Panel – Sat to Strong

Large Bank Perspective on Efforts to Address Heightened Expectations for Strong Risk Management and Audit

Mark Sparano, Chief Audit Executive
Corporate Audit Services

May 2, 2013

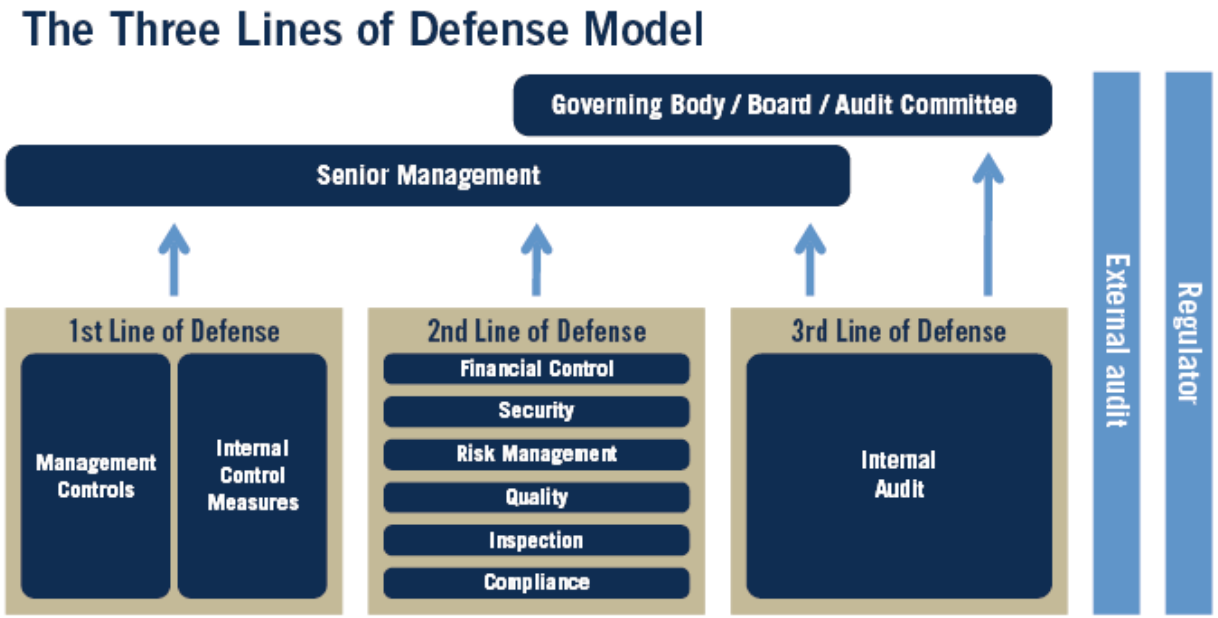
FIRMA 27th National Risk Management Training Conference

All of us serving you®

usbank®

3 Lines of defense model

- U.S. Bank has subscribed to a three lines of defense model.
- The IIA recently published a position paper outlining this model.
- Delineation of roles and responsibilities is key to efficient and effective implementation of the model.



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

https://na.theiia.org/standards-guidance/recommended-guidance/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control.aspx

3 Lines of defense: roles & responsibilities

- Board and Executive Management: Sets overall business strategy, structure, and risk appetite. Responsible for setting culture/tone for strong enterprise governance and risk management.
- 3rd Line of Defense: Internal Audit as independent tester and validator.
- 2nd Line of Defense: Translates strategy and appetite into actionable policies, standards, and other guidance. Oversees risk management and practices over business activities.
  - Policy – leads emerging risk identification and assessment, policy formulation/change management, and regulatory relations.
  - Oversight – provides ongoing oversight of risk, state of policy compliance. Advises, influences, and challenges business practices. Provides upward risk reporting.
- 1st Line of Defense: Establishes and maintains appropriate systems of risk management and internal control to support business objectives and risk appetite/tolerances.
  - Informs and influences policy formulation.
  - Identifies and assesses inherent risks.
  - Establishes and maintains appropriate risk response and control activities.
  - Conducts ongoing self-assessments to proactively identify and remediate risk issues.
  - Provides regular reporting regarding state of risk management including timely escalation of significant concerns.

3 Lines of defense: roles & responsibilities

3rd Line of Defense: Independent Assessment

Provide independent assessment & assurance re: Enterprise Governance, Risk Management, and Control

Advise, Influence, Challenge, Evaluate, Report

Key ongoing risk management actions across the lines of defense

USB Corporate Audit Services has conducted a top-down assessment to support an integrated plan of coverage for Wealth Management governance, risk management, and internal controls.

This coverage supports broader coverage of USB Enterprise Risk Management.

Board & Executive Management

Board and Executive/Managing Committee Level Governance and Risk Management Processes

2nd Line of Defense

Enterprise/Corporate and Vice-Chair Level Governance and Risk Management Processes

1st Line of Defense

Business Level Governance, Risk Management, and Control Processes

Business Processes / Account and Transaction Level Controls

- Board and Executive Management: Risk Committee of the USB board and Executive Risk Committee are established. Key activities include oversight of "risk scorecard" information including **Wealth Management related scorecard results**.
- 2nd Line of Defense: The Chief Risk Officer role has been established across all risk domains. The CRO is developing an Enterprise Risk Management Policy which will formalize many existing risk management practices and further define the company's response to heightened expectations for strong risk management, including articulation of risk appetite and tolerances. **This includes Trust Risk Management Committee and the Corporate Compliance Quality Assurance Testing Program for the Wealth Management business.**
- 1st Line of Defense: USB Wealth Management has established a comprehensive business line risk management framework inclusive of **appropriate committees** which oversee business line and business unit level governance and risk management. Each business unit maintains embedded risk management resources which have a dotted-line accountability to the **Senior Business Line Risk Manager**. Risk management practices at this level include **risk and control self assessments**.