Die (ungleiche) Wahrnehmung des Risikomanagement-Prozesses

Verwaltungsrat, Geschäftsleitung und interne Revision nehmen das Risikomanagement eines Unternehmens unterschiedlich wahr.

Eine kürzlich vom Institute of Internal Audit herausgegebene Publikation zeigt auf, dass Verwaltungsrat, Geschäftsleitung und Leitung der internen Revision ein sehr unterschiedliches Verständnis davon haben, wie die Hauptrisiken innerhalb eines Unternehmens bewertet und gehandhabt werden. Im Hinblick auf den Umgang mit bestimmten Hauptrisiken scheinen die Verwaltungsratsmitglieder durchweg optimistischer zu sein als die Geschäftsleitung oder die interne Revision. Deshalb stellt sich die Frage nach dem Verständnis der verschiedenen Parteien und ob ein systemisches Informationsgefälle zwischen dem Überwachungsgremium und den operativen Funktionen des Unternehmens besteht.

Unternehmen sind mit einer Vielzahl von Risiken konfrontiert, die die Erreichung ihrer strategischen, operativen oder finanziellen Ziele beeinträchtigen können und sich negativ – beispielsweise auf die Finanzen, ihr Ansehen, die Einhaltung von Vorschriften und Gesetzen oder den Geschäftsbetrieb – auswirken können.

Die Pflicht des Verwaltungsrats (VR) ist es sicherzustellen, dass die Geschäftsleitung diese inhärenten Risiken[1] rechtzeitig identifiziert und mit Hilfe verschiedener Arten risikomindernder Massnahmen in geeigneter Weise angeht, um das Restrisiko[2] auf ein akzeptables Niveau zu senken.

Solche risikomindernden Massnahmen können beispielsweise darin bestehen, bestimmte Geschäftsaktivitäten aufzugeben und damit ein Risiko ganz zu beseitigen, Risiken durch interne Kontroll- und Überwachungsinstrumente zu reduzieren, potenzielle Auswirkungen zu versichern oder das Risiko wissentlich und absichtlich selbst zu tragen.

Die interne Revision als dritte Verteidigungslinie ist in der Regel vom Verwaltungsrat beauftragt, eine unabhängige und objektive Beurteilung der Ausgestaltung und Wirksamkeit der Massnahmen vorzunehmen, die vom Unternehmen ergriffen wurden, um den Hauptrisiken entgegenzuwirken.

Falsche Wahrnehmung von Risikofachwissen und -fähigkeiten

Es gehört zu den natürlichen Herausforderungen eines Unternehmens, potenzielle Hauptrisiken, die für das Unternehmen von Bedeutung sind, rechtzeitig zu identifizieren, unter Einbezug aller Parteien (d. h. Verwaltungsrat, Geschäftsleitung, Risikomanage-

Abbildung 1: Der Umgang mit Risiken

[1] Inhärentes Risiko = Bruttorisiko, dem ein Unternehmen ausgesetzt ist, wenn es keine Gegenmassnahmen ergreift

[2] Restrisiko = Nettorisiko nach Berücksichtigung von Massnahmen zur Risikominderung

ment, interne Revision) zu einer gemeinsamen und genauen Bewertung der potenziellen Auswirkungen zu gelangen und dauerhafte risikomindernde Massnahmen effektiv auszugestalten und umzusetzen.

Der kürzlich vom Institute of Internal Audit (IIA) durchgeführten Studie «OnRisk 2020»[3] zufolge nehmen die wichtigsten Parteien das **Wissen** und die **Fähigkeiten** zur Identifizierung und Bewältigung der Hauptrisiken eines Unternehmens unterschiedlich wahr. Zusätzlich besteht eine gewisse Diskrepanz in der Wahrnehmung der Hauptrisiken.

Die Studie bewertete diese Diskrepanz anhand von elf Hauptrisiken[4], die derzeit in der Unternehmenswelt als entscheidend angesehen werden. Die elf Risiken entsprechen jenen, die von KPMG in der aktuellen Publikation «20 key risks to consider by Internal Audit before 2020»[5] als Hauptrisiken genannt werden.

Die Ergebnisse aus den Interviews mit Verwaltungsrats- und Geschäftsleitungsmitgliedern sowie Verantwortlichen für die interne Revision zeigen eine **starke Übereinstimmung beim Wissen und Verständnis**, das nötig ist, um die Hauptrisiken zu erkennen und zu untersuchen. Man könnte daraus schliessen, dass alle Interviewpartner ein gemeinsames Verständnis darüber haben, welches die Hauptrisiken des Unternehmens sind und wie sie bewertet werden sollten (d. h. Schwere, Auswirkung, Wahrscheinlichkeit).

Dieses **Bild ändert sich** jedoch, wenn man die **Wahrnehmung hinsichtlich der Fähigkeiten** des Unternehmens **beurteilt**, diese Risiken effektiv und effizient anzugehen und zu steuern. Die Studie deutet darauf hin, dass **Verwaltungsratsmitglieder die Fähigkeiten des Unternehmens** zur Bewältigung der Hauptrisiken und zur Aufrechterhaltung eines nachhaltigen Systems von risikomindernden Massnahmen **als reifer einschätzen als die Geschäftsleitung**.

Überraschend ist auch, dass die gewöhnlich kritischere Wahrnehmung der **Leitung der internen Revision etwas positiver zu sein scheint** als erwartet und dass diese die Fähigkeiten des Unternehmens zur Risikominderung (Entwicklung und Aufrechterhaltung von Gegenmassnahmen) tendenziell positiver bewertet als die Geschäftsleitung.

Diese Feststellungen führen zu folgenden Fragen:

- Sind die Verwaltungsräte und in einem gewissen Masse die interne Revision etwas zu zuversichtlich im Hinblick auf die Fähigkeiten des Unternehmens, Risiken effektiv zu begegnen, während die Geschäftsleitung den Reifegrad des Risikomanagements zu kritisch beurteilt?
- Besteht trotz Einführung der zweiten (d. h. Risikomanagement, Compliance) und dritten Verteidigungslinie (d. h. interne Revision) ein systemisches Informationsgefälle zwischen den verschiedenen Parteien?

---

[3] Quelle: OnRisk 2020 Report – A Guide to Understanding, Aligning, and Optimizing Risk (2020); Institute of Internal Audit (IIA); na.theiia.org/periodicals/OnRisk/Pages/default.aspx (abgerufen am 25.02.2020)

[4] Zu den Hauptrisiken gehören: Cyber Security, Datenschutz, regulatorische Änderungen, Business Continuity Management, Daten und neue Technologien, Drittunternehmen, Talent Management, Kultur, Verwaltungsratsinformationen, Datenethik, Nachhaltigkeit

[5] Quelle: 20 key risks to consider by Internal Audit before 2020; Luka Zupan; KPMG Switzerland; assets.kpmg/content/dam/kpmg/ch/pdf/key-risks-internal-audit-2018.pdf (abgerufen am 25.02.2020)

Vertrauenslücke

Es überrascht, dass viele der Befragten (VR, GL, IR) – als sie mit dieser Tendenz konfrontiert wurden – angaben, dass diese Fehlwahrnehmung der Fähigkeiten eines Unternehmens für ein **«gesundes Mass an Aufgabentrennung»** spreche, womit sie die Gefahr einer Fehlausrichtung etwas herunterspielten.

Das könnte bedeuten, dass der Verwaltungsrat – ungeachtet der offensichtlichen Diskrepanz – ein natürliches «Vertrauen» in die Geschäftsleitung hat und glaubt, dass diese rechtzeitig und präzise über potenzielle Fälle berichten würde, die auf das Eintreten eines Hauptrisikos bzw. auf den Mangel an risikomindernden Massnahmen im Unternehmen hinweisen.

Diese «gesunde Trennung» lässt sich möglicherweise auch mit dem unterschiedlichen Blickwinkel erklären, aus dem die drei teilnehmenden Gruppen (VR, GL, IR) die Hauptrisiken wahrnehmen. Während alle Befragten ihr persönliches Wissen und Verständnis im Hinblick auf die elf Hauptrisiken ungefähr gleich bewerteten, setzten sie leicht unterschiedliche Schwerpunkte.

Die Leitung der internen Revision stellt die täglichen Abläufe zur Risikoabwehr (d. h. taktisches Reagieren auf Risiken) in den Mittelpunkt. Die Mitglieder des Verwaltungsrats und der Geschäftsleitung hingegen fokussieren auf strategische Aspekte (d. h. die Strategie für den Umgang mit Risiken).

Daraus lässt sich ableiten, dass die einzelnen Parteien zwar über ein fundiertes Verständnis der relevanten Risiken verfügen, doch aus verschiedenen Blickwinkeln (taktisch vs. strategisch) beurteilen, wie gut die organisatorischen Fähigkeiten sind, den Risiken effektiv zu begegnen.

Informationsverzerrung

Eine weitere Erklärung für die Fehlwahrnehmungen ist eine mögliche Informationsverzerrung. Verwaltungsratsmitglieder geben oft an, vom Tagesgeschäft etwas **abgekoppelt** zu sein. Gründe dafür können mangelnde fachliche Erfahrung in der jeweiligen Branche sein, zu wenig für das Mandat eingesetzte Zeit oder eine starke Dominanz der Geschäftsleitung, die den Verwaltungsratsmitgliedern wenig Spielraum lässt, die Richtung des Unternehmens zu bestimmen.

Darüber hinaus sind die Verwaltungsratsmitglieder zur genauen Einschätzung eines potenziellen Risikos vollständig auf Informationen aus dem Unternehmen angewiesen, da sie normalerweise nicht ins Tagesgeschäft involviert sind. Ein möglicher Ausweg aus dieser verzerrten Informationslage besteht darin, die jeweiligen Risikoverantwortlichen aufzufordern, dem Verwaltungsrat ihre Einschätzung und die eingeleiteten risikomindernden Massnahmen darzulegen.

Zwar verbessern solche Präsentationen das Verständnis der inhärenten Risikosituation bei den Verwaltungsratsmitgliedern, aber es bleibt für sie schwierig, die tatsächliche Wirksamkeit der risikomindernden Massnahmen (d. h. taktische Massnahmen zur Risikoabwehr) genau zu beurteilen.

Hier könnte die interne Revision ins Spiel kommen und sich im Rahmen ihres Mandats mit diesem Anliegen befassen. Die Ressourcen dafür sind jedoch in der Regel begrenzt. Sie erfordern ein umfassendes Verständnis der jeweiligen Risikosituation und idealerweise auch den Zugang zu Good-Practice-Beispielen (z. B. Massnahmen zur Sicherstellung einer effektiven Cyber-Sicherheitsstrategie), um einen effektiven Vergleich mit Good Practice zu ermöglichen. Dennoch kann die interne Revision mit den ihr zur Verfügung stehenden Ressourcen und Mitteln (z. B. Fachkompetenz) nicht alle Risiken angemessen und zeitnah untersuchen.

Schlussfolgerung und mögliche Abhilfe

Es bleibt also die Frage, inwieweit der Verwaltungsrat und bis zu einem gewissen Grad die Leitung der internen Revision wegen ihrer uneinheitlichen Einschätzung der Fähigkeit des Unternehmens für die wirksame Abwehr der Hauptrisiken besorgt sein sollten und mit welchen Massnahmen Abhilfe geschaffen werden könnte.

Die Studie zeigt, dass gewisse Unterschiede in der Beurteilung der Fähigkeiten, über die ein Unternehmen für die wirksame Bekämpfung von Risiken verfügt, durchaus nachvollziehbar sind und in der Natur des Informationsgefälles liegen. Die Geschäftsleitung und insbesondere die einzelnen Risikoverantwortlichen werden immer ein besseres und umfassenderes Verständnis der inhärenten und verbleibenden Risikosituation des Unternehmens haben. Es ist daher wichtig, dass im Unternehmen eine proaktive, offene Kommunikation mit dem Verwaltungsrat möglich ist, falls sich die Bewertung eines Risikos geändert hat, schlichtweg falsch ist oder sich risikomindernde Massnahmen als nur teilweise wirksam erweisen.

[6] Quelle: Die Überforderung von Verwaltungsräten (2020; Hansueli Schöchli – Neue Zürcher Zeitung (NZZ); www.nzz.ch/meinung/die-ueberforderung-von-verwaltungsraeten-ld.1541134 (abgerufen am 25.02.2020)

Eine bewährte Strategie gegen unterschiedliche Risikoeinschätzungen besteht darin, dass die Risikoverantwortlichen an Sitzungen des Prüfungsausschusses oder des Verwaltungsrats den Stand ihrer risikomindernden Massnahmen präsentieren. Dadurch kann eine breitere Gruppe die Situation beurteilen, es wird Raum für eine offene Diskussion geschaffen und überlegt, ob die risikomindernden Massnahmen stark genug sind, um dem Risiko wirksam zu begegnen.

Darüber hinaus sollten Verwaltungsratsmitglieder externe Informationsquellen nutzen, um mögliche Verschiebungen in der Risikobewertung persönlich einschätzen zu können und sich über bestimmte neu auftretende Risiken, die bisher nicht oben auf der Prioritätenliste standen, eine Meinung zu bilden (z. B. durch Thought-Leadership-Publikationen, Nachrichten über neue Risiken etc.). Ein gutes Beispiel hierfür sind die jüngsten Entwicklungen im Zusammenhang mit Cyber Security und den damit einhergehenden Angriffen. Erfahrungen haben gezeigt, dass viele Unternehmen dieses Risiko bisher nur teilweise beachtet und ein viel grösseres Restrisiko toleriert hatten, als es der tatsächlichen Risikobereitschaft des Unternehmens entspricht.

Und nicht zuletzt sollte der Verwaltungsrat, wenn dieser die Massnahmen des Unternehmens zur Bekämpfung der Hauptrisiken als unzureichend einschätzt, externe Fachspezialisten beiziehen können, damit diese eine unabhängige, objektive Bewertung der Risikosituation vornehmen. Eine externe Bewertung bietet nicht nur eine frische, unvoreingenommene Sicht auf die Risiken, sondern kann auch Aufschluss darüber geben, ob das Unternehmen im Vergleich zu seinen Mitbewerbern genug unternimmt, um die Hauptrisiken wirksam zu mindern (durch Benchmarkings, Peer Reviews und Good-Practice-Vergleiche).

Schlussendlich besteht die wirksamste Strategie gegen eine uneinheitliche Risikoeinschätzung darin, die Hauptrisiken immer wieder offen zu diskutieren (d. h. die Risikodiskussion als Standardthema auf die Traktandenliste zu setzen) und die Geschäftsleitung zu verpflichten, glaubwürdig und unvoreingenommen darzulegen, wie sie die Situation bezüglich inhärenter Risiken und Restrisiken einschätzt.

Luka Zupan
Partner, Leiter Internal Audit, Risk and Compliance (IARCS)
KPMG Schweiz

lzupan@kpmg.com