher beleuchtet.

Der Nutzen für die Stabilisierung des Unternehmenserfolges hängt wesentlich von den Zielsetzungen der Systeme ab. Schon hierin unterscheiden sich die beiden Konzepte grundsätzlich.

Bei Internen Kontrollsystemen stehen Sicherheits- und Ordnungsmäßigkeitsaspekte im Vordergrund. „Null Fehler" ist die IKS-Maxime. Effizienzaspekte sind nur von untergeordneter Bedeutung; Kontrollen werden unabhängig vom potenziellen wirtschaftlichen Schaden dimensioniert. Wesentlicher Antrieb für Bemühungen im Kontrollsystem sind negative Erfahrungen in der Vergangenheit einerseits und interne und/oder externe Vorgaben (etwa die Grundsätze ordnungsgemäßer Buchführung) andererseits.

Ein ERM hingegen versteht sich als Optimierungsansatz für die Risiko-Situation. Die Erreichung der Unternehmensziele und damit eine langfristige Unternehmenssicherung sollen unter ausdrücklicher Berücksichtigung von Kosten-Nutzen-Aspekten gewährleistet werden. Ein derartiges System ist idealerweise eng mit den unternehmerischen Steuerungsansätzen verzahnt. Die Identifikation von risiko-behafteten Geschäftsbereichen und -prozessen könnte – eine Rückkoppelung zwischen IKS und ERM vorausgesetzt – für die Schwerpunktsetzung von IKS-Arbeiten genutzt werden, so dass kritische Bereiche mit zeitlicher und inhaltlicher Priorität untersucht werden.



Zur Abgrenzung der beiden Systeme dient auch der unterschiedliche Anwendungsbereich. Bei der Betrachtung von Internen Kontrollsystemen stehen in der Regel unternehmensinterne Prozesse (etwa die Erstellung von Einkaufsaufträgen, der Versand von Gütern, die Stammdatenanlage oder der Zahlungsverkehr) im Fokus. Die Untersuchung ausgelagerter Geschäftsprozesse bildet dementsprechend die Ausnahme; dabei haben gerade diese zum Teil erheblichen Einfluss auf das Unternehmen. Unternehmensintern werden erfahrungsgemäß wichtige Primärprozesse (wie Produktion, F&E) ausgeblendet, während administrative Prozesse sehr detailliert beleuchtet werden. Die Untersuchungen betreffen dabei immer den Status quo der Organisation, notwendige Verbesserungen sind statischer Natur. Mit anderen Worten: ein Prozess der kontinuierlicher Verbesserung ist dem IKS-Konzept nicht immanent.

Ein ERM-System umfasst alle Unternehmensbereiche und untersucht sowohl interne als auch externe Einflüsse, die in der Lage sind, die Erreichung der Unternehmensziele zu beeinflussen. Vor allem die (prozess- und abteilungs-) übergreifende Sicht ermöglicht eine Gesamtsteuerung, die das Unternehmen in die Lage versetzen soll, genügend zeitlichen Spielraum zur Ergreifung von Maßnahmen zu schaffen. Diese Maßnahmen sind derart gestaltet, dass ein ähnliches Risiko nicht mehr auftritt oder zukünftig rechtzeitig erkannt wird. So können Kontrollen innerhalb von IKS durchaus konkrete Maßnahmen sein, um einem im ERM-System identifizierten Risiko dauerhaft zu begegnen. Wichtig für ein funktionierendes IKS ist die fortlaufende Kontrolle und proaktive Anpassung an die sich verändernden Bedingungen – einer der Grundpfeiler eines ERM-Systems.

Die Bewertung von Risiken oder Kontrollmängeln erfolgt bei Internen Kontrollsystemen nicht in den von ERM-Systemen bekannten Dimensionen Eintrittswahrscheinlichkeit und Schadenpotenzial. Allenfalls der vermeintliche Schaden wird fallweise zur Priorisierung von Prozessen herangezogen.

Beim ERM hingegen werden die genannten Bewertungsdimensionen einheitlich auf alle Risiken angewandt. Das Schadenpotenzial wird dabei systematisch aus dem GuV-Wertgerüst abgeleitet. Diese Art der Bewertung von Risiken ermöglicht eine effektive Priorisierung von Maßnahmen zur Risiko-Bewältigung. Diese oder eine angepasste Systematik hilft, IKS-Schwerpunkte nach objektiven, wirtschaftlichen Kriterien zu setzen und nicht dem „Bauchgefühl" vertrauen zu müssen. Zudem werden so vielfach die „Augen geöffnet", wenn deutlich wird, dass risiko-behaftete Prozesse andere sind als vielleicht vermutet wurde.

Die Untersuchung bei Internen Kontrollsystemen erfolgt in der Regel prozessorientiert und mit sehr hoher Detailtiefe. Bei den notwendigen Kontrollen ist die Regelungsfreiheit sehr gering, denn viele Kontrollen sind quasi vorprogrammiert, das heißt in einem bestimmten Prozess oder bei einer bestimmten Bearbeitung gelten

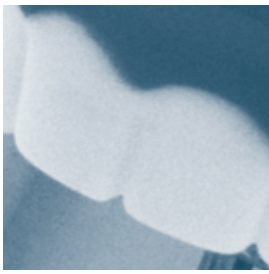


Abb.: Zusammenwirken von IKS und ERM

	Interne Kontrollsysteme	Enterprise Risk Management
Zielsetzung	Sicherheit Ordnungsmäßigkeit Null-Fehler-Prinzip	Erreichen der Unternehmensziele Wirtschaftlicher Risiko-Optimierungsansatz
Anwendungsbereich	Unternehmensinterne Prozesse i. W. administrative (ReWe) Prozesse	Prozessübergreifend in allen Unternehmensbereichen In- und externe Risiken
Betrachtungshorizont	Gegenwartsorientiert reaktiv statisch	Zukunftsorientiert pro-aktiv dynamisch
Bewertungsdimension	Nicht monetär bewertet Eintrittswahrscheinlichkeit wenig relevant	Monetär bewertet nach Eintrittswahrscheinlichkeit, Schadenpotential (abgeleitet aus GuV-Wertgerüst)
Betrachtungsebene & Regelungsfreiheit	prozessorientiert Regelungsfreiheit gering	Mischung aus Aufbau- und Ablauforganisation (hohe) organisatorische und methodische Freiheit

standardisierte Kontrollmechanismen (etwa Funktionstrennung oder Vier-Augen-Prinzip) als probates Mittel.

Für ERM gibt es keinen festen regulatorischen Rahmen. Die anzutreffenden Systeme sind vielfach eine Mischung aus aufbau- und ablauforganisatorischen Regelwerken. Bei der spezifischen Ausgestaltung bestehen im Gegensatz zu Internen Kontrollsystemen hohe organisatorische und methodische Freiheitsgrade.

Die zuvor genannten Abgrenzungsmerkmale zwischen IKS und ERM (vgl. Abb.) verdeutlichen eindrücklich, dass zwischen beiden Konzepten ein essentieller Zusammenhang besteht. Hierbei repräsentiert das ERM grundsätzlich den umfassenderen (Management-)Ansatz, in den ein IKS-System systematisch eingebettet werden sollte. Dass durch eine gezielte Verzahnung beider Themen ein beträchtlicher Zusatznutzen geschaffen werden kann, soll im Folgenden anhand einiger Praxisprobleme konkretisiert werden.

Lessons Learned: Typische Risiko-Fragestellungen aus IKS-Projekten

Die Festlegung der in das Interne Kontrollsystem einzubeziehenden Konzerngesellschaften bereitet vor allem bei komplexen Unternehmensstrukturen vielfach Schwierigkeiten. Oft fehlt ein nachvollziehbarer und plausibler Kriterienkatalog für die Auswahl. Auch sollte sich die Einbeziehung nicht einseitig an Größenmerkmalen (wie etwa ausgewählten GuV- und Bilanzposten oder der Mitarbeiterzahl) orientieren, sondern vor allem das Risiko-Potenzial von Konzerngesellschaften berücksichtigen. Nicht selten bergen auch „kleine" Konzerngesellschaften erhebliche Risiken, etwa weil die Muttergesellschaft über die eigene Beteiligung hinaus Verpflichtungen der Tochter übernommen hat und vielleicht erhebliche technologische und/oder vertriebliche Abhängigkeiten bestehen. Da die Beurteilung der Risiko-Relevanz von Töchtern und Beteiligungen Bestandteil eines guten ERM ist, liegt es nahe, auf diese Bewertungen zurückzugreifen und auch den Geltungsbereich von IKS und ERM zu synchronisieren.

Häufig konzentriert sich die Umsetzung von Internen Kontrollsystemen allein auf die administrativen Geschäftsprozesse, insbesondere im Finanz- und Rechnungswesen. Unter IKS-Aspekten sind aber sämtliche Geschäftsprozesse relevant, welche die Ergebnisse der Finanzberichterstattung nachhaltig/signifikant beeinflussen können. Ein paar Beispiele machen dies deutlich: so sind die Umweltschutz-Experten bei der Rückstellungsbildung für Altlasten einzubinden; der Bereich Sales ist oftmals federführ-

rend bei der Vergabe von Kreditlimiten oder der Fakturierung von Rechnungen; der Personalbereich ist in Vergütungsfragen und die Gehaltsabrechnung involviert; der Einkauf ist für Lieferantenauswahl und -abrechnung verantwortlich. Kaum ein Unternehmen hat bei der SOX-Umsetzung sämtliche Prozesse in den Bereichen Operations/Logistik betrachtet, obwohl Kontrolldefizite auch hier durchaus zu gravierenden Auswirkungen auf die Finanzberichterstattung führen können. So wird etwa bei der in Hochregallagern üblichen so genannten „chaotischen" Lagerhaltung der Untergang der Lagerbestandsdaten eine massive Abwertung von Beständen nötig machen, da die vorhandenen Bestände nur noch unter hohem Zusatzaufwand wirtschaftlich verwertet werden können. Oder ein Anlagenbauer stellt fest, dass Kontrolldefizite beim Prozess der kundenseitigen Abnahme von Großprojekten möglicherweise zu erheblichen Umsatzkorrekturen führen.

Genau genommen darf ein IKS auch nicht an den Unternehmensgrenzen halt machen, vor allem in einer Zeit, in der sich viele Unternehmen immer mehr auf ihr Kerngeschäft zurückziehen. Dementsprechend sollten auch ausgelagerte Geschäftsprozesse mit hoher Risiko-Relevanz kritisch hinterfragt werden. So können bei einem pharmazeutischen Hersteller, der sämtliche Logistikprozesse auf Externe verlagert hat, Defizite im IKS des eingesetzten Logistikdienstleisters zum Untergang von Waren oder einer längeren Betriebsunterbrechung führen – mit entsprechenden Auswirkungen auf Marktpräsenz und Umsatz. Oder ein Finanzdienstleister muss feststellen, dass nach Verlagerung der IT-Services an einen externen Service-Provider die dort bestehende Kontrolldefizite eine Weitergabe sensibler Kundendaten ermöglichen – mit der Folge des Reputationsverlusts und Schadenersatzansprüchen gegen das eigene Haus.

Selbstverständlich ist der jeweilige Dienstleister originär verantwortlich für die Ausgestaltung interner Kontrollen. Aber kann ein IKS darauf „blind" vertrauen – vor allem dann, wenn der Geschäftspartner selbst nicht den strengen IKS-Maßstäben (beispielsweise von SOX) genügen muss? Auch hier kann das unternehmenseigene ERM wichtige Impulse geben. Durch eine systematische Analyse von Counterpartrisiken ist es möglich, wesentliche Abhängigkeiten von externen Dienstleistern zu systematisieren und zu priorisieren. In kritischen Fällen könnte dann – neben anderen Maßnahmen zur Risiko-Steuerung – erwogen werden, strenge Vorgaben mit dem Lieferanten/Dienstleister vertraglich zu vereinbaren und deren Kontrolleffektivität (ähnlich wie bei einem Lieferantenaudit im Rahmen des Qualitätsmanagements) regelmäßig zu testen.

Eine wichtige Herausforderung bei IKS-Projekten besteht darin, die notwendige Kontrollintensität von Geschäftsprozessen kritisch zu hinterfragen. In vielen IKS-Projekten wird beklagt, dass Umfang und Tiefe von Kontrollen nicht oder nicht ausreichend nach dem Risiko-Potenzial von Prozessen differenzieren. Plakativ formuliert: wenn Kontrollintensität und Detaillierungsgrad der Dokumentation eines Supportprozesses (wie etwa der betrieblichen Reisekostenabrechnung oder der Beschaffung von C-Gütern) nach den gleichen Maßstäben erfolgen wie bei einem wichtigen Kernprozess (wie beispielsweise der Debitoren- oder Kreditorenbuchhaltung), leidet nicht nur die Akzeptanz interner Kontrollen, sondern vor allem die Effizienz der Prozesse selbst. Zwar werden in den meisten IKS-Projekten die typischen Risiken generisch erhoben, aber das mögliche Risiko-Ausmaß nicht konsequent monetär bewertet. Es fehlt also in aller Regel die wichtige Zusatzinformation, wie schwerwiegend Kontrolldefizite in einem konkreten Prozess sein können. Hier kann das ERM wesentliche Hilfestellungen geben, sofern dieses konsequent auf die Geschäftsprozesse des Unternehmens ausgerichtet wurde und Risiken entlang der Leistungs- und Unterstützungsprozesse gezielt identifiziert und bewertet werden.

Fazit

In den vergangenen zehn Jahren hat der Ansatz des „Lean Management" interne Kontrollstrukturen Schritt für Schritt aufgeweicht. Nun droht vielen Unternehmen eine hausgemachte „Re-Bürokratisierung" interner Prozesse – von den damit verbundenen Kosten ganz zu schweigen. Nur wenn die IKS-Anstrengungen systematisch auf einem Enterprise-Risk-Management-Ansatz aufsetzen, wird es gelingen, den Blick für das Wesentliche zu schärfen, nämlich Prozessoptimierung und risiko-geleitete Verbesserung der Kontrolleffizienz. ■