IM FOKUS

Risikomanagement als Aufgabe für Aufsichtsräte öffentlicher Unternehmen

Die Mehrheit der öffentlichen Verwaltungen in Deutschland hat große Teile ihrer Aufgaben an privatrechtliche Unternehmen ausgegliedert und damit gleichzeitig die Steuerungs- und Kontrollfunktionen an die Geschäftsführungen und Aufsichtsräte der öffentlichen Unternehmen übertragen. Damit einher geht ein Mangel an direkter Einflussnahme seitens der Kommunalverwaltung. Dieser erlangt besonderes Gewicht, denn trotz der Ausgliederung birgt jedes unternehmerische Handeln der Beteiligungsunternehmen Risiken für die jeweilige Gebietskörperschaft.[1]

Öffentliches Risikomanagement

Die Risiken für öffentliche Unternehmen ergeben sich bereits aus der Tatsache, dass Letztere eine besondere Verpflichtung zum Umgang mit den ihnen anvertrauten Mitteln und zur Aufrechterhaltung des Geschäftsbetriebs haben.[2] Zudem befinden sie sich in einem unausweichlichen Spannungsverhältnis zwischen der Erfüllung des öffentlichen Auftrags im Sinne einer gemeinwohlorientierten Zweckerfüllung und einem betriebswirtschaftlichen Ertragsdenken.[3]

Das Bewusstsein für Risiken, die mit Beteiligungsunternehmen einhergehen, ist in den letzten Jahren in Deutschland sukzessive gestiegen und führte von der Bundes- bis zur kommunalen Ebene zur Einführung von Public Corporate Governance Kodizes (PCGK) und Beteiligungsrichtlinien, die der Erhöhung der Transparenz und Nachvollziehbarkeit der Unternehmensführung und -überwachung der Beteiligungsunternehmen dienen sollen.

Dass das Risikobewusstsein noch nicht ausreichend im Handeln verankert ist, zeigt sich insbesondere darin, dass nur die Hälfte aller Bundesländer und lediglich ein geringer Teil der rund 11.000 Kommunen in Deutschland mittlerweile über einen eigenen PCGK oder eine Beteiligungsrichtlinie verfügen.

Aber auch diejenigen Bundesländer und Kommunen, die bereits über Kodizes verfügen, stehen aufgrund der Vielfalt und Komplexität der Risiken vor großen Herausforderungen. Der von der Privatwirtschaft gelebte Ansatz eines „Konzernrisikomanagements", im Rahmen dessen von der Holding bis in die Konzerngesellschaften ein einheitliches Risikomanagementsystem[4] integriert wird, hat sich bei dem überwiegenden Teil der Beteiligungsverwaltungen noch nicht durchgesetzt.[5] Dies hat zur Folge, dass die Ausgestaltung und Umsetzung eines Risikomanagements, zu dem öffentliche Unternehmen durch das Aktien- und GmbH-Gesetz[6] sowie das Haushaltsgrundsätzegesetz[7] verpflichtet sind, in den meisten Fällen in der Hand der Beteiligungsunternehmen liegen und somit Bund, Länder und Kommunen in der Identifizierung, Steuerung und Überwachung der Risiken eingeschränkt sind.[8]

Der risikoorientierte Aufsichtsrat im Beteiligungsunternehmen

Vor diesem Hintergrund kommen auf die öffentlichen Aufsichtsräte erweiterte Aufgaben und Herausforderungen zu, da sie für die Länder und Kommunen das Bindeglied zu den Beteiligungsunternehmen darstellen.

Die primäre Aufgabe des Aufsichtsrats ist die Überwachung der Unternehmensleitung, die sich ausschließlich auf die Leitungsmaßnahmen, das heißt allein auf die Geschäftsführungs- bzw. Vorstandstätigkeiten beschränkt (§ 111 AktG). Teil dieser Überwachung ist das von der Unternehmensleitung zur Erkennung von bestandsgefährdenden Risiken einzurichtende Risikomanagement (§ 91 Abs. 2 AktG).

Die Überwachung des Risikomanagements wurde in der Vergangenheit häufig als „klassische Kontrollfunktion" gese-

1 Vgl. Schuster, F. et al. (2013): Risikomanagement in Kommunen. In: PublicGovernance Sommer 2013, S. 12 ff.

2 Vgl. PublicGovernance (Sommer 2007): Risikomanagement in öffentlichen Unternehmen, S. 6 ff.

3 Vgl. Oehler, A./Schalkowski, H./Wendt, S. (2013): Risikomanagement in öffentlichen Unternehmen im Spannungsfeld zwischen Daseinsvorsorge und Steuerlast, Working Paper

4 Vgl. analog DIIR Revisionsstandard Nr. 2; IDW PS 340

5 Vgl. Schuster, F. et al. (2013): Risikomanagement in Kommunen. In: PublicGovernance Sommer 2013, S. 12 ff.

6 Siehe § 91 Abs. 2, § 93 Abs. 1 AktG; analog § 43 Abs. 1 GmbHG

7 Siehe § 53 HGrG

8 Vgl. Schuster, F. et al. (2013): Risikomanagement in Kommunen. In: PublicGovernance Sommer 2013, S. 12 ff.

hen, in der vorrangig betrachtet wurde, ob ein Risikomanagement betrieben wird und im besten Fall, ob ein funktionierendes und angemessenes System implementiert wurde.[9] Neben der Überwachungsaufgabe kommt dem Aufsichtsrat heutzutage jedoch auch eine Pflicht zur Beratung der Unternehmensleitung in gewichtigen Fragen wie dem Risikomanagement zu.[10] Um diesem gerecht zu werden, ist der Aufsichtsrat aufgerufen, seine rein „kontrollierende Sichtweise" zu erweitern und als aktiver Ratgeber gegenüber der Unternehmensleitung aufzutreten.

Zur Erfüllung dieser erweiterten Rolle ist es für den Aufsichtsrat von grundlegender Bedeutung, das für alle Beteiligten akzeptable Risikoniveau unter Berücksichtigung des öffentlichen Auftrags gemeinsam mit der Unternehmensleitung zu bestimmen, Mindestanforderungen festzulegen sowie die Funktionsfähigkeit und Wirksamkeit des aktuellen Risikomanagements zu prüfen[11] (beispielsweise mittels externer Wirtschaftsprüfer gemäß IDW PS 340 oder durch eine Interne Revision analog dem DIIR Revisionsstandard Nr. 2). Erst auf dieser Basis ist der Aufsichtsrat in der Lage, als Sparringspartner für die Unternehmensleitung zu agieren.

Besondere Herausforderungen im digitalen Zeitalter

Im Zuge ihrer erweiterten Rolle als aktiver Ratgeber gegenüber der Unternehmensleitung entstehen für die Aufsichtsräte durch die digitale Transformation zusätzliche Herausforderungen. Die Digitalisierung ist mittlerweile ein „wesentlicher Faktor für die Wettbewerbsfähigkeit von Unternehmen und Organisationen".[12] Auch in Zukunft wird sich die Anforderung, Unternehmensprozesse zu digitalisieren und so digitale Geschäftsmodelle zu schaffen, weiter verstärken.

Es gilt daher auch für Aufsichtsräte, hinsichtlich technologischer Entwicklungen und der sich verändernden Bedrohungslandschaft auf dem neuesten Wissensstand zu bleiben. Trends wie Virtualisierung in der Cloud, Echtzeit-Datenanalyse mit Big Data und der mobile Zugriff auf Systeme jederzeit und von überall bringen neue Gefährdungen und Schwachstellen mit sich, aus denen zusätzliche IT-Risiken entstehen.[13] Dies trifft insbesondere öffentliche Unternehmen und Betreiber kritischer Infrastrukturen – zum Beispiel Krankenhäuser, Wasserwerkbetreiber, öffentliche Rundfunkanstalten oder Justizeinrichtungen –, die eine besondere Bedeutung für das staatliche Gemeinwesen haben. Dennoch gilt es, eine positive Grundhaltung zum Umgang mit Cyberrisiken zu entwickeln. Jedes Risiko beinhaltet gleichzeitig eine Chance. Wer die Auswirkungen der zunehmenden Digitalisierung früh erkennt und die damit verbundenen Potenziale nutzt, ist in der Lage, sich entsprechend vorzubereiten; auch in Bezug auf die entstehenden Risiken. Dies zu verstehen und den erforderlichen Veränderungswillen kulturell im Unternehmen voranzutreiben, ist auch Aufgabe der Aufsichtsräte.

Etablierung eines angemessenen IT-Sicherheitsniveaus

„Die digitalen Kunden erwarten Sicherheit und den Schutz ihrer Daten – sie verzeihen Fehler nur selten."[14] Die Überwachungs- und Kontrollpflicht der Aufsichtsräte für das Risikomanagement muss daher die Herstellung und Wahrung eines angemessenen IT-Sicherheitsniveaus umfassen. Klassische Sicherheitsmechanismen müssen überdacht und an neue Technologien und Architekturen angepasst werden. Dies betrifft Bereiche wie Virenschutzstrategien oder die Sicherung und Wiederherstellung von Datenbeständen, zum Beispiel unter Nutzung von Offsite-Backup- und Recovery-Strategien, bei denen kritische Datensicherungen zum Schutz vor physischer Zerstörung außerhalb des Unternehmensstandorts aufbewahrt werden. Auch die Archivierung von Daten im Hinblick auf eine vertrauenswürdige Langzeitspeicherung sollte berücksichtigt werden. Hier geben Richtlinien des Bundesamts für Sicherheit in der Informationstechnik wie TR 03138 und TR 03125 Hinweise und Empfehlungen für die Implementierung.

Im Rahmen eines ganzheitlichen Risikomanagements muss auch die Etablierung eines funktionierenden Notfallmanagements und geeigneter Präventivmaßnahmen adressiert werden. Dies schließt ein, gravierende Risiken für ein Unternehmen frühzeitig zu erkennen und Maßnahmen dagegen zu implementieren. Durch eine zielgerichtete Reaktion im Krisenfall lassen sich so die wichtigsten Prozesse aufrechterhalten bzw. zeitnah wiederherstellen. Zur Etablierung und Aufrechterhaltung des Notfallmanagements bietet der BSI-Standard 100-4 eine ausführliche Methodik. Er kann Aufsichtsräten zur Erfüllung ihrer Überwachungs- und Kontrollpflicht als Orientierung dienen.

Auf dem Weg in die Digitalisierung sind diesbezüglich spezifische Kompetenzen gefragt, auch in den Aufsichtsräten. Diese gehen über klassisches IT-Know-how hinaus. Jedoch stehen Aufsichtsräte mit dieser Aufgabe nicht alleine da. Beispielsweise kann die Interne Revision unterstützend hinzugezogen werden. Da in anderen Bereichen Aufgaben ausgelagert oder Experten ins Haus geholt werden, ist dies auch bei der Überwachung des Risikomanagements eine denkbare Lösung.

Im Hinblick auf die erforderliche digitale Expertise und Erfahrung bei der Gestaltung und Umsetzung digitaler Prozesse bietet sich öffentlichen Unternehmen so die Chance, Risiken frühzeitig und angemessen entgegenzutreten und die digitale Transformation erfolgreich zu bestehen.

Wilhelm Dolle, Robert Dumke, Hanna Lurz, Marie Rupprecht

9 Vgl. DStR 2001, S. 299

10 Vgl. PublicGovernance (Herbst 2013): Neues zu den Rechten und Pflichten des öffentlichen Aufsichtsrats, S. 6 ff.

11 Vgl. Degen, B./Ruhwedel P. (2011): Der Aufsichtsrat und das Risikomanagement. In: Der Aufsichtsrat, Vol. 10, S. 138 ff.; vgl Gleißner, W. (2007): Beurteilung des Risikomanagements durch den Aufsichtsrat: nötig und möglich? In: Der Aufsichtsrat, Vol. 12, S. 173 ff.

12 neuland GmbH & Co. KG (2014): Digital Transformation Report 2014, S. 16

13 Im Sinne des Risikomanagements beschreibt ein Risiko die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens, wobei ein Schaden das Aufeinandertreffen einer Gefährdung und einer dazu passenden Schwachstelle bedingt. Risiken können beispielsweise die Bereiche Liquidität oder Reputation treffen.

14 Ennemann, M. (2015): Dringend benötigt: Der digitale Aufsichtsrat. In: Audit Committee Quarterly, Vol.1, S. 29