



2010 – AUSGABE 1/6 **agens Audit & Risk Newsletter**

Informationen zu Revision,
Risikomanagement und Trainings

agens – gedacht, getan

AKTUELLES

Liebe agens Newsletter Leserinnen und Leser,

ich freue mich, Sie zur 1. Ausgabe des agens Audit & Risk Newsletters im Jahre 2010 begrüßen zu dürfen. Ich hoffe, dass Sie einen guten Start ins neue Jahr hatten und die vor Ihnen liegenden Aufgaben erfolgreich bewältigen werden.

Die neuen gesetzlichen Anforderungen und ein sich ständig änderndes Umfeld stellen immer wieder neue Herausforderungen an die Wahrnehmung unserer Aufgaben dar. Schließlich ist es wichtig, stets auf dem aktuellen Stand der gesetzlichen und regulatorischen Anforderungen zu sein. Unser Newsletter soll Ihnen dabei helfen, den nötigen Überblick zu erhalten und Anregungen für die tägliche Arbeit zu finden.

Ich wünsche Ihnen eine angenehme Lektüre.



Christof Merz
(Geschäftsbereichsleiter)



Agenda

Schwerpunktthema	3
IT Forensik im Rahmen einer Sonderuntersuchung	3
Aktuelles.....	8
Risikomanagement von Investmentgesellschaften	8
Compliance für Investmentgesellschaften	11
InvMaRisk und die Anforderungen an die Interne Revision	12
InvMaRisk Anforderungen an Notfallkonzept	14
Gesetzesentwurf des Bundeskabinetts zur Überwachung von Ratingagenturen	15
Anforderungen an Vergütungssysteme	17
Anforderungen und Pflichten der Mitglieder der Verwaltungs- und Aufsichtsorgane	19
Fraud-Seminare 2010	21
Literatur	22
Seminartermine	23
Microsoft Excel.....	23
Who is Who	26
Impressum.....	27

IT Forensik im Rahmen einer Sonderuntersuchung

Ausgangslage

In den letzten zwei Jahren wurde international nahezu jedes zweite Unternehmen Opfer eines Wirtschaftsdelikt. Keine Branche blieb von Wirtschaftskriminalität verschont. Der Finanzsektor, Handel und Telekommunikation stehen an der Spitze der betroffenen Sparten. Die Risikolage wird zu selten realistisch eingeschätzt. Entsprechend gering sind die Investitionsbereitschaft und das Engagement zur Prävention.

Integraler Bestandteil nahezu allen gesellschaftlichen und unternehmerischen Handelns ist die Informationstechnologie. Aus dem steten Fortschritt ergeben sich immer neue und weitreichendere Potenziale für dolose und deliktische Handlungen.

Unter dolosen Handlungen versteht man Bilanzmanipulationen, Untreue, Unterschlagung und zum Schaden des Unternehmens absichtlich durchgeführte Handlungen. Den Begriff Delikt verwendet der Kriminologe für alle im weitesten Sinne strafrechtlichen Verfehlungen. Als gesetzliche Grundlagen sind die §§ 242 ff. StGB zu berücksichtigen, die auf die Straftatbestände Diebstahl, Unterschlagung, Geldwäsche, Betrug, Subventionsbetrug, Untreue, Urkundenfälschung, Bestechlichkeit und Bestechung im geschäftlichen Verkehr sowie Korruption abstellen. Daneben ergeben sich kodifizierte Anforderungen aus dem KonTraG, dem AktG, dem Corporate Governance Kodex sowie den Prüfungsstandards der Wirtschaftsprüfer und der Internen Revision.

Potenzielle Täter sind in der Regel die eigenen Mitarbeiter des Unternehmens aus allen Hierarchieebenen, aber auch externe Angreifer sind zu nennen. Zur Motivlage gehören eigene Bereicherungsabsichten, die Initiierung durch Dritte oder Geltungsbedürfnisse. Mögliche Hintergründe sind starker Vertriebsdruck und Provisionsstreben, angespannte private finanzielle Verhältnisse, unangemessener Lebensstandard, Spielsucht, Habgier, Erpressungen, Versprechen von Gegenleistungen oder dergleichen.

Verifizierung des Verdachts

Bei bestehenden Anfangsverdachtsmomenten sind die ersten Informationen und Hinweise durch die Interne Revision auf Unregelmäßigkeiten zu beurteilen. Der Anfangsverdacht muss insoweit begründet werden, dass Missbräuche, Manipulationen oder unrechtmäßige Nutzungen vorliegen, die nicht anderweitig belegbar sind. Nur ein vager Verdacht ist absolut unzureichend, schließlich geht es um die Wahrung der Persönlichkeitsrechte der verdächtigen Personen.

Bereits die Begründung für den Verdacht ist lückenlos und nachvollziehbar zu dokumentieren. Dabei ist darzustellen, welche Rechtsgrundlagen und internen Richtlinien zu Grunde gelegt wurden. Vor allem die Verstöße gegen einzelne gesetzliche Bestimmungen sind aufzuführen. Neben der Untermauerung der Verdachtsmomente sind die möglichen Schäden und Folgen für das Unternehmen zu beschreiben, die als Grundlage für spätere zivilrechtliche Ansprüche herangezogen werden können. Dabei spielen auch die Mitbestimmungsregelungen der Mitarbeitervertreter eine große Rolle, da es in der Regel um die Auswertung von Daten geht, die zur Leistungskontrolle herangezogen werden können. Bei der Auswertung personenbezogener Daten, ist das Bundesdatenschutzgesetz (BDSG) maßgebend.

Ist der Verdacht valide, trifft die Leitung der Internen Revision eine Entscheidung über die Einleitung einer Sonderuntersuchung verbunden mit der Freigabe zur weiteren Analyse und Durchführung forensischer Ermittlungen. Sonderuntersuchungen sind nicht nur darauf ausgerichtet, belastende Tatsachen gegen involvierte Mitarbeiter des Unternehmens zu finden, sondern im gleichen Maße auch sie zu entlasten. Ausgehend von bekannten und bewährten Prüfungsansätzen gilt es, sich immer wieder individuellen, neuen und teilweise bisher unbekann-

SCHWERPUNKTTHEMA

ten Prüfungsansätzen zu nähern.

Prüfungsvorbereitung

Im Rahmen der Prüfungsvorbereitung sind möglichst alle relevanten Informationen zu beschaffen. Für jede Sonderuntersuchung sind neben dem entsprechenden Fachwissen und der professionellen Erledigung der „Routineprüfungstätigkeiten“ auch größtmögliche Flexibilität, vernetztes Denken, emotionale Intelligenz, Kreativität sowie Intuition, Instinkt und Erfahrung erforderlich.

Handelt es sich um Delikte unter Zuhilfenahme von Computersystemen, stellt die IT-Forensik das probate Instrument zur Ermittlung und Überführung des potenziellen Täters dar. Mit Hilfe der IT-Forensik können dolose Handlungen und Delikte mit hoher Wahrscheinlichkeit aufgedeckt und gerichtsverwertbar nachgewiesen werden, da jegliche Aktivitäten auf Computern entsprechende digitale Spuren hinterlassen.

Anwendungsfelder in der Wirtschafts- und Computerkriminalität:

- Datenmissbrauch
- Missbräuchliche Nutzung des Internets
- Industriespionage
- Datendiebstahl
- Bilanzfälschung
- Vorsätzliche Datenlöschung
- Veruntreuung

Bei jeder Sonderuntersuchung müssen zwingend die Neutralität der die Sonderuntersuchung durchführenden Personen sowie die Distanz zu den in den Schadens-/Deliktfall involvierten Mitarbeitern gewährleistet sein. Für die Durchführung der forensischen Untersuchungen sind speziell geschulte Mitarbeiter erforderlich. Ggf. ist es angezeigt, spezialisierte Forensiker im Bedarfsfall hinzuziehen. Durch die Einbeziehung solcher externer Spezialisten, wird die Neutralität einmal mehr unterstrichen.

Identifizierung der Beweise

Ist die Prüfungsvorbereitung abgeschlossen, beginnt die eigentliche Prüfungsdurchführung. Zunächst sind die potenziellen Beweise zu identifizieren. Beweise können in Form von Datenbeständen (Stamm- und Bewegungsdaten), Log-Dateien, nicht-flüchtigen Datenbeständen auf Speichermedien, flüchtigen Daten im Arbeitsspeicher, E-Mails oder dergleichen vorliegen. Es ist zu analysieren, wo diese Beweise vorrätig sind, z. B. in Anwendungen, Datenbanken, Betriebssystemen oder Datensicherungen.

Auf diesem Informationsstand ist eine Entscheidung darüber zu treffen, welche Verfahren zur Beweiserhebung verwendet werden sollen. Es ist davon auszugehen, dass in den meisten Unternehmen nur unzureichende Kenntnisse darüber existieren, wie digitale Datenbestände gerichtsverwertbar zu sichern und auszuwerten sind. Dabei geht es um die Vermeidung unsachgemäßer Vorgehensweisen und den zielführenden Einsatz entsprechender Software Tools. Bei der Analyse von IT-Systemen kommt es allerdings mehr auf die IT-Kenntnisse und die Erfahrung in den Köpfen der Forensik Spezialisten an, als auf den Einsatz der technischen Hilfsmittel. Keine Software kann so vielseitig die internen Abläufe in Betriebssystemen analysieren, wie es die IT-Experten mit ihrem produktspezifischen Wissen tun können. Aus unsachgemäßen Handlungen können erhebliche Beeinträchtigungen der Beweiskraft resultieren, im ungünstigsten Fall kann es zu einer Vernichtung der Beweise führen.

Der Rechner sollte nach Möglichkeit unberührt bleiben! Ist der Computer eingeschaltet, bleibt er eingeschaltet, bis er untersucht wurde. Nur im eingeschalteten Zustand ist eine Sicherung des flüchtigen Speichers und der Informationen über den Systemstatus mit geeigneten Tools möglich. Hierbei stehen alle Daten im Vordergrund, die durch ein Ausschalten des Systems ge-

SCHWERPUNKTTHEMA

löscht oder verändert werden könnten; sofern dies auch Daten betrifft, die auf Festplatten temporär zwischengespeichert werden, werden auch diese in die Sicherung mit einbezogen. Im Falle des Abschaltens würden die flüchtigen Datenbestände (RAM-Speicher, Netzwerkverbindungen, offene Dateien) verloren gehen. Ist der Computer ausgeschaltet, bleibt er ausgeschaltet, bis mit geeigneten Hilfsmitteln eine 1:1-Kopie der Originaldaten angelegt und die Datenträger unverändert sichergestellt wurden. Ferner ist zu berücksichtigen, dass Logdateien häufig nur eine begrenzte Zeit verfügbar sind und dass Datensicherungen nur eine befristete Archivierungszeit aufweisen und ebenfalls für die Beweissicherung relevant sein können.

Sicherstellung der Beweise

Bei der Sicherstellung der Beweise ist zu klären wer, was, wann, wo und wie getan hat. Dabei besteht die zentrale Aufgabe darin die Integrität der digitalen Beweise und der Beweiskette aufrecht zu halten.

Weiterhin sind folgende Fragestellungen zu berücksichtigen:

- Zustand des PCs (aktiv/inaktiv)
- Ist es ein Stand-Alone-PC oder Netzwerk-PC?
- Hat der PC einen Internetanschluss und ist die Verbindung aktiv?
- Welche Datenspeichermedien sind im PC integriert?
- Auf welche externen Datenspeicher hat der PC Zugriff?
- Sind Wechseldatenträger oder sonstige externe Datenspeichermedien im Einsatz?

Die eigentliche Untersuchung der Daten erfolgt niemals direkt an den Originaldatenträgern der betroffenen Computer. Die Originaldatenträger oder das erste Image dienen lediglich als Beweismaterial. Bei der Beweissicherstellung sollten Medien benutzt werden, die einmalig beschreibbar sind. Der Einsatz von kryptografischen Verfahren zum digitalen Signieren von Beweisdaten sollte geprüft und wenn möglich angewendet werden, um die Unversehrtheit von Daten gewährleisten zu können.

Analyse

Nachdem die relevanten Beweisdaten erhoben und auf entsprechenden Medien unveränderbar gespeichert sind, folgt eine erste Analyse. Hier ist umfassendes IT-technisches Allroundwissen über Netzwerktopologien, Applikationen, aktuelle und bekannte Systemschwachstellen sowie möglicherweise ein sehr hoher Grad an Improvisationsvermögen gefordert. Das benötigte Wissen geht weit über die pure Administration von Netzwerken oder Betriebssystemen hinaus und verlangt teilweise sogar betriebssystemnahe Programmierkenntnisse.

Dabei geht es auch darum verloren geglaubte Informationen wieder zu rekonstruieren, z. B. den Inhalt von gelöschten Dateien oder E-Mails wiederherzustellen oder Informationen aus temporären Dateien zu gewinnen. Auch beschädigte Dateien werden mittels Software-Werkzeuge wieder lesbar gemacht, so dass alles, was außerhalb des beschädigten Bereiches liegt, wieder gelesen werden kann. So lassen sich auch Dokumente, deren Header beschädigt ist, restaurieren und wieder öffnen, was sonst vom Programm bei beschädigten Dateien verweigert wird. Für die Authentizität des Datenmaterials ist entscheidend, dass physikalisch fehlende Daten – beispielsweise Worte in einem Dokument oder einer E-Mail – niemals ersetzt, sondern als Lücke gekennzeichnet werden. Unter forensischen Gesichtspunkten gilt es, das Original ohne Verfälschung und Ergänzungen eigener Hand so weit wie möglich zu restaurieren. Nur so bleibt der Beweischarakter erhalten.

Handelt es sich um große Datenmengen, kommen Filterfunktionen zum Einsatz, die mit gezielter Schlüsselwortsuche und der Sortierung nach den gewünschten Kriterien die Datenflut reduzieren und separieren, um eine Fokussierung auf die für die Beweisfindung relevanten Daten zu ermöglichen.

Ein weiteres Verfahren zur Eingrenzung des verfügbaren Datenmaterials ist die Eliminierung

SCHWERPUNKTTHEMA

redundanter Informationen, die sich mit entsprechenden Tools durchführen lässt. Liegen die Informationen mehrfach in identischer Form gespeichert vor, so werden die Datenduplikate herausgefiltert, um die Datenmenge zu reduzieren und die Transparenz in der für die Beweisführung notwendigen Daten zu gewährleisten.

Ziel der Analyse ist es, den Sachverhalt einschließlich des materiellen Ausmaßes und der Höhe des voraussichtlichen Schadens mit den Hintergründen und der konkreten Vorgehensweise präzise zu ermitteln, lückenlos zu protokollieren und die gewonnenen Erkenntnisse in einer verständlichen Form aufzubereiten.

Die Protokollierung umfasst u. a. folgende Angaben:

- Identität des Täters/der Täter
- Verwendete User-IDs und Passwörter
- Zugewiesene Zugriffsberechtigungen
- Welche Zugriffe auf Anwendungen und Daten sind zu welcher Zeit und über welche Zeitdauer erfolgt (Zeitskala)
- Welche Operationen wurden ausgeführt
- Häufigkeit der Datenzugriffe
- Differenzierung unautorisierter/autorisierter Zugriffe
- Zeitraum und Umfang der Tat

Interne Information und Befragung des potenziellen Täters

Die Geschäftsleitung, das Personalwesen, IT-Security sowie ggf. die Arbeitnehmervertretung sind über den Sachstand und die Ergebnisse der Analyse zu informieren. Die weiteren Schritte sind mit ihnen abzustimmen.

Im nächsten Schritt sollte mit dem potenziellen Täter ein Gespräch zur Klarstellung des Sachverhaltes geführt werden. Das Gespräch sollte sachlich und ruhig geführt werden, Emotionen sind soweit wie möglich zu unterdrücken. Hierzu sollte im Vorfeld ein Gesprächsleitfaden erstellt werden. Eine professionelle Vorbereitung ist ein wesentlicher Schlüssel zum Gesprächserfolg.

Schritte nach der Überführung des Täters

Ist der Täter überführt, sind weitere Schritte erforderlich. Hierzu gehören bspw.

- Sofortige Beurlaubung des Mitarbeiters
- Erteilen eines Hausverbots
- Rücknahme von Schlüsseln, Firmenhandy und Mitarbeiterausweis
- Beaufsichtigung des Mitarbeiters, Einschränkung der Bewegungsfreiheit im Unternehmen
- Zeitnahe Entscheidung über weitere arbeitsrechtliche Maßnahmen zur Einhaltung arbeitsrechtlicher Fristen
- etc.

Erstellung eines Sonderuntersuchungsberichtes

Nach Abschluss der Ermittlungen ist ein Sonderuntersuchungsbericht zu erstellen; dieser umfasst:

- Management Summary
- Detailschilderung aller Sachverhalte, Vorgehensweise und Feststellungen
- Verstöße gegen Interne Richtlinien und gesetzliche Vorschriften
- Darstellung von systembedingten Schwachstellen, internen Versäumnissen sowie von Mängeln im Führungsverhalten
- Erforderliche und eingeleitete Maßnahmen
- Erklärende Anlagen

SCHWERPUNKTTHEMA

Archivierungstätigkeiten

Bei der Form und Struktur der abschließenden Archivierung und bei dem Inhalt aller aufzubewahrenden Unterlagen ist grundsätzlich der Möglichkeit ausreichend Rechnung zu tragen, dass die Unterlagen seitens der Behörden im Rahmen eines Ermittlungsverfahrens angefordert werden können oder sogar durch behördliche Beschlagnahme und Durchsuchungsbeschluss herausgegeben werden müssen.

Prävention als Risikovorsorge

Um die vorhandenen Risiken zu minimieren, sollten angemessene Vorkehrungen zur Verhinderung von Delikten vorgesehen werden. Als wirksame präventive Maßnahmen sind der Einsatz effizienter Monitoring Tools zu nennen und die Sensibilisierung der Mitarbeiter durch transparente Information hierüber und das stetig steigende Gefahrenpotenzial, das aus der Zunahme der Computerkriminalität resultiert.

Häufig kann die Aufdeckung eines kleinen Vorfalls die Verhinderung eines größeren Deliktes bewirken. Eindeutige Richtlinien zur Nutzung von E-Mail und Internet im Unternehmen schaffen die erforderliche Handlungssicherheit.

Ansprechpartner: Jörg Wöhler (Leitender Berater) und Norbert Neben (Senior Berater)

Risikomanagement von Investmentgesellschaften

Entwurf eines Rundschreibens MaRisk für Investmentgesellschaften in der Fassung vom 25.01.2010

Am 25.01.2010 hat die BaFin einen Entwurf zu den Mindestanforderungen an das Risikomanagement für Investmentgesellschaften (InvMaRisk) veröffentlicht.

Die InvMaRisk sollen sowohl Anwendung auf das verwaltete Investmentvermögen als auch auf für die Gesellschaft wesentlichen Risiken finden. Dabei bleibt es den Gesellschaften überlassen, im Rahmen dieser Anforderungen zu entscheiden, wie sie das Risikomanagementsystem - in Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt ihrer Aktivitäten und der verwalteten Investmentvermögen - angemessen ausgestalten.

Ausgehend von der Geschäftsstrategie hat die Geschäftsleitung eine Risikostrategie zu entwickeln, die die Ziele der Risikosteuerung der wesentlichen Geschäftsaktivitäten beinhaltet. Beide Strategien sind mindestens jährlich von der Geschäftsleitung zu überprüfen und anzupassen und dem Aufsichtsorgan der Gesellschaft bekannt zugeben.

Weitere Bestandteile eines Risikomanagementsystems sind im Allgemeinen die Erfassung, die Messung, die Steuerung und die Überwachung und Kommunikation der wesentlichen Risiken und damit verbundener Risikokonzentrationen. Die InvMaRisk fordern eine mindestens vierteljährliche Gegenüberstellung von Risikodeckungspotenzial und Gesamtrisiko. Unter Berücksichtigung des Risikodeckungspotenzials sind die Risiken zu limitieren und in der Risikostrategie zu dokumentieren. Ein weiterer wesentlicher Bestandteil des Risikomanagementsystems ist das Frühwarnsystem, anhand dessen frühzeitig Gegenmaßnahmen ergriffen werden können. Mit Hilfe regelmäßiger und angemessener Stresstests ist die Verlustanfälligkeit bezüglich außergewöhnlicher Ereignisse zu beurteilen. Die Angemessenheit der Stresstests und zugrunde liegende Annahmen müssen mindestens jährlich überprüft werden. Die Risikoberichterstattung gegenüber der Geschäftsleitung enthält eine Darstellung und Beurteilung der Risikosituation und gegebenenfalls Handlungsvorschläge.

Darüber hinaus bestehen zahlreiche besondere Anforderungen an das Risikomanagement von Investmentgesellschaften, von denen wir Ihnen die wesentlichen im Folgenden vorstellen möchten.

Risk Management Policy

Die Risk Management Policy enthält alle wesentlichen Risiken der Investmentvermögen, die sich aus:

- den Anlagezielen
- der Anlagestrategie
- dem Anlageverhalten bei der Verwaltung der Vermögen sowie
- dem Bewertungsprozess

ergeben.

Als wesentliche Risiken gelten hierbei:

- Marktpreisrisiken
- Liquiditätsrisiken
- Adressenausfallrisiken (Risikokonzentrationen)
- operationelle Risiken

AKTUELLES

Die Risk Management Policy ist in Richtlinien zu dokumentieren und soll mindestens folgendes beinhalten:

- Definition der Prinzipien und Methoden für die periodische Erfassung der wesentlichen Risiken der Investmentvermögen
- Spezifikation der Techniken für die Messung der wesentlichen Risiken
- Methoden gem. DerivateV zur Bestimmung der Auslastung der in § 51 Abs. 1 InvG festgelegten Grenze für das Marktrisiko
- Darlegung der Aufgabenverteilung bzw. Verantwortungsbereiche der verschiedenen Einheiten bzw. Personen, die in den Risikomanagementprozess involviert sind
- Kommunikationswege bzw. Interaktionen zwischen Fondsmanagement und Risikocontrollingfunktion, die insbesondere zur Risikosteuerung notwendig sind
- Definition der Berichterstattung an die Geschäftsleitung (insbesondere Inhalt und Häufigkeit)

Funktionstrennung

Die Gesellschaft hat entsprechend des Proportionalitätsprinzips angemessene und unabhängige Risikocontrollingprozesse einzurichten. Bei einer vollständigen organisatorischen Trennung zwischen Fondsmanagement und Risikocontrollingfunktion ist die Unabhängigkeit bis auf die Ebene der Geschäftsleitung sicherzustellen. Zu den wesentlichen Aufgaben der Risikocontrollingfunktion zählen insbesondere:

- Erfassung, laufende Messung und Überwachung der Risiken
- Implementierung der Risk Management Policy
- Risikoberichterstattung an die Geschäftsleitung

Darüber hinaus hat die Risikocontrollingfunktion eine wesentliche Funktion bei der Festlegung des Risikoprofils bzw. der Anlagestrategie des Investmentvermögens.

Fondsmanagement

Dem Fondsmanagement obliegen verschiedene Pflichten, um die Interessen der Anleger zu wahren. Dazu gehören die Chancen- und Risikobewertung aus der Anlagestrategie für das Investmentvermögen sowie die Beurteilung weiterer Konsequenzen für den Anleger (z.B. steuerliche Aspekte). Eingerichtete organisatorische Verfahren müssen sicherstellen, dass das Investmentvermögen

- in Übereinstimmung mit dem festgelegten Risikoprofil
- der Anlagestrategie
- den Vertragsbedingungen
- den im ausführlichen und vereinfachten Verkaufsprospekt beschriebenen Anlagecharakter des Investmentvermögens
- den jeweils geltenden rechtlichen Bestimmungen

angelegt wird (Compliance). Zudem hat das Fondsmanagement die Auslastung der gesetzlichen und vertraglichen Anlagegrenzen sowie der internen Limitvorgaben zu berücksichtigen.

Abwicklung und Kontrolle

Die Geschäftsabschlüsse für das Investmentvermögen sind laufend zu kontrollieren, insbesondere, ob:

- die Geschäftsunterlagen vollständig und zeitnah vorliegen
- die Angaben der Fondmanager richtig und vollständig sind und, soweit vorhanden, mit den Angaben auf Maklerbestätigungen, Ausdrucken aus Handelssystemen oder Ähnlichen übereinstimmen
- es sich um für das Investmentvermögen zulässige Geschäfte handelt
- relevante Anlagegrundsätze bzw. Anlagegrenzen erfüllt sind (ex-post Anlagegrenzprüfung) sowie die Abschlüsse den sonstigen gesetzlichen Regelungen entsprechen
- die Abschlüsse sich hinsichtlich Art und Umfang im Rahmen der festgesetzten Limite bewegen

AKTUELLES

- marktgerechte Bedingungen vereinbart sind
- die Ausführungswege den vorgegebenen Grundsätzen entsprechen
- Abweichungen von vorgegebenen Standards (z. B. Stammdaten, Anschaffungswege, Zahlungswege) vereinbart sind

Risikocontrolling

Das Risikocontrolling hat die Verfahren zur Messung der Risiken regelmäßig zu überprüfen. Dabei sollte sichergestellt werden, dass die Verfahren auch bei schwerwiegenden Marktstörungen zu verwertbaren Ergebnissen führen.

Eine weitere wesentliche Aufgabe des Risikocontrollings ist die Erstellung eines Limitsystems für die Investmentvermögen. Das Limitsystem sollte mindestens folgende Limite umfassen:

- Liquiditätsrisikolimit
- Marktrisikolimit
- Emittentenlimite
- Ev. Limitierung der Adressenausfallrisiken des Emittenten
- Kontrahentenlimite
- Limite für die Anlage von Bankguthaben nach § 2 Abs. 4 Nr. 4 InvG

Das Fondsmanagement ist über die aktuelle Ausnutzung der relevanten Limite zeitnah zu informieren und für den Fall von eingetretenen oder erwarteten Limitüberschreitungen Prozesse zu definieren und dokumentieren.

Berichterstattung

Die Geschäftsleitung ist in regelmäßigen Abständen über folgende Sachverhalte zu informieren:

- Überblick über das aktuelle Risiko, insbesondere die Konsistenz zwischen aktuellem Risikoniveau und Risikoprofil der jeweiligen Investmentvermögen
- Einhaltung der Limite bzw. Limitüberschreitungen
- Angemessenheit bzw. Effektivität des Risikomanagementprozesses, insbesondere inwiefern angemessene Maßnahmen zur Mängelbeseitigung ergriffen wurden
- Änderungen der wesentlichen Annahmen oder Parameter, die den Verfahren zur Beurteilung bzw. Messung der Risiken zu Grunde liegen

Ansprechpartner: Christof Merz (Geschäftsbereichsleiter) und Beatrice Hammerschmidt (Beraterin)

Compliance für Investmentgesellschaften

Entwurf eines Rundschreibens MaRisk für Investmentgesellschaften in der Fassung vom 25.01.2010

Der Entwurf der InvMaRisk verpflichten Kapitalanlagegesellschaften „über eine ordnungsgemäße Geschäftsorganisation [zu] verfügen, die die Einhaltung von zu beachtenden gesetzlichen Bestimmungen gewährleistet.“ So haben die Gesellschaften Organisationsrichtlinien zu erstellen, die u. a. Regelungen zur Einhaltung gesetzlicher sowie sonstiger Vorgaben (z. B. Datenschutz) enthalten. Im Folgenden stellen wir Ihnen die wesentlichen Anforderungen aus den InvMaRisk zu Compliance vor.

Die Gesellschaften haben angemessene Grundsätze und Verfahren zur Einhaltung der im InvG festgelegten Pflichten festzulegen.

Zu den wesentlichen Anforderungen zählt auch die Einrichtung einer dauerhaften und wirksamen Compliance-Funktion, die folgende Aufgaben wahrnimmt:

- Überwachung und regelmäßige Bewertung von Angemessenheit und Wirksamkeit der eingeleiteten Maßnahmen und Verfahren, sowie der Schritte, die zur Behebung etwaiger Defizite der Gesellschaft bei der Einhaltung ihrer Pflichten unternommen wurden
- Beratung und Unterstützung der für die Dienstleistungen und Tätigkeiten zuständigen relevanten Personen im Hinblick auf die Einhaltung der im InvG für die Gesellschaft festgelegten Pflichten

Die Compliance-Funktion ist dabei unabhängig von der Größe oder des Umfangs der Geschäfte der Gesellschaft einzurichten. Jedoch können die Maßnahmen und Verfahren für die internen Kontrollen dem Umfang und der Art der Geschäfte der Gesellschaft angepasst werden. Ferner ist möglich bei kleineren Gesellschaften weniger Ressourcen für die Einrichtung einer Compliance-Funktion bereitzustellen als bei großen Gesellschaften.

Um die ordnungsgemäße und unabhängige Wahrnehmung der Aufgaben der Compliance-Funktion zu gewährleisten, sollte die Gesellschaft folgendes sicherstellen:

- die mit der Compliance-Funktion betrauten Personen besitzen die notwendigen Befugnisse, Ressourcen und Fachkenntnisse sowie Zugang zu allen relevanten Informationen
- die Ernennung eines Compliance-Beauftragten, der für die Compliance-Funktion und die Erstellung der Compliance-Berichte sowie den jährlichen Versand der Berichte an die Geschäftsleitung verantwortlich ist
- den Ausschluss der mit Compliance-Funktionen betrauten Personen aus dem operativen Geschäft, das es zu überwachen gilt
- das Verfahren zur Vergütung beeinflusst nicht die Objektivität oder lässt diese wahrscheinlich werden

Die Gesellschaft braucht die beiden zuletzt genannten Anforderungen nicht umzusetzen, wenn sie die Unverhältnismäßigkeit sowie die weitere Erfüllung ihrer Aufgabe nachweist, die sich aufgrund der Art, des Umfangs und der Komplexität der Geschäfte bzw. ihrer Dienstleistungen und Tätigkeiten ergeben.

Ansprechpartner: Henning Tenzer (Leitender Berater) und Beatrice Hammerschmidt (Beraterin)

InvMaRisk und die Anforderungen an die Interne Revision

Entwurf eines Rundschreibens MaRisk für Investmentgesellschaften in der Fassung vom 25.01.2010

Neben spezifischen Anforderungen an das Risikomanagement konkretisiert der Entwurf unter anderem auch Anforderungen an die Interne Revision. Gemäß den InvMaRisk soll jede Gesellschaft über eine funktionsfähige Interne Revision verfügen, die je nach Größe der Gesellschaft unterschiedlich ausgestaltet werden kann. Um eine effektive und funktionsfähige Interne Revision zu gewährleisten, sind folgende wesentliche Ansatzpunkte zu beachten:

- Die Interne Revision ist ein Instrument der Geschäftsleitung, ihr unmittelbar unterstellt und berichtspflichtig
- Zur Wahrnehmung ihrer Aufgaben ist der Internen Revision ein vollständiges und uneingeschränktes Informationsrecht einzuräumen
- Weisungen und Beschlüsse der Geschäftsleitung, die für die Interne Revision von Bedeutung sein können, sind ihr bekannt zu geben

Die Interne Revision hat risikoorientiert und prozessunabhängig die Wirksamkeit und Angemessenheit

- des Risikomanagements
- des internen Kontrollsystems
- sowie die Ordnungsmäßigkeit aller Aktivitäten und Prozesse

zu prüfen und zu beurteilen.

Die Interne Revision hat unter Wahrung ihrer Unabhängigkeit und unter Vermeidung von Interessenkonflikten bei wesentlichen Projekten begleitend tätig zu sein. Daneben hat sie die Prüfung von wesentlichen Auslagerungen vorzunehmen, sofern die anderweitig durchgeführte Revisionstätigkeit den Anforderungen für Investmentgesellschaften nicht genügt.

Im Rahmen der Revisionstätigkeit sind die folgenden Grundsätze von der Internen Revision zu beachten:

- Die Interne Revision hat ihre Aufgaben selbständig und unabhängig wahrzunehmen. Insbesondere ist zu gewährleisten, dass sie bei der Berichterstattung und der Wertung der Prüfungsergebnisse keinen Weisungen unterworfen ist.
- Die Mitarbeiter der Internen Revision dürfen grundsätzlich nicht mit revisionsfremden Aufgaben betraut werden. Sie dürfen insbesondere keine Aufgaben wahrnehmen, die mit der Prüfungstätigkeit nicht im Einklang stehen.
- Mitarbeiter, die in anderen Organisationseinheiten der Gesellschaft beschäftigt sind, dürfen grundsätzlich nicht mit Aufgaben der Internen Revision betraut werden. Nur in begründeten Einzelfällen können andere Mitarbeiter aufgrund ihres Spezialwissens zeitweise für die Interne Revision tätig sein.

Die Tätigkeit der Internen Revision basiert auf einem risikoorientierten und jährlich fortzuschreibenden Prüfungsplan, innerhalb dessen die Aktivitäten und Prozesse in einem angemessenen Abstand grundsätzlich von drei Jahren zu prüfen sind. Jedoch kann die Prüfung in Abhängigkeit von Risikogesichtspunkten in einem abweichenden Prüfungsturnus stattfinden. Die Prüfungsplanung, -methoden und -qualität sind regelmäßig und anlassbezogen zu überprüfen und weiterzuentwickeln.

Die Ergebnisse der Prüfungstätigkeiten müssen zeitnah dokumentiert und den fachlich zuständigen Mitgliedern der Geschäftsleitung vorgelegt werden. Im Prüfungsbericht müssen die Prüfungsgegenstände, die Prüfungsfeststellungen sowie die vorgesehenen Maßnahmen dargestellt werden. Die wesentlichen und schwerwiegenden Mängel sind besonders herauszustellen und der Geschäftsleitung in einem schriftlichen Bericht unverzüglich vorzulegen. Bei den schwer-

AKTUELLES

wiegenden Feststellungen gegen den Geschäftsleiter ist den Vorsitzenden des Aufsichtsorgans sowie die Aufsichtsinstiution unverzüglich zu informieren.

Die Interne Revision hat im Rahmen der Revisionstätigkeit zu überwachen, ob die festgestellten Mängel fristgerecht beseitigt sind. Wenn die wesentlichen Mängel nicht fristgerecht beseitigt sind, hat der Leiter der Internen Revision die Geschäftsleitung darüber schriftlich zu informieren.

Ansprechpartner: Christof Merz (Geschäftsbereichsleiter) und Oleksandr Krasnopolskyy (Berater)

InvMaRisk Anforderungen an Notfallkonzept

Entwurf eines Rundschreibens MaRisk für Investmentgesellschaften in der Fassung vom 25.01.2010

In den täglichen Abläufen der Geschäftsprozesse können unerwartete Störungen oder unvorhersehbare Fälle auftreten, die den normalen Betriebsablauf unterbrechen. Um die aufgetretenen Probleme schnell und effektiv zu beheben, sollen die zuständigen Mitarbeiter über Ersatzlösungen verfügen, die eine Geschäftsfortführung sicherstellen. Die Folgen aus fehlenden Ersatzlösungen sind schwer abschätzbar und können zu erheblichen Schäden im Unternehmen führen.

Um in einem Notfall die Fortführung der Geschäftsprozesse sicherzustellen, hat die Gesellschaft gemäß den InvMaRisk ein Notfallkonzept zu erstellen. Das Notfallkonzept soll Transparenz schaffen und somit die Sicherheit im Umgang mit Notfällen fördern.

Das Notfallkonzept muss Geschäftsfortführungs- sowie Wiederanlaufpläne umfassen. Die Wiederanlaufpläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen bzw. das Ausmaß möglicher Schäden reduzieren.

Das Notfallkonzept muss neben praktikablen und schnell einsetzbaren Maßnahmenkatalogen auch die Zuständigkeiten und die Verantwortlichkeiten des Personals in einem Notfall darlegen.

Folgende Punkte sollen im Notfallkonzept ausdrücklich geregelt werden:

- Zuständigkeiten für bestimmte Bereiche oder Aufgaben
- Verantwortlichkeit für die Erledigung der Aufgaben oder für das Treffen der Entscheidung
- die zu verwendenden Kommunikationswege im Notfall

Gemäß den InvMaRisk muss das Notfallkonzept auch Maßnahmen hinsichtlich der Depotbank umfassen für den Fall, dass sie ihre Funktionen nicht bzw. nur noch sehr eingeschränkt wahrnehmen kann. Die Pläne müssen die Maßnahmen zum Depotbankwechsel sowie infrage kommende Depotbanken umfassen.

Die Tauglichkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig durch Notfalltests zu überprüfen. Die Ergebnisse der Notfalltests sind zu dokumentieren und den jeweiligen Verantwortlichen mitzuteilen. Im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen haben die auslagernde Gesellschaft und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte zu verfügen.

Das Notfallkonzept muss in einer schriftlichen Form fixiert werden und allen beteiligten Mitarbeitern in der Gesellschaft zur Verfügung stehen.

Ansprechpartner: Jörg Wöhler (Leitender Berater) und Norbert Neben (Senior Berater)

Gesetzesentwurf des Bundeskabinetts zur Überwachung von Ratingagenturen

Am 13.01.2010 legte das Bundeskabinett einen Gesetzesentwurf zur Überwachung von Ratingagenturen vor und setzt damit die Verordnung Nr. 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 (Ratingverordnung) um. Nachdem den Ratingagenturen Standard & Poor's, Moody's, Fitch und Co. eine maßgebliche Mitverantwortung für die Finanzkrise von vielen Beteiligten zugeschrieben wurde, soll ihre Arbeit künftig besser überwacht und Verstöße mit hohen Bußgeldern belegt werden.

Zukünftig wird der § 17 des Wertpapierhandelsgesetzes die Vorschriften zur Überwachung von Ratingagenturen enthalten. Die wesentlichen Regelungstatbestände lassen sich wie folgt zusammenfassen:

1. Die BaFin wird zukünftig die Überwachung übernehmen. Im Jahr 2011 soll die neue EU-Aufsichtsbehörde – ESMA – die Aufsicht von der BaFin übernehmen.
2. Die BaFin ist verpflichtet, alle zur effektiven Durchsetzung der Vorschriften erforderlichen Maßnahmen - unter Berücksichtigung des verfassungsmäßigen Gebots der Verhältnismäßigkeit - zu ergreifen.
3. Alle Unterlagen, z. B. Anträge, sind der BaFin in deutscher Sprache vorzulegen. Eine Vorlage der Unterlagen in englischer Sprache kann erlaubt sein, wenn das vorlagepflichtige Unternehmen einer Gruppe von Ratingagenturen angehört oder in einem Drittstaat ansässig ist und die Erstellung deutscher Unterlagen für die Unternehmen eine übermäßige Belastung wäre.
4. Die BaFin hat das Recht zu jederzeitigen Prüfungen, ohne dass es dazu einen konkreten Anlass bedarf.
5. Die Ratingagenturen haben jährlich ihre Ratingtätigkeit durch einen Wirtschaftsprüfer oder eine Wirtschaftsprüfungsgesellschaft prüfen zu lassen. Die BaFin behält sich die Beauftragung qualifizierter Prüfer vor, da die Prüfung gerade größerer Unternehmen einen hohen Aufwand bedeutet und die Wirtschaftsprüfer über hinreichende Sachkunde verfügen müssen, um die spezielle und komplexe Materie der EU-Ratingverordnung beurteilen zu können.

Um ein einheitliches Vergabeverfahren zu gewährleisten, legt die BaFin für jede Prüfung das Datum des Prüfbeginns und des Berichtszeitraums fest. Die BaFin kann jederzeit an diesen Prüfungen teilnehmen, um sich vom ordnungsgemäßen Prüfungsablauf zu überzeugen und ggf. Anhaltspunkten für weiteren Untersuchungsbedarf nachzugehen.

6. Die Maßnahmen der BaFin zur Durchsetzung der EU-Ratingverordnung sind sofort umzusetzen.
7. Das Bundesministerium der Finanzen kann eine Rechtsverordnung erlassen, die sie auf die BaFin übertragen kann. In der Rechtsverordnung kann Näheres über die Prüfungen von Ratingagenturen geregelt werden.

AKTUELLES

Verstöße gegen die Vorgaben der EU-Ratingverordnung gelten als Ordnungswidrigkeit und werden mit Bußgeldern belegt. Bis zu einer Millionen Euro Strafe können verhängt werden, wenn eine Ratingagentur:

- ein Rating abgibt, obwohl ein Interessenkonflikt vorliegt
- gegenüber demselben bewerteten Unternehmen oder einem verbundenen Dritten sowohl Beratungs- als auch Ratingleistungen erbringt
- bei einer Veränderung der Methoden, Modelle oder grundlegenden Annahmen, die Auswirkungen auf das Rating hat, kein neues Rating erstellt oder
- trotz des Fehlens verlässlicher Daten nicht auf die Abgabe eines Ratings verzichtet oder ein vorhandenes Rating nicht zurückzieht

Bei anderen Verstößen gegen die EU-Ratingverordnung beträgt der Bußgeldrahmen jeweils bis zu 200.000,- Euro.

Ansprechpartner: Beatrice Hammerschmidt (Beraterin)

Anforderungen an Vergütungssysteme

Am 21.12.2009 hat die BaFin die Rundschreiben Anforderungen an Vergütungssysteme im Versicherungsbereich und von Instituten verabschiedet. Hintergrund waren die Lehren aus der Finanzkrise und der Schluss, dass Vergütungssysteme, die einen großen variablen Anteil aufweisen, zum unverhältnismäßigen Eingang von Risiken führen können.

Die Vergütung, als die Gesamtheit aller monetären oder monetär bewertbaren Leistungen, die ein Geschäftsleiter oder Mitarbeiter im Rahmen seiner beruflichen Tätigkeit vom Unternehmen erhält, unterliegt bestimmten Grundsätzen, die in den Rundschreiben 22/2009 (BA) und 23/2009 (VA) überarbeitet und neu veröffentlicht wurden. Die Grundsätze sind in allgemeine Anforderungen und besondere Anforderungen unterteilt. Die allgemeinen Anforderungen gelten für alle Unternehmen und für die Vergütungssysteme sämtlicher Geschäftsleiter und Mitarbeiter. Die besonderen Anforderungen gelten nur für bedeutende Finanzinstitutionen, z. B. Unternehmen mit einer Bilanzsumme von 90 Milliarden Euro.

1. Allgemeine Anforderungen

1.1 Geschäftsleiter und Mitarbeiter

Die Vergütung des Geschäftsleiters für seine gegenüber dem Unternehmen erbrachten Dienstleistungen ist im Anstellungsvertrag schriftlich und unter Beachtung der in § 87 AktG enthaltenen Grundsätze zu regeln.

Vergütungssysteme sollten:

- in Organisationsrichtlinien festgelegt sein
- mindestens jährlich auf Angemessenheit überprüft und gegebenenfalls angepasst werden
- mit den strategischen Zielen in Einklang stehen
- nicht manipulierbar sein
- negative Anreize vermeiden, z. B. Interessenkonflikte oder das Eingehen unverhältnismäßig hoher Risikopositionen
- sicherstellen, dass sich der variable Teil der Vergütung an dem langfristigen Erfolg des Unternehmens orientiert

Geschäftsleiter und Mitarbeiter sind über die Ausgestaltung der für sie maßgeblichen Vergütungsparameter zu informieren, damit sie ihr Verhalten an ihnen ausrichten können.

Für die Beurteilung der Angemessenheit der Vergütungssysteme informiert sich das Verwaltungs- oder Aufsichtsorgan eines Unternehmens mindestens jährlich über dessen Struktur.

1.2 Vergütung von Aufsichts- oder Verwaltungsratsmitgliedern

Die Satzung oder der Beschluss der Hauptversammlung bzw. der obersten Vertretung legt die Vergütung für Aufsichts- oder Verwaltungsratsmitglieder fest.

Aufsichts- oder Verwaltungsratsmitglieder sollten nicht in einem (wirtschaftlichen) Abhängigkeitsverhältnis zum Unternehmen stehen. Über die Aufsichtsrats- und Verwaltungsratsvergütungen hinausgehende Vergütungen sind vertraglich zu regeln und bedürfen der Zustimmung der zuständigen Gremien des Unternehmens. Eine mehrfache Tätigkeit von Aufsichtsrats- oder Verwaltungsratsmitgliedern, z. B. als selbstständige Versicherungsvermittler im gleichen Unternehmen, sollte vermieden werden.

2. Besondere Anforderungen

2.1 Vergütung von Geschäftsleitern und Mitarbeitern

Besondere Anforderungen an die Vergütung bestehen für Geschäftsleiter und Mitarbeiter, die hohe Risikopositionen begründen können. Dies hat auf Basis einer Selbsteinschätzung zu erfolgen.

AKTUELLES

	A	B	C	D	E	F	G	H	I	J	K	Q	R	S	T	
1	Name: Gesamt		Kriterien													
2	Geschäftsleiter und Mitarbeiter der Abteilungen:		Umsatz/ Geschäfts- volumen	Verbrauch Risikokapital	Volatilität der Position	Konzentratio n bzw. Kumule	Bilanzgewinn	Kostenspar nis	Marktanteil	Neukundenak quisition	:					
3	Lfd.Nr.		1	2	3	4	5	6	7	8	9					
4	Nr.	Gewicht	1	1	1	1	1	1	1	1	1					
5	1	Planung
6	2	(Betriebs-)Organisation
7	3	Interne Revision
8	4	volkswirtschaftliche Abteilung
9	5	Recht
10	6	Steuern
11	7	Kommunikation/Presse
12	8	IT
13	9	Absatz (Vertrieb/Marketing)	10	0	0	10	10	10	10	10	10	10
14	10	Finanzierung (Kapitalanlagen, Zahlungsverkehr)
15	11	Verwaltung (Personal, Rechnungswesen...)
33		Maximum	10,0	0,0	0,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	0,0
34		Mittelwert	10,0	0,0	0,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	0,0
35		Minimum	10,0	0,0	0,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	0,0
36																
37																
38																
39																
40																
41																

Abbildung: Beispiel einer Risikobewertung des Unternehmens anhand ausgewählter Kriterien

Fixe und variable Vergütung müssen in einem angemessenen Verhältnis zueinander stehen. Die variable Vergütung, die einen Verhaltensanreiz darstellen sollte, sollte sich aus dem Gesamterfolg des Unternehmens sowie dem individuellen Erfolg des Mitarbeiters zusammensetzen. Der individuelle Erfolgsbeitrag basiert dabei auch auf der nachhaltigen Wertentwicklung des Unternehmens.

3. Vergütungsausschuss und Offenlegung

Für die Ausgestaltung und Weiterentwicklung der Vergütungssysteme ist der Vergütungsausschuss zuständig. Die Zusammensetzung und Turnus der Zusammenkünfte bleibt hierbei den Unternehmen überlassen. Dieser hat mindestens jährlich einen Vergütungsbericht über die Ausgestaltung, Überprüfung und Weiterentwicklung der Vergütungssysteme zu verfassen. Der Vergütungsbericht ist vom Unternehmen im Sinne einer hinreichenden Transparenz zu veröffentlichen, z. B. auf der eigenen Internetseite.

Ansprechpartner: Christof Merz (Geschäftsbereichsleiter) und Beatrice Hammerschmidt (Beraterin)

Anforderungen und Pflichten der Mitglieder der Verwaltungs- und Aufsichtsorgane

Der Gesetzgeber hat die Notwendigkeit erkannt, dass eine laufende und funktionierende prozessunabhängige Überwachung von Geschäftstätigkeiten ein wirksames Instrument zur Vermeidung bzw. Verringerung von Risiken ist.

Neben der Internen Revision kommt diese Aufgabe auch in verstärktem Maße der Aufsichts- bzw. Verwaltungsrat nach.

Das KWG und VAG enthält Regelungen zur Qualifikation und Aufgaben von Mitgliedern von Aufsichts- und Verwaltungsorganen, die für Institute und Finanzholding-Gesellschaften sowie Erst- und Rückversicherungsunternehmen gelten. Im Folgenden stellen wir Ihnen die wichtigsten materiellen Anforderungen, Anzeigepflichten und Pflichten aus den neuen Vorschriften vor.

1. Materielle Anforderungen (§§ 36 Abs. 3 KWG; 7a Abs. 4 VAG)

Wichtigste Anforderung an Mitglieder der Verwaltungs- und Aufsichtsorgane ist eine entsprechende Sachkunde, d. h. die Mitglieder sollen geeignet sein, die von dem Institut/Unternehmen oder der Finanzholding-Gesellschaft getätigten Geschäfte zu verstehen, deren Risiken zu beurteilen und nötigenfalls Änderungen in der Geschäftsführung durchzusetzen.

Die nötige Sachkunde der Mitglieder der Verwaltungs- und Aufsichtsorgane richtet sich dabei nach der Größe, Komplexität und systemtechnischen Relevanz des Unternehmens und kann bereits durch Tätigkeiten in derselben Branche erworben worden sein, z. B. Geschäftsführung eines vergleichbaren beaufsichtigten Unternehmens.

Die Aufsichtsbehörde nimmt regelmäßig das Vorliegen der erforderlichen Sachkunde an, wenn:

- Vertreter in mitbestimmten Aufsichts- und Verwaltungsorganen unmittelbar in die wirtschaftlichen und rechtlichen Abläufe des Tagesgeschehens des beaufsichtigten Unternehmens eingebunden sind
- Hauptverwaltungsbeamte einer Gebietskörperschaft Tätigkeiten ausüben oder ausgeübt haben, die maßgeblich auf wirtschaftliche oder rechtliche Fragestellungen ausgerichtet sind
- die erforderlichen Kenntnisse durch Fortbildung erworben werden (vor oder bis sechs Monate nach Bestellung). Ein Teilnahmenachweis ist nach Abschluss der Fortbildung bei der Aufsichtsbehörde einzureichen. Die Fortbildung umfasst im Wesentlichen:
 - grundlegende wirtschaftliche und rechtliche Abläufe im Tagesgeschehen
 - Risikomanagement
 - Funktion und Verantwortung der Mitglieder des Verwaltungs- oder Aufsichtsorgans in Abgrenzung zur Geschäftsleitung
 - Grundzüge der Bilanzierung
 - Grundzüge des Aufsichtsrechts, z.B.
 - § 54 VAG: Anlagegrundsätze für das gebundene Vermögen; Anzeigepflichten
 - BaFin-Rundschreiben 15/2005: Anlage des gebundenen Vermögens; Anlagemanagement und interne Kontrollverfahren
 - § 7 Abs. 2 VAG: Regelungen über den Einsatz von Derivaten
 - BAV-Rundschreiben 3/1999: Strukturierte Produkte
 - BAV-Rundschreiben 3/2000: Derivate

2. Anzeigepflichten (§§ 24 Abs. 1 Nr. 15 KWG; 5 Abs. 5 Nr. 9, 13d Nr. 12 VAG)

Seit dem 01.08.2009 ist die Erstbestellung von Mitgliedern von Verwaltungs- und Aufsichtsorganen anzeigepflichtig. Eine entsprechende Absicht zur Bestellung der Mitglieder ist nicht anzeigepflichtig.

Für die Prüfung der Zuverlässigkeit und Sachkunde von Mitgliedern von Aufsichts- und Verwaltungsorganen durch die Aufsichtsbehörde, sind der Anzeige der Bestellung ein Lebenslauf und eine Straffreiheitserklärung beizufügen. Im Lebenslauf sind andere Mandate der betreffenden Person in Kontrollorganen von beaufsichtigten Unternehmen bzw. Handelsgesellschaften, die gesetzlich einen Aufsichtsrat zu bilden haben, anzugeben. Zusätzlich ist von deutschen Staatsbürgern ein Führungszeugnis bzw. bei ausländischen Aufsichts- und Verwaltungsorganmitgliedern ein dem Führungszeugnis entsprechendes Dokument vorzulegen.

3. Pflichten von Mitgliedern von Aufsichts- und Verwaltungsräten (§§ 36 Abs. 3 KWG, 87 Abs. 8, 121c Abs. 6 VAG)

Zu den Aufgaben der Mitglieder von Aufsichts- und Verwaltungsorganen gehört die Beobachtung und Beurteilung der Geschäftsstrategie und Risikosituation des Unternehmens. Die umfasst insbesondere die Teilnahme an Sitzungen und deren Vorbereitung genauso wie eine enge Begleitung der Entwicklung des Unternehmens zwischen den Sitzungen, sollte sich die Risikosituation des Unternehmens erheblich ändern. Es ist die Pflicht der Mitglieder von Aufsichts- und Verwaltungsorganen ihre Überwachungs- und Kontrollfunktion sorgfältig auszuüben, um wesentliche Verstöße der Geschäftsleiter gegen die Grundsätze einer ordnungsgemäßen Geschäftsführung zu entdecken und zu beseitigen. Gemäß dem Rundschreiben 15/2009 (MaRisk BA) ist sicherzustellen, dass der Vorsitzende des Aufsichtsorgans unter Einbeziehung der Geschäftsleitung direkt bei dem Leiter der Internen Revision Auskünfte einholen kann. Im Rundschreiben 3/2009 (MaRisk VA) wird die Interne Revision als ein Instrument der Geschäftsleitung benannt, die ihr unmittelbar unterstellt und berichtspflichtig ist. Ein Informationsrecht des Aufsichtsorgans bei der Internen Revision ist nicht explizit geregelt.

Aus unserer Erfahrung eignen sich insbesondere folgende Instrumente/Berichte für den Aufsichtsrat zur laufenden Wahrnehmung seiner Kontrollaufgaben:

- Turnusmäßiger Risikobericht
- Risikostrategie
- Jahresbericht der Internen Revision sowie Berichte mit einem negativen Gesamtergebnis
- ALM-Untersuchung (bei Versicherungen)

Erfüllen die Mitglieder von Aufsichts- und Verwaltungsorganen ihre Pflichten nicht, so können sie von der Aufsichtsbehörde verwarnet und bei Fortsetzung der Pflichtverletzung abberufen werden. Bei einer wesentlichen Pflichtverletzung, die die Zuverlässigkeit oder Sachkunde des Mitglieds des Aufsichts- oder Verwaltungsorgans in Frage stellt, kann die Aufsichtsbehörde die Abberufung auch ohne Verwarnung verlangen. Unter den gleichen Voraussetzungen kann die Aufsichtsbehörde ein Tätigkeitsverbot aussprechen.

Ansprechpartner: Christof Merz (Geschäftsbereichsleiter) und Beatrice Hammerschmidt (Beraterin)

AKTUELLES

Fraud-Seminare 2010

Es erwarten Sie vier Fraud-Specials und ein Fraud-Grundlagen-Seminar in Köln



Fraud-Specials:

- 13.07.10: **Fraud-Präventionsmaßnahmen nach erfolgter Risiko- und Gefährdungsanalyse**
Weitere Informationen:
http://www.agens.com/de/Unternehmen/Publikationen_und_News/News/2009/fraud_13072010.php
- 14. – 15.07.10: **Fraud-Sonderuntersuchungen und Deliktrevisionen**
Weitere Informationen:
http://www.agens.com/de/Unternehmen/Publikationen_und_News/News/2009/fraud_1415072010.php
- 28.09.10: **Juristische Grundlagen für das Fraud-Management**
Weitere Informationen:
http://www.agens.com/de/Unternehmen/Publikationen_und_News/News/2009/fraud_280910.php
- 29.09.10: **IT-Forensik**
Weitere Informationen:
http://www.agens.com/de/Unternehmen/Publikationen_und_News/News/2009/fraud_29092010.php

Fraud-Grundlagen-Seminar:

Darüber hinaus bieten wir Ihnen Ende des Jahres eine Fraud-Prävention-Tagesveranstaltung an. Hier wird Fraud Grundlagen Know-how vermittelt und die Möglichkeit gegeben, Erfahrungen mit anderen Teilnehmern auszutauschen:

- 25.11.10: **„Prävention von wirtschaftskriminellen Handlungen
Aktuelles, Trends und Praxisbeiträge“**
Weitere Informationen:
http://www.agens.com/de/Unternehmen/Publikationen_und_News/News/2009/fraud_251110.php

Wir freuen uns über Ihre Teilnahme!

Ansprechpartner: Doris Jeska (Assistentin Vertrieb)

LITERATUR



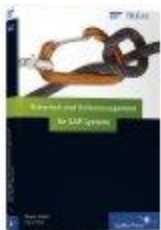
Excel-Tools für das Controlling

Heiko Heimrath
ISBN-10: 3866456662
([Mehr ...](#))



Integriertes Revisionsmanagement

Praxismodell für eine ganzheitliche Organisation der Internen Revision
Marcus Bauer
ISBN-10: 3503120637
([Mehr ...](#))



Sicherheit und Risikomanagement für SAP-Systeme

Mario Linkies, Horst Karin
ISBN-10: 3836214210
([Mehr ...](#))



Benchmarking in der Internen Revision

Mehr Effizienz durch Kostenkalkulation und Leistungsmessung
Julia Busch
ISBN-10: 3503124403
([Mehr ...](#))



Einführung in das Risikomanagement

Heinz Cremers, Walter Sanddorf-Koehle
ISBN-10: 3540881433
([Mehr ...](#))



Handbuch Treasury

Ganzheitliche Risikosteuerung in Finanzinstituten
Hendryk Braun, Henning Heuter
ISBN-10: 3791028472
([Mehr ...](#))



Pragmatisches IT-Projektmanagement

Softwareentwicklungsprojekte auf Basis des PMI PMBoK Guide führen
Niklas Spitzcok von Brisinski, Guy Vollmer
ISBN-10: 3898646513
([Mehr ...](#))



Beschwerdemanagement in Banken und Versicherungen

Oliver Ratajczak
ISBN-10: 3834915211
([Mehr ...](#))

SEMINARTERMINE

Im Folgenden möchten wir Ihnen wieder ausgewählte Seminare des agens Revisionsteams vorstellen.

März bis April 2010

Prüfen der Wirtschaftlichkeit von Geschäftsprozessen - DIIR (Mehr ...)	15. – 17.03.2010
Die 10 „S“ für Revisionsleiter - Modul 7: Schnittstelle Interne Revision und Riskmanagement - DIIR (Mehr ...)	16.03.2010
Personalbedarfsplanung - Einsatz moderner Verfahren der Personalbemessung - DVA (Mehr...)	16. – 17.03.2010
Projekte prüfen aus Sicht der Internen Revision - DIIR (Mehr ...)	16. – 17.03.2010
Die 10 „S“ für Revisionsleiter - Modul 1: Skills für Revisionsleiter - DIIR (Mehr ...)	17.03.2010
Die 10 „S“ für Revisionsleiter - Modul 4: Sicherung der Qualität in der Internen Revision (QA) - DIIR (Mehr ...)	18.03.2010
Wirtschaftlichen Einsatz der IT prüfen und bewerten - DIIR (Mehr ...)	18. – 19.03.2010
Einführung in die Interne Revision - DIIR (Mehr ...)	22. – 25.03.2010
Berichterstattung der Internen Revision - DIIR (Mehr ...)	24. – 26.03.2010
Revisionseinstieg in die Welt der SAP Systeme - DIIR (Mehr ...)	25. – 26.03.2010
Einführung in die IT-Revision - DIIR (Mehr ...)	12. – 15.04.2010
Einführung in die Interne Revision - DIIR (Mehr ...)	12. – 15.04.2010
Einführung in die Interne Revision - DVA (Mehr ...)	19. – 22.04.2010
Grundlagen von Kapitalmarktprodukten - Die Einführung in die Kapitalanlagetätigkeit - DVA (Mehr ...)	20. – 21.04.2010
Interne Kontrollsysteme gestalten und prüfen (IKS II) - DIIR (Mehr ...)	26. – 28.04.2010
Die 10 „S“ für Revisionsleiter - Modul 2: Strategie für Revisionsleiter (GRC) - DIIR (Mehr ...)	26.04.2010
Fraud nachhaltig vermeiden - DIIR (Mehr ...)	29. – 30.04.2010
Der Revisionsbericht - Teil 1 – Haub + Partner (Mehr ...)	29. – 30.04.2010

Spezielle Seminare für den öffentlichen Dienst und die EU-Finanzkontrolle von März bis April 2010

Arbeitsergebnisse darstellen – agens (Mehr ...)	20. – 22.04.2010
---	------------------

Ansprechpartner: Dr. Peter Wesel (Senior Berater)

MICROSOFT EXCEL

Microsoft Excel

Auch wenn Microsoft Excel ein weit verbreitetes Standardprodukt in vielen Unternehmen ist, bleiben jede Menge Funktionen im Alltag verborgen. Wir möchten an dieser Stelle Hilfeleistung bieten und Ihnen regelmäßig über ausgewählte Funktionen/Formeln berichten.

Erstellen von Dropdown-Liste aus Zellbereichen in Excel 2007

In Microsoft Office Excel besteht für die Nutzer die Möglichkeit, in eine Zelle beliebige Daten einzugeben. Dabei ergibt sich manchmal die Notwendigkeit:

- in eine Zelle die Daten einzugeben, die sich regelmäßig wiederholen oder
- die Einträge in dieser Zelle auf bestimmte vom Entwickler definierte Elemente zu beschränken

In solchen Fällen ist es empfehlenswert eine Dropdown-Liste zu erstellen, anhand derer die definierten Daten schnell in die Zelle eingegeben und die Einträge auf bestimmte Elemente beschränkt werden können.

Beispiel:

Im Rahmen der Bearbeitung der Kundendaten soll ein Sachbearbeiter jedem Kunden ein bestimmtes Produkt zuordnen. Dafür wird eine Dropdown-Liste erstellt, um die Bezeichnung des Produktes nicht jedes Mal manuell einzugeben und die Eingaben von nicht existierenden Produkten zu verhindern.

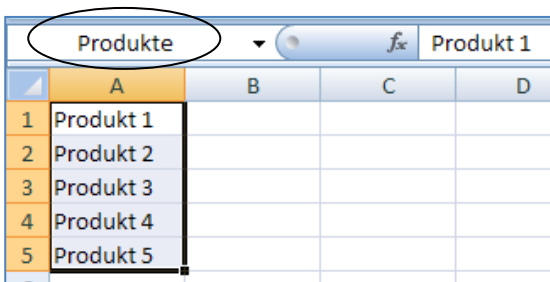
Für die Erstellung einer Dropdown-Liste sollen folgende Schritte vorgenommen werden:

Schritt 1: Zuerst sind die Einträge in einer einzelnen Spalte oder Zeile einzugeben für die eine Dropdown-Liste erstellt werden soll.

Die Daten können in einem aktuellen oder einem anderen Arbeitsblatt angegeben werden. Es wird jedoch empfohlen, die Daten in einem anderen Arbeitsblatt einzugeben und dieses auszublenden oder zu schützen, damit die Daten durch andere Nutzer nicht geändert werden können.

Wenn ein anderes Arbeitsblatt verwendet wird, dann soll:

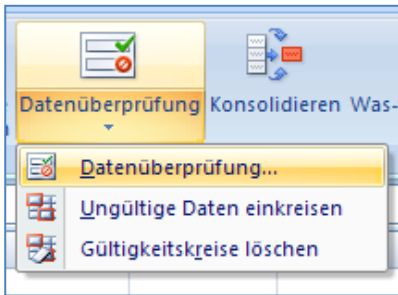
- die eingegebene Liste in diesem Arbeitsblatt markiert werden und
- ein Name (z. B. Produkte) für die Liste in der Bearbeitungsleiste ganz links in den Bereich der Zellennennung festgelegt werden.



	A	B	C	D
1	Produkt 1			
2	Produkt 2			
3	Produkt 3			
4	Produkt 4			
5	Produkt 5			

Schritt 2: Nachdem die Einträge für die Dropdown-Liste festgelegt sind, ist die Zelle auszuwählen, in der die Dropdown-Liste eingefügt werden soll. Danach ist auf der Registerkarte „Daten“ in der Gruppe „Datentools“ das Menü „Datenüberprüfung“ festzulegen.

MICROSOFT EXCEL



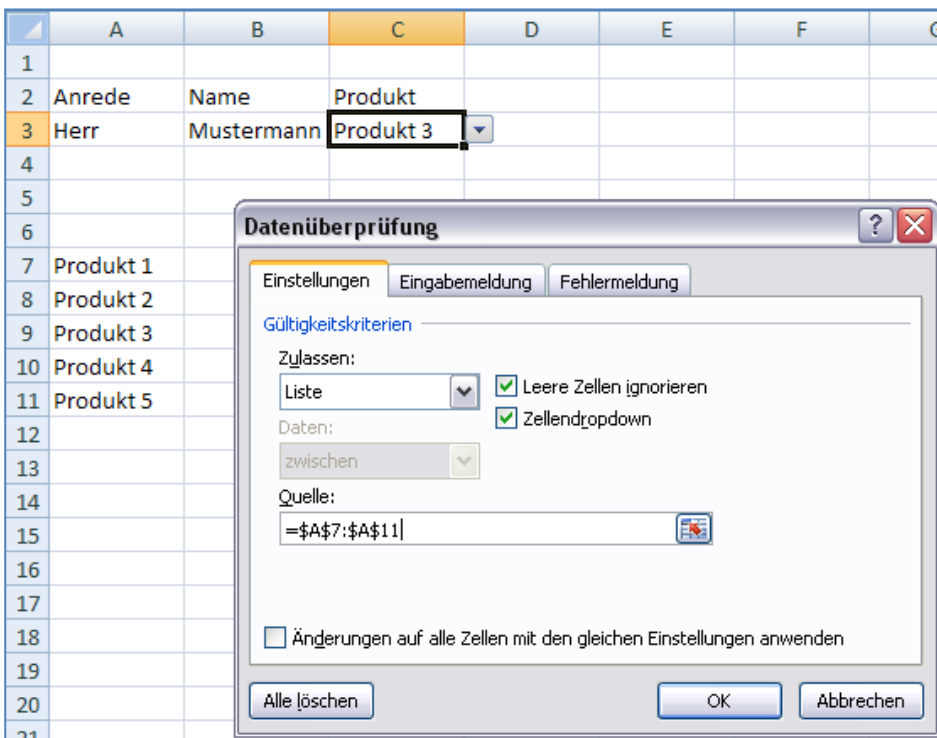
Schritt 3: Im Fenster „Datenüberprüfung“ ist die Registerkarte „Einstellungen“ auszuwählen. (Siehe Bild unten)

Schritt 4: In der Registerkarte „Einstellungen“ wird im Feld „Zulassen“ der Menüpunkt „Liste“ gewählt und im Feld „Quelle“ wird ein Bezug auf die Liste eingegeben.

Wenn sich die Liste in einem anderen Arbeitsblatt befindet, soll der festgelegte Name der Liste (im unserem Fall „Produkte“, siehe Bild oben) im Feld „Quelle“ angegeben werden.

Schritt 5: Es ist sicherzustellen, dass das Kontrollkästchen „Zellendropdown“ aktiviert ist. Das Kontrollkästchen „Leere Zellen ignorieren“ kann aktiviert oder deaktiviert werden, um anzugeben, ob die Zelle leer bleiben kann.

Nach der Angabe aller erforderlichen Daten wird die Funktion durch „Enter“ beendet. In der ausgewählten Zelle steht nun eine Dropdown-Liste zur Verfügung, aus der die definierten Daten ausgewählt werden können.



Ansprechpartner: Oleksandr Krasnopolskyy (Berater)

WHO IS WHO



Welches war Ihr schönstes Musikerlebnis?

Die Geräuschkulisse im Regenwald vor, während und nach einem schweren Regen

Welche Freizeitaktivitäten üben Sie aus?

Joggen, Yoga, Lesen

Was hat Sie am meisten beeindruckt?

Geglückte Notlandung bei vereisten Chassis

Was können Sie besonders gut kochen?

Schaschlik, Blinis

Was beherrschen Sie im Haushalt besonders gut?

Staubsaugen

Was haben Sie als schönstes Käuferlebnis empfunden?

Der „Kauf“ meines kleinen Bruders

Was gefällt Ihnen an der agens am besten?

Vielfältigkeit an Aufgabestellungen

Was treibt Sie an?

Streben nach Existenzsicherheit

Welche Themen würden Sie gern beschleunigen?

Verringerung der Umweltverschmutzung und der Menschenrechtsverletzungen

Was sind Ihre persönlichen Motivationen?

Wertvolles, erfülltes Dasein

Wen bewundern Sie am meisten?

Madonna

Was tun Sie, um sich zu entspannen?

Meditation, Musik hören

Wo hätten Sie gern Ihren Zweitwohnsitz?

Seychellen

Nennen Sie ein unentdecktes Traumreiseziel:

Nicht bekannt

IMPRESSUM



agens Consulting GmbH
Buchenweg 11 - 13, 25479 Ellerau
Ein Unternehmen der [agens Gruppe](#)
HRB 3660 NO AG Kiel

Fon: +49(0)4106-7777-0

Fax: +49(0)4106-7777-333

Internet: <http://www.agens.com>

E-Mail: <mailto:info@agens.com>

Geschäftsführer (vertretungsberechtigt im Sinne § 6 EGG/§ 6 TDG):

Dr. Stefan Giesecke, Florian Lang, Klaus Leitner

USt.-IDNr. : DE 176972447

Aktuelle Anzahl der Ausgaben (im Zwei-Monatsrhythmus): ca. 6.500

Zum Bestellen bzw. Abbestellen des „agens Audit & Risk Newsletters“ schicken Sie bitte eine E-Mail mit dem jeweiligen Betreff und Ihrem Namen an die folgende E-Mail Adresse:

rev-ace-newsletter-akte-pf@agens.com

Disclaimer

Alle Links zu externen Anbietern wurden zum Zeitpunkt ihrer Aufnahme auf ihre Richtigkeit überprüft. Da sich das Internet jederzeit wandelt, kann die agens Consulting GmbH nicht garantieren, dass diese Links zum Zeitpunkt des Besuchs a) noch zum Ziel führen oder b) noch dieselben Inhalte besitzen, wie zum Zeitpunkt der Aufnahme.

Insbesondere macht sich die agens Consulting GmbH nicht die Inhalte der Links zu Eigen und übernimmt dafür auch keine Verantwortung. Links zu externen Anbietern stellen keine Wertung oder eine Empfehlung der agens Consulting GmbH dar.

Der Inhalt dieses Newsletters ist urheberrechtlich geschützt. Ohne Genehmigung der agens Consulting GmbH darf der Inhalt dieser Seite in keiner Form reproduziert und/oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© agens Consulting GmbH, Ellerau, Deutschland, 2010. All rights reserved.

Stand: 28.Februar 2010