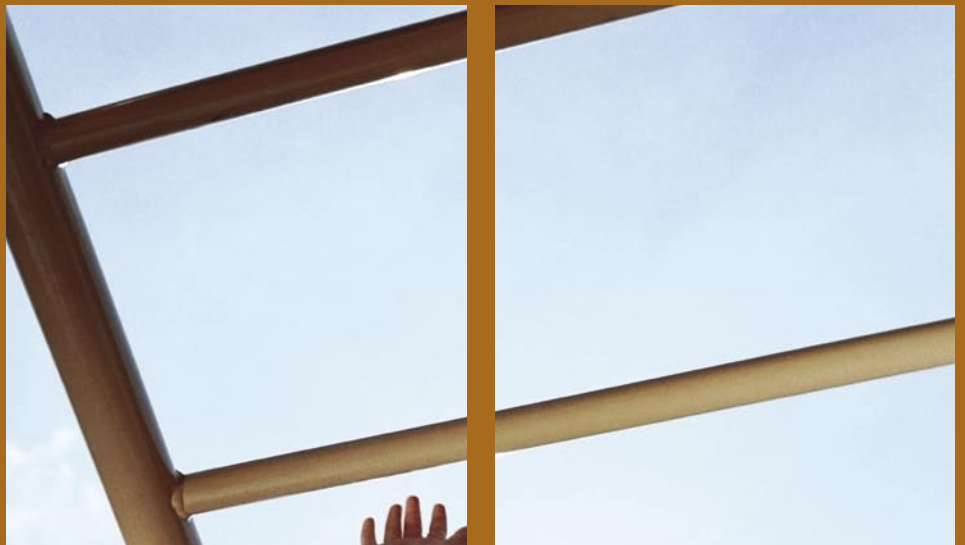


# PwC Financial Services\*

Banken · Fonds · Real Estate · Versicherungen

Ausgabe 51, April 2009

Risikomanagement und internes Kontrollsystem bei Versicherungen



# Risikomanagement und internes Kontrollsystem bei Versicherungen

Versicherungen haben ein internes Kontrollsystem zu führen, das den Anforderungen des Unternehmens entspricht. Sie haben ferner Prozesse zur Identifikation, Bewertung und Steuerung der Risiken einzurichten, um die dauernde Erfüllbarkeit der Verpflichtungen aus Versicherungsverträgen sicherzustellen.

Mit einer am 1. Jänner 2008 in Kraft getretenen VAG-Novelle wurden unter anderem die Bestimmungen zum Prüfungsausschuss neu gefasst. Nunmehr gehört zu den Aufgaben des Prüfungsausschusses auch die Überwachung der Wirksamkeit des internen Kontrollsystems, der Internen Revision und des Risikomanagements.

Grundlage für die Überwachungstätigkeit des Aufsichtsrates kann nur eine ausreichende Dokumentation des Risikomanagements (RM) und des internen Kontrollsystems (IKS) sein. Auch der Versicherungsverband (VVO) hält es für wesentlich und unumgänglich, dass eine durchgängige Dokumentation aufgebaut und ein Vorgehen zur Überwachung der Wirksamkeit eingerichtet werden.

## Bedeutung von RM und IKS

RM und IKS sind wichtige Führungsinstrumente eines Unternehmens. Zwar verfügen viele Firmen von jeher über ein RM und IKS, doch sind die Anforderungen der verschiedenen Interessengruppen an die internen Kontrollen, das RM und deren Prüfung in den letzten Jahren stark gestiegen. Neben externen Interessengruppen, die ein wirksames RM und IKS zunehmend als wesentlichen Bestandteil guter Corporate Governance betrachten, benötigen auch der Aufsichtsrat und die Geschäftsleitung verlässliche Informationen über die Zuverlässigkeit und die Wirksamkeit des RM und IKS.

## Definition, Ziele und Verantwortung

Risiken sind Ereignisse und mögliche Entwicklungen innerhalb und außerhalb des Unternehmens, die sich negativ auf die Erreichung der Unternehmensziele auswirken können. Unter RM versteht man die Gesamtheit aller organisatorischen Regelungen und Maßnahmen zur Risikoeerkennung und zum Umgang mit den Risiken unternehmerischer Betätigung.

Unter IKS versteht man die Gesamtheit aller von der Geschäftsleitung angeordneten Vorgänge, Methoden und Maßnahmen (Kontrollmaßnahmen), die dazu dienen, einen ordnungsgemäßen Ablauf des betrieblichen Geschehens sicherzustellen. Die organisatorischen Maßnahmen der internen Kontrolle sind in die Betriebsabläufe integriert, das heißt, sie erfolgen arbeitsbegleitend oder sind den Arbeitsgängen unmittelbar vor- oder nachgelagert. Interne Kontrollen sind Maßnahmen, die aus der Überwachung und Beurteilung von Risiken abgeleitet werden. Demzufolge ist das IKS ein integraler Bestandteil eines unternehmensweiten Risikomanagements; es trägt dazu bei, die Einhaltung der unternehmerischen Ziele zu gewährleisten. Während das IKS gegenwarts- und vergangenheitsorientiert ist, richtet sich das RM auch in die Zukunft indem mögliche Entwicklungen berücksichtigt und eingeschätzt werden.

Es liegt in der Verantwortung des Aufsichtsrates, das Unternehmen und die Geschäftsleitung zu überwachen und sicherzustellen, dass Risiken, die unternehmerische Ziele gefährden können, rechtzeitig erkannt und angemessene Maßnahmen eingeleitet werden. Die Überwachung des RM und des IKS ist Teil dieser Verantwortung.

Zur Wahrnehmung seiner Überwachungsfunktion muss der Aufsichtsrat die Qualität des RM und des IKS regelmäßig mit der Geschäftsleitung erörtern. In größeren Unternehmen unterstützt in der Regel die Interne Revision den Aufsichtsrat und die Geschäftsleitung bei der Beurteilung des RM und des IKS.

## Komponenten von RM und IKS

Die Anforderungen an ein IKS wurden in verschiedenen Rahmenwerken beschrieben. Das Bekannteste ist das „COSO - Internal Control Framework“. COSO gliedert den Inhalt und den Aufbau eines IKS in Komponenten, deren Zusammenwirken gewährleisten soll, dass die Ziele des IKS erreicht werden. Das Rahmenwerk wurde 2004 mit COSO II „Enterprise Risk Management – Integrated Framework“ erweitert. COSO II baut auf dem ursprünglichen Konzept auf und fokussiert noch stärker auf ein an den Unternehmenszielen ausgerichtetem unternehmensweitem Risikomanagement.

## Dokumentation von RM und IKS

Die IKS-Dokumentation konzentriert sich häufig auf die COSO-Komponente „Kontrollaktivitäten“. Die übrigen Komponenten des Rahmenwerks dürfen aber unter keinen Umständen vernachlässigt werden. Diese sind:

- Kontrollumfeld (Control Environment)
- Risikobeurteilung (Risk Assessment)
- Information und Kommunikation (Information & Communication)
- Überwachung (Monitoring)

Diese vier Komponenten haben einen starken Einfluss auf die Effektivität von einzelnen Kontrollaktivitäten, die in den jeweiligen Prozessen ausgeführt werden. Sind die Komponenten unzureichend ausgestaltet, können prinzipiell wirksame Kontrollaktivitäten in ihrer Ausführung beeinträchtigt werden oder ineffektiv sein.

Aufgrund unterschiedlicher Verantwortungen hat es sich in der Praxis bewährt, die Dokumentation des RM und des IKS wie folgt zu strukturieren:

- Dokumentation der Rahmenbedingungen des IKS (z.B. in Form einer IKS-Richtlinie in der die Verantwortung und die organisatorische Ausgestaltung des IKS festgelegt sind)
- Dokumentation der wesentlichen Prozesse und Kontrollen (z.B. in Form einer Prozesslandkarte, Flowcharts und Kontrollmatrizen)
- Dokumentation des Risikomanagementprozesses (z.B. in Form einer RM-Richtlinie)

## Dokumentation der Prozesse und Kontrollen

Die vollständige Beschreibung eines IKS soll die Angemessenheit des Systems in Bezug auf die zu erreichenden Kontrollzwecke sicherstellen und ist Voraussetzung für die Beurteilung seiner Wirksamkeit. Hierfür ist eine grafische und/oder textliche Abbildung der Prozesse einschließlich Kontrollen sinnvoll. Die verschiedenen gesetzlichen oder regulatorischen Anforderungen enthalten hierzu keine detaillierten Vorschriften. So bleibt es der Geschäftsleitung überlassen, einen dem Unternehmen entsprechenden Dokumentationsstandard zu definieren.

## Prozesslandkarte als Rahmenwerk der Dokumentation

Für die Darstellung empfiehlt sich die Verwendung einer Prozesslandkarte. Sie bildet auf der oberen Detaillierungsebene den Gesamtprozess ab. Abbildung 1 zeigt eine mögliche Prozesslandkarte.

### Detaillierungsgrad der Dokumentation

Die Prozesslandkarte stellt eine Orientierungshilfe zur Dokumentation der Prozesse dar. In der praktischen Anwendung ist nun zu entscheiden, welcher Detaillierungsgrad zu wählen ist.

Der für die Darstellung eines Prozesses bzw. Teilprozesses zu wählende Detaillierungsgrad hängt von seiner Bedeutung und den Risiken, die aus diesem Prozess oder Teilprozess resultieren, ab. Für Prozesse oder Prozessteile, aus denen kein signifikantes Risiko resultiert, genügt die Dokumentation auf einer relativ hohen Ebene. Wir empfehlen interne Kontrollen gesondert als solche zu kennzeichnen.

Da kein Format für die Dokumentation vorgeschrieben wird, sind bereits im Konzern verfügbare Dokumentationen und Dokumentationsstandards auf ihre Eignung für das IKS zu überprüfen. Aus Effizienzgründen empfehlen wir bei der Auswahl einer Methode für die Detaildokumentationen auf das Know-how externer Experten für Prozess- und Kontrollmodellierung zuzugreifen.

### Dokumentation bestehender Prozesskontrollen

Zusätzlich zur Detaildokumentation der Prozessschritte empfehlen wir eine getrennte Dokumentation der internen Kontrollen. Kontrol-

len stellen Prozessaktivitäten mit einer speziellen Zielsetzung dar. Sie sollen bestehende Risiken kompensieren und einen ordnungsgemäßen Prozessablauf sicherstellen. Die Dokumentation der Kontrolle muss übersichtlich und strukturiert sein. Als Darstellungsform empfehlen wir eine Kontroll-Matrix, die dann als Übersicht für die Beurteilung der internen Kontrollen genutzt werden kann. In der Praxis hat sich bewährt, die Kontrollmatrix um die jeweiligen Risiken zu erweitern. Dies zeigt, welche identifizierten Risiken durch Kontrollen tatsächlich bzw. nicht abgedeckt werden. Abbildung 2 stellt beispielhaft eine solche Risiko-Kontroll-Matrix dar.

Um die Zuordnung von Risiko-Kontroll-Matrizen zu den Detail-Prozessdokumentationen zu ermöglichen, schlagen wir eine einheitliche Kontrollreferenz je Kontrolle in beiden Dokumenten vor.

### Dokumentation des Risikomanagementprozesses

Neben den in den Prozessen integrierten Kontrollen ist es im Sinne eines umfassenden Risikomanagements auch erforderlich, mögliche Risiken und ihren Einfluss auf die Zielerreichung des Unternehmens zu berücksichtigen. Zu diesem Zweck ist es erforderlich einen standardisierten Prozess mit klar definierten Verantwortungen einzurichten. In einer periodischen Risikoberichterstattung an die Geschäftsleitung werden die wesentlichen Risiken anhand der vom

Management festgelegten Kriterien berichtet. Dabei sind auch die versicherungstypischen Risikoklassen mit zu berücksichtigen (versicherungstechnisches Risiko, Kreditrisiko, Marktrisiko, operationales Risiko, ...).

Eine sorgfältige Dokumentation des IKS und RM ist auch eine ausgezeichnete Grundlage für die Erfüllung der Anforderungen von Säule II gemäß Solvency II. Ergänzend zu den Leitlinien zum RM vom Versicherungsverband raten wir die von der BaFin in Deutschland veröffentlichten Mindestanforderungen an das RM von Versicherungsunternehmen (MaRisk VA) zu beachten und entsprechend zu dokumentieren.

Abbildung 1: (Quelle: PwC – Systems and Process Assurance)

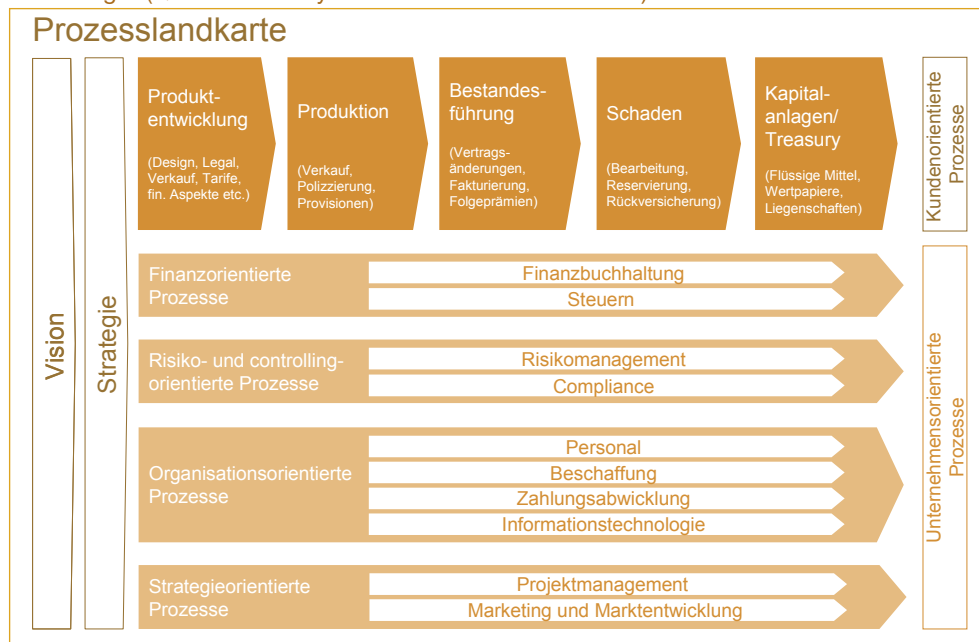


Abbildung 2: (Quelle: PwC – Systems and Process Assurance)

	Risikoinventar			Kontrollinventar																				
	Risikobeschreibung	Beurteilung		Kontrolle	Risikoabdeckung	Kontrollziele					Art der Kontrolle	Verantwortlich	Kontrollfrequenz	IT Anwendung										
Teilprozess	Beschreibung der Risiken	Schadensausmaß Eintrittswahrscheinlichkeit	Risikokennzahl	Nr. Beschreibung der Kontrolle (Input, Tätigkeit; Output inkl. der nachvollziehbare Nachweis der Kontrollausführung)	Operationelle Risiken	Strategische Risiken	Compliance Risiken	Financial Reporting Risiken	Darstellung & Offenlegung	Periodengerechte Abgrenzung	Existenz / Vorhandensein	Rechte und Pflichten	Richtigkeit der Transaktion/Daten	Bewertung	Vollständigkeit	Restricted Access	Defektive Kontrollen	Präventive Kontrollen	Programmierte Kontrollen	Manuelle Kontrollen		Q = Quartal / J = Jährlich	L = Laufend / T = Täglich W = Wöchentlich M = Monatlich	
1. Schaden eröffnen	Nicht- oder nicht korrekte Erfassung eines Schadens.	mittel		1.1 Durchführung geeigneter Auswertungen, zur Erkennung von Backlogs.	X		X	X	X	X	X			X			X				Leiter Schaden	L		Schaden-Anwendung
				1.2 Automat. Plausibilitäts-tests: Automat. Kontrollen, dass die erfassten Daten vorgegebene Kriterien erfüllen und vollständig sind. Bei nicht ausgefüllten obligatorischen Feldern ist die Weiterbearbeitung nicht möglich.		X		X							X	X		X	X				Leiter Schaden	L



## Zum Autor

Josef Renner

Mag. Josef Renner ist als Wirtschaftsprüfer bei PricewaterhouseCoopers tätig. Er ist Senior Manager in der Abteilung Systems and Process Assurance und verfügt über 15 Jahre Erfahrung in der Durchführung und im Management von Implementierungs- und Prüfungsprojekten im Bereich Risikomanagement und Interne Revision, Sarbanes Oxley, COSO I / COSO II, COBIT, ITIL und ähnlicher Rahmenwerke als auch in der Jahresabschlussprüfung nach HGB und IFRS. Im Bereich der Versicherungen hat Herr Renner insbesondere Erfahrung im Aufbau und der Durchführung von Internen Revisionen im Outsourcing.

## Tipps

### Nützliche Links

International anerkanntes Rahmenwerk für Risikomanagement und Interne Kontrolle

[www.coso.org](http://www.coso.org)

Leitlinien zum Risikomanagement in Versicherungsunternehmen

[www.vvo.at/mitgliederleitlinien](http://www.vvo.at/mitgliederleitlinien)

Rundschreiben 3/2009

Aufsichtsrechtliche Mindestanforderungen an das Risikomanagement (MaRisk VA)

[www.bafin.de](http://www.bafin.de)

Solvency II

[www.pwc.com/solvencyII](http://www.pwc.com/solvencyII)

Broschüre „Bereit für Solvency II?“

Praktische Umsetzung von Solvency II im Unternehmen

[www.pwc.at/publikationen](http://www.pwc.at/publikationen) – Thema: Financial Services

Rundschreiben des VVO zur Umsetzung des URÄG 2008 –

Überwachungsaufgaben des Aufsichtsrates vom 18. Sept. 2008

## Themenvorschau

### Thema der nächsten Ausgabe

#### Special Purpose Acquisition Companies (SPACs)

Auf einer Sonderkonferenz der Europäischen Kommission im Februar 2009, wurden auf breiter Front härtere Regeln für Private Equity Firmen gefordert. Dies deshalb, weil diese nicht genügend Transparenz bieten und nicht in der Lage wären durch Mechanismen, wie den code of conduct sich selbst zu regulieren.

Eine mögliche Antwort auf eine verbesserte Form des Private Equity's bieten SPACs. SPACs sind Unternehmenshüllen ohne operative Tätigkeit, die nach ihrem Initial Public Offering nur ein Ziel verfolgen, eine Unternehmensübernahme durchzuführen. Da SPACs der Börsenaufsicht unterliegen, sind sie transparent und bieten dem Anleger besondere Mitspracherechte. Im deutschsprachigen Raum relativ unbekannt, machten sie 2007 in den USA bereits 22 % aller IPOs aus. Seit ihrem Geburtsjahr 2003, haben Sie kumuliert ein Emissionsvolumen von 21 Mrd. US-Dollar generiert. Dieses in Europa noch relativ wenig eingesetzte Vehikel wird näher dargestellt.

## [www.pwc.at](http://www.pwc.at)

Medieninhaber und Herausgeber: PwC PricewaterhouseCoopers, Erdbergstraße 200, 1030 Wien

Für den Inhalt verantwortlich: Mag. Andrea Cerne-Stark, [andrea.cerne-stark@at.pwc.com](mailto:andrea.cerne-stark@at.pwc.com)

Für Änderungen der Zustellung verantwortlich: Lucija Dzojic, [lucija.dzojic@at.pwc.com](mailto:lucija.dzojic@at.pwc.com), Tel.: 01/501 88-3602, Fax: 01/501 88-648

Der Inhalt dieses Newsletters wurde sorgfältig ausgearbeitet. Er enthält jedoch lediglich allgemeine Informationen und spiegelt die persönliche Meinung des Autors wider, daher kann er eine individuelle Beratung im Einzelfall nicht ersetzen. PwC übernimmt keine Haftung und Gewährleistung für die Vollständigkeit und Richtigkeit der enthaltenden Informationen und weist darauf hin, dass der Newsletter nicht als Entscheidungsgrundlage für konkrete Sachverhalte geeignet ist. PwC lehnt daher den Ersatz von Schäden welcher Art auch immer, die aus der Verwendung dieser Informationen resultieren, ab.