Fortbestand des Unternehmens sichern

Risikomanagement als Teil der integrierten Assurance

Risikomanagement ist eine nicht übertragbare Aufgabe des Verwaltungsrats und gesetzlich verankert im Obligationenrecht. Damit der Verwaltungsrat seiner Aufgabe gerecht wird, braucht er in Abhängigkeit der Grösse des Unternehmens Assurance-Funktionen, die Risiko- und Compliance-Management-Tätigkeiten überwachen.

Corinne Posch, Alexander Loistl, Christian Zipper

Weder in der Praxis noch in der Literatur gibt es eine einheitliche Meinung zur Assurance und zur Zusammenarbeit unter Assurance-Funktionen. Vorliegend wird unter Assurance die Gesamtheit aller Überwachungs- und Kontrolltätigkeiten mit dem Ziel, den Fortbestand des Unternehmens zu sichern, verstanden. In jedem Unternehmen gibt es aufgrund des Geschäftszwecks spezifische Assurance-Funktionen. So kommt zum Beispiel der Arbeitssicherheit in einem Bauunternehmen eine andere Bedeutung zu als in einem Dienstleistungsunternehmen.

In den diversen Unternehmen, die von der Autorin befragt wurden, ist der Reifegrad der Zusammenarbeit unterschiedlich. Assurance-Funktionen stimmen sich teilweise informell und ohne konkreten Auftrag des Verwaltungsrats ab. Das kann dazu führen, dass sich die operativen Bereiche des Unternehmens immer wieder mit ähnlichen Risiko- und Compliance-Themen beschäftigen und dieselben Themen in unterschiedliche vorberatende Ausschüsse rapportieren müssen. Dies führt zu Mehraufwand und Produktivitätsverlust im Unternehmen. Um eine solche Situation zu vermeiden, müssen Assurance-Funktionen so organisiert sein, dass sie strukturiert und koordiniert und somit effizient zusammenarbeiten.

Kriterien zur Identifikation von Assurance-Funktionen

Der Verwaltungsrat eines Schweizer Unternehmens hat nach dem geltenden Obligationenrecht eine Reihe von Aufgaben, die er nicht an andere Funktionen des Unternehmens delegieren kann. Dazu zählen umfassende Kontroll- und Überwachungspflichten, die auch komplexe Risiko- und Compliance-Themen umfassen. Hierfür benötigt der Verwaltungsrat eine Organisation, die ihn bei der Beschaffung der nötigen Informationen und bei der Vorbereitung von Entscheidungen effizient und zuverlässig unterstützt. Genau hier setzt die Assurance-Organisation des Unternehmens an. Eine solche Assurance-Organisation sollte folgende Anforderungen erfüllen:

1. Unabhängigkeit: Jede Assurance-Funktion steht in einer Dreiecksbeziehung zwischen dem Verwaltungsrat als Entscheidungsträger und Auftraggeber sowie dem überwachten Bereich («Auditee»). Sie sollte keine operative Aufgabe im Unternehmen wahrnehmen und unmittelbar und unabhängig an den Verwaltungsrat rapportieren. Eine organisatorische Ansiedlung beim Verwaltungsrat ist dabei nicht zwingend notwendig.
2. Risikobasierter Ansatz: Die Assurance dient der Minimierung von schädigenden Entwicklungen und Ereignissen im Unternehmen sowie der Einhaltung von Vorschriften. Da die Assurance-Funktionen nicht alle Tätigkeiten permanent beaufsichtigen können (und sollen), sollte ein risikobasiertes Vorgehen gewählt werden.
3. Einsichtsrecht in alle relevanten Unterlagen: Assurance-Funktionen müssen über umfassende und tiefgreifende Audit- und Kontrollrechte verfügen. Nur so kann sichergestellt werden, dass der Verwaltungsrat alle Informationen erhält, die er für die Erfüllung seiner Kontroll- und Überwachungspflichten benötigt.

Zur Zuordnung der Funktionen kann das «Three Line Model» des Institute of Internal Auditors herangezogen werden. Nach diesem Modell werden alle operativen Geschäftsfunktionen der 1. Linie zugeordnet. Die Funktionen der 2. Linie (zum Beispiel eine Sicherheitsfunktion) als auch der 3. Linie (zum Beispiel die interne Revision) sind Assurance-Funktionen, die die oben genannten Kriterien erfüllen müssen. Die 3. Linie muss hierbei gegenüber der 2. Linie unabhängig sein, damit sie diese kontrollieren und beaufsichtigen kann. Eine integrale Zu-

Autoren

Corinne Posch ist Fachleiterin Safety Risk Management bei den SBB. Sie hat einen Master in Integrated Risk Management der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) in Winterthur.
Alexander Loistl ist Legal Counsel bei der Vetropack Holding AG und Leiter CAS Risikomanagement und Recht an der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) in Winterthur.
Dr. Christian Zipper ist Studienleiter für Integriertes Risikomanagement und Dozent an der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) in Winterthur.

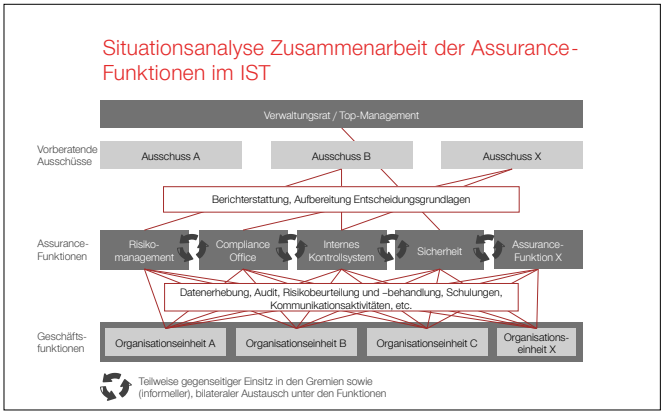

Abbildung 1: Beispielhafte Darstellung der Zusammenarbeit unter den Assurance-Funktionen.

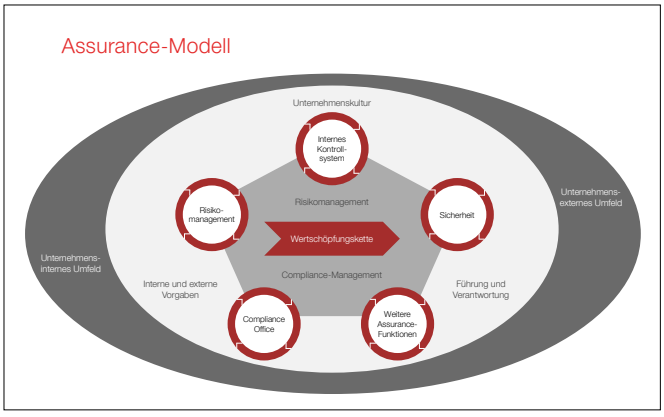

Abbildung 2: Zusammenarbeitsmodell unter den Assurance-Funktionen.

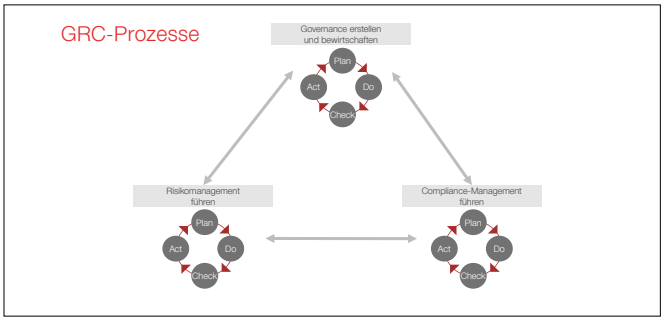

Abbildung 3: Organisation der Zusammenarbeit unter den Assurance-Funktionen.

sammenarbeit zwischen der 2. und der 3. Linie sollte deshalb nicht stattfinden.

Modell zur integrierten Assurance

Mit klarer Koordination und Optimierung der Zusammenarbeit zwischen den Assurance-Funktionen soll einerseits der Aufwand für die operativen Bereiche minimiert werden. Andererseits soll sichergestellt werden, dass der Verwaltungsrat für die Erfüllung seiner Aufgaben relevante und abgestimmte Informationen erhält.

Es sind verschiedene Zusammenarbeitsformen denkbar. Die Zusammenarbeit sollte stufenweise organisiert und weiterentwickelt werden, damit Veränderungsprozesse geführt und begleitet werden können. Besteht bis anhin lediglich eine informelle Zusammenarbeit, kann mittels eines konkreten Auftrags des Verwaltungsrats ein Schritt in Richtung Formalisierung und Koordination erfolgen. Organisationsstrukturen werden beibehalten, soweit dies erforderlich und sinnvoll ist. Die organisatorische Weiterentwicklung ist aber jederzeit möglich.

Die Zusammenarbeit der Assurance-Funktionen sollte sich an der Wertschöpfungskette orientieren, damit die operativen Bereiche nicht unnötig belastet und sinnvoll in den Assurance-Prozess eingebunden werden. Risiko- und Compliance-Management sind grundlegende Assurance-Aufgaben zur Minimierung der Risiken und Einhaltung der bestehenden Vorschriften. Als Basis der Organisation und gemeinsamer Tätigkeiten sollten die ISO-Normen SN ISO 31000:2018 für das Risikomanagement und SN ISO 37301:2021 für das Compliance-Management herangezogen werden. Bei der Zusammenarbeit sollten im ersten Basiskreis die Strategie und die Organisationsstruktur (in der Abb. 2 als «Führung und Verantwortung» symbolisiert), die internen und externen Vorgaben und die Unternehmenskultur berücksichtigt werden. In einem weiteren Kreis sollte der interne und externe Kontext beobachtet werden. Der Aufbau und die Zusammenarbeit unter den Assurance-Funktionen sollten kommunikativ und mittels Schulungsmassnahmen unterstützt werden.

Eigene Assurance-Governance

Zur Organisation der integrierten Assurance braucht es einen Governance-Regelkreis. Nebst einer Kontextanalyse werden im Regelkreis der Anwendungsbereich sowie die Ziele und Strukturen der integrierten Assurance festgelegt. Später folgt eine Überprüfung und Bewertung im Rahmen eines Management-Reviews. Daraus werden Verbesserungsmassnahmen abgeleitet.

Der Governance-Regelkreis steht in Abhängigkeit zum Risiko- und Compliance-Management. In diesem Prozessdreieck findet sich eine GRC-Logik(Governance, Risk, Compliance), auf die häufig auch in der Literatur hingewiesen wird. Das bedeutet, dass es neben dem Risiko- und Compliance-Management eine eigene Assurance-Governance braucht, damit innerhalb der Assurance Rahmen und Leitfaden für die Tätigkeiten festgelegt werden können.

Fazit: In der integrierten Assurance stellt das Risiko- und Compliance-Management die Gemeinsamkeit dar. In einer strukturierten Zusammenarbeit sorgen die Assurance-Funktionen für eine effiziente Überwachungs- und Kontrolltätigkeit für den Verwaltungsrat sowie für eine Entlastung der operativen Bereiche. Doppelspurigkeiten und Lücken werden verhindert, Ressourcen priorisiert und Mitarbeitende gemeinsam weiterentwickelt. ■