

Risikomanagement und Interne Kontrolle für Aufsichtsräte

Neue Herausforderungen und praxisgerechte
Lösungen



Vorwort

Die kontinuierliche Überwachung der Unternehmensführung und eine periodische Evaluierung des Risikomanagement- und Internen Kontrollsystems gehören zu den strategischen Aufgaben des Aufsichtsrates. Nur so können Wirksamkeit und Nachhaltigkeit guter Corporate Governance und eine adäquate Anpassung an das sich dynamisch ändernde Umfeld des Unternehmens sichergestellt werden.

Das Unternehmensrechts-Änderungsgesetz (URÄG 2008) hat diese Aufgaben, insbesondere für Unternehmen, die einen Prüfungsausschuss einzurichten haben, konkretisiert. Aber auch in Unternehmen ohne Prüfungsausschuss entwickelt sich diese Überwachungsfunktion des Aufsichtsrates zu einer wichtigen Kernaufgabe.

Der Aufsichtsrat sollte sich dabei als Coach und Impulsgeber für die Unternehmensleitung verstehen und deren Maßnahmen und Informationen kritisch hinterfragen.

Diese Broschüre wendet sich an Aufsichtsrats- und Prüfungsausschussmitglieder kapitalmarktorientierter und

anderer großer Unternehmen. Sie beleuchtet die aktuellen Herausforderungen in einem turbulenten Wirtschaftsumfeld und zeigt praxisgerechte Lösungen auf.

Viel Erfolg beim Meistern dieser Herausforderungen!

Ihr



Werner Krumm

Partner

Leiter Wirtschaftsprüfung PwC Österreich

Inhalt

Einführung	7
Aufgaben des Aufsichtsrates im Hinblick auf Risikomanagement- und Internes Kontrollsystem	8
Praktische Empfehlungen für die Überwachung durch den Aufsichtsrat	10
Kritisches Hinterfragen des Risikomanagement- und Internen Kontrollsystems durch den Aufsichtsrat	14
Fragenkatalog	16
Fazit	19
Publikationen zum Thema	20
Ansprechpartner	22

Einführung

Auch bedingt durch das Unternehmensrechts-Änderungsgesetz (URÄG 2008) haben viele Unternehmen verstärkt begonnen, ihr Risikomanagement- und Internes Kontrollsystem weiter auszugestalten und zu dokumentieren.

Gerade die aktuelle Wirtschafts- und Finanzsituation erfordert eine laufende effiziente Anpassung der Unternehmensabläufe und steigert die Anforderungen an verlässliche Risikoeinschätzungen und Führungsinformationen. Darüber hinaus ist die Zunahme doloser Handlungen, wie Unterschlagung und wissentliche Manipulation der Finanzberichterstattung, oftmals eine Begleiterscheinung tiefgreifender Wirtschaftskrisen. Zahlreiche aktuelle Fälle bestätigen dies. Dem gilt es nun mehr denn je vorzubeugen.

Daher sollte das Risikomanagement- und Interne Kontrollsystem des Unternehmens verstärkt im Fokus der Aufsichtsräte stehen. Die Aufsichtsräte müssen die strategischen Weichen für eine unternehmensgerechte Weiterentwicklung und Nachhaltigkeit dieser Systeme anstoßen.

Aufgaben des Aufsichtsrates im Hinblick auf Risikomanagement- und Internes Kontrollsystem

Obwohl die tatsächliche Gestaltung und Umsetzung eines Risikomanagement- und Internen Kontrollsystems Aufgabe der Unternehmensleitung ist, ergeben sich auch in diesem Bereich Kernaufgaben für den Aufsichtsrat. Die Vorgaben und Rahmenbedingungen für einen effektiven Aufbau und ein effizientes Funktionieren der Systeme und Prozesse sind durch den Aufsichtsrat zu initiieren und die Umsetzung durch die Geschäftsleitung begleitend zu überwachen.

- **Bestimmung des angemessenen Ansatzes für das Risikomanagement- und Interne Kontrollsystem:** Konzeption von Rahmenbedingungen (in der Praxis häufig in Anlehnung an das COSO Framework) und Vorgabe von Richtlinien für eine praxisgerechte Ausgestaltung der einzelnen Komponenten des Frameworks (im Wesentlichen Zielfestlegung, Ereignisidentifikation, Risikobeurteilung, Risikosteuerung, Kontrollaktivitäten, Information und Kommunikation sowie Überwachung).

- **Entwicklung der Zielsetzung:** Konzeption eines der Struktur, der Organisation und den Geschäftsaktivitäten des Unternehmens angepassten Risikomanagement- und Internen Kontrollsystems. Wichtig ist, dass sich dies zwischen den Polen einer minimalen Erfüllung der gesetzlichen Bestimmungen und eines voll integrierten unternehmensweiten Risikomanagement- und Internen Kontrollsystems bewegt. Die Zielsetzung sollte auch Aussagen zum angestrebten Sollzustand und Reifegrad des Risikomanagement- und Internen Kontrollsystems vorgeben.
- **Überwachung:** Kontinuierliche Überwachung der Unternehmensleitung und regelmäßige Evaluierung des Risikomanagement- und Internen Kontrollsystems mit dem Ziel einer ständigen Optimierung entsprechend den strategischen Zielsetzungen des Unternehmens.

In der Praxis ergeben sich daraus zahlreiche komplexe Herausforderungen für den Aufsichtsrat, diesen Aufgaben gerecht zu werden. Diese betreffen im Wesentlichen:

- Nachhaltigkeit des implementierten Risikomanagement- und Internen Kontrollsystems und seine Anpassung an das sich ständig ändernde Unternehmensumfeld

- Notwendigkeit, sich angesichts eingeschränkter finanzieller Mittel, insbesondere aber auch begrenzter Ressourcen auf das Wesentliche zu fokussieren
- Abhängigkeit von Informationen, die durch die Geschäftsleitung vorbereitet und dem Aufsichtsrat zur Verfügung gestellt werden

Praktische Empfehlungen für die Überwachung durch den Aufsichtsrat

Die Komplexität dieser Herausforderungen erfordert, dass die Aufgaben des Aufsichtsrates im Hinblick auf das Risikomanagement- und Interne Kontrollsystem sachkundig wahrgenommen werden.

Bei kapitalmarktorientierten und „sehr großen“ Kapitalgesellschaften liegt diese Verantwortung bei dem verpflichtend einzurichtenden Prüfungsausschuss. Die Mitglieder des Prüfungsausschusses haben unter anderem die spezielle Aufgabe, die Aktivitäten der Geschäftsleitung kritisch zu hinterfragen und diese als Coach dabei zu begleiten, das Risikomanagement- und Interne Kontrollsystem entsprechend den strategischen Vorgaben kontinuierlich weiterzuentwickeln.

Sofern kein Prüfungsausschuss eingerichtet ist, kann der Gesamt-Aufsichtsrat – unter Umständen gemeinsam mit einer dafür eingesetzten Arbeitsgruppe – diese Verantwortung wahrnehmen.

Weiters sollten Aufsichtsrat oder Prüfungsausschuss mehrere oder alle der folgenden Maßnahmen ergreifen und vorgeben:

Formale, periodische Berichterstattung

Für eine wirksame Überwachung ist eine periodische Berichterstattung durch die Geschäftsleitung an den Aufsichtsrat unerlässlich. Je nach den spezifischen Rahmenbedingungen des Unternehmens kann diese einige wenige Leistungskennzahlen (KPIs) enthalten oder aus einem voll integrierten, automatisierten Überwachungssystem bestehen. Die Berichterstattung sollte dabei insbesondere auch einen regelmäßigen Soll-Ist-Vergleich beinhalten. Zusätzlich ist ein aktualisierter Maßnahmenkatalog zu präsentieren, wie – und bis wann – die Lücken zum Sollzustand geschlossen werden.

Self-Assessment

Die einzelnen Unternehmensbereiche sollten regelmäßig selbst die Verlässlichkeit und den Reifegrad der jeweils für sie relevanten Teilbereiche des Risikomanagement- und

Internen Kontrollsystems einschätzen. Dabei müssen auch potenzielle Schwierigkeiten mit Systemen und Prozessen erhoben und beurteilt sowie Vorschläge für eine effizientere Ausgestaltung des Risikomanagement- und Internen Kontrollsystems entwickelt werden. Besonderes Augenmerk sollte dabei auf die für das Unternehmen kritischen operativen Bereiche gelegt werden.

Unternehmensinterne Überprüfung und Austausch von „Best Practices“

Periodische unabhängige Überprüfungen des Risikomanagement- und Internen Kontrollsystems durch eine spezifische Funktion des Unternehmens, insbesondere durch die Interne Revision oder eine Compliance-Funktion, lassen Rückschlüsse auf die Nachhaltigkeit und den Reifegrad des gelebten Risikomanagement- und Internen Kontrollsystems zu. Daraus können auch gute Erfahrungen aus einem Unternehmensteil für andere Bereiche im Sinne eines Austausches von Best Practices genutzt werden.

Nutzung der Ergebnisse der Abschlussprüfung

Wesentliche Schwächen im Internen Kontrollsystem fallen unter die Redepflicht des Abschlussprüfers. Geschäftsleitung und Aufsichtsrat sind darüber unverzüglich zu unterrichten.

Darüber hinaus empfiehlt es sich, auch wenn keine wesentlichen Schwächen festgestellt wurden, den Abschlussprüfer zu seiner Einschätzung des Risikomanagement- und Internen Kontrollsystems und zu Verbesserungsvorschlägen zu befragen.

Der Abschlussprüfer bietet sich daher als unabhängiger Ansprechpartner für den Aufsichtsrat in allen Fragen rund um das Risikomanagement- und Interne Kontrollsystem an. Allerdings gilt die Einschränkung, dass der Fokus der Abschlussprüfung auf jenen, für die Finanzberichterstattung relevanten Risiken und internen Kontrollen liegt, deren Beurteilung für die Erlangung eines Prüfungsurteils notwendig ist. Risiken und interne Kontrollen hinsichtlich strategischer, operationeller und Compliance-Ziele sind nicht das unmittelbare Ziel einer Abschlussprüfung. Da der Abschlussprüfer aber häufig fundiertes Prozess- und Risikowissen über die Finanzberichterstattung hinaus besitzt, kann er über gesonderte Aufträge in den genannten Bereichen wertvolle Analysen durchführen.

Spezifische Evaluierung durch unabhängige Experten

Weiters kann der Aufsichtsrat auch gezielt Aufträge an unabhängige Experten vergeben, um spezifische Evaluierungen

des Risikomanagement- und Internen Kontrollsystems einzelner Unternehmensbereiche durchführen und Verbesserungsvorschläge entwickeln zu lassen. Der Österreichische Corporate Governance-Kodex verlangt sogar diese Evaluierung durch den Abschlussprüfer. Zu empfehlen ist ein proaktives Vergeben solcher Evaluierungen, ehe das Eintreten negativer Vorfälle diese nötig werden lassen. Leider ist in der Praxis aber meist ein reaktives Verhalten zu beobachten, nachdem es in Unternehmensabläufen zu erheblichen Problemen (z.B. wesentliche Fehler in der Finanzberichterstattung, Forderungsverluste, Betrug) gekommen war.

Kritisches Hinterfragen des Risikomanagement- und Internen Kontrollsystems durch den Aufsichtsrat

Um die Unternehmensleitung angemessen als Coach begleiten und überwachen zu können, sollte der Aufsichtsrat stets die Einschätzung des Risikomanagement- und Internen Kontrollsystems seitens der Unternehmensleitung kritisch hinterfragen. Gleiches gilt für sämtliche diesbezüglichen Informationen, die ihm seitens der Unternehmensleitung präsentiert werden.

In bestimmten Situationen, insbesondere dann wenn sich der Aufsichtsrat sonst kein umfassendes Bild verschaffen kann, ist auch die direkte Befragung bestimmter Mitarbeiter in Stabsfunktionen (z.B. aus den Bereichen Finanzwesen, Recht, Steuern oder IT) oder aus der Linie (z.B. Leiter Produktion, Einkauf oder Verkauf wesentlicher Tochtergesellschaften) möglich.

Der folgende Fragenkatalog soll dem Aufsichtsrat für diese anspruchsvolle Aufgabe Anregungen geben. Selbstverständlich können diese Fragen auch für die Diskussion des Aufsichtsrats mit der Internen Revision und dem Abschlussprüfer herangezogen werden. Sie können gleichzeitig auch dazu dienen, sich auf allfällige Fragen der Gesellschafter an den Aufsichtsrat vorzubereiten.

Fragenkatalog

Fragen zum Risikomanagement- und Internen Kontrollsystem

- Wurde eine umfassende Risikoanalyse und -bewertung für das Gesamtunternehmen durchgeführt beziehungsweise aktualisiert?
- Werden durch das Risikomanagementsystem alle Risikokategorien (strategische und operative Ziele, Ziele hinsichtlich der Finanzberichterstattung sowie Compliance-Ziele) abgedeckt?
- Wie ist das Interne Kontrollsystem in das unternehmensweite Risikomanagementsystem integriert?
- Wie werden ablauf- und aufbauorganisatorische Anforderungen sowie die entsprechenden Kontrollen (z.B. die Trennung kritischer Funktionen und Tätigkeiten) in den wesentlichen IT-Systemen umgesetzt?
- Wie werden die unternehmensspezifischen Kontrollanforderungen bei ausgelagerten Dienstleistungen (z.B. IT-Betrieb, Logistik) sichergestellt?
- Wurden aus der Risikobeurteilung angemessene Maßnahmen zur Risikobewältigung, insbesondere Anpassung des Internen Kontrollsystems, abgeleitet?

- Kennen Sie den aktuellen Status der Umsetzung dieser Maßnahmen?
- Welche Prioritäten sieht die Unternehmensleitung hinsichtlich kontinuierlicher Verbesserung des Risikomanagement- und Internen Kontrollsystems in den Folgeperioden?
- Welche weitergehende Automatisierung der Abläufe und Kontrollen bietet sich an beziehungsweise welche Effizienzgewinne in diesen Bereichen strebt die Unternehmensleitung an?
- Hat die Unternehmensleitung die Ergebnisse der Internen Revision und des Abschlussprüfers – sowie gegebenenfalls unabhängiger Spezialisten – mit diesen diskutiert und eventuell festgestellte Schwächen im Risikomanagement- und Internen Kontrollsystem und diesbezügliche Verbesserungsvorschläge in ihrem Maßnahmenkatalog berücksichtigt?
- Welche allgemeinen Vorgaben (z.B. Code of Conduct) gibt es und wie lebt die Unternehmensleitung die Einhaltung von Abläufen und Kontrollen vor?
- Wie schätzt die Unternehmensleitung das Kontrollbewusstsein der Mitarbeiter ein?
- Reichen die vorhandenen Kontrollen, um eventuelle dolose Handlungen wie Unterschlagung und Manipulation der Finanzberichterstattung von Mitarbeitern zu verhindern? Oder zumindest zeitnah aufzudecken?

Fragen eines jeden Aufsichtsrats an sich selbst

- Kann ich mich auf das Risikomanagement- und Interne Kontrollsystem des Unternehmens und auf die darauf basierenden Informationen der Unternehmensleitung verlassen?
- Sind die erhaltenen Informationen konsistent mit meinem sonstigen Wissen über das Unternehmen, das Umfeld und die Branche?
- Wäre ich überrascht, morgen von einem Betrugsfall im Unternehmen informiert zu werden?
- Bin ich mir bewusst, was ich alles nicht weiß, aber eventuell wissen sollte, um die Verlässlichkeit und Qualität des Risikomanagement- und Internen Kontrollsystems beurteilen zu können?
- Was würde ich auf diesbezügliche Fragen der Gesellschafter antworten können?

Fazit

Das Thema Risikomanagement- und Internes Kontrollsystem wird den Aufsichtsrat dauerhaft begleiten. Im Sinne guter Corporate Governance, aber auch einer angestrebten Business Excellence sollte der Aufsichtsrat es daher als seine Aufgabe betrachten, als Coach und Impulsgeber der Unternehmensleitung zu agieren. Es gilt, das Risikomanagement- und interne Kontrollsystem nachhaltig an das sich permanent ändernde Unternehmensumfeld anzupassen und angemessene Optimierungspotenziale zu realisieren.

Publikationen zum Thema

Fragen des Aufsichtsrates an den Abschlussprüfer Anregungen und Herausforderungen

Anregungen für den Aufsichtsrat, um das nachhaltige Verständnis des Abschlussprüfers für die Geschäftstätigkeit des Unternehmens und sein Umfeld zu überprüfen.

Aufsichtsrat von A bis Z

Praktisches Nachschlagewerk mit den wichtigsten Themen der Aufsichtsratsmitglieder.

Der Prüfungsausschuss

Praxisleitfaden zur effizienten Überwachung

Rahmenbedingungen für die Bildung eines Prüfungsausschusses und deren Tätigkeit sowie Darstellung von Best Practices.

Interne Revision

Überwachung und Nutzen für Aufsichtsorgane

Aufgaben und Verantwortlichkeiten des Aufsichtsrates in der Internen Revision sowie Abhandlungen zu den wichtigsten Fragen der Informationsbeschaffung.

IFRS für Aufsichtsräte

Überblick und Leitfaden für die Überwachung

Grundlegender Überblick zu einzelnen wesentlichen Bilanzierungsfragen rund um die immer wichtiger werdende IFRS-Berichterstattung.

Nachhaltigkeit und Unternehmensverantwortung

Gemeinsame Pflichten und neue Herausforderungen

Als Kontrollorgan kommt hierbei gerade dem Aufsichtsrat eine besondere Bedeutung zu.

Kostenlose Bestellung bei Ulrike Hammer

Tel.: +43 1 501 88-5101

E-Mail: ulrike.hammer@at.pwc.com

www.pwc.com/at/Publikationen

Ansprechpartner

WP/StB Dr. Aslan Milla

Partner

Tel.: +43 1 501 88-1700

Fax: +43 1 501 88-623

aslan.milla@at.pwc.com

Mag. Markus Ramoser

Unternehmensweites Risikomanagement

Tel.: +43 1 501 88-2129

Fax: +43 1 501 88-641

markus.ramoser@at.pwc.com

PwC PricewaterhouseCoopers GmbH

Erdbergstraße 200

1030 Wien

www.pwc.at

Mit PricewaterhouseCoopers wird das Netz der Mitgliedsunternehmen von PricewaterhouseCoopers International Limited bezeichnet. Jedes Mitgliedsunternehmen ist eine eigenständige und unabhängige juristische Person.

www.pwc.at

© 2010 PricewaterhouseCoopers. Alle Rechte vorbehalten.