T. FLEMMING RUUD
ADRIAN KYBURZ

GEDANKEN ZUM THREE LINES OF DEFENSE MODELL – WAS IST MIT VERTEIDIGUNG GEMEINT?

Analyse des Governance-Modells aus der Sicht des internen Audits

Das Three Lines of Defense Modell hat in den vergangenen Jahren auch in Schweizer Unternehmen als Rahmenwerk für ein ganzheitliches Governance-System im Hinblick auf die Risikosteuerung stark an Bedeutung gewonnen. Dieser Artikel analysiert verschiedene Aspekte des Modells aus der Perspektive des internen Audits.

1. EINLEITUNG

Mit dem *Three Lines of Defense* Modell ist ein umfassender Bezugsrahmen zur Organisation eines effektiven Governance-Systems geschaffen worden. Rahmenwerke dieser Art dienen der Förderung eines systematischen Ansatzes zur Identifikation und Handhabung von Unternehmensrisiken. Das Three Lines of Defense Modell wurde als Folge der Veröffentlichung der 8. EU-Richtlinie von 2006, der sogenannten Abschlussprüfer-Richtlinie, einem breiteren Publikum präsentiert und war dazu gedacht, die betroffenen Unternehmen bei der Umsetzung der neuen Vorgaben zu unterstützen. Ausschlaggebend war vor allem Art. 41 der besagten Richtlinie, der mitunter die Errichtung eines *Audit Committee (AC)* verlangt, welches «die Wirksamkeit des internen Kontrollsystems, gegebenenfalls des internen Revisionssystems und des Risikomanagementsystems des Unternehmens» überwacht. Somit wurde in Zusammenarbeit zwischen der *European Confederation of Institutes of Internal Auditing (ECIIA)* und der *Federation of European Risk Management Associations (FERMA)* die sogenannte *Guidance on the 8th EU Company Law Directive* veröffentlicht [1]. Diese Richtlinie stösst bis heute auf breite Akzeptanz und kann als massgeblicher Treiber der Popularität des Modells betrachtet werden.

Mit der Veröffentlichung eines Position Paper zur umfassenden Beschreibung des Three Lines of Defense Modells wurde das Rahmenwerk im vergangenen Jahr auch durch das *Institute of Internal Auditors (IIA)*, den weltweit agierenden Berufsverband und Standard-Setter des internen Audits, und damit auch durch dessen nationale Vertretung, den *Schweizerischen Verband für Interne Revision (SVIR)*, anerkannt [2]. Diese Publikation hat das Three Lines of Defense Modell endgültig zu einem weltweit beachteten *Best Practice*-Ansatz gemacht.

Aufgrund dieser Entwicklung ist es an der Zeit, verschiedene Aspekte des Modells einer weitergehenden Analyse zu unterziehen und dabei auch auf die Gefahren, die einer zu plakativen Adaption des Modells im eigenen Unternehmen zugrunde liegen, hinzuweisen.

Im Folgenden werden zuerst die Grundlagen und der Kern des Three Lines of Defense Modells vorgestellt, bevor die Implikationen des Rahmenwerks für die Berichterstattung diskutiert werden. Es folgt eine Analyse verschiedener Aspekte, um das Rahmenwerk aus neuen Perspektiven zu beleuchten und zu hinterfragen. Das zuvor erwähnte Position Paper des IIA dient als primäre Grundlage dieser Diskussion. Ein zusammenfassendes Fazit wird den Artikel beschliessen.

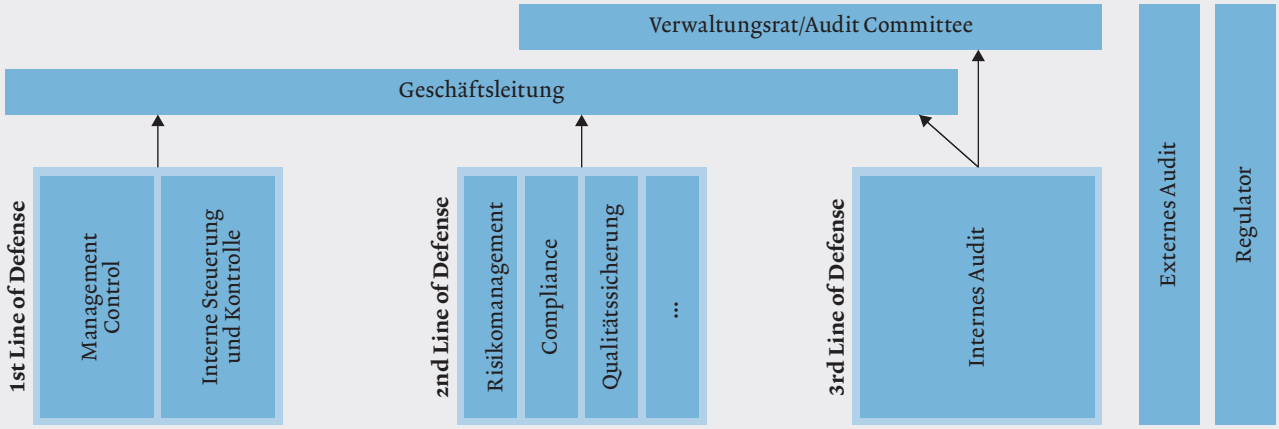
2. THREE LINES OF DEFENSE MODELL

2.1 Grundlagen. Das Three Lines of Defense Modell illustriert, wie in *Abbildung 1* ersichtlich, eine systematische Organisation der Akteure und Komponenten des *internen Steuerungs- und Kontrollsystems (IKS)*. Als Rahmenwerk für den Aufbau und das Zusammenspiel dieser das Unternehmensrisiko steuernden Einheiten verfolgt das Modell primär die folgenden Ziele:

T. FLEMMING RUUD, PROF. PHD, WP (N), PROFESSOR FÜR BETRIEBSWIRTSCHAFTSLEHRE (INTERNAL CONTROL/ INTERNAL AUDIT), UNIVERSITÄT ST. GALLEN, ST. GALLEN

ADRIAN KYBURZ, MSC, DOKTORAND, WISSENSCHAFTLICHER MITARBEITER VON PROF. T. FLEMMING RUUD, UNIVERSITÄT ST. GALLEN, ST. GALLEN

Abbildung 1: **THREE LINES OF DEFENSE MODELL**

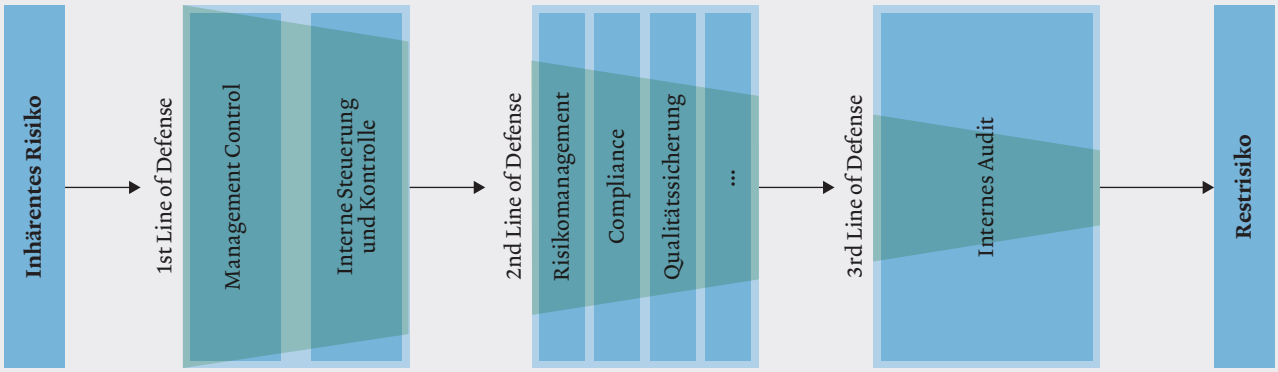


→ Definition klarer Rollen und Verantwortlichkeiten verschiedener Organisationseinheiten im Bereich des Risikomanagements sowie des IKS. → Aufzeigen einer effektiven und effizienten Koordination dieser Einheiten zur Vermeidung von Kontrolllücken und Doppelspurigkeiten. → Einbettung der einzelnen Risiko- und Kontrolleinheiten in ein ganzheitliches Governance-System.

In Schweizer Unternehmen basiert die Organisation der Governance auf Art. 716a Abs. 1 des Schweizerischen Obligationenrechts (OR). Demzufolge obliegt dem *Verwaltungsrat (VR)* neben der Oberleitung der Gesellschaft auch die ultimative Verantwortung für das Risikomanagement und das IKS. Zur Wahrnehmung dieser Aufgaben, d. h. der Gewährleistung effizienter operativer Abläufe sowie eines funktionierenden IKS, hat der VR gewisse Delegationsmöglichkeiten, weshalb die Ausführungsverantwortung in der Regel bei der Geschäftsleitung anzusiedeln ist. Trotz dieser Übertragung exekutiver Rechte behält der VR als höchste, von der Generalversammlung eingesetzte Unternehmensinstanz seine Aufsichtsfunktion (Monitoring). Weiter muss der VR der Geschäftsleitung eine Unternehmensstrategie sowie die dabei einzuhaltenden Grenzen des aggregierten Geschäftsrisikos (Risk Appetite) vorgeben. Im Rahmen dieser Direktiven organisiert die exekutive Führung des Unternehmens ein IKS, um die Erreichung der operativen Ziele mit höchst möglicher Wahrscheinlichkeit zu gewährleisten. Somit hat die Geschäftsleitung die Aufgabe, die verschiedenen risikosteuernden Einheiten zu organisieren und zu führen.

2.2 Kern des Modells. Das Three Lines of Defense Modell stellt für die leitenden Unternehmensorgane eine Möglichkeit zur effizienten Wahrnehmung ihrer Funktionen und Verantwortlichkeiten dar. Es zeigt – wie der Name sagt – drei voneinander unabhängige Ebenen unterhalb der Unternehmensführung, die der Steuerung des Unternehmensrisikos dienen:
→ Die *1st Line of Defense* ist beim operativen Management angesiedelt und kann bei allen Unternehmen *einheitlich* mit den Steuerungs- und Kontrollelementen im Wertschöpfungsprozess beschrieben werden. Die Geschäftsleitung implementiert dazu verschiedene Steuerungs- und Kontrollmassnahmen entlang der Wertschöpfungskette, d. h. direkt in den operativen Prozessen, und gibt diese in die Verantwortung der Prozesseigner. Damit wird die Grundlage geschaffen, potenzielle Risiken, die jeder operativen Tätigkeit inhärent sind, präventiv zu verhindern oder möglichst früh im Prozess aufzudecken und zu korrigieren.
→ Im Gegensatz zur 1st Line hängt die Ausgestaltung der ebenfalls prozessabhängigen *2nd Line of Defense* bei verschiedenen Unternehmen vom jeweiligen Geschäftsmodell und den damit verbundenen Risiken ab. Die dieser Stufe zuzuordnenden Geschäftseinheiten sind somit unternehmensindividuell durch den VR und die Geschäftsleitung zu definieren. Hier anzusiedeln sind zum Beispiel die Compliance-Funktion, die Qualitätssicherung, das Controlling oder die Legal-Einheiten. Diese nehmen verschiedene Funktionen in der Aufsicht, der Kontrolle und der Unterstützung des operativen Managements zur Risikosteuerung wahr. Im Auftrag der Geschäftsleitung werden von den Risikomanagement-Funktionen Richtlinien und Frameworks zur Umsetzung der vorgegebenen Strategie erlassen, übergeordnete Gefahren und Trends identifiziert oder die themenspezifische Aus- und Weiterbildung der Angestellten organisiert.
→ Durch die enge Verbindung der 2nd Line of Defense zum operativen Management und zur Geschäftsleitung fehlt ihr jedoch die notwendige Distanz, um die Geschäftsprozesse und deren Risiken mit der notwendigen Unabhängigkeit beurteilen zu können. Daraus entsteht der Bedarf für eine *3rd Line of Defense* als letzte risikosteuernde Instanz, welche die leitenden Unternehmensorgane unabhängig über operationelle Potenziale und Risiken informiert. Für diese zentrale Aufgabe zur Steuerung und Kontrolle der Unternehmensrisiken ist das interne Audit vorgesehen (siehe auch Abschnitt 3.3). Das interne Audit wird vom VR und der Geschäftsleitung risikoorientiert und unabhängig vom Wertschöpfungsprozess eingesetzt, um *Assurance* über den Zustand der Prozesse – sei es auf Ebene der 1st oder der 2nd Line of Defense – zu erhalten. Möglich ist auch die Erbringung von Beratungsdienstleistungen, zum Beispiel zu Schulungs- oder zu Moderationszwecken.

Abbildung 2: **REDUKTION DES UNTERNEHMENSRISIKOS DURCH DAS THREE LINES OF DEFENSE MODELL**



Mit dieser dreifachen, aber nicht sequentiellen, sondern parallel agierenden Absicherung der inhärenten Unternehmensrisiken stehen dem VR und der Geschäftsleitung die notwendigen Instrumente zur Verfügung, um sicherzustellen, dass das verbleibende Restrisiko im Einklang mit dem vorgegebenen *Risk Appetite* des Unternehmens ist (vgl. *Abbildung 2*).

Zusätzlich zu den drei Verteidigungslinien sind auch das externe Audit sowie der Regulator Bestandteile des Modells. Diese bilden eine Art *4th Line of Defense*, werden jedoch als unternehmensexterne Einheiten nicht zum Kernmodell gezählt. Dies ist vor allem auch ihrem punktuellen Agieren sowie ihrem primär auf den finanziellen Bereich limitierten Fokus geschuldet. Es soll jedoch auch erwähnt sein, dass diese Erweiterung in Form einer 4th Line of Defense den nicht abschliessenden Charakter des Modells zeigt. Je nach Unternehmenssituation bzw. spezifischer Risikoexposition kann die Notwendigkeit entstehen, weitere externe Funktionen hinzuzuziehen, die eine Assurance-Funktion für den VR und die Geschäftsleitung wahrnehmen.

2.3 Berichterstattung. Damit die Verantwortlichen aller drei Lines of Defense ihre Aufgaben zur Risikosteuerung optimal wahrnehmen können, müssen klare Berichterstattungswege implementiert werden. Wie im Modell in Abbildung 1 illustriert, unterstehen die Prozesseigner direkt der Geschäftsleitung, d. h. in der Regel dem CEO, und sind dieser auch Rechenschaft über die Prozesse schuldig. Dies gibt der Geschäftsleitung die Möglichkeit, Eingriffe und Korrekturen direkt an der Quelle anzubringen, sofern unerwünschte Abweichungen oder nicht akzeptable Risiken auftreten. Zur Unterstützung dienen an dieser Stelle – wie bereits zuvor erwähnt – die Risikomanagement-Funktionen. Daraus kann bereits abgeleitet werden, dass auch diese primär der Geschäftsleitung unterstehen. Ein Blick in die Praxis zeigt jedoch, dass aufgrund der auch auf VR-Ebene weiterhin zu-

nehmenden Bedeutung der Risiko-Thematik die Einheiten der 2nd Line of Defense immer öfter über eine zusätzliche, direkte Berichterstattungslinie zum VR verfügen [3]. Der Bedarf für eine auf diese Weise erweiterte Berichterstattung existiert vor allem dann, wenn es die Dringlichkeit der Situation gebietet und ein schnelles Handeln auf höchster Unternehmensstufe unabdingbar ist. Im regulären Unternehmensalltag ist der direkte Berichterstattungsweg zum VR bzw. zum AC jedoch der 3rd Line of Defense, d. h. dem internen Audit, vorbehalten.

Best-Practice-Standards [4] fordern, dass das interne Audit eine direkte, funktionale Berichterstattungslinie zum Präsidenten des VR oder zum AC hat, wobei eine duale Unterstellung – d. h. eine zusätzliche, administrative Berichterstattungslinie zur Geschäftsleitung – möglich ist. Dies dient der Sicherstellung der Unabhängigkeit des internen Audits vom Management und ermöglicht objektive Analysen in allen Unternehmensbereichen zugunsten des VR und des AC.

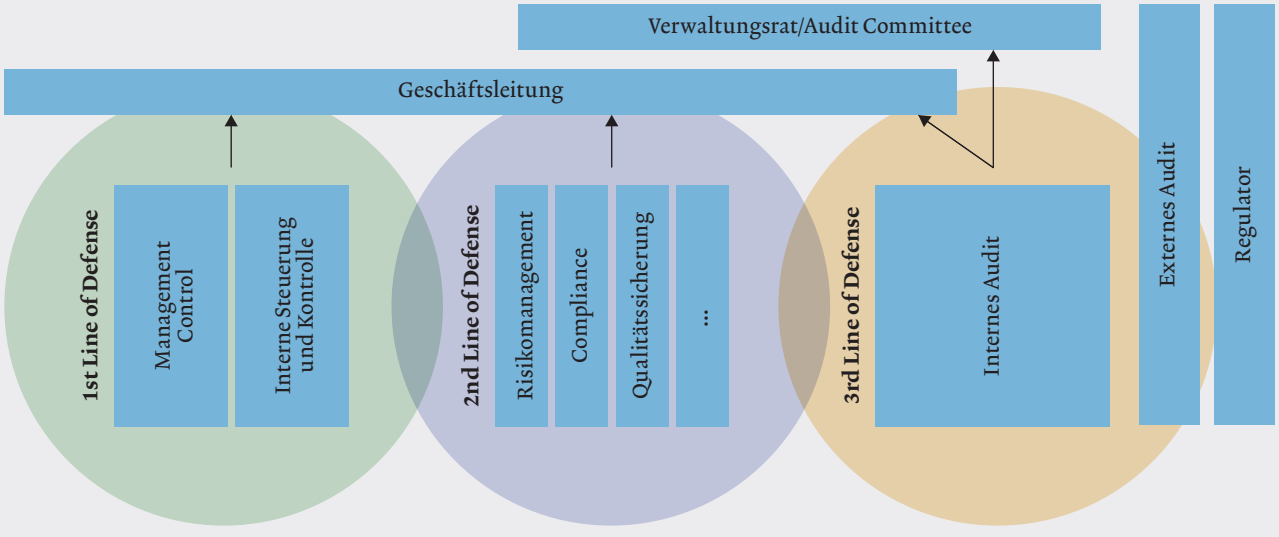
3. ANALYSE UND DISKUSSION

Im Folgenden werden verschiedene Aspekte des Three Lines of Defense Modells diskutiert und hinterfragt. In einem ersten Teil werden mögliche Implikationen und Interpretationen der im Modell verwendeten Terminologie dargelegt. Darauf werden in einem zweiten Teil die Grenzen der grundlegenden Dreiteilung besprochen. Abschliessend wird die Position des internen Audits und dessen Anspruch, die 3rd Line of Defense zu verkörpern, analysiert.

3.1 Verteidigung vs. Mehrwertschaffung. Als erstes wird an dieser Stelle die Bezeichnung des Rahmenwerks als «*Defense*»-*Modell*, d. h. als Modell zur *Verteidigung* des Unternehmens, diskutiert. Durch die Verwendung dieser Terminologie kann dem Modell und somit der gesamten Risiko- und Kontrollstruktur eine rein abwehrende Funktion zugeschrieben werden. Dies ist vor allem ein Problem bei der Benützung der deutschen Übersetzung des Begriffs, da im deutschsprachigen Raum «Verteidigung» als primär abwehrende Funktion verstanden wird. Der Grundsatz «Angriff ist die beste Verteidigung» ist dagegen in der englischen Bezeichnung «Defense» deutlich tiefer verankert, womit die proaktive Rolle der *Three Lines* zum Ausdruck kommt. Diese Argumentation gilt nicht nur bei der Modell-Überschrift, sondern auch gleichermassen bei der Bezeichnung der einzelnen Modell-Bestandteile. Um den wertschöpfenden Charakter sowohl des internen Audits als auch der Risikomanagement-Funktionen zu betonen, könnte man auch von *Lines of Control* sprechen und den im englischen Begriff *Control* enthaltenen Steuerungsaspekt bewusst betonen. Zur Abgrenzung und Verdeutlichung der Funktion des internen Audits als unabhängiger *Assurance-Provider* für den VR bzw. das AC könnte man auch von *3rd Line-Assurance* sprechen. Schliesslich hat gerade der Berufsstand der internen Auditoren in den vergangenen Jahrzehnten grosse Anstrengungen unternommen, sein früheres Image als *Polizei der Geschäftsleitung* zu verändern und sich als wertschöpfende Einheit im Dienst des VR bzw. des AC zu positionieren. Auch im Bereich Risikomanagement hat sich zuletzt die Ansicht durchgesetzt, dass die Abwehr von Risiken nicht die alleinige Aufgabe solcher Funktionen ist. Stattdessen wird dem Wahrnehmen von Opportunitäten mindestens ebenso viel Gewicht beigemessen.

«Die Besinnung auf die Kernkompetenzen des internen Audits in den Bereichen Finance, Operations sowie Compliance könnte effektiver sein als eine stete Kompetenzerweiterung.»

Abbildung 3: **ÜBERSCHNEIDUNG DER THREE LINES OF DEFENSE**



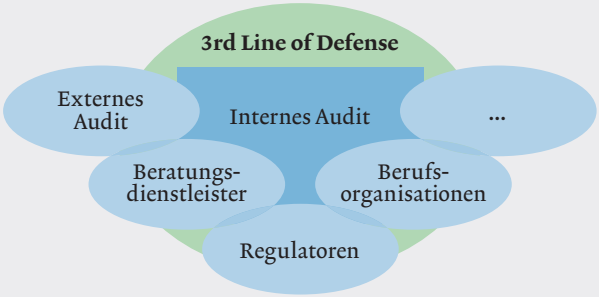
3.2 Trennungsmodell vs. Zusammenarbeit. Grund zur Diskussion ist auch die im Modell illustrierte Trennung der drei Linien, welche als Silo-Denken interpretiert werden könnte. Spätestens seit dem zur Jahrtausendwende das Thema *Enterprise Risk Management (ERM)* die traditionelle Silo-basierte Denkweise zu verdrängen begann, hat sich die Wichtigkeit der vernetzten und integrierten Risikobetrachtung in Forschung und Praxis etabliert.

Auch im Position Paper des IIA wird die Wichtigkeit der Koordination zwischen den drei Linien im Sinne der Zuteilung spezifischer Aufgaben und klarer Verantwortlichkeiten betont. Gleichzeitig wird aber die Eigenständigkeit der drei Linien als Stärke des Modells hervorgehoben. An dieser Stelle kann jedoch auch argumentiert werden, dass ein aktiver Austausch von Ressourcen und Wissen, d. h. eine Überlappung der drei Linien wie in *Abbildung 3*, die Effizienz steigern kann. Um sowohl Kontrolllücken als auch Doppelspurigkeiten zu vermeiden, sind eine effiziente Koordination und der gegenseitige Austausch zwischen den verschiedenen Linien unerlässlich. So sollte das interne Audit als 3rd Line für bestimmte Prüfungen auf Experten aus den beiden anderen Linien zurückgreifen, und es bedarf einer Abstimmung bei der Prüfungsplanung und in der Risikobeurteilung mit der 2nd Line. Auch die prozessabhängigen ersten zwei Linien sollten zu einem bestimmten Grad eine Verzahnung aufweisen. Dies speziell im Sinne eines freien Informationsflusses zur Optimierung der Wertschöpfungsfähigkeit.

3.3 Third Line Assurance. Sowohl in der Fassung des Modells von 2010 als auch im Position Paper des IIA von 2013 verkörpert alleine das interne Audit die 3rd Line of Defense und wird somit als einziger Assurance-Provider für den VR beschrieben. Dieser Zustand bedingt, wie auch in den Publikationen des IIA mehrfach gefordert, eine breit abgestützte Involvierung des internen Audits in die Unternehmensprozesse. So beinhaltet die aktuelle Version der IIA-Standards von 2013 zum Beispiel den Anspruch, dass das interne Audit das IKS und das Risikomanagement auch im Hinblick auf die strategischen Ziele des Unternehmens hin prüft. Mehr denn je stellt sich daher die Frage nach der praktischen Umsetzbarkeit solcher Forderungen. In Anbetracht der meist limitierten Ressourcen und des komplexen, globalisierten Umfelds könnte die Besinnung auf die Kernkompetenzen des internen Audits in den Bereichen *Finance, Operations* sowie *Compliance* effektiver sein als eine stete Kompetenzerweiterung.

Im Gegensatz zur Modellbeschreibung des IIA ist in der Literatur sowohl die Verwendung des Assurance-Begriffs als auch die Beschreibung der 3rd Line of Defense sehr uneinheitlich. Den verschiedenen Definitionen von *Assurance*

Abbildung 4: **THREE LINE ASSURANCE**



ist gemein, dass es dabei um die Stärkung des Vertrauens durch das Erbringen verlässlicher Informationen geht. Allerdings werden dafür neben dem internen Audit häufig weitere *unabhängige Assurance-Provider* zur 3rd Line of Defense gezählt. Wie bereits in Abschnitt 2.2 erwähnt, wird hier unter anderem das externe Audit genannt. Weiter finden verschiedene externe Anbieter von Beratungsdienstleistungen oder auch privat-organisierte Berufsorganisationen und regulatorische Körperschaften des Staates Erwähnung. Solche externen Einheiten, die den VR mit unabhängigen Informationen beliefern, können zwar als unabhängig betrachtet werden, ihr Engagement birgt jedoch auch Risiken, wie die mangelnde Vertrautheit mit den Unternehmensprozessen und der Kultur oder die Gefährdung der Datensicherheit. Aufgrund der mangelnden Unternehmenszugehörigkeit anderer Assurance-Provider sowie deren häufig auf Spezialthemen eingeschränkten Sichtweise ist die Zuteilung des internen Audits als alleiniger Vertreter der 3rd Line nachvollziehbar. Dennoch scheint es näher an der praktischen Realität, wenn die 3rd Line of Defense wie in *Abbildung 4* mit dem internen Audit als zentrale Einheit und weiteren externen Dienstleistern als unterstützend agierende Satelliten-Einheiten dargestellt wird.

4. FAZIT

Mit dem Three Lines of Defense Modell steht den Unternehmen ein anschauliches Rahmenwerk zur Organisation einer effizienten Governance-Struktur zur Verfügung. Es zeigt den Unternehmen in einem Top-down-Ansatz, welche Elemente zur gezielten Steuerung der Unternehmensrisiken vorhanden sein müssen und mit welchen Kompetenzen diese auszustatten sind, um möglichst wirksam zu sein. Wie in den vorhergehenden Abschnitten beschrieben, birgt eine zu plakative Anwendung, d. h. ohne Rücksichtnahme auf unternehmensindividuelle Gegebenheiten, auch verschiedene Gefahren – einerseits für das Unternehmen als Ganzes, andererseits für die einzelnen Einheiten und deren Berufsstände. Allem voran gilt es, die wertschöpfenden Eigenschaften der Risiko- und Kontroll-Funktionen zu nutzen und keine rein abwehrende Erwartungshaltung zu entwickeln. Dies ist die Aufgabe der leitenden Unternehmensorgane, welche eine proaktive Risiko-Kultur implementieren und vorleben müssen. Der so entstehende *Tone at the Top* muss auch mit dem Commitment entsprechender Ressourcen untermauert werden. Des Weiteren müssen der Austausch und die Koordination zwischen den verschiedenen Risiko- und Kontroll-Einheiten speziell gefördert werden. Auf diese Weise können nicht nur Kontrolllücken und Doppelspurigkeiten vermieden, sondern auch neue Potenziale – und somit ein Mehrwert für das Unternehmen – erschlossen werden. Nicht zuletzt muss der *3rd Line Assurance* besondere Beachtung geschenkt werden. Damit der VR seine Entscheidungen auf verlässliche Informationen stützen kann, bedarf es einer effizienten *Risk Assurance*, mit dem internen Audit als zentralem Element, punktuell unterstützt von Experten anderer interner und externer Unternehmenseinheiten sowie weiterer Assurance-Provider.

Das IIA betont in seinem Position Paper, dass das Three Lines of Defense Modell in jedem Unternehmen – unabhängig von dessen Komplexität und Grösse – zur Anwendung

> *«Mit dem Three Lines of Defense Modell steht den Unternehmen ein Rahmenwerk zur Organisation einer effizienten Governance-Struktur zur Verfügung.»*

kommen kann, um den Unternehmensrisiken effektiv zu begegnen. Dabei sollten alle drei Linien in *irgendeiner Form* existieren. Nur mit diesem Zusatz kann die generalisierende Anwendbarkeit des Modells gestützt werden. Gerade in kleineren Unternehmen gilt der Hinweis *no one size fits all*, denn häufig fehlen diesen die notwendigen Ressourcen zum Aufbau und zur Aufrechterhaltung der entsprechenden Kompetenzen. In kleinen Unternehmen kann die Adaption eines einfacheren *Quality Assurance Modells* bereits ausreichend sein, sofern dieses eine effektive Steuerung der Unternehmensrisiken ermöglicht. Wichtig ist dabei jedoch die Grundlage, dass den Risiken vom operativen Management direkt im Prozess begegnet wird (Risk Ownership), eine Überwachung und Unterstützung durch die Geschäftsleitung implementiert wird (Risk Control) und dass der VR bzw. das AC seine Entscheidungen auf unabhängige und somit verlässliche Informationen abstützen kann (Risk Assurance). ■

Anmerkungen: 1) Die zweiteilige Guidance on the 8th EU Company Law Directive steht online zum freien Download zur Verfügung unter: http://www.ferma.eu/about/publications/eciia-ferma-guidance. **2)** Das IIA Position Paper The Three Lines of Defense in Effective Risk Management and Control (Januar 2013) steht in sechs verschiedenen Sprachen (u. a. auf englisch und französisch) im Internet zum freien Download zur Verfügung: http://na.theiia.org/standards-guidance/recommended-guidance/Pages/Position-Papers.aspx. Die IIA Position Papers sind Bestandteil ausdrücklich empfohlener, aber auch für IIA-Mitglieder nicht verpflichtender Richtlinien, die sich mit über das interne Audit hinausgehenden Themen befassen. Sie dienen somit vor allem dem Verständnis in den Bereichen Governance, Risikomanagement sowie der internen Steuerung und Kontrolle. **3)** Vgl. Swiss Qualitative Assessment (SQA II) der Finma von 2013 und Thematic Review on Risk Governance des Financial Stability Board von 2013. **4)** Vgl. Swiss Code of Best Practice for Corporate Governance und IIA Standard 1110.