Three Lines of Defense Modell

Eine Adaption für Finanzdienstleister


Prof. Dr. oec. Michèle F. Sutter-Rüdisser, Titularprofessorin für Organizational Control und Corporate Governance an der Universität St. Gallen, Gastprofessorin für Banking and Insurance an der Università Commerciale Luigi Bocconi in Mailand. Cornel Germann, Doktorand und wissenschaftlicher Mitarbeiter an der Universität St. Gallen. Gemeinsam engagieren Sie sich für das Network for Innovative Corporate Governance (www.nicg.net).

Der Aufsichtsrat von Finanzdienstleistern ist durch die sich steigenden regulatorischen und gesetzlichen Anforderungen einer Vielzahl an Kontroll- und Compliance-Prozessen ausgesetzt. Dies erfordert Folgeaktivitäten auf operationeller und formaler Ebene, bestenfalls eingebettet in einem Enterprise Risk Management (ERM)-Ansatz. Das im 2013 vom Institut of Internal Auditors (IIA) eingeführte Three Lines of Defense Modell (TLDM), das wohl am häufigsten zur Abbildung und Organisation von Kontroll- und Aufsichtsfunktionen verwendet wird, steht vermehrt in der Kritik. Eine Reformation an die gesetzlichen Neuerungen und aufkommenden ökonomischen Theorien wird seitens Praktikern und Akademikern längst gefordert. Der Beitrag erläutert die in der Kritik stehenden Bereiche und schlägt den Wechsel zum Three Lines of Control Modell (TLCM) mit sechs wesentlichen Adaptionen vor.

I. Einführung

Seit der Einführung erfuhr das Three Line of Defense Modell (TLDM) eine stetig zunehmende Aufmerksamkeit. Eine Vielzahl von Organisationen integrieren das Modell in dessen Enterprise Risk Management (ERM) oder Corporate Governance-Berichten. Die implementierten Modelle unterscheiden sich jedoch vom ursprünglich vorgeschlagenen Konzept. In diesem Zusammenhang ist insbesondere die zweite Verteidigungslinie (Risikomanagement und Compliance) zu erwähnen. Regulatorische Anforderungen und das Risikomanagement und Compliance haben enorm an Bedeutung gewonnen. Die daraus sich erzeugende fundamentale Informationsbasis ermöglicht es, neben weiteren Entscheidungsfindungsprozessen, den Pflichten des Aufsichtsrats (AR) nachzukommen. Die Etablierung von formalen Kommunikationswegen zwischen den operativen Einheiten und dem Vorstand respektive dem Vorstand und dem AR sind deshalb essenziell. Nur so kann der AR den gesetzlichen Pflichten gerecht werden. Das TLDM ist jedoch mit zunehmender Kritik konfrontiert. Wissenschaft und Praxis fordern gemeinsam ein überarbeitetes Modell, das aktuelle ökonomische Theorien widerspiegelt.[1] Eine Reformation setzt den Fokus auf dessen Stärken, Nutzen und Anwendungsbereiche voraus, um einen praktischen und sinnstiftenden Nutzen zu ermöglichen.[2] Unser Three Lines of Control Modell (TLCM) baut auf dem bestehenden Ansatz auf und ergänzt dieses mit aktuellen wissenschaftlichen Erkenntnissen und international akzeptierten regulatorischen Guidelines. Im Detail konzentrieren wir uns auf Finanzdienstleistungsgesellschaften und dessen zweite und dritte Verteidigungslinie (v.a. Risikomanagement, Compliance und Interne Revision) und wie dessen Berichtslinien zu den oberen Führungsebenen zur Erfüllung der regulatorischen Standards aufgestellt werden sollten.

1 Leech, T. J. & Hanlon, L. C., Three Lines of Defense versus Five Lines of Assurance (New Jersey, 2016), S. 335-355.

2 Institut of Internal Auditors (IIA), The Three Lines of Defense in Effective Risk Management and Control (Positionspapier, 2013).

INHALT

Keywords
Finanzdienstleister; Finanzindustrie; Three Lines of Defense Modell

II. Reformation des Three Lines of Defense Modell (TLDM)

Bei der Betrachtung der implementierten Modelle versäumt das ursprüngliche TLDM vorgeschriebene Gesetze, Richtlinien und bestimmte Dynamiken in der Praxis korrekt ab-

zubilden. Die weitreichende Applikation auf verschiedene Branchen und Bereiche und damit verbunden der entsprechende generelle, einfache Charakter des Designs, sind wohl die offensichtlichsten Gründe. Da Themen wie Risiko, Compliance und Interne Revision zum Kernstück in Verbindung von Kontrolle und Leistung wurden, ist es jedoch an der Zeit, diese Faktoren ebenfalls im TLDM zu implementieren. Wir schlagen im TLCM, im Vergleich zu IIAs TLDM, folgende sechs Reformationen vor:

1. Regulator

Wir sehen die Positionierung/Rolle des Regulators differenzierter. Die Regulierungs- und Aufsichtsbehörden (bei Finanzdienstleistern in Deutschland vor allem die BaFin) spielen indirekt eine zentrale Rolle bei der Festlegung der Organisationsstruktur und dessen operativer Umsetzung. Die Aufsichts- und Regulierungsbehörden bilden die Grundlage für den Aufbau einer Organisationsstruktur; insbesondere hinsichtlich der Risikobewertung. Besonders Finanzunternehmen sehen sich mit zunehmenden Vorschriften konfrontiert, die einen unmittelbaren Einfluss auf ihre Struktur und die Art und Weise der operativen Geschäftstätigkeit aufweisen. Im Hinblick dessen ist es angemessen, den nationalen sowie internationalen Behörden eine zentralere und grundlegendere Rolle zu übertragen. Deshalb sehen wir die Aufsichts- und Regulierungsbehörde als Fundament und erste Instanz im Kontrollmechanismus.

2. Kollaboration der drei Funktionslinien

Die zweite Anpassung bezieht sich auf die Kohäsion der ersten, zweiten und dritten Verteidigungslinie respektive – bezüglich unseres Vorschlags – auf die Steuerungs- und Überwachungslinien (Lines of Control). Wir sehen in der vollständig voneinander unabhängigen Abwicklung der Instanzen ein Konfliktpotenzial. Die Funktionen der Internen Revision sind so strukturiert, dass dessen Tätigkeiten spezifisch auf die individuellen Gegebenheiten des Geschäfts und dessen operativer Umsetzung der ersten beiden Funktionen entsprechen, wobei sich diese erheblich von denen der Wettbewerber am Markt unterscheiden können. Dessen Kontrollaktivitäten sind daher abhängig vom Geschäft und dem Umfang der identifizierten, bestehenden (operativen) Risiken. Eine enge Zusammenarbeit mit den ersten beiden Linien zur Sicherung der Kontrollinstrumente und deren Steuerungsfunktionen ist deshalb unvermeidlich.[3] Unser Modell stellt daher die drei Funktionen eingebettet in ein grau unterlegtes Rechteck dar, Symbol für eine grundsätzliche homogene, aber in sich individuell verantwortliche Einheit. Ziel der drei Funktionen ist die operative Geschäftsführung zu ermöglichen, entsprechende Risiken daraus zu identifizieren und, zu guter Letzt, die daraus ableitenden Kontrollmaßnahmen zur operativen Zielerreichung zu implementieren; ein kooperativer und partnerschaftlicher Ansatz analog dem ERM.

3. Risk Management und Compliance

Seit der Finanzkrise 2008 sind Finanzdienstleister mit einem immer

3 Ruud, T. F. & Kyburz, A., Gedanken zum Three Lines of Defense Modell – Was ist mit Verteidigung gemeint? (Der Schweizer Treuhänder, 2014), S. 761–766.

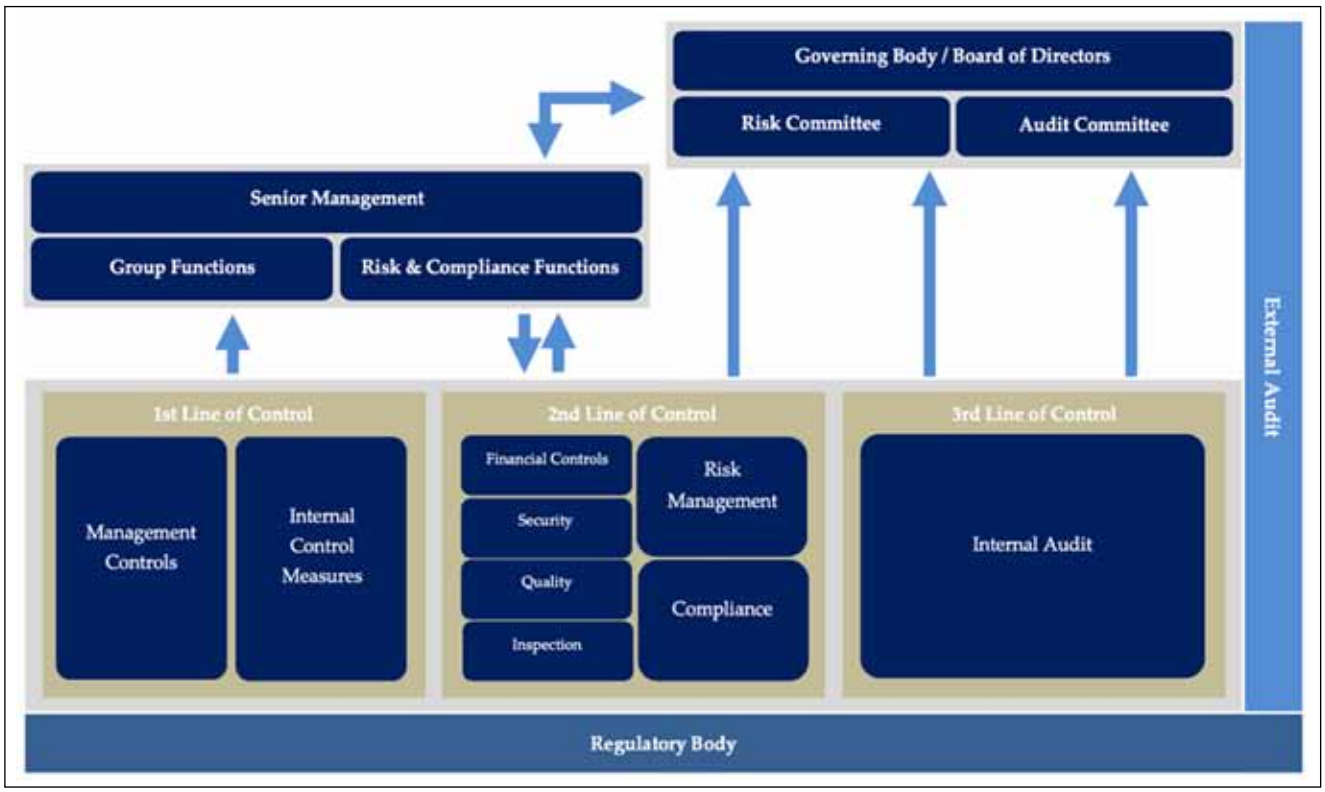

Abb. 1: Das Three Lines of Control Modell (TLCM)

umfassenderen Regulierungsapparat konfrontiert (z.B. Basel III). Im Gegensatz zum traditionellen Modell nimmt das Risikomanagement, Compliance und Interne Kontrollsystem (IKS) eine übergeordnete Rolle ein. Dieser Umstand sollte ebenfalls im Modell berücksichtigt werden; verdeutlicht und betont durch die Größe der Rechtecke. Durch eine höhere (finanzielle und personelle) Ressourcenausstattung soll die Effektivität und Effizienz der Kontrollmaßnahmen hinsichtlich der bestehenden Risiken und internen Richtlinien gewährleistet werden.[4] Hier gilt, je früher die entsprechende Zuteilung und Positionierung erfolgt, desto schneller können Maßnahmen eingeleitet werden. Ein wirksames Instrument zur Überwachung der Risikoneigung und Risikobereitschaft (Expected vs. Realized Risk); besonders bei Finanzgesellschaften essenziell.[5] Die höhere Ressourcenausstattung erlaubt es der zweiten Funktionslinie auch vermehrt eine Aufsichts- anstatt eine Risikoförderungsrolle einzunehmen (Risk Challenger vs. Risk Enabler).[6]

4. Steuerungs- und Überwachungslinien (Lines of Control)

Neben einer besseren Ressourcenausstattung und engeren Zusammenarbeit zwischen den drei Funktionen, sehen wir es als nötig an, den Begriff Verteidigung (Defense) durch Kontrolle (Control) zu ersetzen. Unserer Ansicht nach verfehlt die Bezeichnung Verteidigung (Defense) die Intention des Modells, bestehende Risiken zu managen, zu kontrollieren und einen nachhaltigen Wettbewerbsvorteil gegenüber unseren Wettbewerbern zu erzielen. Verteidigung hingegen impliziert ein passives, reagierendes Verhalten; die stetige Abwehr von Risiken. Ziel jedoch sind Risiken so einzusetzen, dass Wettbewerbsvorteile erzielt werden können. Gefragt ist Proaktivität (agieren anstatt reagieren). Der Begriff Verteidigung verfehlt diese Absicht zu verkörpern. Es vermittelt eher den Eindruck, dass die Gesellschaften gezwungen sind aus einer Position der Schwäche entsprechende Maßnahmen zu lancieren; adhoc-Entscheidungen als letztes Mittel. Das Modell soll es dem Unternehmen ermöglichen aus einer gestärkten Position heraus bestehende Risiken und Problembereiche frühzeitig anzugehen und entsprechende Maßnahmen einzuleiten. Aus unserer Sicht scheint Kontrolle anstatt Verteidigung deshalb angemessener.

5. Risiko- und Prüfungsausschuss auf Stufe AR und Vorstand

Im Gegensatz zu IIAs Modell, schlagen wir zusätzlich einen Risiko- und Prüfungsausschuss in direkter Unterstellung des AR vor. Der AR kann Aufgaben an die Ausschüsse delegieren, behält aber die ihm nach dem Gesetz zugewiesene Verantwortung. Während sich der Prüfungsausschuss in der Regel auf die Bereiche IKS und Compliance konzentriert, setzt sich der Risikoausschuss mit operationellen und geschäftlichen Risiken auseinander. Eine Unterteilung (anstatt Kombination) in einen Prüfungs- und Risikoausschuss bringt zwei wesentliche Vorteile. Erstens erfolgt eine bessere Zuordnung der Handlungsspielräume, sodass Verantwortlichkeiten explizit verfolgt werden können. Eine Doppelausführung/ Überschneidung von Kontrollen wird verhindert, was die Wirksamkeit und Effektivität fördert. Zusätzlich erwirkt dies einen Kompetenzgewinn. Durch die Zuordnung von Aufgaben finden Diskussionen mit komplexen Inhalten Anklang und können – auch in Kooperation mit anderen Funktionsträgern – gelöst werden. Compliance und Risiko Manager und Interne Revisoren haben somit das Privileg, komplexe Thematiken direkt mit Experten aus den Ausschüssen zu diskutieren und, für fachspezifische Inhalte, entsprechende gemeinsam erforderliche Lösung zu generieren. Zweitens nimmt der AR seine aufsichtsrechtliche Kontrollfunktion wahr. Die Aufnahme der beiden Ausschüsse in das Modell legt den AR nicht nur – im Hinblick auf die Umbenennung von Defense zu Control – als letzte Kontrolllinie fest (Last Line of Control), sondern weist den Komitees auch die Rolle des „verlängerten Arms" zu. Wie bereits bei den einzelnen Kontrolllinien bildet der AR sowie der Risiko- und der Prüfungsausschuss eine verbundene Einheit (grau eingefärbtes Rechteck), in welchem ein Informationsaustausch stattfindet.

Finanzdienstleister (im Vergleich zu Unternehmen aus anderen Branchen) sind höheren Risiken ausgesetzt. Die Kapazitäten des AR sind begrenzt (Stichwort Ressourcen und Zeit). Die Ausschüsse respektive der Vorstand wird deshalb mit weiteren Kompetenzen ausgestattet, um ebenfalls die Aufsichts- und Kontrollfunktionen zu stärken. In Anbetracht dessen empfehlen wir, neben der Zuweisung eines Risiko- und Prüfungsausschusses auf Stufe des AR, einen (Finanz- und) Risikoausschuss auf der Stufe des Vorstands zu etablieren. Komplexität und Materialität spielen hier eine Rolle. Der Vorstand überwacht die ersten beiden Kontrollfunktionen und fungiert als Sparringspartner für die Finanz-, Compliance- und Risikomanagementabteilung. Diese zugleich als Aufsicht- und Partnerschaftsstruktur definierte Funktion basiert auf einer vertrauenswürdigen Beziehung, da die entsprechend behandelten und weitergeleiteten Informationen für die Entscheidungsfindung unerlässlich sind. Eine nicht zu unterschätzende Gratwanderung. Es ist deshalb essenziell, diesen Begebenheiten mit adäquaten Massnahmen Sorge zu

4 Basel Committee on Banking Supervision (BCBS), Guidelines. Corporate governance principles for banks (2015).
5 Ernst & Young (EY), Risk management formations – an alternative approach to the 3 lines of defense model (The Journal of Financial Perspectives, vol. 2., 2014).
6 Mabwe, K., Ring, P. J. & Webb, R., Operational risk and the three lines of defence in UK financial institutions (Journal of Operational RISK, 2017), 12(1), 53–69.

tragen. Das angepasste TLCM trägt diesem Umstand Rechnung. Einerseits durch die Einführung einer administrativen und funktionalen Berichtslinie von der zweiten Kontrollfunktion an den Vorstand respektive den AR sowie andererseits, durch die zusätzliche Einrichtung eines (Finanz- und) Risikoausschusses auf Ebene des Vorstandes. Durch die beiden Adaptionen kann die Stellung der zweiten Funktionslinie zum Vorstand gestärkt werden.[7] Ziel der Struktur ist es, den AR zu entlasten und Prozesse, im Hinblick „administrativer Hintergründe", zu beschleunigen. Dennoch muss die Unternehmensleitung sicherstellen, dass dem AR die Informationen rechtzeitig zufließen. Die vorgeschlagene zweifache Berichtsstruktur seitens der zweiten Kontrolllinie (an den Vorstand sowie den AR) stellt zum einen die formalen Kommunikationswege sowie zum anderen eine vollständige Informationsbasis sicher. So ist gewährleistet, dass alle Beteiligten über den Vorfall informiert sind. Eine empfehlenswerte Möglichkeit, um Gegenmassnahmen angemessen zu diskutieren und gemeinsam umzusetzen. Die Verantwortlichen der einzelnen zweiten Funktionsbereichslinien bilden in diesem Falle das Rückgrat in der prozessualen Implementierung. Der Vorstand hat deshalb die Pflicht, im Voraus festzulegen, wann und in welchem Stil die Kommunikation erfolgen soll (Stichwort interne Richtlinien). Eine sachgemäße Berichtsstruktur erlaubt es, dem heutigen digitalen Zeitalter und den sich schnell wechselnden Umständen entgegenzuwirken und entsprechend notwendige Entscheidungen, die rasches handeln fordern, ad-hoc umzusetzen.

6. Interne Revision

Zur Vervollständigung der Kontrollfunktion und internen Berichterstattung ist die Interne Revision, neben bislang nur dem Prüfungsausschuss, auch mit einer direkten Berichtslinie an den Risikoausschuss ausgestattet.[8] Wir betrachten dies im Hinblick des notwendigen Informationsaustausches als existenziell. Durch die umfassenden Kontrollmaßnahmen der Internen Revision können implizit gewonnene Informationen nicht nur für den Prüfungs- sondern auch für den Risikoausschuss von Interesse sein. Nicht nur neue, bisher unbekannte Schwachstellen oder Risiken können identifiziert, sondern auch entsprechende Maßnahmen ergriffen werden. Ebenso fördert dies den Austausch zwischen allen drei Kontrollfunktionsbereichen. So kann ein Informationsaustausch auf vertikaler (Interne Revision und Ausschüsse) und auf horizontaler Ebene (Prüfungs- und Risikoausschuss und AR) stattfinden.

III. Fazit

Unsere Erläuterungen zeigen die Notwendigkeit von Reformansätzen im ursprünglichen TLDM. Konkret ist es notwendig, die sich intensivierenden regulatorischen und gesetzlichen Anforderungen im Modell zu implementieren, sodass der AR respektive der Vorstand die entsprechenden Kontrollmaßnahmen effizient umsetzen können. Das vorgeschlagene TLCM präsentiert erste Ideen, wie dies in der Theorie und Praxis umgesetzt werden könnte. Zwei Faktoren spielen hierbei eine wichtige Rolle: Die in einem Unternehmen herrschende Dynamik mit dem AR als letzte Kontrollinstanz und die gesetzlichen Vorgaben und Best Practice Standards. Finanzunternehmen sind diesbezüglich besonders geprägt. Wir setzen uns deshalb dafür ein, den einzelnen Funktionsbereichen (v.a. Compliance und Risikomanagement) vermehrt Kompetenzen und Ressourcen zur Verbesserung der Kontroll- und Kommunikationsprozesse zuzuweisen.

7 Financial Stability Institute (FSI), The "four lines of defence model" for financial institutions (2015).

8 Protiviti, Applying the Five Lines of Defense in Managing Risk (2015).