Anforderungen an Risikomanagement und internes Kontrollsystem – das neue FINMA-Rundschreiben zur Corporate Governance

Die Eidgenössische Finanzmarktaufsicht FINMA publizierte am 1. November 2016 ihr neues Rundschreiben 2017/1 „Corporate Governance – Banken“, welches die Anforderungen des Aufsichtsorgans in Bezug auf Corporate Governance, Risikomanagement und internes Kontrollsystem umfasst.

Die neuen Anforderungen sollten nicht unterschätzt werden

Das neue Rundschreiben 2017/1 fasst die Bestimmungen des Rundschreibens 2008/24 („Überwachung und interne Kontrolle bei Banken“) sowie die mit den damit verbundenen FAQs und in anderen Rundschreiben definierten Anforderungen zusammen. Die FINMA überarbeitete dabei auch die Rundschreiben 2008/21 („Operationelle Risiken – Banken“) und 2010/1 („Vergütungssysteme“).

Diese neuen und angepassten Rundschreiben enthalten die neuesten Erkenntnisse aus der Finanzkrise und den internationalen Standards. Die überarbeiteten Rundschreiben wurden am 1. November 2016 publiziert und berücksichtigen teilweise die Kommentare, die von der Branche während der Konsultationsphase erhoben wurden. Sie treten am 1. Juli 2017 in Kraft.

Prinzipienbasierte Regulierung

Die FINMA strafft ihre Regulierung, indem sie die überarbeiteten Anforderungen in Bezug auf die zugrunde liegenden Prinzipien definiert. Das Prinzip der Verhältnismässigkeit wird in den überarbeiteten Anforderungen verankert, wodurch die Institute die Anforderungen so umsetzen können, dass ihrem spezifischen Geschäftsmodell und ihrem Risikoprofil Rechnung getragen wird.

Moderne Anforderungen an die Corporate Governance

Das neue Rundschreiben „Corporate Governance – Banken“ unterstreicht die Bedeutung einer modernen Corporate Governance. Es legt Minimalanforderungen für die Zusammensetzung des Verwaltungsrats und die Qualifikationen seiner Mitglieder fest. Auch die Anforderungen für die Entwicklung und Implementierung eines umfassenden Risikomanagements inklusive eines internen Kontrollsystems wurden neu definiert.

Wir sind der Meinung, dass die erhöhten Anforderungen im Bereich Rahmenkonzept für das institutsweite Risikomanagement und internes Kontrollsystem Änderungen an den bestehenden Organisationen erfordern werden. Es dürfte anspruchsvoll werden, diese Änderungen zu implementieren. Gleichzeitig können aber dadurch die Institute ihre Risikokultur und ihr Kontrollbewusstsein über die ganze Organisation hinweg verbessern.

pwc

1 Rahmenkonzept für das institutsweite Risikomanagement und Aufsicht durch den Verwaltungsrat

Gemäss dem FINMA-Rundschreiben müssen alle Banken ein umfassendes Rahmenkonzept für das institutsweite Risikomanagement implementieren.

Das Rahmenkonzept ist ein übergreifendes Dokument, welches die *Risikopolitik, Risikotoleranz und Risikolimiten* einer Bank abdeckt. Weiter müssen die Banken die verwendeten Instrumente und organisatorischen Strukturen beschreiben, mit welchen die definierten Risiken innerhalb jeder Risikokategorie identifiziert, bewertet, überwacht und gemeldet werden.

Der Verwaltungsrat muss das Rahmenkonzept für das institutsweite Risikomanagement jährlich evaluieren und genehmigen. Die Genehmigung durch den Verwaltungsrat geht weiter, als nur die Einhaltung rein formaler Aspekte zu bestätigen. Der Schlüssel liegt in der Beurteilung, ob das Rahmenkonzept effektiv umgesetzt wurde.

Schlüsselfragen …

- Haben Sie alle Risiken im Zusammenhang mit den Tätigkeiten ihres Institutes identifiziert und dokumentiert?
- Haben Sie Ihre Risikotoleranz in Bezug auf diese Tätigkeiten festgelegt und dokumentiert?
- Wurde die Risikotoleranz durch eine Reihe von Limiten und Schlüsselindikatoren definiert?
- Stellen Ihre bestehenden Prozesse, Richtlinien und Verfahren ein umfassendes Rahmenkonzept für das institutsweite Risikomanagement dar? Sind sie dokumentiert?
- Verfügt Ihre Organisation über angemessene Kontrollen, um diese Risiken zu überwachen?
- Sind die Kontrollen dokumentiert? Beurteilen Sie deren Wirksamkeit regelmässig?
- Erhält Ihr Verwaltungsrat zeitgerecht präzise und vollständige Informationen über die Risiken und internen Kontrollen, um die Einhaltung des Risiko Rahmenkonzeptes sicherzustellen und um die eingegangenen Risiken zu hinterfragen und weitere Entscheidungen zu treffen?
- Stellt Ihr Prozess zur Risikoidentifizierung und -beurteilung die zeitgerechte Identifikation neuer Risiken sicher?

2 Implementierung von Kontrollinstanzen

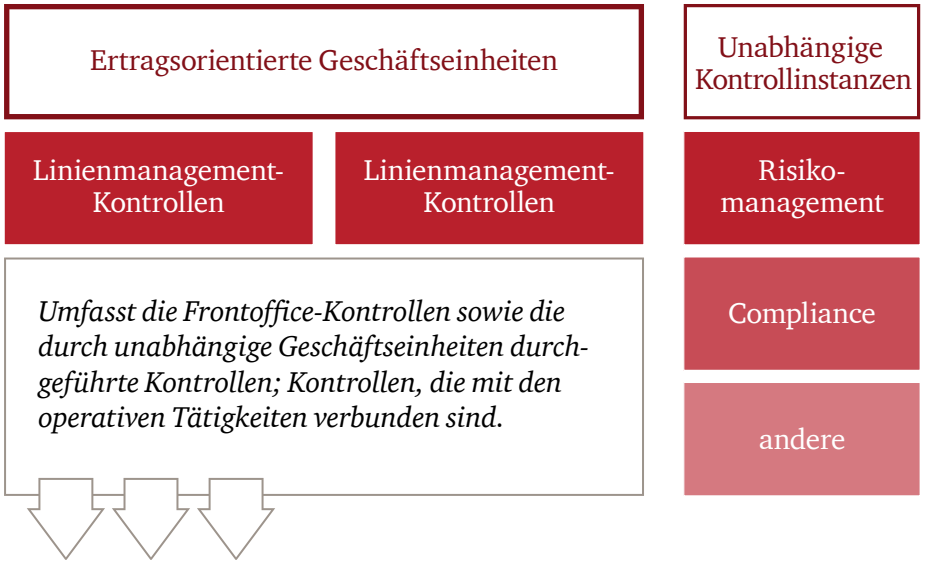
Im Rahmen des internen Kontrollsystems benötigen die Banken mindestens zwei Kontrollinstanzen: *die ertragsorientierten Geschäftseinheiten und die unabhängigen Kontrollinstanzen*. Von den Banken wird implizit die Implementation des „Three Lines of Defence"-Modell erwartet, basierend auf Frontoffice-Kontrollen, Support-Funktionen/Back-office-Kontrollen und der Internen Revision. Dies ist ein international anerkannter Standard.

Kontrollen der ertragsorientierten Geschäftseinheiten

Das Ziel von Kontrollen in den ertragsorientierten Geschäftseinheiten ist die Übernahme der Verantwortung von eingegangenen Risiken durch das Frontoffice. Dies erfordert Kontrollen, um die Einhaltung der internen Richtlinien und Vorschriften der Bank sicherzustellen, einschliesslich der Verantwortung für die Einhaltung der Risikostrategie der Bank. Die Anreizsysteme der Banken sollten die ertragsorientierten Geschäftseinheiten darin bestärken, die Risiken effektiv und innerhalb der festgelegten Regeln zu verwalten. Es sollten interne Prozess definiert werden, um Ausnahmen richtig zu handhaben.

Unabhängige Kontrollinstanzen

Die unabhängigen Kontrollinstanzen überwachen Risiken, die Einhaltung interner Richtlinien sowie rechtliche und regulatorische Anforderungen. Normalerweise werden die unabhängigen Kontrollinstanzen als „Risiko"- und „Compliance"-Funktionen definiert.



Schlüsselfragen …

- Wie unterscheiden Sie zwischen den Kontrollen der ertragsorientierten Geschäftseinheiten und den unabhängigen Kontrollinstanzen?
- Haben Sie in den ertragsorientierten Geschäftseinheiten Kontrollen definiert und dokumentiert (1. Line of Defence)?
- Wer ist für die Kontrollen der ertragsorientierten Geschäftseinheiten verantwortlich?
- Wie überwachen und erstatten Sie Bericht über die Kontrollen in den verschiedenen Kontrollinstanzen?
- Ist das Anreizsystem auf die Risikotoleranz ausgerichtet?
- Gibt es einen formalisierten Prozess für die Handhabung von Ausnahmen (Folgenmanagement)?

Kontakte

PwC
Birchstrasse 160
Postfach, 8050 Zürich

Andrin Bernet
Partner
andrin.bernet@ch.pwc.com
+41 58 792 24 44

Yousuf Khan
Senior Manager
yousuf.khan@ch.pwc.com
+41 58 792 15 62

Alena Nicolai
Senior Manager
alena.nicolai@ch.pwc.com
+41 58 792 27 28

Alexandra Burns
Senior Manager
alexandra.burns@ch.pwc.com
+41 58 792 46 28