DuD
Datenschutz und Datensicherheit

MaRisk

Jochen Schlichting

Hintergrund

Die MaRisk (Mindestanforderungen an das Risikomanagement – 2006) sind die neue bindende Vorgabe[1] der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) für die Ausgestaltung des Risikomanagements in Kreditinstituten, die in Deutschland zugelassen sind. Sie sind die Umsetzung der bankaufsichtlichen Überprüfungsprozesse für die in Basel II geregelten Eigenkapitalvorschriften in deutsches Recht, die sogenannte „zweite Säule" von Basel II.

In den MaRisk hat die BaFin zusammen mit praxisnahen qualitätssichernden Gremien aus der Bankwirtschaft auf Basis des § 25a Abs.1 Kreditwesengesetz (KWG) die bestehenden Mindestanforderungen an das Betreiben von Handelsgeschäften (MAH – 1995), die Mindestanforderungen an die Ausgestaltung der Innenrevision (MaIR – 2000) und die Mindestanforderungen an das Kreditgeschäft (MaK – 2002) der Kreditinstitute zusammengefasst, aktualisiert und ergänzt. Sämtliche aus den MaH, MaIR und MaK in die MaRisk überführten bzw. modifizierten Anforderungen gelten weiterhin. Der Wegfall bisheriger Regelungen eröffnet den Kreditinstituten ein deutlich größeres Maß an Flexibilität in der Ausprägung. Neu hinzugekommene Anforderungen müssen jedoch erst mit Inkrafttreten von Basel II zum 1. Januar 2007 umgesetzt sein.

Das MaRisk-Rundschreiben ist modular stukturiert: Im allgemeinen Teil (Modul AT) befinden sich grundsätzliche Prinzipien für die Ausgestaltung des Risikomanagements. Im besonderen Teil (Modul BT) sind spezifische Anforderungen an die Organisation bzw. die Prozesse für das Management und Controlling von Adressenausfallrisiken, Marktpreisrisiken, Liquiditätsrisiken sowie operationellen Risiken niedergelegt. Außerdem wird dort ein Rahmen für die Ausgestaltung der internen Revision vorgegeben.

Bedeutung

Für die BaFin stellen die MaRisk den zentralen Baustein der qualitativen Aufsicht dar. Alle durch die MaRisk betroffenen Parteien (Aufsichtsbehörde, Kreditinstitute, Vorstände, Chief Compliance Officers, Chief Information Security Officers, Risikomanager, Datenschützer, Sicherheits- und Business Continuity-Spezialisten, Revisoren und Wirtschaftsprüfer) können jetzt auf einem einheitlichen Regelwerk aufsetzen. Durch die geforderte Umsetzung eines umfassenden Risikomanagements im Unternehmen werden zukünftig deutlich besser definierte Schnittstellen zwischen den beteiligten Gruppen existieren.

IT-Bezug

Im Zusammenspiel mit der in Basel II geforderten Gesamtrisikosteuerung in den Instituten konkretisiert die BaFin mit den am 20.12.2005 in Kraft getretenen MaRisk auch die Anforderungen an die IT über das bisher aus MaH, MaIR und MaK bekannte Maß hinaus. Neu sind die Anforderungen an das Management von operationellen Risiken (BTR 4), für die die MaRisk eine mindestens jährliche Identifizierung und Beurteilung, eine unverzügliche Analyse bedeutender Schadensfälle und ein Reporting an die Geschäftsleitung vorsieht. Dies betrifft sowohl die Steuerungs- als auch die operativen Prozesse und die damit verbundenen IT-Systeme. Das in diesem Kontext im Rahmen eines Notfallkonzeptes zu erstellende IT-Notfallmanagement ist nach den MaRisk als ein integraler Teil des gesamten Notfallmanagements des Unternehmens zu verstehen. Die IT-spezifischen Sachverhalte werden im Abschnitt 7 „Ressourcen" in den Unterabschnitten AT 7.2 „Technisch-organisatorische Ausstattung" und AT 7.3 „Notfallkonzept" dargelegt.

Ebenfalls neu ist die Anforderung, die Ausgestaltung und den Betrieb der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards (im Sinne von anerkannten Vorgehensweisen – „Stand der Technik" / „best-practice") abzustellen. Dabei werden in der Anlage 1 des MaRisk (Regelungstext mit Erläuterungen) beispielhaft das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der internationale Sicherheitsstandard ISO 17799 aufgeführt. Gemeinsam ist beiden ein strategisch-organisatorisches Informationssicherheitsmanagement-System, welches über klare Schnittstellen in das unternehmensweite Risikomanagement einzubinden ist. Funktionieren kann dies auf Basis praktischer Erfahrungen nur, wenn die Sicherheitsmetriken in der IT bekannt sind und nicht theoretische Key Performance Indikatoren (KPIs) das Gesamtbild verzerren. MaRisk wird damit selbst zu einem Prüfstandard.

Prüfung

Mit einer Prüfung der ergänzten Elemente in den Mindestanforderungen durch die BaFin ist nicht vor dem 01. Januar 2008 zu rechnen. Auf ein umfassendes Notfallmanagement mit einer spezifischen Ausprägung für den Bereich IT sowie risikosenkende Prozesse und Maßnahmen sollte dennoch nicht verzichtet werden. Verantwortliche dürfen bei Untätigkeit nicht auf Nachsicht hoffen. Elementar ist in diesem Zusammenhang der Paradigmenwechsel zu einem risikoorientierten Prüfungsansatz, der an den institutsspezifischen Gegebenheiten ansetzt (z.B. Geschäftsprozesse, Geschäftsumfang, Komplexität der betriebenen Geschäfte), um angemessene Feststellungen treffen zu können. Die Zeiten formeller Checklisten sind zwar noch nicht ganz vorbei, aber die Compliance mit den MaRisk erfordert zukünftig einen hohen Grad an professionellem Sicherheitsverständnis, kombiniert mit Erfahrung und Projektmanagementkenntnissen.

Handlungsbedarf

Von den deutschen Finanzinstituten wurde das Thema der MaRisk als ein Schlüsselthema erkannt, und spätestens seit dem 2. Quartal 2006 wird die Umsetzung mit hoher Intensität verfolgt, gilt es doch bis zum 01. Januar 2007 die Organisation von Verantwortlichkeit, Haftung und fortlaufender Risikokontrolle entsprechend den Mindestanforderungen zu implementieren.

Allein die Komplexität der unternehmensweiten Verkettungen und Abhängigkeiten, die aus den MaRisk erwachsen, wird oft unterschätzt – die MaRisk fordern eben deutlich mehr als ein simples Notfallhandbuch.

[1] http://www.bundesbank.de/bankenaufsicht/bankenaufsicht_marisk.php, veröffentlicht durch Rundschreiben 18/2005 am 20. Dezember 2005.