Anhang 1: Beschreibung des Referenzmodells (Soll-Objekts) zu § 63 Abs. 4 zweiter Satz BWG

Kontrollumfeld

Das Kontrollumfeld stellt den Rahmen eines wirksamen IKS dar und beeinflusst sowohl die Grundeinstellung einer Organisation hinsichtlich Risiko und Kontrollen als auch die Art und Weise, wie Kontrollen in die Arbeitsabläufe des Unternehmens eingebunden werden. Es beinhaltet die Risikophilosophie und das Risikobewusstsein der Organisation sowie Überwachungs- und Leitungsfunktionen der Geschäftsleitung.

Das Kontrollumfeld eines Unternehmens wird im Wesentlichen von den folgenden Elementen geprägt:

- Integrität und ethische Werte: Einwandfreie Integrität und ethische Werte, insbesondere auf den oberen Führungsebenen, sind entwickelt, werden verstanden und bilden die Verhaltensregel für das Durchführen der Geschäftsprozesse.
- Geschäftsleitung: Die Geschäftsleitung versteht und verfolgt ihre Überwachungsverantwortung in Bezug auf die Geschäftsprozesse und die entsprechende interne Überwachung.
- Führungsphilosophie und Geschäftsgebaren: Der Führungsstil und das Geschäftsgebaren der Führungskräfte unterstützen eine wirksame interne Überwachung der Geschäftsprozesse.
- Organisationsstruktur: Die Organisationsstruktur des Unternehmens fördert eine wirksame interne Überwachung der Geschäftsprozesse.
- Befähigung zur Finanzberichterstattung: Das Unternehmen beschäftigt Experten im Bereich der Geschäftsprozesse und der diesbezüglichen Überwachungsfunktionen.
- Entscheidungskompetenz und Verantwortlichkeit: Führungskräften und Mitarbeitern werden sachgerecht Verantwortlichkeit und Verantwortung zugeordnet, um eine wirksame Überwachung der Geschäftsprozesse zu ermöglichen.
- Personal: Personalvorschriften und -vorgehensweisen sind so gestaltet und umgesetzt, dass sie eine wirksame Überwachung der Geschäftsprozesse fördern.

Risikobeurteilungsprozess des Unternehmens

Der Risikobeurteilungsprozess des Unternehmens identifiziert jene Risiken, welche in das IKS einbezogen werden müssen. Hierbei werden die einzelnen Risiken im Hinblick auf ihre Auswirkungen und Eintrittswahrscheinlichkeiten untersucht und Maßnahmen definiert, um diese zu vermeiden bzw. zu verringern.

Relevante Informationssysteme, damit verbundene Geschäftsprozesse und Kommunikation

Dies beinhaltet all jene Informationssysteme, welche für die aufsichtsrechtlichen Anforderungen relevant sind. Es ist von wesentlicher Bedeutung, dass alle benötigten Informationen erkannt, erfasst und verarbeitet werden. Nur so wird es den Mitarbeitern ermöglicht, ihre Verantwortlichkeit zu übernehmen. Wirksame Kommunikation erfolgt hierbei abwärts, lateral und aufwärts in der Organisation.

Kontrollaktivitäten

Kontrollaktivitäten sind Vorschriften und Verfahren, welche sicherstellen sollen, dass Risikoreaktionen wirksam ausgeführt werden. Dadurch soll sichergestellt werden, dass jene

Maßnahmen ergriffen werden, die notwendig sind, um Risiken entgegenzuwirken. Kontrollaktivitäten werden auf allen Ebenen einer Organisation und in sämtlichen Funktionen wahrgenommen. Unter anderem können die folgenden Kontrollaktivitäten durchgeführt werden:

- Autorisierung
- Leistungskontrolle
- Informationsverarbeitung
- physische Kontrolle
- Funktionentrennung/Vier-Augen-Prinzip

Im Zuge der Beurteilung von Kontrollaktivitäten durch die Geschäftsleitung wird analysiert, inwiefern einzelne Kontrollen oder Kombinationen von Kontrollen geeignet sind, Verstöße gegen aufsichtsrechtliche Bestimmungen zu vermeiden oder aufzudecken.

Die Geschäftsleitung muss auch in angemessener Art und Weise auf jene Risiken eingehen, welche im Zusammenhang mit der Nutzung von IT entstehen. Hierbei müssen IT-Kontrollen durchgeführt werden, welche sicherstellen, dass die Integrität und Sicherheit von Daten gewährleistet ist.

Überwachung der Kontrollen

Die Gesamtheit des unternehmensweiten Risikomanagements wird überwacht und, wenn erforderlich, angepasst. Somit soll sichergestellt werden, dass die Vorgaben des IKS eingehalten werden.

Die Überwachung wird von der Geschäftsleitung koordiniert. Sie kann hierbei auf verschiedene Mittel zurückgreifen, zum Beispiel können Kontrollen durch die Interne Revision oder andere Mitarbeiter überwacht werden.