Prüfung von Internen Revisionssystemen (Quality Assessments)

Im April 2017 veröffentlichte das DIIR – Deutsches Institut für Interne Revision e. V. – den Revisionsstandard Nr. 3 über den Inhalt der Prüfung eines Internen Revisionssystems und definiert die berufsständischen Anforderungen für die Durchführung einer Qualitätsbeurteilung gemäß den Internationalen Standards für die berufliche Praxis der Internen Revision des Institute of Internal Auditors (IIA) (IIA-Standards; hier insbesondere AS 1300 ff. - Quality Assessment).

Dieser Revisionsstandard wurde gemeinschaftlich mit dem Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) erarbeitet, welches einen inhaltlich weitestgehend gleichlautenden Standard für Prüfungen von Internen Revisionssystemen zur Nutzung durch Wirtschaftsprüfer herausgegeben hat (IDW PS 983: „Grundsätze ordnungsmäßiger Prüfung von Internen Revisionssystemen").

Die Prüfung eines Internen Revisionssystems (im Folgenden auch: IRS-Prüfung) kann sich aus den Internationalen Grundlagen für die berufliche Praxis der Internen Revision (International Professional Practices Framework – IPPF) des IIA (The Institute of Internal Auditors) oder aus aktienrechtlichen Vorgaben ergeben.

Nach dem vom IIA herausgegebenen Attribute Standard AS 1312 – Externe Beurteilungen – muss mindestens alle fünf Jahre eine externe Beurteilung der Internen Revision von einem qualifizierten und unabhängigen Beurteiler durchgeführt werden, um eine von Interessenkonflikten freie Beurteilung über die Übereinstimmung mit der Definition der Internen Revision und den Standards sowie die Einhaltung der Berufspflichten (Ethikkodex) zu gewährleisten. Andernfalls kann eine Aussage zur Übereinstimmung mit den international anerkannten Standards für die berufliche Praxis der Internen Revision nicht abgegeben werden (AS 1321).

§ 107 Abs. 3 Satz 2 AktG sieht vor, dass der Aufsichtsrat aus seiner Mitte einen Prüfungsausschuss bestellen kann, der sich neben der Überwachung der Abschlussprüfung befasst mit

- der Überwachung des Rechnungslegungsprozesses,
- der Wirksamkeit
- des internen Kontrollsystems,
- des Risikomanagementsystems und
- des internen Revisionssystems.

In der Gesetzesbegründung zum BilMoG wird ausgeführt, dass die in § 107 Abs. 3 Satz 2 AktG (der zunächst lediglich die innere Ordnung des Aufsichtsrats betrifft) genannten Bereiche als eine Konkretisierung der allgemeinen Überwachungsaufgabe des Aufsichtsrats aus § 111 Abs. 1 AktG anzusehen sind. Zudem wird in der Gesetzesbegründung klargestellt, dass der Aufsichtsrat die genannten Aufgaben selbst wahrzunehmen hat, wenn er keinen Prüfungsausschuss einrichtet. Die Überwachungsaufgaben des Aufsichtsrats umfassen auch die Maßnahmen des Vorstands, die sich auf die Begrenzung der Risiken aus möglichen Verstößen gegen gesetzliche Vorschriften und interne Richtlinien (Compliance) beziehen. Dem trägt Ziffer 5.3.2 des Deutschen Corporate Governance Kodex (DCGK) Rechnung, der zu den Aufgaben des Prüfungsausschusses ausführt, dass sich der Prüfungsausschuss – falls kein anderer Ausschuss damit betraut ist – auch mit der Compliance des Unternehmens befasst.

Während die Befassung durch den Aufsichtsrat und den Prüfungsausschuss voraussetzt, dass die entsprechenden Systeme vorhanden sind, ist – ungeachtet der Pflichten nach § 91 Abs. 2 AktG – die Einrichtung, Ausgestaltung und Überwachung der Systeme eine im Organisationsermessen des Vorstands stehende unternehmerische Entscheidung, durch die der Vorstand vor dem Hintergrund der unternehmensindividuellen Gegebenheiten seinen allgemeinen Organisations- und Sorgfaltspflichten nachkommt. Die konkrete Ausgestaltung ist hierbei insbesondere von Art, Umfang und Komplexität der Geschäftstätigkeit des Unternehmens abhängig.

Die durch den Aufsichtsrat bzw. den Prüfungsausschuss zu überwachenden Corporate Governance Systeme

- Internes Kontrollsystem (IKS),
- Risikomanagementsystem (RMS),
- Internes Revisionssystem (IRS) und
- Compliance Management System (CMS)

sind weder im Gesetz noch in der Literatur eindeutig definiert. Zur Systematik des Zusammenspiels dieser Corporate Governance Systeme lehnt sich dieser DIIR Revisionsstandard an das COSO-Rahmenwerk zum unternehmensweiten Risikomanagement an.

Bei der Überwachung der eingerichteten Corporate Governance Systeme wird der Vorstand regelmäßig von der Internen Revision unterstützt. Dabei prüft die Interne Revision auch das unternehmensweite Interne Kontrollsystem und Risikomanagementsystem. Darüber hinaus unterliegt das Interne Revisionssystem selbst einer regelmäßigen Selbstbeurteilung und einem externen Quality Assessment. Für den Aufsichtsrat bzw. Prüfungsausschuss kann es als Grundlage für die eigene Beurteilung ebenfalls von Interesse sein, dass einzelne oder mehrere Corporate Governance Systeme durch die Interne Revision geprüft werden bzw. ein Prüfer für Interne Revisionssysteme[DIIR] mit der Prüfung des Internen Revisionssystems nach diesem Revisionsstandard beauftragt wird. Die Prüfung der Wirksamkeit dieser Systeme durch eine unabhängige und objektive Interne Revision bzw. einen Prüfer für Interne Revisionssysteme[DIIR] kann dem objektivierten Nachweis der ermessensfehlerfreien Ausübung der Organisations- und Sorgfaltspflichten des Vorstands und des Aufsichtsrats dienen.

Dieser DIIR Revisionsstandard behandelt die Prüfung der Internen Revision als eine wesentliche Funktion innerhalb des Corporate Governance Systems und als dritte Verteidigungslinie im Three-Lines-of-Defense Modell. Das Three-Lines-of-Defense Modell beschreibt die möglichen Verteidigungslinien in einem Unternehmen innerhalb des Corporate Governance Systems. In der ersten Verteidigungslinie sind die Kontrollaktivitäten der operativen Prozesse enthalten. Die zweite Verteidigungslinie überwacht die Kontrollaktivitäten der ersten Verteidigungslinie und stellt einen wesentlichen Bestandteil des Risiko- und Compliance-Managements des Unternehmens dar. Die dritte Verteidigungslinie ist eine unabhängige Instanz, die weder in die operativen Prozesse des Unternehmens noch in die Steuerungs- und Kontrollaktivitäten der zweiten Verteidigungslinie eingebunden ist. Sie wird regelmäßig durch die Interne Revision wahrgenommen.

Die Zielsetzung einer nach diesem DIIR Revisionsstandard durchgeführten Systemprüfung liegt in der Beurteilung, inwieweit das Unternehmen durch Einrichtung eines IRS Vorsorge getroffen hat, dass die Einrichtung einer Internen Revisionsfunktion und die unabhängige und objektive Erbringung von Prüfungs- und Beratungsdienstleistungen durch die Interne Revision in Übereinstimmung mit den verbindlichen Elementen des IPPF erfolgen. Ziel ist es dagegen nicht, eine Aussage darüber zu treffen, ob einzelne oder sämtliche Revisionsaufträge durch die Revisionsfunktion fehlerfrei durchgeführt wurden oder ob einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder durchgeführte Maßnahmen als Reaktion auf Feststellungen der Internen Revision geeignet oder wirtschaftlich sinnvoll sind.

Für die Prüfung der Führungs-, Überwachungs-, Risikomanagement- und Kontrollprozesse durch die Interne Revision hat das IIA die Internationalen Grundlagen für die berufliche Praxis der Internen Revision (IPPF) herausgegeben. In Ergänzung dazu hat das DIIR gesonderte Revisionsstandards u. a. zur Prüfung des Risikomanagementsystems und des Anti-Fraud-Management-Systems veröffentlicht.

Die Prüfung des IRS ist von der Beurteilung der Internen Revision im Rahmen von Abschlussprüfungen zu unterscheiden. Hat ein Abschlussprüfer die Interne Revision als voraussichtlich relevant für die Abschlussprüfung eingestuft und will er deren Ergebnisse verwerten, muss er eine Einschätzung zur Wirksamkeit der Internen Revision vornehmen. Diese Einschätzung entspricht in Art und Umfang nicht einer Systemprüfung nach diesem DIIR Revisionsstandard und es wird dafür kein eigenständiges Prüfungsurteil erteilt.

Dieser DIIR Revisionsstandard ist erstmals anzuwenden bei Prüfungen von IRS, die nach dem 30.04.2017 beauftragt werden.