CORPORATE GOVERNANCE

UNTERNEHMENSSTEUERUNG UND ÜBERWACHUNG MIT SYSTEM

Unternehmensrisiken fordern eine stetige Steuerung und Überwachung zur Sicherstellung einer guten Corporate Governance. Wichtig ist, dass die unterschiedlichen Systeme ineinandergreifen.

Die systematische Steuerung von Unternehmensrisiken ist ein Komplex von betriebswirtschaftlich sinnvollen und rechtlich notwendigen Maßnahmen. Ein diffuses Risikoumfeld und die möglichen Konsequenzen für die Unternehmen erfordern zunehmend betriebswirtschaftliche Reaktionen in einem ganzheitlichen Managementsystem zur nachhaltigen Wahrung einer guten Unternehmensführung (Corporate Governance).

Steuerungs- und Überwachungspflichten

Die Ausgestaltung der Überwachung im Unternehmen ist ein wesentlicher Eckpfeiler guter Unternehmensführung, für dessen Einrichtung und Funktionsfähigkeit die Geschäftsleitung und das Aufsichtsorgan zuständig und verantwortlich sind. Das Gesellschaftsrecht verlangt von der Geschäftsleitung, bei der Führung der Geschäfte die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Die hieraus abzuleitende abstrakte Sorgfaltspflicht ist somit Grundlage jeglichen Handelns im Geschäftsverkehr und wirft zugleich die Frage nach der Art und Weise der Ausgestaltung auf.
Die Sorgfaltspflicht wurde durch das Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG) vom 27. April 1998 in § 91 Abs. 2 AktG (für GmbH gemäß Gesetzesbegründung analog anwendbar) insoweit konkretisiert, dass die Geschäftsleitung zur Einrichtung eines Überwachungssystems zur Früherkennung von bestandsgefährdenden Entwicklungen verpflichtet ist. Die Begründung zum Regierungsentwurf verdeutlicht, dass die Geschäftsleitung für ein angemessenes Risikomanagementsystem (RMS) und eine angemessene interne Revision (IR) zu sorgen hat, wobei die Ausprägung solcher Systeme auch von der Unternehmensgröße und Branche abhängen kann. Obwohl ein Compliance Management System (CMS) nicht explizit genannt wird, lässt sich aus dem beschriebenen Regelungsumfang des RMS, das auch Verstöße gegen gesetzliche Vorschriften erkennen soll, ein direkter Compliance-Bezug herleiten. Das Interne Kontrollsystem (IKS) kann als logische Konsequenz oder gar als integraler Bestandteil des RMS verstanden werden. Die Entscheidung über den Grad der Ausgestaltung liegt im Ermessen der Geschäftsleitung.

In Abhängigkeit der zu steuernden Risiken müssen oder können für bestimmte Unternehmensbereiche und Prozesse konkrete Anforderungen aus den rechtlichen und regulatorischen Vorgaben abgeleitet werden. Das Fehlen eines solchen Systems kann allerdings eine Pflichtverletzung nach § 93 Abs. 2 AktG darstellen. Im Zweifelsfall trifft den Vorstand die Beweislast. Das Aufsichtsorgan hat nach § 107 Abs. 3 S. 2 AktG i. V. m. § 111 Abs. 1 AktG den Pflichtenrahmen der Geschäftsleitung wirksam zu überwachen. Die Konkretisierung der Überwachungsaufgaben des Aufsichtsorgans durch das Gesetz zur Modernisierung des Bilanzrechts (BilMoG) vom 29. Mai 2009 verdeutlicht zwar mittelbar jedoch konkreter im Verhältnis zu § 91 Abs. 2 AktG die Notwendigkeit zur Einrichtung der vorangestellten Teilsysteme durch die Geschäftsleitung.
Verstoßen Vorstand oder Aufsichtsrat gegen die genannten Pflichten, bietet das Gesellschaftsrecht und das Deliktrecht Anspruchsgrundlagen für Haftung und Schadenersatz, während sich Bußgeldansprüche bei unterlassener Aufsicht aus dem OWiG ergeben können. Der Deutsche Corporate Governance Kodex (DCGK) katalogisiert und konkretisiert fakultativ die Grundsätze guter Unternehmensführung und somit auch die Einrichtung von Überwachungssystemen insbesondere für börsennotierte Unternehmen. Die dargestellten Sorgfalts- und Aufsichtspflichten lassen sich folglich in die vier Säulen guter Unternehmensführung einteilen:

- das Risikomanagementsystem (RMS)
- das interne Kontrollsystem (IKS)
- das Compliance Management System (CMS)
- das interne Revisionssystem (IRS)

Für Zwecke dieses Artikels wird Corporate Governance auf die oben dargestellten Systeme reduziert, gleichwohl werden diese durch den erweiterten Regelungskreis des DCGK und sonstige (Selbst)verpflichtungen und Standards ergänzt.

Teilsysteme der Corporate Governance

Risiken existieren in jedem Unternehmen und können mit erheblichen finanziellen Schäden, Reputationsschäden und Haftungsrisiken für das Unternehmen und die Unternehmensorgane verbunden sein. Ausgehend davon stehen Un-

ternehmen zunehmend vor der Herausforderung, geeignete methodische Ansätze für eine systematische und juristisch belastbare Identifikation, Bewertung und Steuerung von Risiken zu entwickeln. Wesentliches Ziel des Risikomanagements ist die systematische Erfassung und Dokumentation der relevanten Unternehmensrisiken als Basis für die gezielte Ableitung von risikomindernden Maßnahmen und Kontrollen auf Unternehmens- und Prozessebene. Das IKS, hier stellvertretend für Grundsätze, Verfahren, Maßnahmen und Kontrollen, umfasst die von den gesetzlichen Vertretern im Unternehmen eingeführten Regelungen, die auf die ordnungsgemäße Durchführung der Unternehmensprozesse gerichtet sind, um Risiken zu begegnen (IDW PS 261 Tz. 19).

Die interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, die darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation dabei, ihre Ziele zu erreichen, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen, Führungs- und Überwachungsprozesse bewertet und zu verbessern hilft (IPPF des Institute of Internal Auditors).

Bedingt durch die besondere Relevanz von Compliance-Risiken für das Unternehmen, seine Stakeholder und gegebenenfalls eine Aufsichtsbehörde verbunden mit den organisatorischen Anforderungen, werden Compliance-Risiken üblicherweise durch ein gesondertes CMS erfasst, bewertet (Compliance RMS) und gesteuert (Compliance IKS). Unter einem CMS sind die eingeführten Grundsätze und Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie gegebenenfalls von Dritten abzielen, das heißt auf die Einhaltung bestimmter Regeln und damit auf die Verhinderung von wesentlichen Regelverstößen (IDW PS 980 Tz. 6). Die Abgrenzung der Systeme kann und sollte nicht überschneidungsfrei sein, denn erst das Ineinandergreifen lässt einen ganzheitlichen und effizienten Umgang mit allen Risiken zu.

Steuerung und Überwachung am Beispiel Einkauf

Am Beispiel eines vereinfachten Einkaufsprozesses wird das Zusammenspiel der Teilsysteme aufgezeigt. Der Beschaffung von Waren und Dienstleistungen liegen beispielsweise Risiken der Fehlinvestition, Produktionsausfallrisiken, Vermögensschäden durch Mitarbeiter (Fraud) und Risiken des unlauteren Wettbewerbs zugrunde. Aufgrund der durch das RMS bewerteten Risikoanfälligkeit von Einkaufstransaktionen wird eine Einkaufsrichtlinie (IKS) erstellt, um Prozesse und Vorgaben zu definieren. Diese kann abstrakt folgende Prozessschritte vorgeben: 1. Bedarfsmeldung, 2. Investitionsentscheidung, 3. Ausschreibung und Lieferantenauswahl, 4. Bestellung, 5. Rechnungs- und Wareneingangsprüfung und 6. Zahlung. Nun können ergänzend und innerhalb der einzelnen Arbeitsschritte zusätzliche Prozessrisiken wie unautorisierte Bestellungen, unwirtschaftlicher Lieferant oder unvollständige Lieferungen entstehen, die für gewöhnlich in einem kausalen und somit konkretisierenden Zusammenhang zu den übergeordneten Risiken im Einkauf stehen und daher einer weitergehenden Überwachung (IKS) unterliegen sollten. Folglich ist dem Unternehmen zu raten, zum Beispiel Funktionstrennungen, Zugriffsbeschränkungen oder Vier-Augen-Prinzipien in den jeweiligen Prozessschritten zu implementieren. Das Risiko des unlauteren Wettbewerbs und Fraud, welches typischerweise als Compliance-Risiko geführt und durch ein CMS gesteuert wird, ist eng mit dem vorhandenen IKS verknüpft und kann durch spezifische Compliance-Maßnahmen wie etwa Lieferanten-Integritäts-Screenings und Compliance-Schulungen ergänzt werden. Die IR prüft ausgehend von ihrer eigenen Risikoeinschätzung, die in der Regel vom RMS nicht substanziell abweichen sollte, das zugrunde liegende IKS, CMS und auch das für die Risikoeinschätzung ursächliche RMS.

Plädoyer für eine stärkere Verzahnung

Das RMS bestimmt die Tragweite und den Umfang des IKS. Die wirksame Ausgestaltung des IKS bestimmt wiederum das Maß und somit die Bewertung des Restrisikos, aber auch die Intensität der internen Revisionstätigkeiten. Die Verzahnung von Identifikations- und Bewertungsmechanismen für sämtliche Unternehmensrisiken, die Verknüpfung und einheitliche Dokumentation von zugrunde liegenden Prozessen, Maßnahmen und Kontrollen mit den jeweiligen Risiken sowie die Festlegung von (neuen) Kontrollsystemen auf Basis eines gemeinsamen Ausgestaltungsstandards (Control Framework) steigert die Sicherheit, Effektivität und Qualität der einzelnen Teilsysteme. Im Ergebnis bündelt ein integrativer Ansatz ablauf- und aufbauorganisatorische Corporate-Governance-Teilsysteme im Unternehmen, um insbesondere die Synergien zwischen den Funktionsbereichen zu heben und Interdependenzen zu identifizieren (Governance, Risk und Compliance-Ansatz), woraus schließlich ein ganzheitliches und somit integriertes Managementsystem hervorgeht.

DER AUTOR

Florian Maciuca ist als Wirtschaftsprüfer und Senior Manager im Bereich Corporate Governance Assurance bei Deloitte tätig und verfügt über langjährige Erfahrung in der weltweiten Prüfung und Beratung von Corporate Governance Systemen.