Oktober 2016

DAS MODELL DER DREI VERTEIDIGUNGSLINIEN ZUR STEUERUNG DES RISIKOMANAGEMENTS IM UNTERNEHMEN

„Vertrauen ist gut – Kontrolle ist besser" – Governance Risk & Compliance auf der Grundlage des Three Lines of Defense Modells

1. ANFORDERUNGEN AN DIE STEUERUNG DES RISIKOMANAGEMENTS IM UNTERNEHMEN

Vorstand und Geschäftsführer von Unternehmen haben die gesetzliche Verpflichtung für ein umfassendes und wirksames Risikomanagement zu sorgen. Im Rahmen der Einführung des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wurden die verschärften Anforderungen an das Risikomanagement im Aktiengesetz (§91 AktG) und GmbH-Gesetz (§ 43 Absatz 1,2 GmbH-Gesetz) verankert. Für eine Verletzung dieser Pflichten können Vorstände persönlich haftbar gemacht werden. Neben diesen grundsätzlichen Anforderungen im Rahmen der Sorgfaltspflichten existieren zahlreiche branchenspezifische Vorschriften, wie die Mindestanforderungen an das Risikomanagement (MaRisk) im Finanzdienstleistungsbereich. Mit dem IT-Sicherheitsgesetz, der nationalen Umsetzung der NIS-Richtlinie (Richtlinie über Maßnahmen zur Gewährleistung einer hohen Netz- und Informationssicherheit in der Union – 2013/0027 (COD)) sowie der vieldiskutierten aktualisierten „Konzeption zivile Verteidigung" des Bundes kommen neue gesetzliche Anforderungen insbesondere auf die Betreiber kritischer Infrastrukturen zu.

Die Einhaltung dieser schnell wachsenden Anforderungen an das Risikomanagement im Rahmen der Compliance erfordert in den Unternehmen wirksame und effiziente Prozesse sowie klare Organisationsstrukturen für das Risikomanagement. Aufgaben, Kompetenzen und Verantwortung für das Risikomanagement müssen in der Organisation eindeutig und transparent verankert werden. Als ein Modell zur Organisation des Risikomanagements hat in den

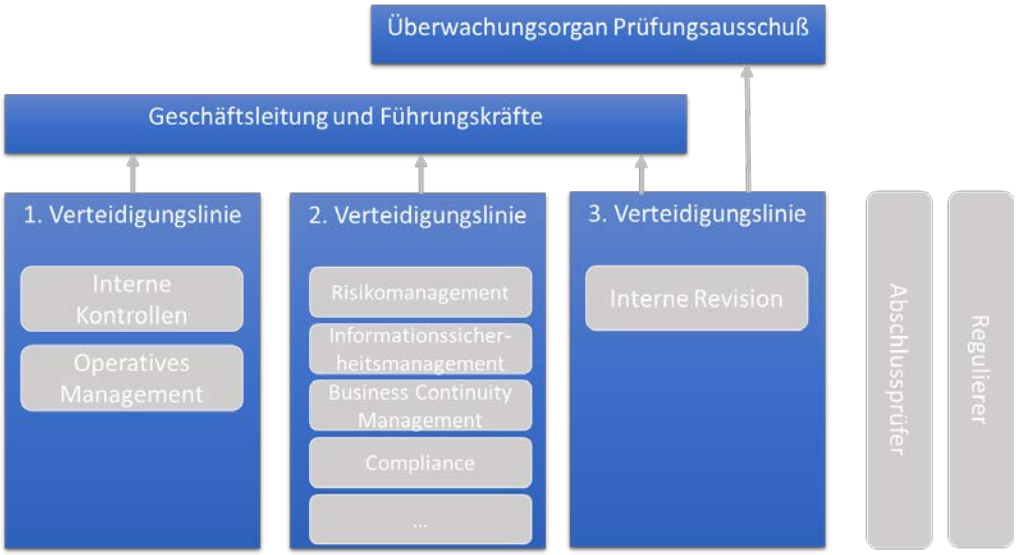
vergangenen Jahren das „Three Lines of Defense“ – Modell (TLoD) sehr schnell weite Verbreitung gefunden.

2. DAS MODELL DER DREI VERTEIDIGUNGSLINIEN – „THREE LINES OF DEFENSE“

Das Organisationsmodell zur Steuerung des Risikomanagements in einem Unternehmen hat in den vergangenen Jahren insbesondere im Finanzdienstleistungsbereich weite Verbreitung gefunden. Herausgegeben wurde das Corporate-Governance-Modell „Three Lines of Defence Model for internal governance“ (TLoD) vom Dachverband der europäischen Revisionsinstitute (ECIIA). Das etwas martialisch klingende Modell beschreibt die unterschiedlichen Rollen zur Steuerung (Governance) des Risikomanagements.

Das Modell besteht aus den drei „Verteidigungslinien"

- Die erste „Verteidigungslinie“ besteht aus den Fachbereichen mit dem operativen Management. Sie hat als „Risiko-Eigentümer“ die Verantwortung für die Beurteilung, Steuerung, Überwachung und Reduktion von Risiken.
- Die zweite „Verteidigungslinie“ dient der Steuerung und Überwachung der Risikomanagementfunktionen der ersten „Verteidigungslinie“ für eine bestmögliche Effektivität. Hierzu gehört die Festlegung von Methoden und Verfahren für das Risikomanagement, die Vorgaben durch Leit- und Richtlinien, die Überwachung der Risiken sowie das Reporting an die Unternehmensleitung.
- Die dritte "Verteidigungslinie“ stellt als objektive und unabhängige Prüfungs- und Beratungsinstanz die Interne Revision dar. Die Interne Revision unterstützt in dieser Funktion Unternehmensleitung, operatives Management und Überwachungsinstanzen. Sie soll der Unternehmensleitung die Gewähr dafür bieten, dass die Risiken wirksam erkannt, bewertet und gesteuert werden.
- Zusätzlich können auch externe Instanzen, wie z.B. der Abschlussprüfer und Aufsichtsbehörden, die Überwachungsstruktur der Organisation unterstützen und somit eine tragende Rolle einnehmen. Dieses externe Audit kann als vierte Verteidigungslinie angesehen werden.



in Anlehnung an Three Lines of Defence Model, 8th European Company Law Directive on Statutory Audit DIRECTIVE 2006/43/EC – Art. 41-2b, 14.12.2011

3. DAS THREE LINES OF DEFENSE MODELL FÜR BUSINESS CONTINUITY- UND INFORMATIONSSICHERHEITSMANAGEMENT

Das Modell der drei Verteidigungslinien gilt für alle Disziplinen des Risikomanagements. In diesem Beitrag werden Vorteile und Herausforderungen der Implementierung an den Disziplinen Informationssicherheitsmanagement (ISM) und Business Continuity Management (BCM) aufgezeigt.

Die Implementierung von Sicherheitsaufgaben und -verantwortungen erfolgt häufig „von oben nach unten“: von der Unternehmensleitung wird der Handlungsbedarf für die Themen ISMS und BCM erkannt. Auslöser mit akut folgendem Handlungsdruck sind meist Prüfungsergebnisse von Abschlussprüfungen oder Sonderprüfungen durch Aufsichtsbehörden (Bsp. „§44 KWG-Prüfungen“ im Finanzdienstleistungs-bereich). In der Folge werden Mitarbeitern die Rollen des Business Continuity Managers und Informationssicherheitsbeauftragten übertragen. Die zweite Verteidigungslinie neben der bereits bestehenden dritten Verteidigungslinie „ist geboren“. Nicht jeder dieser ernannten Mitarbeiter sieht diese „Übertragung“ jedoch als feierlichen Ritterschlag an. Denn ein Ritter alleine hat kann keine Schlacht gewinnen – um im martialischen Bild des TLoD-Modells zu bleiben. Ein Heer wird dem neuen Ritter allerdings in der Regel leider nicht mit auf den Weg gegeben. In dieser Situation hilft das TLoD-Modell, in dem es die Rollen für die Umsetzung des Sicherheits- und Risikomanagements identifiziert und die Verteilung von Aufgaben, Kompetenzen und Verantwortlichkeiten unterstützt. Der einsame Ritter kann so doch noch zu seinem Heer in Form der Fachbereiche und Führungskräfte mit Hilfe der ersten Verteidigungslinie kommen.

Die erste Verteidigungslinie ist für die operative Umsetzung des Risikomanagements auf Basis der methodischen Vorgaben und Richtlinien durch die zweite Verteidigungslinie verantwortlich.

Hierzu zählen im Informationssicherheitsmanagement

- die regelmäßige Durchführung der Schutzbedarfs-Feststellung für die Informationswerte
- die Durchführung und Aktualisierung der Bedrohungs- und Risikoanalyse
- die Identifikation und Meldung von Informationssicherheits-Risiken und Schwachstellen
- die Umsetzung risikomindernder Maßnahmen
- die Meldung von Informationssicherheits- und Verdachtsfällen sowie die Mitwirkung der Behandlung von Informationssicherheitsvorfällen
- die Durchführung prozessintegrierter Kontrollen.

Im Business Continuity Management zählen zu den Aufgaben der ersten Verteidigungslinie

- die Identifikation geschäftskritischer Prozesse und Ressourcen im Rahmen der Business Impact Analyse
- das Risk Assessment zur Identifikation der Risiken für die Prozesse und Ressourcen in der Rolle als Risikoeigentümer
- die Entwicklung von Kontinuitäts-Konzepten für den Ausfall von Prozessen und Ressourcen
- die Erstellung und Pflege von Krisen- und Notfallplänen
- die Umsetzung von Maßnahmen für die Notfallvorsorge
- die Durchführung von Tests und Übungen der Notfall-Konzepte und -Pläne.

Den Fachbereichen und Führungskräften kommt somit eine tragende Verantwortung für die operative Umsetzung des Risikomanagements zu. Das Modell der drei Verteidigungslinien macht diese zentrale Rolle deutlich.

Die zweite „Verteidigungslinie“ im TLoD-Modell beinhaltet die zentralen Funktionen für Risikomanagement, Informationssicherheit, Business Continuity Management, Unternehmenssicherheit, Datenschutz und Compliance.

Diese Zentralfunktionen sind für die methodischen Vorgaben und Richtlinien verantwortlich. Sie steuern und überwachen deren Umsetzung in den operativen Bereichen. Die Überprüfung der Reifegrade sowie die Weiterentwicklung der Managementsysteme liegt ebenfalls in der Verantwortung der zweiten „Verteidigungslinie“.

Interne Revision als dritte „Verteidigungslinie“ sowie externe Audits geben der Unternehmensführung ein unabhängiges Bild über den Umsetzungsgrad des Risikomanagements.

Nur im effektiven Zusammenwirken aller drei „Verteidigungslinien“ lässt sich ein Risikomanagement im Unternehmen erfolgreich implementieren.

Ein großer Vorteil des TLoD-Modells besteht nicht nur in der Differenzierung der Rollen zwischen diesen drei Verteidigungslinien, sondern auch in der Koordination der Disziplinen innerhalb der zweiten Verteidigungslinie.

Die Vorgaben der zweiten Verteidigungslinie müssen den gesetzlichen und regulatorischen Anforderungen entsprechen, von der Unternehmensstrategie abgeleitet sowie inhaltlich und methodisch konsistent zwischen den Disziplinen abgestimmt sein.

Gerade die neuen gesetzlichen und regulatorischen Anforderungen zum Beispiel aus IT-Sicherheitsgesetz und EU Datenschutz Grundverordnung erfordern eine enge inhaltliche Abstimmung, um Doppelarbeiten und Inkonsistenzen zwischen Vorgaben, Methoden und Richtlinien zu vermeiden. Regulierer und Prüfer haben ein immer strengeres Auge gerade auf diese Schnittstellen.

Die zweite Verteidigungslinie ist auch für das Berichtswesen über den Stand der Umsetzung von Maßnahmen sowie von Risiken, Informationssicherheitsvorfällen und Datenpannen verantwortlich. Das Berichtswesen muss inhaltlich aufeinander abgestimmt sein, damit der Vorstand ein vollständiges und widerspruchsfreies Bild der Risikosituation des Unternehmens erhält.

Durch die explizite Definition der zweiten Verteidigungslinie wird die Abstimmung zwischen den Verantwortungsträgern auf dieser Ebene gefördert.

Diese enge Zusammenarbeit der Disziplinen für das Sicherheits- und Risikomanagement wird zum Beispiel aktuell durch die am 25. Mai 2016 in Kraft getretene EU-Datenschutz-Grundverordnung explizit gefordert. Eine Umsetzung der umfangreichen gesetzlichen Anforderungen gelingt nur in einer engen Zusammenarbeit zwischen Datenschutz und den anderen Disziplinen des Sicherheits- und Risikomanagements.

4. FAZIT

Das Modell der drei „Verteidigungslinien“ mutet zunächst einmal etwas martialisch an. Auch dies hat bei mir zunächst einmal Skepsis ausgelöst. Doch zeigt sich bei näherer Betrachtung und längerem Umgang mit dem Organisationsmodell, dass es hilft, die Rollen und Verantwortlichkeiten für das Risikomanagement im Unternehmen zu schärfen. Ein unternehmensübergreifendes Rollenmodell dient zudem der besseren Kommunikation zwischen Unternehmen und mit externen Prüfern. Das Modell der drei „Verteidigungslinien“ ist einfach und klar strukturiert. Es ist damit eine gute Grundlage für die Ausprägung des individuellen Prozess- und Organisationsmodells für das Risikomanagement im Unternehmen. Im Finanzdienstleistungsbereich ist das Modell bereits weit verbreitet und anerkannt.

Matthias Hämmerle MBCI
haemmerle-consulting
www.haemmerle-consulting.de