Unternehmensorganisation

Integration von Assurance-Funktionen

Für die organisatorische Einbettung von Assurance-Funktionen in eine Unternehmung gibt es lediglich rudimentäre (aufsichts-)rechtliche Vorgaben, und auch ein eindeutiger Best-Practice-Ansatz hat sich bis dato nicht etabliert. Als Herausforderung wird insbesondere die Sicherstellung der Unabhängigkeit angesehen. Was sind mögliche Massnahmen dazu?

Bertrand Volken

«Die Compliance-Abteilung hat versagt», «Die Hinweise seitens Risikomanagement wurden ignoriert», so oder ähnlich tönt es in den Medien, wenn ungebührliches Geschäftsgebaren aufgedeckt wird. Oftmals zeigt sich in der Analyse, dass in den betroffenen Unternehmen Assurance-Funktionen zwar installiert wurden, deren Durchsetzungskraft aber beschränkt war. Woran kann das liegen?

Vorgaben bezüglich Organisation von Assurance-Funktionen

Für Banken und Versicherungen gelten die FINMA-Rundschreiben Corporate Governance 2017/1 bzw. 2017/2, welche die Anforderungen an die zentralen Assurance-Funktionen Risikomanagement und Compliance als Elemente eines wirksamen IKS erläutern. Während die Aufsichtsbehörde bei den systemrelevanten Banken insbesondere die organisatorische Einbettung des Risk Officers konkret regelt (FINMA RS 2017/1, Rz 68), fehlen entsprechende Vorgaben im für die Versicherungen relevanten Rundschreiben.

Neben den FINMA-Rundschreiben gibt es weitere Dokumentationen wie den Prüfungsstandard PS980 (EXPERTsuisse), welcher zentrale Merkmale einer (Compliance-) Organisation wie Festlegung von Rollen und Verantwortlichkeiten, Kompetenzen und Ressourcen sowie Berichtslinien nennt.

Gemeinsam ist diesen Vorgaben, dass explizit die Objektivität und Unabhängigkeit der Assurance-Funktionen (Kontrollinstanzen) gefordert wird, ohne aber weiter auf die diesbezüglich sinnvolle Organisationsform einzugehen. Insofern besteht die Chance, eine auf die jeweilige Unternehmensgrösse und -komplexität angepasste Einbettung zu gestalten.

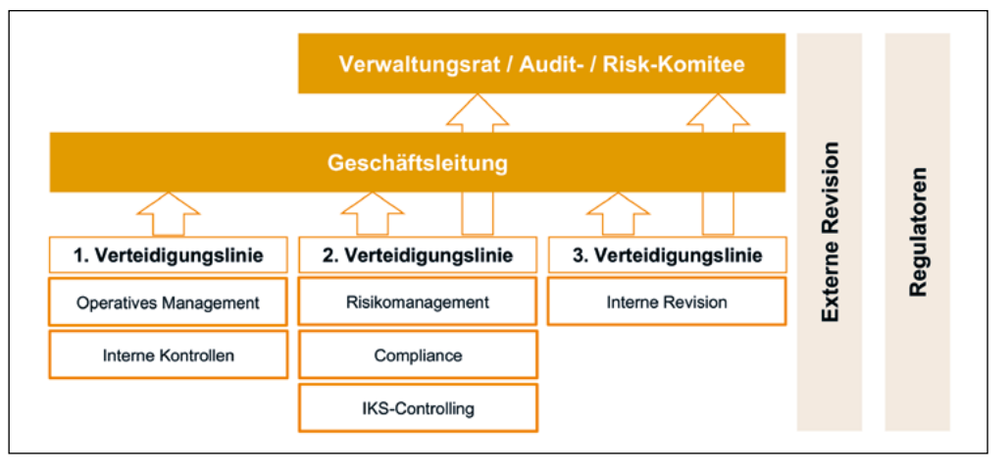
Das Modell der drei Verteidigungslinien

Als ein Modell zur Förderung der Unabhängigkeit von Assurance-Funktionen hat sich das Modell der drei Verteidigungslinien («three lines of defense») etabliert. Dieses wird auch von der FINMA in ihrem Erläuterungsbericht zu den beiden erwähnten Governance-Rundschreiben als Ansatz zur Definition von Rollen und Verantwortlichkeiten im Governance-System erwähnt. Die Assurance-Elemente Risk Management, Compliance und IKS werden dabei in der 2. Linie gebündelt und vom Tagesgeschäft (1. Linie) getrennt, um die Unabhängigkeit sicherzustellen. Neben den vorgenannten Assurance-Elementen werden oftmals auch die Bereiche Datenschutz, Informationssicherheit und Qualitätsmanagement als Einheiten der 2. Verteidigungslinie betrachtet. Die 3. Verteidigungslinie beinhaltet die interne Revisionsstelle. Der fehlende Einbezug der externen Revision und des Regulators ins Modell (z.B. im Sinne einer 4. und 5. Verteidigungslinie) wird in der Lehre zum Teil kritisiert.

> *«Die Organisationsform von Assurance-Funktionen ist von der Unternehmensgrösse abhängig.»*

Das vorgenannte Modell veranschaulicht zwar das Zusammenspiel der drei Verteidigungslinien und ihrer Berichtslinien, gibt aber keine konkreten Anweisungen für deren organisatorische Einbettung. Verschiedene Studien zeigen diesbezüglich eine grosse Heterogenität auf. So können Assurance-Funktionen

- als Einzelpositionen in verschiedenen Einheiten implementiert sein;
- organisatorisch in einer Stabsstelle gebündelt werden;
- einer ertragsorientierten Einheit untergeordnet sein; oder



Modell der drei Verteidigungslinien (eigene Darstellung).

Bertrand Volken ist Vorstandsmitglied im Netzwerk Risikomanagement.

– gar mit ertragsorientierten Funktionen personell vermischt sein.

Die Organisationsform von Assurance-Funktionen ist zudem von der Unternehmensgrösse abhängig. Ab einer gewissen Anzahl Mitarbeitenden sollten die Funktionen der 2. Verteidigungslinie durch vom Tagesgeschäft unabhängige Personen wahrgenommen werden. Bei kleinen und mittelgrossen Unternehmen können alle Assurance-Funktionen in einer Person vereint werden. Bei grösseren Unternehmen ergibt es hingegen Sinn, wenn die Funktionen durch verschiedene Personen wahrgenommen werden. Je kleiner eine Unternehmung, desto eher werden Funktionen der 2. Verteidigungslinie durch operativ tätige Personen wahrgenommen. Gerade in solchen Situationen ist es bedeutsam, dass die Funktionsträger über die nötige Persönlichkeit und Integrität verfügen bzw. das sich stetig wandelnde Wertesystem der Gesellschaft verinnerlicht haben, um ihre Kontrolltätigkeit objektiv und unabhängig auszuüben.

Eine Alternative bietet allenfalls die Ausgliederung der Kontrolltätigkeit an Dritte (z.B. Revisionsgesellschaften oder Anwaltskanzleien).

Durch die Heterogenität der Organisationsformen müssen die regulatorisch geforderte Objektivität und Unabhängigkeit unternehmensspezifisch beurteilt werden.

Massnahmen zur Wahrung der Unabhängigkeit

Welche Opportunitäten gibt es, die einen Best-Practice-Ansatz bezüglich der organisatorischen Einbettung von Assurance-Funktionen und somit implizit auch einer möglichst hohen Unabhängigkeit begünstigen?

Assurance-Funktionen

Assurance-Funktionen umfassen alle Funktionen einer Organisation, um die strategischen und operationellen Risiken sowie die daraus entstehenden Reputationsrisiken effektiv und effizient zu steuern. Typische Assurance-Funktionen decken die Bereiche Risikomanagement und Compliance als Teil eines wirksamen IKS ab, mit denen die Einhaltung der Corporate Governance kontrolliert und unterstützt wird.

(bv)

Organisatorische Zusammenführung

Die Assurance-Elemente Risikomanagement und Compliance stellen gemeinsam als wirksames IKS die Einhaltung der Corporate Governance sicher. Damit Synergien entstehen, erscheint daher die Zusammenführung dieser Bereiche in eine organisatorische Einheit sinnvoll. Gerade zwischen Risikomanagement und Compliance gibt es Überschneidungen. So sind Compliance-Risiken

> ***«Assurance-Funktionen sollten als Teil der risikoorientierten Unternehmensführung betrachtet werden.»***

letztlich operationelle Risiken, welche die Basis für ein risikoorientiertes internes Kontrollsystem (IKS) bilden. Im Weiteren können Redundanzen im Berichtswesen zu Händen der Geschäftsleitung und des Verwaltungsrates vermieden werden, indem nicht nur die zeitliche Publikation solcher Berichte, sondern auch der inhaltliche Fokus auf die einzelnen Themen teamintern integral abgestimmt werden. Durch Einsitz in die Geschäftsleitung, z.B. ohne Stimmrecht, um Interessenskonflikte bei der Entscheidfindung zu vermeiden, kann zudem der Leitung einer solchen Assurance-Einheit ein zusätzliches Gewicht (tone-at-the-top) gegeben werden.

Personelle Entflechtung von 1. und 2. Verteidigungslinie

Wenn aufgrund der Unternehmensgrösse möglich, sind die Assurance- strikt von operativen Tätigkeiten zu entkoppeln. Mindestens die jeweiligen Leitungen der 2. Verteidigungslinie sollten von der 1. Verteidigungslinie, insbesondere in personeller Sicht, unabhängig sein. So werden potenzielle Interessenkonflikte zwischen Handlungen als Geschäftspartner versus Gatekeeper (Kontrollinstanz) vermieden bzw. werden Kontrollinstanzen nicht zu «risk takers».

Ernennung und Abberufung durch ein nicht operatives Organ

Während die interne Revision als 3. Verteidigungslinie der Oberleitung (Verwaltungsrat oder Ausschuss) unterstellt ist, sind die Assurance-Funktionen in der Regel einer ertragsorientierten Einheit unterstellt. Dies gilt auch für eine Stabsstelle beim CEO. Um die Unabhängigkeit zu wahren, kann die Ernennung oder Abberufung einer leitenden Assurance-Funktion von der Genehmigung durch die Oberleitung (VR oder dessen Risikoausschuss) abhängig gemacht werden. Weiterführende Optionen sind z.B. ein Quasi-Kündigungsschutz, durch den Stelleninhabende einer Assurance-Funktion für eine bestimmte Zeitdauer nicht abgesetzt werden dürfen.

Keine Anreize durch variable, erfolgsorientierte Entschädigung

Die Nicht-Berücksichtigung der Assurance-Funktionen bei monetär entschädigten Erfolgskomponenten hat sich heute als Standard etabliert und wird auch seitens des Regulators als eine Komponente für die Wahrung der Unabhängigkeit propagiert (vgl. FINMA-Rundschreiben Corporate Governance).

Fazit

Die Einbettung von Assurance-Funktionen in die Unternehmensführung lässt sich nur teilweise im Sinne eines Best-Practice-Ansatzes beantworten.

Gerade unter dem Aspekt der grösstmöglichen Unabhängigkeit lassen sich aber Entwicklungsfelder erkennen, die den Ansatz ermöglichen.

Zentral erscheinen drei Aspekte:
- der organisatorischen Zusammenführung,
- der personellen Entkopplung von operativen Entscheidungsfunktionen,
- der Delegation von Personalentscheiden an die Oberleitung und
- der Vermeidung von Anreizen durch eine variable Entschädigung.

Inwiefern diese implementiert werden können, hängt immer auch von der Unternehmensgrösse und der Unternehmenkultur ab. Dabei sollten Assurance-Funktionen stets als Teil der risikoorientierten Unternehmensführung, nicht jedoch als reaktive Kontrollinstanz angesehen werden. ■

Dieser Fachartikel erscheint in einer MQ-Serie, die von Experten und Expertinnen des «Netzwerk Risikomanagement» beigesteuert wird: www.netzwerk-risikomanagement.ch.