

Session 3C: First Line, Second Line, Third Line? Whose Line is it Anyway?

Moderator:

Matthew John Stahl, ASA, CERA, MAAA

Presenters:

Brian Joseph O’Neill, FSA, CERA, MAAA

Joanna O’Neill



Canadian
Institute of
Actuaries



Institut
canadien
des actuaires



SOCIETY OF
ACTUARIES



Enterprise
Risk Management
Symposium







Whose Line is it Anyway?

Topics

- Overview of the 3 Lines of Defense Model
- Factors Influencing the design of governance models
- Risk and Compliance functions
- Group vs. Business Units
- Scenarios – Voting
- Summary

Presenter Information

| Team Member | Background |
|---|---|
|  <p>Brian O'Neill CERA, CFA, FSA, MAAA Senior Manager Deloitte Consulting LLP</p> | <p>Brian is a Senior Manager in the insurance consulting practice at Deloitte. Brian has extensive experience developing robust Economic Capital Modeling (ECM) and Asset Liability Management (ALM) functions and implementing these functions into the larger ERM framework of insurance organizations. Brian has worked with large and small organizations and has worked with both direct carriers and reinsurers in performing these projects.</p> <p>Brian is a Fellow in the Society of Actuaries (FSA), a member of the American Academy of Actuaries (MAAA), a Chartered Financial Analyst (CFA), and a Chartered Enterprise Risk Analyst (CERA). He is the Chair of the Life Operational Risk Work Group for the American Academy of Actuaries.</p> |
|  <p>Joanna O'Neill MBA, ARM, CPCU Risk Advisory Manager Deloitte & Touché, LLP</p> | <p>Joanna has 12 years experience in providing enterprise risk management (ERM) and Operational Risk advisory services to insurance companies. She has served in management roles including Assistant Director for a Corporate Risk Institute with executive Board members from Industry and Academia. She started her career in a national property and casualty company and has since been in various insurance risk consulting roles, leading national and global projects. Joanna has provided risk management solutions including designing ERM and Operational Risk programs, governance reviews, executive risk communication & reporting guidance, rating agency and risk regulation optimization, and utilizing GRC technology to support her clients' risk management processes</p> |

Three Lines of Defense

Risk management responsibility can be viewed as three lines of defense

| Board of Directors | | |
|---|--|---|
| First line of defense | Second line of defense | Third line of defense |
| Top management and new business development | Risk management function | Internal audit |
| <ul style="list-style-type: none"> Promote a strong risk culture and sustainable risk-return decision making Portfolio optimization on the macro and micro level Promote a strong culture of adhering to limits and managing risk exposure Ongoing assessment and monitoring of risks | <ul style="list-style-type: none"> Combination of watchdog, trusted advisor, enforcer Understand how the business makes money—and actively challenge initiatives if appropriate Independent from management and staff that originate risk exposures Overarching risk oversight unit across all risk types and business units | <ul style="list-style-type: none"> Good understanding of the business and risk management Challenge the front office and risk management function Independent oversight function with ability to enforce fulfillment of findings Ability to link business and risk with process and IT know-how |

External auditor

Regulator

Design of Risk Governance Models

Key areas of market divergence in relation to the allocation of responsibilities

| | |
|----------------------------------|---|
| Advisory | 2 nd Line materially involved in decision making vs. oversight and monitoring with little, if any, advisory or decision making |
| Capital modelling and validation | First Line vs. 2 nd Line performing modelling and validation activity |
| Own Risk Solvency Assessment | First Line Finance Function role vs. 2 nd Line Risk role |
| Risk processes | Process execution vs. Process oversight |
| Reporting | Risk reporting responsibility quantitative vs. qualitative |
| Risk technology | Ownership of risk technology |

Key factors to consider include

- The **size, complexity and risk profile** of the group
- The **level of independence required** in relation to the assignment of conflicting roles e.g. the design and development of risk models versus their validation
- The availability of specialist resource and / or the **need to optimise the use of specialist resource** e.g. actuarial
- The **maturity of the risk management practices**
- The **need for specific / sophisticated risk management approaches** that are more closely aligned to the nature and complexity of a given business and / or local regulatory requirements

The principles of the 'three lines of defense' governance model have been widely adopted by firms who have tailored their approaches resulting in differing allocations of functions that sit in 1st and 2nd lines, as well as differing allocations of risk management responsibilities.

High Level Risk and Compliance Design Options

Combined Risk & Compliance function

Second line of defence



Key features of the approach

- A combined Risk & Compliance function exists in the 2nd line of defence
- The head of the Compliance function reports directly to the CRO and independently of the head of Risk
- The CRO reports directly to the CEO

Potential benefits

- Enables the alignment of risk and compliance policies, processes and reporting
- Better enables the risk and compliance functions to leverage each others work and avoid duplication
- More readily enables the CRO to monitor the overall aggregate risk profile of the business
- May enable resource efficiencies across the Risk and Compliance functions
- Helps to limit the number of direct reports to the CEO

Potential concerns

- May dilute the profile of Compliance within the firm
- May reduce Board access to Compliance expertise

Separate Risk & Compliance functions

Second line of defence



Key features of the approach

- Separate Compliance and Risk functions exist in the 2nd line of defence
- The Compliance function reports directly to a Chief Compliance Officer (CCO) and the Risk function reports to a CRO
- Both the CCO and the CRO report independently and directly to the CEO

Potential benefits

- Raises the profile of Compliance within the firm
- May better enable Board access to Compliance expertise

Potential concerns

- May result in misalignment of risk and compliance policies, processes and reporting
- Dilutes the CRO's ability to monitor the overall aggregate risk profile of the business
- May reduce the ability of the risk and compliance functions to leverage each others work and result in some duplication
- May result in increased fragmentation and sub-optimal use of Risk and Compliance resource
- CEO capacity / appetite to accommodate an additional direct report

Combined Legal & Compliance function

Second line of defence



Key features of the approach

- A combined Legal & Compliance exists in the 2nd line of defence
- The Compliance function reports to the Head of General Counsel and the Risk function reports to a CRO
- Both the Head of General Counsel and the CRO report independently and directly to the CEO

Potential benefits

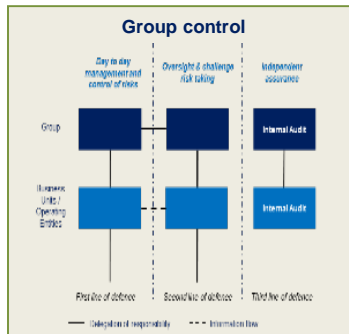
- Aligns common compliance and legal competencies and may enable resource efficiencies
- Consolidates monitoring changes in the regulatory and legal environment

Potential concerns

- May result in misalignment of risk and compliance policies, processes and reporting
- Potential conflict – Legal protects business; Compliance uncovers issues
- Dilutes the CRO's ability to monitor the overall aggregate risk profile of the business
- May reduce the ability of the risk and compliance functions to leverage each others work and result in some duplication
- May result in increased fragmentation and sub-optimal use of Risk and Compliance resource

A variety of high level design options exist in relation to the positioning of Risk and Compliance functions. Key examples are set out including the related potential benefits and concerns of the approach which would need to be tailored and enhanced to better reflect the nature of the firm.

Control Functions - Interrelationships



Key features of the approach

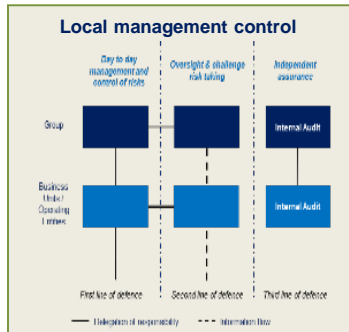
- Local control functions within the businesses report directly to Group who oversee and control their activities
- The local control functions within the businesses provide reports to local management and Group on local risk control related matters

Potential benefits

- Increased independence of the local control functions within the 2nd line of defence
- Better enables the consistent application of Group defined risk control practices across the group as well as the consistent reporting of risk control information

Potential concerns

- May dilute 1st line accountability for the management of risk within their business
- Group defined risk control practices and reporting may need to be tailored/augmented in order to meet any more specific local regulatory requirements and/or business needs
- May result in inefficiencies arising from multiple levels of review and challenge



Key features of the approach

- Local control functions report independently and directly to local management who direct and control their activities
- Whilst there is flow of information between the Group and business level functions, there is no formal reporting relationship between these functions

Potential benefits

- Helps maintain / reinforce 1st line of defence accountability for the management of risk within their business
- Better enables risk control practices and reporting to be tailored/augmented in order to meet any more specific local regulatory requirements and/or business needs

Potential concerns

- Working under the direction and control of local management may dilute the independence of the local control functions
- May result in the inconsistent application of Group defined risk control practices across the group as well as inconsistent reporting of risk control information

Polling Scenarios

- To be provided during the session

Deloitte

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

About Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2017 Deloitte Development LLC. All rights reserved.